УНИВЕРЗИТЕТ „СВ. КИРИЛ И МЕТОДИЈ“
СКОПЈЕ
ФАКУЛТЕТ ЗА ЕЛЕКТРОТЕХНИКА И
ИНФОРМАЦИСКИ ТЕХНОЛОГИИ

м-р Нецибе Сејфули-Рамадани

МОДЕЛ ЗА ПРОВЕРЛИВОСТ И ЗАШТИТА НА ПРИВАТНОСТА ВО СИСТЕМИТЕ ЗА ПОЛНЕЊЕ ЕЛЕКТРИЧНИ ВОЗИЛА СО BLOCKCHAIN-БАЗИРАН ДОКАЗ ЗА ПОЛНЕЊЕ

Докторски труд

Скопје, 2026

Докторанд: Нецибе Сејфули-Рамадани

Тема: Модел за проверливост и заштита на приватноста во системите за полнење електрични возила со blockchain-базиран доказ за полнење

Ментор: проф. д-р Александар Ристески,

Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за електротехника и информациски технологии

Комисија за одбрана:

проф. д-р Владимир Атанасовски, претседател

Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за електротехника и информациски технологии

проф. д-р Александар Ристески, ментор

Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за електротехника и информациски технологии

проф. д-р Марко Порјазоски, член

Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за електротехника и информациски технологии

проф. д-р Валентин Раковиќ, член

Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за електротехника и информациски технологии

проф. д-р Флорим Идризи, член

Универзитет во Тетово, Факултет за природно-математички науки

Лектор: Валентина Великова

Научна област: Електротехника и информациски технологии

Датум на одбрана:

Нецибе Сејфули-Рамадани

МОДЕЛ ЗА ПРОВЕРЛИВОСТ И ЗАШТИТА НА ПРИВАТНОСТА ВО СИСТЕМИТЕ ЗА ПОЛНЕЊЕ ЕЛЕКТРИЧНИ ВОЗИЛА СО BLOCKCHAIN-БАЗИРАН ДОКАЗ ЗА ПОЛНЕЊЕ

– А п с т р а к т –

Зголемената примена на електричните возила и проширувањето на инфраструктурата за нивно полнење ја наметнуваат потребата од сигурни и проверливи механизми за управување со податоците што се создаваат во текот на сесиите за полнење, со кои се обезбедува заштита на приватноста. Податоците за потрошената енергија, времетраењето на полнењето, тарифниот контекст и наплатата се основа за доверливо функционирање на системите за полнење електрични возила, особено во средини каде што се вклучени повеќе учесници, како оператори на станици за полнење, даватели на услуги за електрична мобилност и роаминг платформи. Сепак, постојните централизирани пристапи често обезбедуваат ограничена можност за независна проверка на точноста и непроменливоста на записите, што може да доведе до недоверба, спорови при наплатата и потешкотии при докажување на интегритетот на податоците.

Оваа дисертација го предлага моделот *Proof-of-Charge* базиран на блокчејн (blockchain), технологија на блоковски вериги, која овозможува создавање проверливи дигитални потврди за сесии на полнење електрични возила. За секоја завршена сесија се формира потврда што ги содржи основните податоци за сесијата, енергетските и пресметковните вредности, како и криптографска врска со мерниот тек. Преку хеш-вредности (*hash values)* и Мерклови (*Merkle)* структури, потврдите можат да се проверат поединечно или да се групираат во заедничка коренска вредност *(root value)* што се закотвува во блокчејн околина. На овој начин се овозможува проверка на интегритетот на записите, без потреба деталните и чувствителни податоци да се откриваат или директно да се запишуваат на блокчејн.

Во рамките на дисертацијата е развиен прототип на предложениот систем, преку кој се реализираат процесите на креирање потврди, хеширање, групно закотвување, блокчејн интеграција и подоцнежна проверка. Експерименталната евалуација покажува дека предложениот модел овозможува доследно генерирање проверливи потврди, намалување на бројот на блокчејн операциите преку групно закотвување и откривање можни измени во зачуваните записи. Притоа, деталните податоци остануваат во *off-chain* слојот, додека блокчејн се користи како дополнителна точка за независна проверка.

Главниот придонес на дисертацијата е воспоставување блокчејн-базиран модел *Proof-of-Charge* кој обезбедува проверливост, интегритет, заштита на приватноста и практична применливост во системите за полнење електрични возила. Предложениот пристап може да се разгледува како дополнителен слој над постојните OCPP и OCPI

процеси, со потенцијал за примена во ревизија, решавање спорови при наплата, роаминг сценарија и поширок системи за доверливо управување со податоци во инфраструктурата за електрична мобилност.

Nexhibe Sejfuli – Ramadani

PROOF-OF-CHARGE: BLOCKCHAIN-BASED MODEL FOR VERIFIABILITY AND PRIVACY PROTECTION IN ELECTRIC VEHICLE CHARGING SYSTEMS

– A b s t r a c t –

The increasing adoption of electric vehicles and the expansion of charging infrastructure create a growing need for secure, verifiable, and privacy-preserving mechanisms for managing the data generated during charging sessions. Data related to energy consumption, charging duration, tariff context, and billing form the basis for trustworthy operation of electric vehicle charging systems, especially in environments involving multiple stakeholders, such as charge point operators, e-mobility service providers, and roaming platforms. However, existing centralized approaches often provide limited opportunities for independent verification of the accuracy and immutability of records, which may lead to reduced trust, billing disputes, and difficulties in proving data integrity.

This dissertation proposes a blockchain-based Proof-of-Charge model that enables the creation of verifiable digital receipts for electric vehicle charging sessions. For each completed session, a receipt is generated containing the basic session information, energy and billing-related values, as well as a cryptographic link to the metering data stream. Through hash values and Merkle structures, receipts can be verified individually or grouped into a shared root value that is anchored in a blockchain environment. In this way, the integrity of the records can be verified without the need to disclose detailed and sensitive data or to store them directly on the blockchain.

Within the dissertation, a prototype of the proposed system was developed, implementing the processes of receipt creation, hashing, batch anchoring, blockchain integration, and subsequent verification. The experimental evaluation shows that the proposed model enables consistent generation of verifiable receipts, reduces the number of blockchain operations through batch anchoring, and supports the detection of possible changes in stored records. At the same time, detailed data remain in the off-chain layer, while blockchain is used as an additional point for independent verification.

The main contribution of the dissertation is the establishment of a blockchain-based Proof-of-Charge model that provides verifiability, integrity, privacy protection, and practical applicability in electric vehicle charging systems. The proposed approach can be considered an additional layer on top of existing OCPP and OCPI processes, with potential application in auditing, billing dispute resolution, roaming scenarios, and broader systems for trustworthy data management in electric mobility infrastructure.

Благодарност **до моето семејство и менторот**

Изјавувам дека докторскиот труд е оригинален труд што го имам изработено самостојно.

Своерачен потпис на докторандот

Изјавувам дека електронската верзија на докторскиот труд е идентична со отпечатениот докторски труд.

Потпис на авторот, с.р.

СОДРЖИНА

ЛИСТА НА СЛИКИ

ЛИСТА НА ТАБЕЛИ

ЛИСТА НА ЛИСТИНГ

ЛИСТА НА СКРАТЕНИЦИ

ACM – Association for Computing Machinery
API – Application Programming Interface
CDR – Charge Detail Record
DB – Database
eMSP – E-Mobility Service Provider
EV – Electric Vehicle
EVSE – Electric Vehicle Supply Equipment
EVM – Ethereum Virtual Machine
FIPS – Federal Information Processing Standards
HTTP – Hypertext Transfer Protocol
ID – Identifier
IEC – International Electrotechnical Commission
IEEE – Institute of Electrical and Electronics Engineers
IPFS – InterPlanetary File System
ISO – International Organization for Standardization
JCS – JSON Canonicalization Scheme
JSON – JavaScript Object Notation
JSON-RPC – JavaScript Object Notation Remote Procedure Call
NFC – Near Field Communication
NIST – National Institute of Standards and Technology
OCA – Open Charge Alliance
OCPI – Open Charge Point Interface

OCPP – Open Charge Point Protocol
OWASP – Open Worldwide Application Security Project
P2P – Peer-to-Peer
PoC – Proof-of-Charge
RFC – Request for Comments
RPC – Remote Procedure Call
SHA – Secure Hash Algorithm
SHA-256 – Secure Hash Algorithm 256-bit
SQL – Structured Query Language
UI – User Interface
V2G – Vehicle-to-Grid

1. ВОВЕД

Дигиталната трансформација на енергетските системи и транспортниот сектор претставува еден од најважните правци во современите процеси на декарбонизација, одржлив развој и енергетска транзиција. Зголемената употреба на електрични возила создава нови технички, организациски и безбедносни барања за инфраструктурата за полнење. Овие системи треба да обезбедат ефикасно управување со енергијата, сигурна размена на податоци, транспарентна наплата и доверлива комуникација меѓу различни учесници. Затоа, инфраструктурата за полнење електрични возила не претставува само физичка мрежа за снабдување со електрична енергија туку и сложена дигитална средина во која се создаваат, обработуваат и зачувуваат податоци со висока техничка и економска важност [1], [2].

Секоја сесија за полнење создава податоци поврзани со времето на започнување и завршување, потрошената енергија, тарифниот контекст, применетите цени, идентификаторите на станицата и трансакциските информации. Овие податоци се користат за наплата, ревизија, усогласување меѓу операторите, управување со инфраструктурата и анализа на потрошувачките модели. Нивната точност и непроменливост се особено важни во средини каде што се вклучени повеќе страни, како оператори на станици за полнење, даватели на услуги за електрична мобилност, роаминг платформи, корисници и регулаторни тела [3], [4].

Постојните системи најчесто се потпираат на централизирани заднински архитектури, во кои собирањето, обработката и зачувувањето на податоците се контролираат од еден или од ограничен број доверливи ентитети. Таквиот пристап овозможува функционално управување со сесиите, но ја ограничува независната проверка на податоците. Корисникот, роаминг партнерот или аудиторската страна најчесто имаат пристап само до агрегирани вредности, како вкупната потрошена енергија, времетраењето и цената, без едноставен механизам за проверка дали тие вредности навистина произлегуваат од оригиналните мерни податоци. Ова може да доведе до недоверба, особено во случаи на спор околу наплатата, евиденцијата или размената на податоци [5], [6].

Во екосистемот за полнење електрични возила значајна улога имаат стандардите и протоколите за комуникација. OCPP овозможува размена на податоци помеѓу станицата за полнење и заднинскиот систем на операторот, додека OCPI ја поддржува комуникацијата помеѓу операторите, давателите на услуги за електрична мобилност и роаминг платформите [7], [8]. Иако овие стандарди се важни за интероперабилноста, тие не се примарно дизајнирани за криптографска проверливост на записите за полнење. Поради тоа, потребни се дополнителни механизми што ќе обезбедат проверка на интегритетот на податоците, без нарушување на постојната комуникациска рамка.

Покрај проверливоста, важен предизвик е и заштитата на приватноста. Деталните мерни податоци од сесиите за полнење, како време, локација, фреквенција и времетраење, можат индиректно да откријат информации за навиките и движењето на корисникот. Затоа, во современите системи не е доволно да се обезбеди само транспарентност, потребен е

пристап што овозможува проверка на податоците, но со минимално откривање на чувствителни информации [6], [9].

Блокчејн технологијата се наметнува како релевантна основа за системите во кои довербата не зависи исклучиво од централниот ентитет. Преку дистрибуираната евиденција, криптографската заштита и непроменливоста на записите, таа овозможува создавање дигитални докази што можат да се користат во средини со повеќе независни учесници [10], [11]. Во енергетскиот сектор и електричната мобилност, блокчејн се разгледува како средство за подобрување на транспарентноста, следливоста, ревизорската проверливост и доверливата размена на податоци [1] – [3].

Досегашните истражувања ја разгледуваат примената на блокчејн во повеќе насоки, како идентификација, наплата, енергетска размена, управување со податоци, офлајн модели и ревизорски траги за сесии на полнење [12]–[15]. Сепак, голем дел од постојните пристапи се насочени кон плаќање, авторизација или складирање на податоци, додека помалку внимание се посветува на создавање компактна и криптографски проверлива потврда за секоја завршена сесија. Во практичните услови, потребна е јасна врска помеѓу оригиналните мерни податоци, агрегираниот резултат од сесијата и записот што се користи за наплата, ревизија или размена меѓу операторите.

Како одговор на овој предизвик, моделот *Proof-of-Charge* се поставува како пристап за создавање проверливи дигитални потврди за сесии на полнење електрични возила. Основната идеја е секоја сесија да добие потврда што ги содржи клучните податоци за полнењето, додека деталниот мерен тек се поврзува со неа преку *х*еш *(hash)*-функции и Мерклови (*Merkle)* структури [16]. На ниво на една сесија се овозможува проверка на врската помеѓу потврдата и мерните податоци, а на ниво на повеќе сесии потврдите можат да се групираат и да се закотват преку заедничка коренска (*root)* вредност. На тој начин се избегнува потребата сите податоци да се запишуваат на блокчејн, а сепак се задржува можноста за независна проверка.

Имплементацијата на ваков модел бара разгледување на повеќе аспекти, меѓу кои сигурност, приватност, перформанси, латентност, дополнителен простор за складирање и скалабилност. Затоа, истражувањето не се ограничува само на теоретско дефинирање на моделот, туку опфаќа и практична имплементација и експериментална евалуација. Преку генерирање, обработка и проверка на различен број сесии за полнење, се оценува способноста на моделот да обезбеди проверливост, откривање можни измени и прифатливо временско и просторно оптоварување.

Во овој контекст, докторската дисертација има цел да развие и евалуира блокчејн-базиран модел со доказ за полнење, кој овозможува сигурно и проверливо управување со податоците од сесиите за полнење електрични возила, со заштита на приватноста Истражувањето ги поврзува блокчејн технологијата, криптографските механизми, Мерклovите структури, групното закотвување и постојните стандарди за полнење, со цел да се создаде практично применлив модел за зголемување на довербата во современите системи за полнење.

1.1 Мотивација за изработка на докторската дисертација

Мотивацијата за изработка на оваа докторска дисертација произлегува од сè поголемата потреба за доверливи и проверливи податоци во системите за полнење електрични возила. Со проширувањето на инфраструктурата за полнење, податоците за потрошената енергија, времетраењето на сесијата, тарифите и наплатата стануваат важни не само за операторите туку и за корисниците, давателите на услуги за електрична мобилност, роаминг партнерите и регулаторните институции.

Во постојните системи, најголем дел од овие податоци се чуваат и обработуваат во заднинските системи на операторите. Тоа овозможува нормално функционирање на процесот на полнење, но не секогаш обезбедува едноставен начин за независна проверка. Овој недостаток станува особено видлив кога се јавуваат несогласувања околу потрошената енергија, цената или времетраењето на полнењето. Во такви ситуации, корисникот, или друга засегната страна, најчесто мора да се потпре на записите што ги обезбедува операторот.

Дополнителен проблем е приватноста на корисниците. Податоците од сесиите за полнење можат индиректно да покажат каде, кога и колку често корисникот го полни возилото. Затоа е потребен пристап што ќе овозможи проверка на точноста на записите, но без непотребно откривање на чувствителни информации.

Ова истражување е мотивирано од идејата дека секоја сесија за полнење може да добие проверлива дигитална потврда, поврзана со мерните податоци преку криптографски механизми. Со користење хеш-вредности, Мерклови структури и групно закотвување, можно е да се обезбеди подоцнежна проверка на записите, без да се нарушат постојните OCPP и OCPI процеси.

Затоа, дисертацијата се насочува кон развој на модел што може да придонесе за поголема доверба, транспарентност и сигурност во системите за полнење електрични возила. Таквиот модел е особено значаен во средините каде што податоците се разменуваат меѓу повеќе учесници и каде што е потребна јасна основа за проверка и решавање можни спорови.

1.2 Предмет на истражување и хипотеза

Предмет на ова истражување е развој, имплементација и евалуација на модел со доказ за полнење, базиран на блокчејн (технологија на блоковски вериги), односно моделот *Proof-of-Charge*, за обезбедување проверливост, интегритет и заштита на приватноста на податоците во системите за полнење електрични возила.

Истражувањето се насочува кон проблемот што постојните системи за полнење најчесто се потпираат на централизирани заднински платформи. Иако ваквите платформи овозможуваат управување со сесиите, наплатата и размената на податоци, тие не секогаш обезбедуваат доволно јасен механизам за независна проверка на записите. Во практични

услови, ова може да биде проблем кога треба да се потврди дали финалниот запис за една сесија навистина произлегува од оригиналните мерни податоци.

Во оваа дисертација *Proof-of-Charge* се разгледува како модел преку кој секоја завршена сесија за полнење добива проверлива дигитална потврда. Потврдата содржи основни и агрегирани информации за сесијата, како идентификатор на сесијата, идентификатор на станицата за полнење, временски ознаки, вкупна потрошена енергија и тарифен контекст. Деталните мерни податоци не се изложуваат јавно, туку се поврзуваат со потврдата преку хеш-вредности и Мерклови структури.

Клучен дел од истражувањето е хиерархиската проверливост на податоците. На ниво на една сесија, Мерклovата коренска вредност (*Merkle Root value*) овозможува да се провери врската помеѓу потврдата и мерните податоци. На ниво на повеќе сесии, хеш-вредностите на потврдите се групираат во заедничка коренска вредност, која може да се закотви во блокчејн околината или да се зачува во надворешен проверлив регистар. Со тоа се овозможува подоцнежна проверка од страна на аудитор, роаминг партнер или друг овластен учесник.

Предметот на истражување ја опфаќа и практичната имплементација на предложениот модел. Во таа насока се разгледуваат процесите на креирање потврди, пресметување *хеш*-вредности, формирање Мерклов корен (*Merkle Root)* и групни коренски (*batch root)* вредности, зачувување на доказните записи и нивна подоцнежна проверка. Евалуацијата се насочува кон утврдување на проверливоста, можноста за откривање измени, времето на обработка, дополнителниот простор за складирање и применливоста на моделот при различен број сесии за полнење.

Основната хипотеза на дисертацијата е дека моделот *Proof-of-Charge,* базиран на блокчејн, може да обезбеди записи за сесии на полнење електрични возила, кои се проверливи и ја штитат приватноста, без потреба деталните мерни податоци директно да се запишуваат на блокчејн. Со поврзување на потврдите со криптографски докази и со групно закотвување на повеќе записи, може да се постигне независна проверка на интегритетот, намалување на бројот на блокчејн операции и подобра заштита на чувствителните податоци.

Дополнителна претпоставка е дека предложениот модел може да се интегрира со постојните OCPP и OCPI процеси како дополнителен слој за проверливост, без потреба од промена на нивната основна комуникациска рамка. На тој начин, истражувањето се фокусира на создавање модел што е теоретски заснован, технички изводлив и практично применлив во современи системи за полнење електрични возила.

1.3 Цели и придобивки од истражувањето

Главната цел на ова истражување е да се развие и евалуира моделот *Proof-of-Charge,* базиран на блокчејн, за сигурно и проверливо управување со податоците во системите за полнење електрични возила, кои воедно ја штитат приватноста Истражувањето се насочува

кон пристап преку кој податоците од една сесија за полнење можат подоцна да се проверат, без целосно изложување на деталните мерни записи.

Основната идеја е секоја сесија за полнење да биде претставена преку проверлива дигитална потврда. Таа ги содржи клучните информации за сесијата, како потрошена енергија, временски ознаки, тарифен контекст и пресметковни вредности, додека врската со оригиналните мерни податоци се обезбедува преку криптографски механизми. За таа цел се користат хеш-вредности, Мерклови структури и групно закотвување (*batch anchoring)*.

Една од целите е да се намали зависноста од целосна доверба во централизираните заднински системи. Во постојните решенија, проверката на точноста и целосноста на записите најчесто зависи од системите на операторите. Со предложениот модел се создава можност за независна проверка од страна на аудитори, роаминг партнери или други овластени учесници, без потреба сите податоци да се запишуваат на блокчејн.

Посебно внимание се посветува на рамнотежата помеѓу проверливоста и приватноста. Податоците од сесиите за полнење можат индиректно да откријат информации за навиките, движењето или локациите на корисниците. Затоа, моделот има цел да овозможи проверка на записите, но без непотребно откривање чувствителни информации.

Во рамките на истражувањето се предвидува и практична имплементација на предложениот модел. Таа опфаќа креирање потврди, пресметување хеш-вредности, формирање Мерклова коренска вредност *(Merkle Root)* за мерните податоци, групирање на повеќе потврди преку групна коренска (*batch root)* вредност и можност за закотвување на доказните вредности во блокчејн околина или во друг проверлив регистар.

Практичната применливост се оценува преку експериментална евалуација со различен број сесии за полнење. Во евалуацијата се разгледуваат времето на креирање и проверка на потврдите, дополнителниот простор за складирање, скалабилноста и способноста на системот да открие можни измени во зачуваните записи. Со тоа се добива појасна слика за однесувањето на моделот во контролирана експериментална околина.

Важна цел е предложениот модел *Proof-of-Charge* да остане компатибилен со постојните индустриски стандарди и процеси. Тој не се поставува како замена за OCPP и OCPI, туку како дополнителен слој за проверливост и ревизиска контрола. На тој начин се овозможува потенцијална интеграција во постојните инфраструктури за полнење, без промена на нивната основна комуникациска рамка.

Придобивките од истражувањето се од научен, технички и практичен карактер. Од научен аспект, се предлага модел што ја поврзува блокчејн технологијата со криптографските докази за проверливост на сесиите за полнење електрични возила. Од технички аспект, се овозможува хиерархиска проверка преку Мерклов корен, хеш-вредности на потврдите и групен корен (*batch root)*. Од практичен аспект, моделот може да придонесе кон поголема доверба меѓу корисниците, операторите, давателите на услуги за електрична мобилност и роаминг партнерите.

Со тоа, истражувањето придонесува кон развој на посигурни и потранспарентни системи за полнење електрични возила, кои ја штитат приватноста. Предложениот пристап овозможува проверливост на податоците, откривање можни измени и практична примена во современи инфраструктури за електрична мобилност.

1.4 Структура на докторската дисертација

Докторската дисертација е организирана во девет меѓусебно поврзани поглавја. Структурата е поставена така што истражувањето постепено се развива од воведната рамка и прегледот на литературата, преку предложениот модел и неговата архитектура, до имплементација, анализа на резултатите и заклучни согледувања.

Првото поглавје го претставува воведот во истражувањето. Во него се обработуваат мотивацијата за изработка на дисертацијата, предметот на истражување, хипотезата, целите, очекуваните придобивки и структурата на трудот. Ова поглавје ја поставува основата за разбирање на потребата од механизми во системите за полнење електрични возила, кои се проверливи и ја штитат приватноста.

Второто поглавје содржи преглед на релевантната литература. Во него се анализираат истражувања поврзани со блокчејн технологијата, системите за полнење електрични возила, комуникациските протоколи, заштитата на приватноста, офлајн моделите и ревизиската проверливост. Преку овој преглед се идентификуваат ограничувањата на постојните решенија и истражувачката празнина што ја мотивира предложената насока.

Третото поглавје ја прикажува архитектурата на системот за управување со полнење електрични возила, базиран на блокчејн. Во него се опишуваат главните актери, компонентите на системот, текот на податоците и поврзувањето со постојните OCPP и OCPI процеси. Ова поглавје ја објаснува улогата на блокчејн технологијата како дополнителен слој за доверба и проверливост.

Четвртото поглавје го разработува моделот *Proof-of-Charge* и криптографската проверка на сесиите за полнење. Во ова поглавје се објаснува структурата на дигиталната потврда, поврзувањето со мерните податоци, употребата на хеш-вредности, Мерклова коренска вредност (*Merkle Root)*, групна коренска (*batch root)* вредност и групно закотвување (*batch anchoring)*. Посебно внимание се посветува на можноста за откривање можни измени во записите и независна проверка на интегритетот.

Петтото поглавје се фокусира на офлајн моделите и интеграцијата со реалните системи. Во него се разгледуваат сценарија со ограничена или привремено недостапна мрежна поврзаност, локално евидентирање на податоци, синхронизација и можноста моделот *Proof-of-Charge* да се примени како дополнителен слој над постојната инфраструктура за полнење.

Шестото поглавје ја разгледува улогата на блокчејн технологијата во обезбедување проверливост, интегритет и приватност во системите за полнење електрични возила. Во

него се анализираат основните карактеристики на блокчејн системите, криптографските механизми, *on-chain* и *off-chain* пристапите, паметните договори и примената на блокчејн во енергетски и електромобилни системи.

Седмото поглавје ја прикажува имплементацијата на предложениот систем на *Proof-of-Charge*. Во ова поглавје се опишуваат технолошката поставеност на прототипот, структурата на податоците, креирањето потврди, групното закотвување (*batch anchoring)*, блокчејн интеграцијата, механизмите за проверка и ограничувањата на имплементацијата.

Осмото поглавје содржи анализа и дискусија на резултатите. Во него се разгледуваат експерименталната поставеност, генерирањето *Proof-of-Charge* потврди, групирањето на потврдите, блокчејн трошоците, проверката на интегритетот и практичната вредност на предложениот пристап. Резултатите се користат за да се оцени изводливоста и применливоста на моделот во контролирана експериментална околина.

Деветтото поглавје ги содржи заклучните согледувања и идните насоки за истражување. Во него се сумираат главните резултати и придонеси на дисертацијата, како и можностите за понатамошно проширување на моделот кон реални податоци, јавни тест-мрежи, подобра заштита на приватноста, надворешно складирање и практична интеграција со системи за полнење електрични возила.

По главните поглавја следуваат користената литература и, доколку е потребно, прилози со дополнителни материјали поврзани со имплементацијата, експериментите, податочните структури или резултатите од истражувањето.

1.5 Очекуван научен придонес и примена на резултатите од истражувањето

Очекуваниот научен придонес на ова истражување се состои во развој на моделот *Proof-of-Charge,* базиран на блокчејн, за управување со податоците во системите за полнење електрични возила, кој е проверлив и ја штити приватноста. Придонесот произлегува од поврзувањето на блокчејн технологијата, криптографските механизми и инфраструктурата за полнење во пристап што овозможува посигурна проверка на записите.

Посебен придонес претставува дефинирањето на дигитална потврда за секоја сесија за полнење. Во неа се опфаќаат основните информации за сесијата, како потрошена енергија, временски ознаки, тарифен контекст и пресметковни вредности, додека врската со мерните податоци се обезбедува преку криптографски докази. На тој начин, записите за полнење не се третираат само како административни или пресметковни податоци, туку како проверливи дигитални објекти.

Научната вредност на моделот се гледа и во хиерархискиот начин на проверка. На ниво на една сесија, Мерклова коренска вредност (*Merkle root value*) ја поврзува потврдата со мерниот тек. На ниво на повеќе сесии, групната коренска (*batch root)* вредност

овозможува групна проверка во избран временски период. Овој пристап создава основа за поефикасна ревизија и за откривање можни измени во податоците.

Дополнителен придонес е развојот на експериментална рамка за проверка на предложениот модел. Преку анализа на времето на креирање и проверка на потврдите, дополнителниот простор за складирање, скалабилноста и способноста за откривање измени, се добива појасна процена за применливоста на *Proof-of-Charge* во реални сценарија за полнење електрични возила.

Предложениот модел има и практична вредност бидејќи може да се користи како дополнителен слој над постојните OCPP и OCPI процеси. Тој не бара промена на основната комуникациска рамка, туку додава механизам за проверливост и ревизиска контрола. Ова е особено важно во средини каде што податоците се разменуваат меѓу повеќе независни страни.

Резултатите од истражувањето можат да бидат корисни за операторите на инфраструктурата за полнење, давателите на услуги за електрична мобилност, роаминг платформите, регулаторните тела, технолошките компании и академската заедница. Операторите можат да го користат моделот за поголема доверба во наплатата и евидентирањето, додека роаминг партнерите и давателите на услуги можат да добијат појасна основа за усогласување на податоците и решавање можни несогласувања.

Во поширок контекст, предложениот пристап може да придонесе кон развој на алатки за автоматизирана проверка, ревизија на записи и интеграција со надворешни регистри или системи за складирање. Со тоа се отвора можност за посигурни и потранспарентни дигитални услуги во инфраструктурата за електрична мобилност.

Од научен аспект, резултатите можат да послужат како основа за понатамошни истражувања во областа на блокчејн технологиите, криптографската проверка, електричната мобилност, кибербезбедноста и управувањето со енергетски податоци. На тој начин, дисертацијата придонесува не само кон решавање конкретен проблем во системите за полнење, туку и кон поширокото истражување на доверливи и проверливи дигитални инфраструктури.

2. ПРЕГЛЕД НА ЛИТЕРАТУРА

2.1 Вовед во прегледот на литературата

Развојот на јавната инфраструктура за полнење електрични возила создава потреба од нови модели за управување со податоци, доверба, проверливост и заштита на приватноста. Во ваквите системи, податоците за полнењето, мерењето на потрошената енергија, тарифите, автентикацијата на корисниците и размената на записи меѓу операторите претставуваат критични елементи за правилно функционирање на целокупниот екосистем за електрична мобилност. Поради тоа, современите истражувања сè повеќе ја разгледуваат блокчејн технологијата како можен механизам за обезбедување транспарентност, непроменливост, децентрализирана доверба и проверливост на дигиталните записи во енергетските и транспортните системи [1], [2].

Блокчејн технологијата овозможува складирање и верификација на податоци преку дистрибуирана структура, каде што интегритетот на записите се обезбедува со криптографски механизми и консензус меѓу учесниците во мрежата. Овие својства ја прават оваа технологија применлива во различни домени, вклучувајќи енергетски системи, Интернет на нештата, паметни договори, автомобилска индустрија и системи за управување со дигитални трансакции [10] – [12]. Во контекст на електричните возила, блокчејн технологијата се користи за енергетска размена меѓу корисници, управување со доверба, безбедно плаќање, верификација на трансакции и зачувување на интегритетот на податоците поврзани со возилата и нивната инфраструктура [2], [3].

Системите за полнење електрични возила се потпираат на постојни комуникациски протоколи и оперативни платформи. Open Charge Point Protocol (OCPP) се користи за комуникација меѓу полначите и заднинските системи на операторите, додека Open Charge Point Interface (OCPI) овозможува размена на податоци меѓу операторите, платформите за роаминг и давателите на услуги за електрична мобилност [7], [8]. Овие протоколи обезбедуваат интероперабилност и стандардизирана комуникација, но постојната литература укажува дека тие не обезбедуваат целосна криптографска проверливост на податоците од мерењето, наплатената енергија, ценовниот контекст и деталните записи за полнење [4].

Покрај интероперабилноста, значаен предизвик претставува и заштитата на приватноста. Податоците за сесиите на полнење можат да откријат информации за движењето, навиките и однесувањето на корисниците. Затоа, повеќе истражувања предлагаат модели за полнење електрични возила со заштита на приватноста, кои користат блокчејн, анонимизација, криптографски техники и контролирано откривање на податоци [5], [6], [9]. Сепак, голем дел од постојните решенија се фокусираат на плаќање, автентикација или анонимност, додека помалку внимание се посветува на создавање проверлива потврда која ја поврзува финалната наплата со оригиналните вредности од мерењето.

Во литературата се среќаваат повеќе истражувања кои ја анализираат примената на блокчејн технологијата во различни домени, вклучувајќи: енергетски системи, автомобилска индустрија, децентрализирани апликации, модели за офлајн плаќања и механизми за ревизија на инфраструктурата за полнење електрични возила [3], [12]–[15]. Во таа насока, ова поглавје ги анализира релевантните истражувања од областа на блокчејн технологијата, протоколите за полнење електрични возила, криптографската заштита, наплатата со заштита на приватноста и механизмите за ревизија базирани на блокчејн. Целта е да се идентификуваат ограничувањата на постојните решенија и истражувачката празнина која ја мотивира потребата од модел за проверливи потврди за јавни сесии на полнење електрични возила [16].

2.2 Блокчејн технологија во електричните возила и автомобилските системи

Блокчејн технологијата првично се развива како основа за децентрализиран електронски паричен систем, но нејзината примена денес е многу поширока од криптовалутите [10]. Нејзините основни карактеристики, како децентрализација, непроменливост, транспарентност, криптографско хеширање и можност за извршување паметни договори, ја прават применлива во системите каде што податоците се разменуваат меѓу повеќе независни учесници [11].

Во енергетскиот сектор, овие својства се особено важни поради присуството на различни актери, како производители, потрошувачи, оператори, агрегатори, оператори на дистрибутивни системи и платформи за тргување со енергија. Истражувањата покажуваат дека блокчејн може да поддржи енергетска размена меѓу корисници, управување со дистрибуирани енергетски ресурси, автоматизирани трансакции и потранспарентна евиденција на енергетски податоци [1].

Во контекст на електричните возила, блокчејн технологијата се разгледува како поддршка за нови модели на енергетска размена и управување со доверба. Во [2] е предложена примена на *consortium blockchain* за локализирано тргување со електрична енергија меѓу *plug-in hybrid electric vehicles*. Овој пристап покажува дека електричните возила не треба да се разгледуваат само како потрошувачи на енергија, туку и како активни учесници во децентрализираните енергетски пазари.

Примената на блокчејн во автомобилската индустрија е поврзана и со други аспекти, како идентификација на возила, управување со податоци, следење на настани, безбедна размена на информации и поддршка на дигитални услуги. Во овие сценарија, блокчејн може да обезбеди непроменлива евиденција и појасна трага за активностите што вклучуваат повеќе страни [3].

Покрај тоа, истражувањата за архитектурите на блокчејн и децентрализираните апликации обезбедуваат поширока основа за разбирање на можностите и ограничувањата на оваа технологија [12], [13]. Тие покажуваат дека блокчејн може да се користи како слој за доверба и проверка, но дека неговата примена треба внимателно да се дизајнира, особено

кога се работи за голем обем на податоци, трошоци за трансакции, приватност и интеграција со постојни системи.

Во однос на системите за полнење електрични возила, овие согледувања се важни затоа што податоците од сесиите за полнење имаат и техничка и економска вредност. Тие се користат за наплата, ревизија, усогласување меѓу оператори и решавање можни спорови. Затоа, блокчејн технологијата може да има улога не како место за складирање на сите податоци, туку како дополнителен слој за проверка на нивната веродостојност.

Во оваа дисертација, блокчејн се разгледува токму од таа перспектива. Наместо деталните податоци од сесиите за полнење директно да се запишуваат на блокчејн, се користат компактни криптографски вредности што можат да послужат како доказ за интегритет. Овој пристап е основа за понатамошното дефинирање на моделот *Proof-of-Charge*, каде што блокчејн има улога на надворешна точка за доверлива и независна проверка.

2.3 Протоколи за полнење електрични возила и безбедносни предизвици

Јавната инфраструктура за полнење електрични возила претставува дигитално-енергетски систем во кој учествуваат повеќе страни: оператори на полначи, корисници, даватели на услуги за електрична мобилност, роаминг платформи, заднински системи и платежни сервиси. За да се овозможи координирана комуникација меѓу овие учесници, современите системи најчесто се потпираат на протоколи како OCPP и OCPI [7], [8].

За комуникација меѓу полначот, односно опремата за снабдување електрични возила со енергија, и заднинскиот систем на операторот, се користи OCPP [7]. Преку овој протокол се разменуваат информации за започнување и завршување на сесија, автентикација, мерни вредности, статус на полначот, грешки, конфигурации и други оперативни податоци. Овие записи се основа за пресметување на испорачаната енергија, времетраењето на сесијата и наплатата кон крајниот корисник. Затоа, нивниот интегритет е важен за правилно функционирање на процесот на полнење.

Безбедносните прашања поврзани со OCPP се разгледуваат во повеќе истражувања. Во [4] се нагласува дека инфраструктурата за полнење може да биде изложена на ризици како неовластен пристап, манипулација со пораки, компромитирање на заднински системи, нарушување на достапноста и злоупотреба на податоците што се разменуваат меѓу полначите и операторите. Овие ризици покажуваат дека функционалната комуникација не е доволна сама по себе, доколку не постои и механизам за доверлива проверка на записите.

Од друга страна, OCPI овозможува размена на податоци меѓу оператори, даватели на услуги за електрична мобилност и роаминг платформи [8]. Преку овој протокол се поддржуваат информациите за локации на полначи, тарифи, достапност, сесии, наплата и роаминг процеси. Во ваква средина, податоците често минуваат низ повеќе системи и

организации, што ја зголемува потребата од јасна евиденција и можност за подоцнежна проверка.

Иако OCPP и OCPI имаат различна улога, двата протоколи се значајни за функционирањето на инфраструктурата за полнење електрични возила. OCPP ја поддржува комуникацијата помеѓу полначот и операторот, додека OCPI ја овозможува размената на податоци меѓу различни пазарни учесници. Сепак, нивната основна цел е интероперабилност и оперативна размена на информации, а не создавање криптографски проверливи докази за секоја сесија.

Ова ограничување е важно за темата на оваа дисертација. Податоците што се разменуваат преку OCPP и OCPI се користат за наплата, усогласување и ревизија, но најчесто не се поврзани со независен доказ што подоцна може да ја потврди нивната точност. Поради тоа, потребен е дополнителен слој што ќе ја задржи компатибилноста со постојните протоколи, но ќе овозможи проверка на интегритетот на записите.

Во овој контекст, моделот *Proof-of-Charge* може да се разгледува како дополнување на постојната комуникациска рамка. Тој не ја заменува улогата на OCPP или OCPI, туку додава механизам преку кој податоците од сесијата можат да се поврзат со проверлива дигитална потврда. На тој начин, системите за полнење можат да ја задржат постојната интероперабилност, а истовремено да добијат посилен механизам за доверба, ревизија и откривање можни измени во записите.

2.4 Механизми за наплата со заштита на приватноста и ревизија базирана на блокчејн

Покрај интероперабилноста и безбедноста на комуникациските протоколи, значаен предизвик во системите за полнење на електрични возила е заштитата на приватноста при мерењето, наплатата и размената на податоци. Во текот на една сесија се создаваат записи за времето на пристап, времетраењето на полнењето, количината на потрошена енергија, локацијата на полначот, применетата тарифа и идентификацијата на корисникот. Доколку овие податоци се чуваат или споделуваат без соодветна заштита, тие можат индиректно да откријат информации за движењето, навиките и однесувањето на корисниците.

Во литературата се предложени повеќе модели за полнење на електрични возила со заштита на приватноста. Нивната цел е да овозможат наплата и обработка на трансакциите без целосно откривање на идентитетот на корисникот или деталните податоци за потрошувачката. Во [5] е предложен блокчејн-базиран модел за полнење електрични возила со динамички тарифни одлуки, што покажува дека блокчејн може да се користи во процеси каде што се комбинираат наплата, доверба и заштита на корисничките податоци.

Другите истражувања се насочени кон анонимните или механизмите за плаќање со заштита на приватноста. Во [6] се разгледува моделот за еднократни сметки и анонимно плаќање во блокчејн-базирани системи за полнење. Таквиот пристап ја намалува директната поврзаност помеѓу корисникот и конкретната сесија, но главно се фокусира на

плаќањето и идентитетот, а не на врската помеѓу финалниот запис и оригиналните мерни вредности.

Заштитата на приватноста е важна и при размената на податоци меѓу повеќе страни. Во [9] се анализираат пристапи за полнење со заштита на приватноста, чија цел е да се намали изложувањето на чувствителни информации, а сепак да се овозможи функционална обработка на сесиите. Овие пристапи се значајни, но најчесто се насочени кон идентитетот, пристапот и плаќањето.

Од друга страна, ревизијата базирана на блокчејн се фокусира на тоа записите да останат проверливи и по завршување на сесијата. Во ваков пристап, деталните податоци не мора директно да се запишуваат на блокчејн. Наместо тоа, може да се користат криптографски докази, хеш-вредности и надворешни регистри преку кои подоцна се проверува дали одреден запис бил изменет. Овој принцип е особено важен во роаминг сценаријата, каде што податоците за една сесија можат да поминат низ повеќе системи.

Постојните решенија покажуваат дека блокчејн може да придонесе кон доверба, приватност и ревизиска проверливост. Сепак, останува отворено прашањето како финалната потврда за сесијата да се поврзе со оригиналниот мерен тек, без да се откриваат сите детални податоци. Оваа врска е важна за решавање спорови при наплата, усогласување меѓу операторите и независна проверка на записите.

Во оваа дисертација, моделот *Proof-of-Charge* се надоврзува на овие истражувања, но фокусот го поставува на проверлива дигитална потврда за секоја сесија за полнење. Наместо да се потпира само на платежен запис или на интерни дневници на операторот, моделот ја поврзува потврдата со мерните податоци преку хеш-вредности, Мерклова коренска (*Merkle* R*oot)* вредност и групно закотвување (*batch anchoring)*. На овој начин се задржува приватноста, а се додава можност за подоцнежна проверка на интегритетот на записите.

2.5 Офлајн модели и интеграција со реалните системи

Во практичните системи за полнење електрични возила не може секогаш да се претпостави постојана и стабилна интернет врска. Полначите можат да бидат поставени на локации каде што комуникациската инфраструктура е ограничена, нестабилна или привремено недостапна. Такви ситуации можат да се појават во руралните средини, на приватните паркинзи, кампуси, индустриски зони, привремените станици за полнење или на други места каде што пристапот до мрежа не е секогаш сигурен. Поради тоа, во литературата се разгледуваат и офлајн модели, кои овозможуваат дел од процесите да продолжат и кога врската со централниот систем е прекината.

Во [14] е предложен модел за интеграција на офлајн платежни механизми, базирани на блокчејн, во постапката за автентикација и полнење електрични возила. Овој пристап покажува дека идентификацијата на корисникот, пристапот до полначот и започнувањето на сесијата можат да се разгледуваат и во услови кога директната комуникација со

централниот систем не е достапна. Тоа е важно затоа што системите за полнење треба да бидат отпорни и во ситуации што не се идеални.

Кај офлајн сценаријата, особено значајно е локалното зачувување на податоците. Системот треба да зачува доволно информации за сесијата за подоцна да може да се изврши проверка и синхронизација. Истовремено, тие записи треба да бидат заштитени од неовластени измени. Кога мрежната врска повторно ќе биде достапна, податоците треба да се пренесат кон заднинскиот систем или кон друг проверлив регистар, без да се изгуби довербата во нивната точност.

Оваа идеја е блиска до предложениот модел *Proof-of-Charge*. Ако една сесија заврши во услови на ограничена поврзаност, системот може локално да создаде дигитална потврда и да ја поврзе со мерните податоци преку хеш-вредности и Мерклова коренска (*Merkle* R*oot)* вредност. Подоцна, кога врската ќе се воспостави, потврдата или нејзината доказна вредност може да се синхронизира со заднинскиот систем или да се вклучи во процесот на групно закотвување *(batch anchoring)*.

Интеграцијата со реални системи треба да биде внимателно поставена, за да не ја наруши постојната комуникациска рамка. Во практична примена, OCPP и понатаму може да ја поддржува комуникацијата меѓу полначот и операторот, додека OCPI може да се користи за размена на податоци меѓу оператори, даватели на услуги за електрична мобилност и роаминг платформи. Во таква поставеност, *Proof-of-Charge* не ја заменува постојната инфраструктура, туку додава слој преку кој записите од сесијата можат подоцна да се проверат.

Овој пристап е важен затоа што реалните системи често се соочуваат со прекини, доцнења, нецелосни записи или разлики меѓу податоците зачувани кај различни учесници. Ако потврдите се создаваат на јасен и повторлив начин, а нивната врска со мерните податоци се обезбедува преку криптографски докази, подоцнежната проверка станува посигурна и помалку зависна од еден централен извор.

Во оваа дисертација, офлајн моделите и интеграцијата со реални системи се разгледуваат како важен дел од практичната применливост на *Proof-of-Charge*. Тие покажуваат дека моделот не треба да се ограничи само на идеални онлајн услови, туку може да се прошири и кон сценарија каде што податоците прво се создаваат локално, привремено се зачувуваат, а потоа се синхронизираат со поширокатa инфраструктура за полнење електрични возила.

Релевантните истражувања разгледани во ова поглавје се систематизирани во табелата 2.1. Во неа се прикажани главните области, фокусот на секој пристап и нивната поврзаност со истражувачката празнина што ја мотивира предложената архитектура на *Proof-of-Charge*.

Табела 2.1: Преглед на релевантни истражувања поврзани со блокчејн, ЕВ-полнење и проверливост.

Реф.	**Област**	**Главен фокус**	**Ограничување / релевантност за дисертацијата**
[1]	Блокчејн во енергетика	Систематски преглед на блокчејн во енергетскиот сектор	Покажува потенцијал, но не се фокусира конкретно на потврди за ЕВ полнење.
[2]	*ЕВ* и енергетска размена	*Peer-to-peer* тргување со енергија кај електрични возила	Фокус на енергетско тргување, не на проверлив запис за полнење.
[4]	OCPP безбедност	Безбедносни предизвици кај OCPP	Ги покажува ризиците, но не предлага receipt-centric криптографска проверка.
[5], [6], [9]	Приватност и плаќање	*Privacy-preserving* модели за *ЕВ* полнење	Повеќе се фокусираат на плаќање и анонимност отколку на проверливост на записот.
[15]	Блокчејн ревизија	*Immutable audit* со блокчејн и IPFS	Обезбедува audit механизам, но *Proof-of-Charge* оди кон потврди за поединечни сесии.
[16]	*Proof-of-Charge*	Проверливи потврди за *ЕВ* полнење	Основен модел за криптографска проверка и *privacy-preserving receipts*.
[17]	Мерклови (Merkle) структури	Криптографски структури за проверка	Техничка основа за Мерклови корени *(Merkle roots)* и групни потврди.
[18]	Energy data audit	*Tamper-EBident* енергетски податоци	Поддржува идеја за хибриден модел со *off-chain* податоци и *on-chain* докази.
[19], [20]	Наплата со заштита на приватноста	Блокчејн, *homomorphic encryption, reservation/payment privacy*	Корисни за споредба со *Proof-of-Charge*.

Врз основа на систематизираниот преглед може да се издвојат неколку ограничувања на постојните решенија, кои се разгледуваат во следното потпоглавје.

2.6 Ограничувања на постојните решенија и истражувачка празнина

Анализираната литература покажува дека блокчејн технологијата има значаен потенцијал за примена во енергетски системи, автомобилска индустрија и инфраструктура за полнење електрични возила [1]–[3], [12]. Во постојните истражувања таа најчесто се користи за децентрализирана доверба, непроменливост на записите, автоматизирани трансакции и дополнителна проверка на податоците [10], [11], [13]. Сепак, овие решенија не ги опфаќаат целосно предизвиците поврзани со точна наплата, приватност, интегритет на мерењата и независна ревизија на сесиите за полнење.

Едно од главните ограничувања е директното запишување податоци на блокчејн. Иако таквиот пристап обезбедува високо ниво на непроменливост, складирањето детални мерни вредности, записи за сесии и пресметковни податоци може да предизвика високи трошоци, ограничена скалабилност и дополнителни ризици за приватноста [1], [15], [18]. Затоа, кај системите за полнење електрични возила е потребен повнимателен пристап, во кој не се користи блокчејн како место за чување на сите податоци, туку како слој за проверка на нивниот интегритет.

Друго ограничување е тоа што голем дел од постојните модели се насочени кон плаќање, автентикација, анонимност или енергетска размена. Овие аспекти се важни, но не обезбедуваат секогаш јасна врска помеѓу финалниот запис за сесијата и оригиналниот мерен тек [5], [6], [9], [19], [20]. Во практични услови, токму оваа врска е значајна за ревизија, усогласување меѓу операторите и решавање можни спорови при наплата.

Дополнително, постојните комуникациски протоколи, како OCPP и OCPI, овозможуваат интероперабилност и размена на податоци меѓу различни учесници [7], [8]. Нивната основна улога, сепак, е оперативна комуникација, а не создавање криптографски проверлива потврда за секоја сесија. Поради тоа, потребен е дополнителен механизам што ќе ја задржи компатибилноста со овие процеси, но ќе овозможи подоцнежна независна проверка.

Од овој преглед произлегува истражувачката празнина на која се фокусира дисертацијата: недостиг од интегриран модел што истовремено обезбедува проверлива потврда за поединечна сесија, заштита на приватноста, можност за групирање на повеќе потврди и применливост во реални системи за полнење. Таков модел треба да ја поврзе финалната потврда со мерните податоци преку криптографски докази, без деталните записи да се изложуваат или директно да се запишуваат на блокчејн.

Моделот *Proof-of-Charge* ја адресира оваа празнина преку користење хеш-вредности, Мерклови структури, групни коренски *(batch root)* вредности и групно закотвување (*batch anchoring)* [16], [17]. Деталните мерни податоци остануваат во *off-chain* слојот, додека блокчејн околината се користи само за закотвување компактни доказни вредности. На овој начин се постигнува рамнотежа меѓу проверливост, приватност, скалабилност и компатибилност со постојните системи за полнење електрични возила.

Со ова, прегледот на литературата покажува дека постојните истражувања обезбедуваат важна основа, но дека останува потребата од модел што ги поврзува овие елементи во единствен работен процес. Оваа истражувачка празнина претставува основа за следното поглавје, во кое се разработува архитектурата на системот за управување со полнење електрични возила базиран на блокчејн.

3. АРХИТЕКТУРА НА СИСТЕМОТ ЗА УПРАВУВАЊЕ СО ПОЛНЕЊЕ ЕЛЕКТРИЧНИ ВОЗИЛА БАЗИРАН НА БЛОКЧЕЈН

3.1 Вовед во предложената архитектура

Во ова поглавје се претставува архитектурата на предложениот систем за управување со полнење електрични возила базиран на блокчејн технологија. Архитектурата произлегува од ограничувањата идентификувани во прегледот на литературата, особено во однос на проверливоста на мерните податоци, заштитата на приватноста, довербата во заднинските системи и потребата од независна ревизија на сесиите за полнење.

Предложениот систем не ја заменува постојната инфраструктура за полнење, туку ја надградува со дополнителен слој за проверка на интегритетот на записите. Во таа поставеност, процесите OCPP и OCPI продолжуваат да ја поддржуваат оперативната комуникација и размената на податоци, додека блокчејн технологијата се користи за зачувување компактни криптографски докази [7], [8], [16].

Основната идеја е секоја завршена сесија за полнење да се претстави преку проверлива дигитална потврда. Таа потврда ги поврзува мерните податоци, испорачаната енергија, тарифниот контекст и финалниот запис за наплата. Наместо деталните мерни вредности да се запишуваат директно на блокчејн, тие остануваат во заднинскиот систем, а за проверка се користат хеш-вредности, Мерклови коренски вредности и групни криптографски докази [16], [17].

Ваквата архитектура овозможува поделба меѓу оперативниот дел на системот и слојот за проверливост. Оперативниот дел ги опфаќа полначите, корисниците, операторите и постојните комуникациски протоколи. Слојот за проверливост, пак, обезбедува можност податоците од сесијата подоцна да се проверат без целосно откривање на чувствителните информации.

На овој начин, предложениот систем создава основа за посигурно управување со записите од полнењето. Тој овозможува подобра доверба меѓу корисниците, операторите, роаминг партнерите и ревизорските страни, а истовремено ја задржува компатибилноста со постојните процеси во инфраструктурата за полнење електрични возила.

Во продолжение на поглавјето се разгледуваат главните актери и компоненти на системот, начинот на интеграција со OCPP и OCPI, текот на податоците во предложената архитектура, како и безбедносните и приватносните карактеристики на предложениот пристап.

3.2 Главни актери и компоненти на системот

Предложената архитектура опфаќа повеќе актери и функционални компоненти кои учествуваат во процесот на полнење, евидентирање, наплата и подоцнежна проверка на записите. Секој од нив има посебна улога во текот на една сесија за полнење, од иницирање на сесијата до создавање проверлива дигитална потврда.

Главен учесник во системот е корисникот на електрично возило. Тој ја иницира сесијата за полнење и се автентицира преку механизам поддржан од операторот, како мобилна апликација, картичка, токен или друг идентификациски метод. По успешната автентикација, корисникот добива пристап до полначот и започнува сесија за полнење.

Полначот, односно опремата за снабдување електрични возила со енергија, ја извршува физичката испорака на електрична енергија. Во текот на сесијата тој создава податоци за времето на започнување и завршување, статусот на сесијата, испорачаната енергија и мерните вредности. Овие податоци се основа за пресметка, наплата и подоцнежна проверка.

Операторот на инфраструктурата за полнење управува со полначите, сесиите, тарифите, автентикацијата и заднинските процеси. Неговата улога е да обезбеди правилно функционирање на системот, да ги зачува релевантните записи и да ги проследи потребните податоци кон други учесници, како даватели на услуги за електрична мобилност или роаминг платформи.

Давателот на услуги за електрична мобилност ја поврзува услугата со крајниот корисник. Тој може да обезбеди пристап до полнење, управување со кориснички сметки, пресметка на трошоци и размена на податоци со операторите. Во роаминг сценаријата, неговата улога е особено важна бидејќи податоците за една сесија можат да поминат низ повеќе системи пред да се формира финалниот запис.

Роаминг платформата овозможува размена на податоци помеѓу различни оператори и даватели на услуги. Таа помага корисникот да пристапи до инфраструктура што не е директно управувана од неговиот давател на услуга. Во вакви услови, проверливоста на записите станува особено значајна, бидејќи повеќе страни се вклучени во процесот на усогласување и наплата.

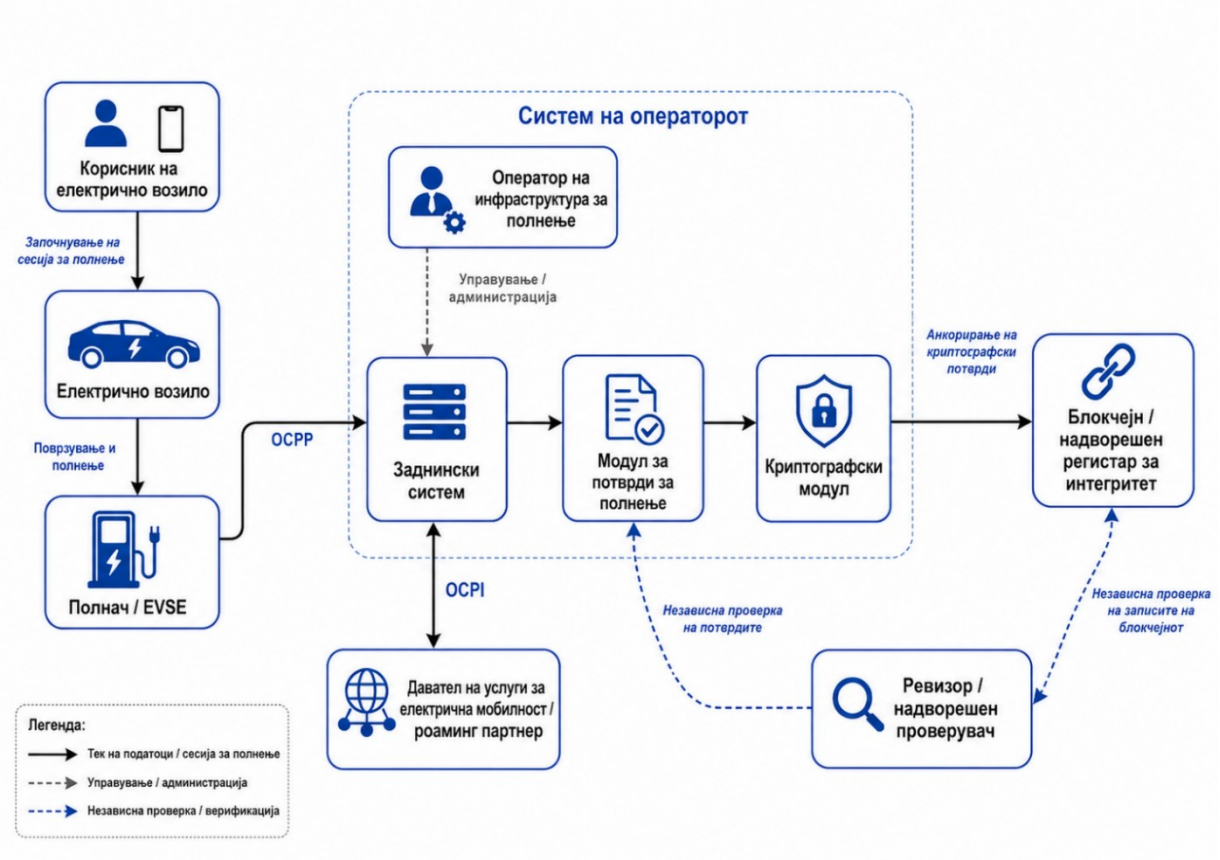
Заднинскиот систем претставува централна компонента за управување со сесиите, корисниците, тарифите, мерните податоци и пресметковните записи. Во предложената архитектура, тој не е само место каде што се чуваат оперативните податоци, туку и точка од која се формираат податоците потребни за *Proof-of-Charge* потврдата.

Компонентата за *Proof-of-Charge* потврди ја создава проверливата дигитална потврда за завршената сесија. Таа ги поврзува основните податоци за сесијата со мерниот тек преку хеш-вредности и Мерклова коренска вредност. На тој начин, финалниот запис може да се провери подоцна, без повторно изложување на сите детални мерни податоци.

Блокчејн слојот се користи за закотвување на компактни криптографски вредности. Наместо деталните податоци од сесијата да се запишуваат на блокчејн, во овој слој се зачувуваат само вредности што служат како доказ за интегритет. Ова овозможува независна проверка, но без непотребно оптоварување на блокчејн околината.

Ревизорската компонента овозможува подоцнежна проверка на потврдите и доказните вредности. Таа може да се користи од оператор, роаминг партнер, регулаторна институција или друга овластена страна за да се провери дали одреден запис е изменет по неговото создавање.

Главните актери и компоненти на предложениот систем се прикажани на сликата 3.1, додека нивните улоги се систематизирани во табелата 3.1.



Слика 3.1: Главни актери и компоненти на системот на предложениот систем за управување со полнење електрични возила базиран на блокчејн

Во табелата се прикажани нивните основни улоги во рамките на архитектурата, почнувајќи од корисникот и полначот, преку заднинскиот систем и давателот на услуги за електрична мобилност, па сè до модулите за потврди, криптографска обработка, блокчејн закотвување и независна ревизија. Ваквата поделба овозможува појасно разбирање на одговорностите на секој актер и покажува како оперативните процеси на полнење се поврзуваат со механизмите за проверливост и заштита на интегритетот на податоците.

Табела 3.1: Актери и нивните улоги

Актер/компонента	**Улога во системот**
Корисник на електрично возило	Иницира сесија на полнење, се автентицира и користи инфраструктура за полнење.
Електрично возило	Се поврзува со полначот и ја прима испорачаната електрична енергија.
Полнач/*EVSE*	Ја извршува физичката испорака на енергија и генерира податоци од мерењето.
Оператор на инфраструктура за полнење	Управува со полначите, сесиите, тарифите, наплатата и заднинскиот систем.
Заднински систем	Ги обработува податоците од сесијата, ја пресметува испорачаната енергија и го подготвува записот за наплата.
Давател на услуги за електрична мобилност	Овозможува пристап на корисникот до полначи од различни оператори, особено во роаминг сценарија.
Модул за потврди за полнење	Генерира проверлива потврда за секоја завршена сесија на полнење.
Криптографски модул	Пресметува хеш-вредности, Мерклов корен (*Merkle root*) и групни криптографски потврди.
Блокчејн/надворешен регистар за интегритет	Зачувува минимални криптографски докази за последователна проверка.
Ревизор/надворешен проверувач	Ја проверува валидноста на потврдите и интегритетот на записите за полнење.

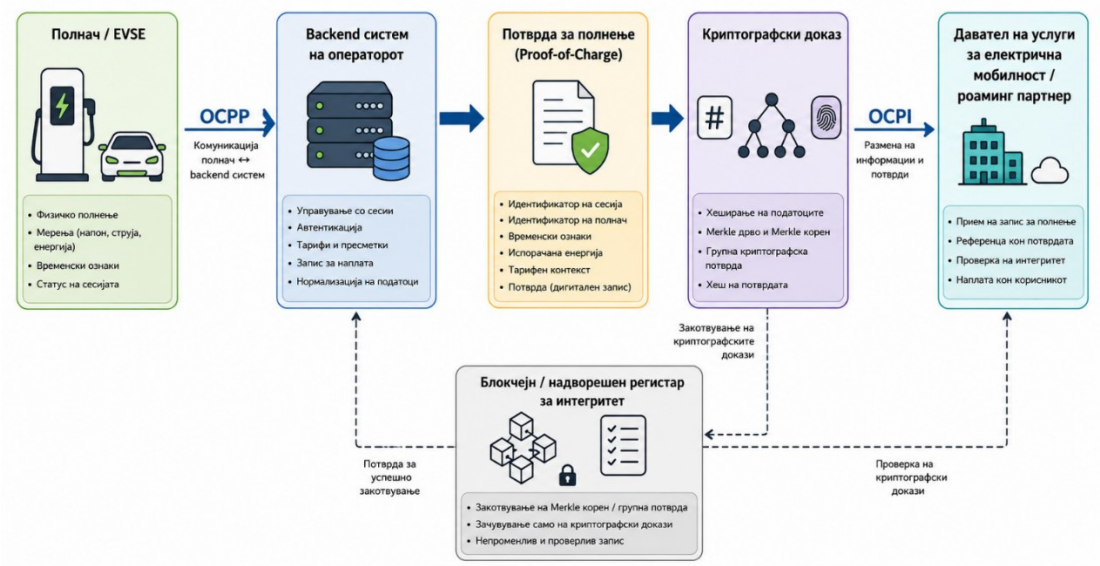
Функционалната поделба на предложената архитектура по слоеви е прикажана во табелата 3.2. Секој слој има јасно дефинирана улога и создава податоци кои се користат од следните слоеви за обработка или ревизија.

Табела 3.2: Слоеви на предложената архитектура и нивните функции

Слој на архитектурата	**Главна функција**	**Податоци / излез од слојот**
Слој за полнење и мерење	Ја опфаќа физичката сесија на полнење, поврзувањето на електричното возило со полначот и создавањето на вредности од мерењето.	Временски ознаки, вредности од мерењето, испорачана енергија, статус на сесијата.
Заднински оперативен слој	Управува со сесиите на полнење, автентикацијата, тарифите, пресметката на енергијата и подготовката на записот за наплата.	Податоци за сесијата, корисничка автентикација, тарифен контекст, финален запис за наплата.
Слој за потврди за полнење	Генерира проверлива потврда за секоја завршена сесија на полнење. Потврдата ги поврзува податоците од мерењето со финалниот запис за наплата.	Потврда за полнење, идентификатор на сесијата, идентификатор на полначот, вкупна енергија, ценовен контекст.
Криптографски слој за обработка	Пресметува хеш-вредности, Мерклов корен (*Merkle Root)* и групни криптографски потврди за проверка на интегритетот.	Хеш-вредности, Мерклов корен (*Merkle Root*), групна криптографска потврда.
Слој за блокчејн-закотвување	Ги зачувува минималните криптографски докази на блокчејн или надворешен регистар за интегритет, без складирање на детални податоци од сесиите.	Закотвен Мерклов корен, закотвена групна потврда, запис за време на закотвување.
Слој за проверка/ ревизија	Овозможува независна проверка на потврдите за полнење и откривање на можни измени, бришења или неконзистентности во записите.	Резултат од проверка, потврден или неусогласен запис, ревизорски извештај.

Како што е прикажано во табелата 3.2, предложената архитектура ја задржува стандардната оперативна логика на системите за полнење електрични возила, но ја надградува со дополнителни слоеви за потврди, криптографска обработка, блокчејн закотвување и независна ревизија. Ова овозможува моделот да се интегрира со постојни OCPP/OCPI процеси, без нарушување на нивната основна функционалност [7], [8], [16].

Слоевитата организација на предложената архитектура е прикажана и графички на сликата 3.2. Оваа слика го претставува преминот од физичката сесија за полнење и оперативната обработка на податоците, кон создавање потврди, криптографска обработка, блокчејн закотвување и ревизиска проверка.



Слика 3.2: Слоеви на предложената архитектура и нивните функции

Како што е прикажано на сликата 3.2, предложената архитектура е организирана во повеќе логички слоеви. Првите слоеви се поврзани со реалното извршување на сесијата за полнење и обработката на оперативните податоци. Следните слоеви ја додаваат проверливоста преку потврди за полнење, криптографска обработка, блокчејн закотвување и ревизиска проверка. На овој начин, системот ја задржува постојната функционалност на инфраструктурата за полнење, но добива дополнителен механизам за доверба и проверка на записите.

Ваквата поделба на архитектурата овозможува јасно разграничување меѓу оперативните процеси за полнење и механизмите за проверливост. Полначот, заднинскиот систем и учесниците во услугата ја обезбедуваат основната функционалност на сесијата, додека слоевите за потврди, криптографска обработка, блокчејн закотвување и ревизија додаваат можност за подоцнежна проверка на записите. За оваа архитектура да биде применлива во реални услови, потребно е да се разгледа нејзиното поврзување со постојните комуникациски протоколи, пред сè со OCPP и OCPI, што е предмет на следното потпоглавје.

3.3 Интеграција со OCPP и OCPI

Интеграцијата со постојните комуникациски протоколи е важна за предложената архитектура да може да се примени во реална инфраструктура за полнење електрични возила. Во практичните системи веќе постојат воспоставени процеси за управување со сесии, размена на податоци и наплата. Затоа, *Proof-of-Charge* не се поставува како замена за тие процеси, туку како дополнителен слој што ја зголемува довербата во записите што тие ги создаваат [16], [17].

Во оваа архитектура, OCPP ја задржува својата основна улога во комуникацијата меѓу полначот и заднинскиот систем на операторот. Преку него се разменуваат податоци за започнување и завршување на сесијата, идентификација на корисникот, мерни вредности, статус на полначот и други оперативни информации [7]. Токму овие податоци се почетна основа за создавање проверлива потврда за полнење.

Протоколот OCPI има различна, но исто така важна улога. Тој овозможува размена на податоци меѓу оператори, даватели на услуги за електрична мобилност и роаминг платформи [8]. Во вакви сценарија, една сесија може да биде обработена преку повеќе системи, па затоа е важно финалниот запис да може подоцна да се поврзе со доказ за неговата точност.

Во предложениот пристап, податоците што веќе се создаваат преку OCPP и OCPI се користат за формирање дигитална потврда. Деталните мерни записи остануваат во заднинскиот или *off-chain* слој, додека потврдата се поврзува со нив преку хеш-вредности и Мерклова коренска вредност. Повеќе потврди потоа можат да се групираат преку групно закотвување (*batch anchoring)*, со што се добива поефикасен начин за подоцнежна проверка [16], [17].

Ваквата поставеност помага да се зачува приватноста на корисниците. Деталните временски серии, личните податоци и информациите што можат да откријат навики на користење не мора да се споделуваат со сите учесници. Наместо тоа, за проверка се користат компактни криптографски докази, доволни за да се утврди дали записот останал непроменет.

На овој начин, OCPP и OCPI продолжуваат да ја обезбедуваат оперативната комуникација, додека *Proof-of-Charge* додава механизам за доверлива проверка. Архитектурата останува компатибилна со постојните системи, но добива дополнителна вредност во ситуации каде што се потребни ревизија, усогласување на податоци или решавање можни несогласувања при наплата [7], [8], [16], [17].

3.4 Тек на податоците во предложениот систем

Текот на податоците во предложениот систем започнува со иницирање на сесија за полнење. Корисникот се автентицира преку постојниот механизам на операторот, по што полначот ја започнува испораката на електрична енергија. Во оваа фаза се евидентираат времето на започнување, идентификаторот на полначот, статусот на сесијата и почетните мерни вредности. Овие информации се пренесуваат кон заднинскиот систем преку OCPP процесите [7].

Во текот на полнењето, полначот испраќа мерни вредности што ја опишуваат испорачаната енергија и состојбата на сесијата. Заднинскиот систем ги поврзува овие записи со тарифниот контекст, времетраењето и пресметковните податоци. По завршувањето на сесијата се формира финален запис што се користи за наплата, евиденција и евентуална размена со други учесници во системот.

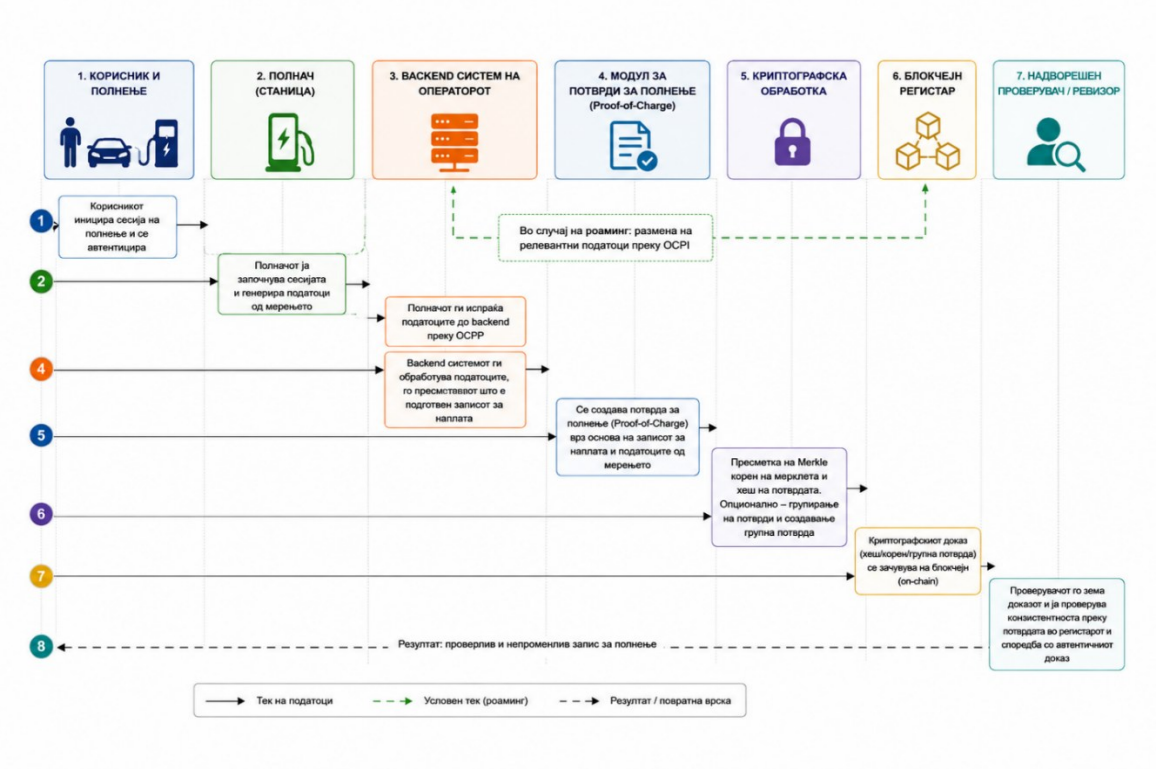
Следниот чекор е создавање проверлива дигитална потврда. Во предложената архитектура, *Proof-of-Charge* потврдата се формира врз основа на завршената сесија и ги поврзува енергетските вредности, пресметковниот резултат и мерниот тек преку хеш-вредности и Мерклова коренска вредност. На тој начин, потврдата не останува само административен документ, туку добива криптографска основа за подоцнежна проверка [16], [17].

Повеќе потврди можат да се групираат преку batch anchoring. Во овој процес, хеш-вредностите на поединечните потврди се користат за формирање заедничка коренска (*batch root*) вредност, која може да се закотви на блокчејн или во друг надворешен регистар за интегритет. На овој слој не се зачувуваат детални мерни записи или лични информации, туку само компактни криптографски вредности [15], [18].

Во роаминг сценарија, дел од податоците за сесијата може да се разменат и преку OCPI со давател на услуги за електрична мобилност или роаминг платформа [8]. Во таква поставеност, финалниот запис може да содржи референца кон потврдата или кон закотвената доказна вредност. Ова им овозможува на учесниците во роаминг процесот да ја проверат конзистентноста на записот, без пристап до сите детални мерни податоци.

Последната фаза е ревизиската проверка. Овластен проверувач, како оператор, роаминг партнер или ревизор, може повторно да ги пресмета релевантните криптографски вредности и да ги спореди со зачуваните или закотвените докази. Совпаѓањето покажува дека записот останал непроменет, додека несовпаѓањето укажува на можна измена, бришење или неконзистентност [16], [17].

Целокупниот тек на податоците, од започнување на сесијата до закотвување на доказите и подоцнежна проверка, е прикажан на сликата 3.3.



Слика 3.3: Тек на податоците од сесија на полнење до криптографска проверка

Како што е прикажано на сликата 3.3, предложениот систем ја задржува оперативната логика на постојната инфраструктура за полнење, но додава криптографски слој за доверба. Мерните податоци остануваат во заднинскиот или *off-chain* слој, додека блокчејн или надворешниот регистар се користи само за закотвување на доказни вредности. Со тоа се овозможува проверка на интегритетот, без непотребно откривање чувствителни информации.

Овој тек ја покажува врската меѓу оперативните процеси, дигиталната потврда и ревизиските механизми. Во следното потпоглавје се разгледуваат безбедносните и приватносните карактеристики што произлегуваат од ваквата архитектурна поставеност.

3.5 Безбедносни и приватносни карактеристики на архитектурата

Предложената архитектура е дизајнирана така што сигурноста, приватноста и доверливоста на записите се вградени во самиот работен процес. Ова е важно затоа што сесиите за полнење содржат податоци со техничка, финансиска и приватносна вредност, како мерни вредности, идентификатори на сесии, информации за полначот, тарифен контекст и записи за наплата.

Првата важна карактеристика е зачувувањето на интегритетот на мерните податоци. Вредностите што се создаваат во текот на сесијата се основа за пресметување на испорачаната енергија и за формирање на финалниот запис за наплата. Во предложениот пристап, тие се поврзуваат со потврдата за полнење преку хеш-вредности и Мерклова коренска вредност. Со тоа, секоја подоцнежна измена во мерниот тек може да се открие при повторна проверка [16], [17].

Втората карактеристика е отпорноста на неовластени промени. Наместо деталните записи од сесијата да се запишуваат директно на блокчејн, архитектурата користи компактни криптографски докази. Така се намалува количината на изложени податоци, а сепак останува можноста да се утврди дали записот бил изменет.

Заштитата на приватноста е особено значајна затоа што податоците за време, локација, навики на полнење и кориснички идентификатори можат да откријат чувствителни информации. Поради тоа, деталните мерни записи остануваат во заднинскиот или *off-chain* слој, додека за проверка се користат само неопходните криптографски вредности. Со ваков пристап се избегнува непотребно споделување лични или чувствителни податоци со сите учесници во системот.

Архитектурата овозможува и независна проверка. Овластена страна, како оператор, роаминг партнер или ревизор, може повторно да ги пресмета релевантните вредности и да ги спореди со зачуваните или закотвените докази. На тој начин, валидноста на записот не зависи само од доверба во еден оператор, туку може да се потврди преку јасен криптографски процес [16], [17].

Дополнителна предност е компатибилноста со постојните протоколи и системи. Архитектурата не бара замена на OCPP и OCPI, туку ги користи податоците што веќе се создаваат во процесите на полнење и роаминг [7], [8]. Така, *Proof-of-Charge* може да се постави како дополнителен слој за ревизиска контрола, без значителни промени во полначите, комуникациските протоколи или оперативните процеси.

Скалабилноста се постигнува преку групирање на потврдите и создавање заедничка коренска вредност (*batch root)* вредност. Доколку секоја сесија би се запишувала директно на блокчејн, системот би се соочил со повисоки трошоци и ограничувања во перформансите. Со групниот пристап, еден закотвен доказ може да се однесува на повеќе сесии, што го намалува бројот на блокчејн записи и ја зголемува применливоста на моделот во реална инфраструктура [16], [18].

Главните безбедносни и приватносни карактеристики на предложената архитектура се систематизирани во табелата 3.3.

Табела 3.3: Безбедносни и приватносни карактеристики на предложената архитектура

Карактеристика	Опис	Релевантност за системот
Интегритет на податоците од мерењето	Поврзување на вредностите од мерењето со потврдата за полнење преку хеширање и Мерклови структури.	Овозможува откривање на измени во податоците од сесијата.
Отпорност на неовластени промени	Зачувување минимални криптографски докази наместо целосни податоци на блокчејн.	Го намалува ризикот од манипулација со записите.
Заштита на приватноста	Деталните податоци од мерењето не се објавуваат јавно и не се споделуваат со сите учесници.	Ги заштитува навиките, движењето и идентитетот на корисникот.
Независна проверливост	Ревизорот или партнерот за роаминг може самостојно да ги провери криптографските докази.	Ја намалува зависноста од доверба во еден оператор.
Компатибилност	Архитектурата се надградува врз постојните OCPP и OCPI процеси.	Овозможува интеграција со постојните системи без промена на основната инфраструктура.
Скалабилност	Се користат групни криптографски потврди и закотвување.	Се намалуваат трошоците и бројот на записи на блокчејн.

Сумирано, предложената архитектура ја комбинира оперативната логика на постојните системи за полнење со криптографски механизми за доверба и ревизија. Деталните податоци остануваат надвор од блокчејн, додека закотвените доказни вредности овозможуваат подоцнежна проверка. Со тоа се постигнува рамнотежа меѓу безбедноста, приватноста, применливоста и компатибилноста со реалната инфраструктура за полнење електрични возила.

3.6 Заклучок на поглавјето

Во ова поглавје беше претставена архитектурата на предложениот систем за управување со полнење електрични возила базиран на блокчејн технологија. Таа е поставена така што ја задржува постојната логика на инфраструктурата за полнење, но додава слој преку кој записите од сесиите можат подоцна да се проверат.

Во архитектурата се опфатени главните учесници во процесот: корисникот, полначот, операторот, давателот на услуги за електрична мобилност, роаминг платформата и ревизорската компонента. Нивната улога е разгледана во однос на создавањето, обработката и користењето на податоците од сесиите за полнење.

Посебно значење има тоа што предложениот модел *Proof-of-Charge* не ги заменува постојните OCPP и OCPI процеси, туку се надоврзува на нив [7], [8], [16], [17]. Податоците што веќе се создаваат во текот на полнењето се користат за формирање проверлива дигитална потврда, додека деталните мерни записи остануваат во заднинскиот или *off-chain* слој.

Важен заклучок од ова поглавје е дека блокчејн не треба да се користи како место за складирање на сите податоци. Во предложената поставеност, на блокчејн или во надворешен регистар се закотвуваат само компактни криптографски вредности. Така се намалува изложувањето на чувствителни информации, а се задржува можноста за доверлива проверка на записите [16], [17].

Со ова поглавје се поставува архитектурната основа за понатамошното разработување на моделот *Proof-of-Charge*. Во следното поглавје фокусот се насочува кон структурата на потврдата, нејзиното поврзување со мерните податоци и криптографските механизми што овозможуваат проверливост.

4. МОДЕЛ ЗА PROOF-OF-CHARGE И КРИПТОГРАФСКА ВЕРИФИКАЦИЈА

4.1 Вовед во моделот *Proof-of-Charge*

Моделот *Proof-of-Charge* претставува еден од главните придонеси на оваа дисертација. Неговата цел е секоја завршена сесија за полнење електрично возило да се претстави преку проверлива дигитална потврда, која може подоцна да се искористи за проверка на точноста и непроменливоста на записот. За разлика од класичните записи за наплата, кои најчесто остануваат во заднинскиот систем на операторот, овој модел ја поврзува финалната потврда со мерните податоци и со применетиот ценовен контекст преку криптографски механизми [16].

Основната идеја е по завршување на сесијата системот да формира потврда што ги содржи најважните информации за полнењето: идентификатор на сесијата, идентификатор на полначот, време на започнување и завршување, испорачана енергија, тарифен контекст и пресметковни вредности. Деталниот мерен тек не мора целосно да се открива, но неговата врска со потврдата се зачувува преку хеш-вредностите и Мерклovата коренска *(Merkle Root)* вредност.

Со ваквата поставеност, потврдата не е само административен документ за завршена сесија. Таа станува проверлива структура што може повторно да се пресмета и да се спореди со зачуваните криптографски вредности. Ако подоцна се измени дел од мерните податоци, пресметковните вредности или содржината на потврдата, таа промена треба да се одрази и во криптографскиот резултат.

Моделот е поставен така што деталните податоци остануваат во заднинскиот или *off-chain* слој, додека блокчејн се користи само за закотвување компактни доказни вредности. Овој пристап ја намалува количината на податоци што се објавуваат надвор од системот, а сепак овозможува подоцнежна независна проверка.

Во следните потпоглавја се разгледуваат структурата на потврдата за полнење, криптографското поврзување со мерните податоци, процесот на генерирање потврда, групирањето преку групно закотвување (*batch anchoring)*, верификацијата и ограничувањата на предложениот пристап. Со тоа, ова поглавје ја поставува основата за имплементацијата и експерименталната евалуација на системот.

4.2 Структура на потврдата за полнење

Потврдата за полнење претставува основниот дигитален објект во моделот *Proof-of-Charge*. Нејзината улога е да ги обедини клучните податоци за една завршена сесија и да создаде врска меѓу финалниот запис за наплата, мерните вредности и криптографските докази. За разлика од класичниот пресметковен запис, кој најчесто останува во заднинскиот

систем на операторот, оваа потврда е дизајнирана така што може подоцна независно да се провери [16], [17].

Структурата на потврдата треба да биде доволно целосна за да ја опише сесијата, но и доволно ограничена за да не открива непотребни чувствителни информации. Затоа, во неа се вклучуваат само потребните идентификациски, временски, енергетски, пресметковни и криптографски елементи. Деталните временски серии од мерењето не мора да се објавуваат или да се споделуваат со сите учесници, што е важно за заштита на приватноста на корисникот [5], [6], [9].

Основните елементи на потврдата за полнење се прикажани на сликата 4.1.

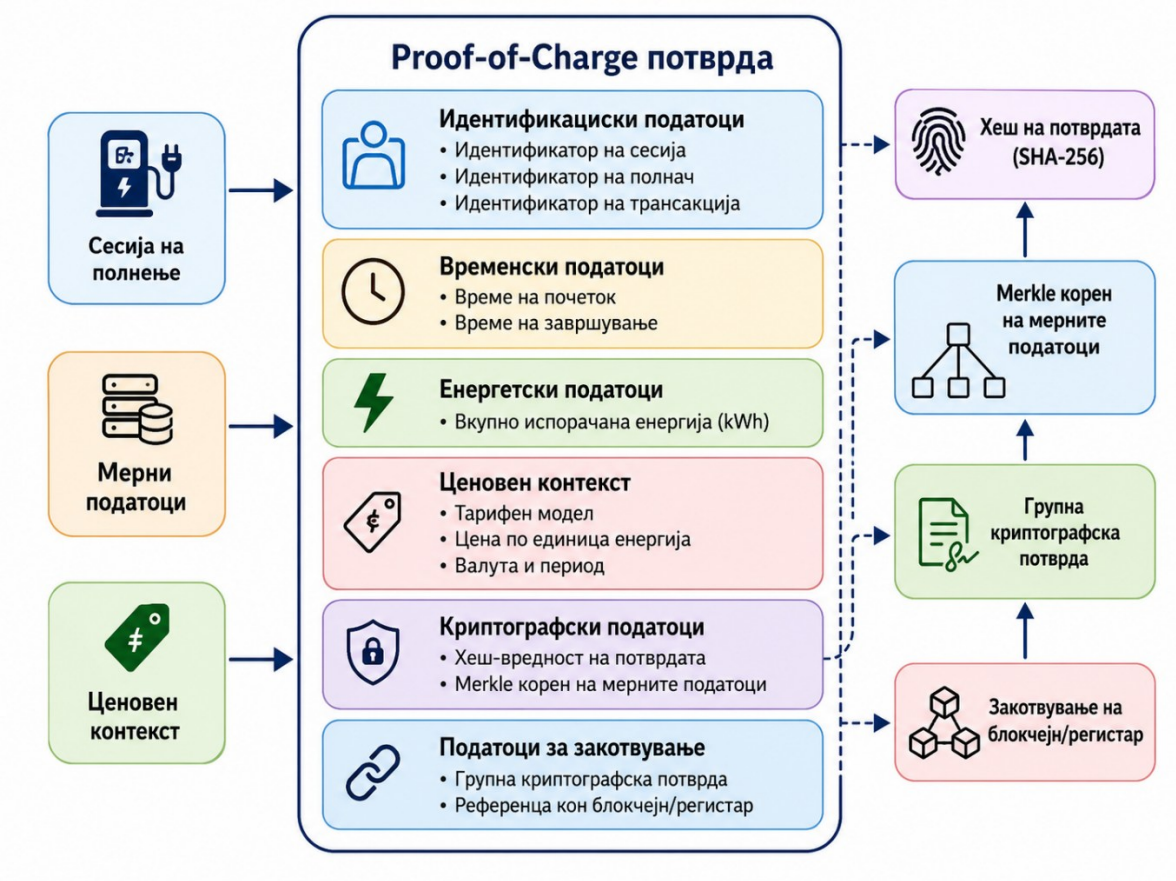
Категорија	Поле / податок	Улога во моделот
Идентификациски податоци	Идентификатор на сесија	Единствено ја означува сесијата на полнење.
	Идентификатор на полнач	Го поврзува записот со конкретна опрема.
	Идентификатор на трансакција	Овозможува поврзување со backend/OCPP.
Временски податоци	Време на почеток	Го означува почетокот на сесијата.
	Време на завршување	Го означува крајот на сесијата.
Енергетски податоци	Вкупно испорачана енергија (kWh)	Служи како основа за проверка на енергијата.
Ценовен контекст	Тарифен модел	Го опишува начинот на пресметка на цената.
	Цена по единица енергија	Овозможува проверка на финалната пресметка.
	Валута и период на примена	Дефинира ценовен контекст и валидност.
Криптографски податоци	Хеш-вредност на потврдата	Обезбедува проверка дека потврдата не е изменета.
	Merkle корен на мерните податоци	Ги поврзува агрегираниот износ и оригиналните мерења.
Податоци за закотвување	Групна криптографска потврда	Ги поврзува повеќе потврди во една група.
	Референца кон блокчејн/регистар	Овозможува независна проверка и ревизија.

Слика 4.1: Основни елементи на потврдата за полнење

Како што е прикажано на сликата 4.1, потврдата ги содржи главните информации потребни за опис и проверка на сесијата. Тука спаѓаат идентификаторот на сесијата, идентификаторот на полначот, временските ознаки, вкупната испорачана енергија, тарифниот контекст и пресметковниот резултат. Овие податоци ја даваат основата за поврзување на сесијата со финалниот запис за наплата.

Покрај описните и пресметковните полиња, потврдата содржи и криптографски елементи. Во овој дел спаѓаат хеш-вредноста на потврдата, Мерклovата коренска вредност поврзана со мерниот тек, како и вредностите што подоцна можат да се користат во групното закотвување (*batch anchoring)*. Овие елементи овозможуваат содржината на потврдата да се провери без повторно да се изложуваат сите детални мерни податоци [16], [17].

Структурата на *Proof-of-Charge* потврдата е прикажана на сликата 4.2.



Слика 4.2: Структура на *Proof-of-Charge* потврда за полнење

Сликата 4.2 ја прикажува логичката организација на потврдата. Таа ги одвојува податоците што ја опишуваат сесијата од криптографските вредности што служат за проверка на нејзиниот интегритет. Ваквата поделба е важна затоа што овозможува потврдата да биде разбирлива за оперативна употреба, но истовремено и доволно силна за ревизиска проверка.

Доколку подоцна е потребна проверка, мерните вредности можат повторно да се обработат и да се споредат со зачуваната Мерклова коренска вредност (*Merkle Root value*). Ако добиената вредност се совпаѓа со вредноста во потврдата, тоа покажува дека мерниот тек не бил изменет. Ако постои несовпаѓање, системот може да укаже на можна промена, бришење или неконзистентност во записите.

На овој начин, структурата на потврдата овозможува практична употреба на записот, ограничено изложување на чувствителни податоци и основа за независна проверка. Деталното криптографско поврзување на мерните податоци се разгледува во следното потпоглавје.

4.3 Криптографско поврзување на мерните податоци

Криптографското поврзување со мерните податоци е клучен дел од моделот *Proof-of-Charge*. Неговата цел е да обезбеди јасна и проверлива врска меѓу потврдата за полнење и мерниот тек што бил создаден за време на сесијата. На тој начин, финалниот запис за сесијата не се разгледува изолирано, туку како резултат што може да се поврзе со оригиналните вредности од мерењето [16], [17].

Во текот на една сесија за полнење, полначот создава повеќе мерни вредности. Тие можат да содржат временска ознака, моментална или акумулирана енергија, моќност, статус на сесијата и други технички информации. Овие записи се важни затоа што врз нивна основа се пресметуваат испорачаната енергија, времетраењето и финалниот износ за наплата.

Во поширок контекст, ваквиот пристап се надоврзува на основните принципи на блокчејн технологијата, каде што криптографските вредности се користат за непроменливост, следливост и проверка на записите [19]. Дополнително, кај современите системи за полнење треба да се земе предвид дека сесијата не мора секогаш да опфаќа само еднонасочно полнење, туку може да вклучи и сценарија со враќање енергија кон мрежата, што ја зголемува потребата за јасно дефинирани енергетски и пресметковни записи [20]. Во оваа насока, моделот *Proof-of-Charge* се надоврзува на претходно предложени пристапи за проверливи потврди со *off-chain* хеширање и *on-chain* закотвување [21].

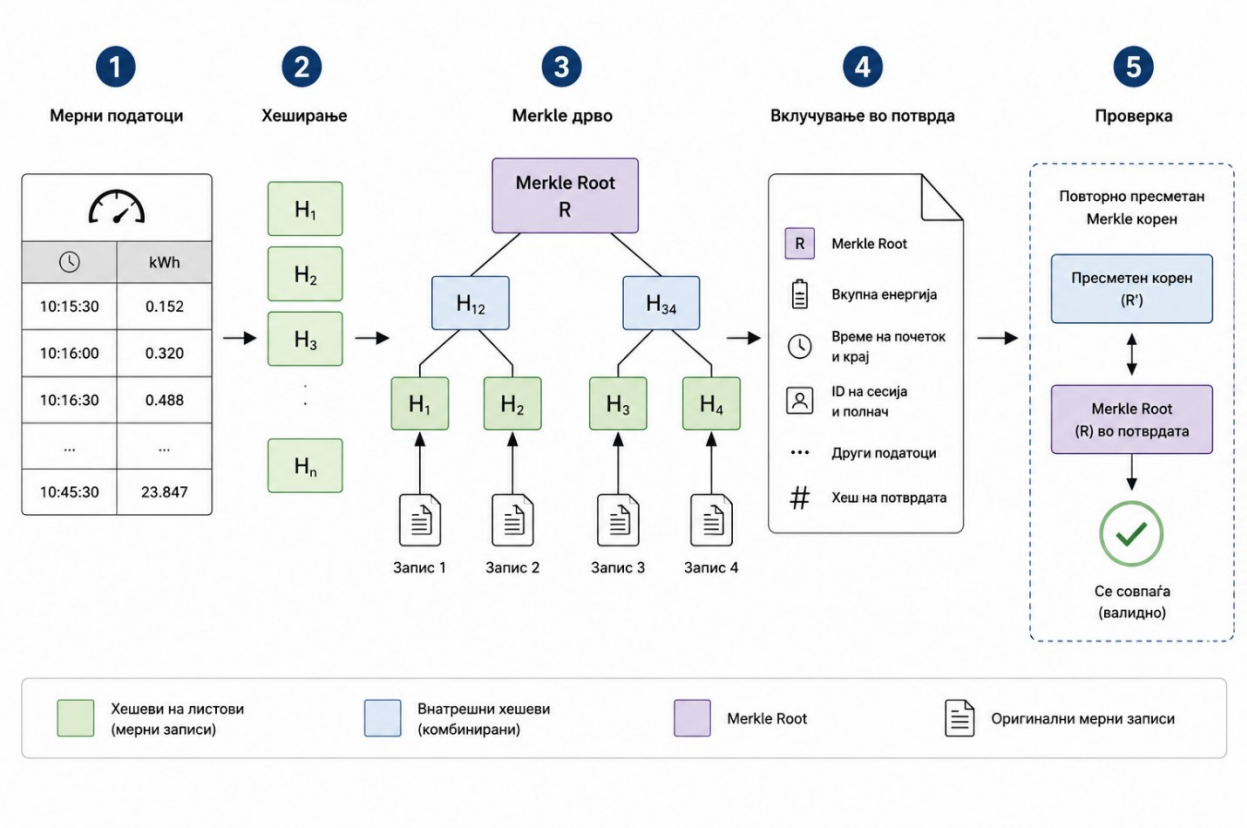
Наместо сите мерни вредности директно да се вклучат во потврдата или да се запишат на блокчејн, предложениот модел користи криптографски отпечатоци. Секоја мерна вредност или нормализиран запис од мерниот тек може да се претстави преку хеш-вредност. Потоа, овие вредности се организираат во Мерклова структура, од која се добива една заедничка Мерклова коренска вредност [22], [23], [24], [25].

Меркловата коренска вредност има улога на компактен доказ за целиот мерен тек. Таа не ги открива деталните мерни податоци, но овозможува подоцнежна проверка дали тие податоци останале непроменети. Доколку се измени само една мерна вредност, се менува и нејзината хеш-вредност, а со тоа и конечната Мерклова коренска вредност. Ова овозможува откривање на измени, бришења или неконзистентности во записите.

Криптографското поврзување се изведува во неколку чекори. Најпрво, мерните записи се подготвуваат во јасен и повторлив формат. Потоа, за секој запис се пресметува хеш-вредност. Добиените вредности се користат како листови во Меркловата структура, од која се пресметува Мерковиот корен (*Merkle Root*). Таа вредност се внесува во потврдата за полнење и станува дел од нејзината криптографска содржина.

Важен услов во овој процес е податоците секогаш да се обработуваат на ист начин. Доколку форматот, редоследот или претставувањето на вредностите не се јасно дефинирани, истите мерни податоци можат да дадат различен криптографски резултат. Затоа, во моделот е потребна доследна нормализација и канонична претстава на записите пред нивно хеширање.

Процесот на поврзување на мерните податоци со потврдата е прикажан на сликата 4.3.



Слика 4.3: Криптографско поврзување на мерните податоци преку Мерклова структура

Како што е прикажано на сликата 4.3, мерните вредности прво се претвораат во хеш-вредности, потоа се организираат во Мерклова структура, а добиената Мерклова коренска вредност се внесува во потврдата за полнење. Со ова се создава врска меѓу деталниот мерен тек и финалниот запис, без сите вредности да се изложуваат надвор од системот.

Доколку подоцна е потребна проверка, системот повторно ги обработува мерните записи и ја пресметува новата Мерклова коренска вредност. Ако таа се совпаѓа со вредноста зачувана во потврдата, се потврдува дека мерниот тек е конзистентен со потврдата. Ако вредностите не се совпаѓаат, тоа укажува дека е можна промена во записите или дека податоците не се обработени според истиот формат.

Со ваквиот пристап, моделот *Proof-of-Charge* обезбедува проверлива врска меѓу мерните податоци и потврдата за полнење, без непотребно откривање на деталните вредности. Овој механизам претставува основа за понатамошното генерирање на потврдата, што се разгледува во следното потпоглавје.

4.4 Генерирање на Proof-of-Charge потврда

Генерирањето на *Proof-of-Charge* потврда е процес преку кој една завршена сесија за полнење електрично возило се претвора во проверлив дигитален запис. Овој процес започнува по завршување на сесијата, кога заднинскиот систем располага со мерните вредности, временските ознаки, идентификаторите на сесијата и полначот, како и со тарифниот контекст потребен за пресметување на финалниот запис за наплата [16], [17].

За потврдата да може подоцна да се провери, нејзиното создавање мора да биде доследно и повторливо. Тоа значи дека истите влезни податоци треба секогаш да доведат до иста структура на потврдата и до иста хеш-вредност. Доколку редоследот на полињата, форматот на временските ознаки или начинот на претставување на бројните вредности се менува, може да се добијат различни криптографски резултати иако сесијата е иста. Затоа, во моделот се користи канонска претстава на податоците пред нивно хеширање [22], [23], [24], [25].

Во поширок контекст, потребата од проверливи и јасно структурирани записи е уште поизразена кај современите системи за полнење, особено кога се разгледуваат сценарија со двонасочен проток на енергија и доверлива размена меѓу повеќе учесници [26]. Таквите сценарија бараат потврдата да може да ги претстави не само основните податоци за сесијата, туку и енергетските и пресметковните вредности на начин што овозможува подоцнежна проверка.

Канонската репрезентација и хеширањето на потврдата се прикажани на сликата 4.4.

Слика 4.4: Канонска JSON репрезентација и хеширање на *Proof-of-Charge* потврда

Како што е прикажано на сликата 4.4, податоците од сесијата најпрво се организираат во јасна и стабилна структура. Потоа таа структура се претставува во канонски JSON формат, врз кој се пресметува хеш-вредноста на потврдата. Оваа вредност претставува дигитален отпечаток на целата потврда и се користи како основа за подоцнежна проверка.

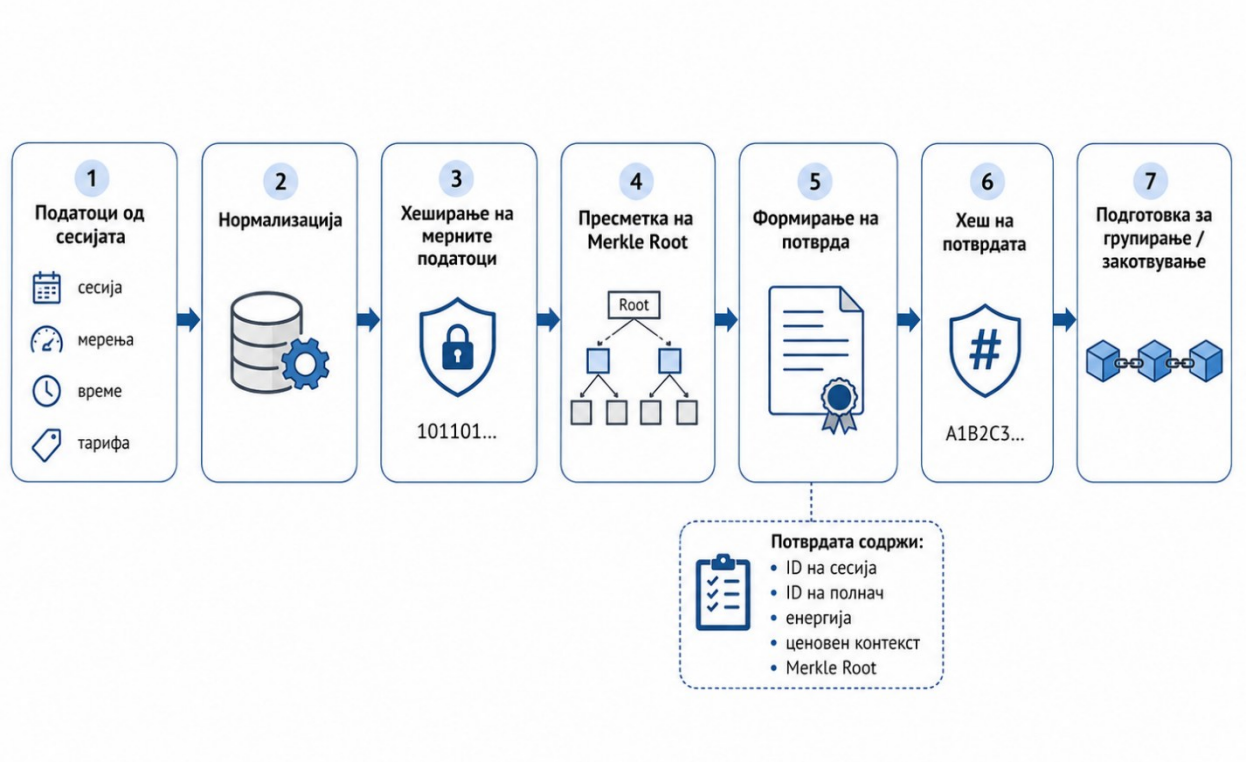
Важноста на канонската претстава може да се види преку примерот во табелата 4.1. Истите податоци можат да бидат претставени со различен редослед на полињата или со различен формат на сериализација, што може да доведе до различна хеш-вредност. Поради тоа, пред хеширањето потребно е да се користи стабилна и повторлива претстава на потврдата.

Табела 4.1: Пример за влијание на JSON серијализација врз хеш-вредноста

Варијанта	JSON претстава	Хеш-вредност	Толкување
A – неканонска претстава	Полињата се прикажани во еден редослед, на пример: session_id, *EVSE*_id, energy_kwh, start_time.	Се добива една хеш-вредност.	Иако содржината е иста, редоследот на полињата може да влијае врз конечната хеш-вредност.
B – неканонска претстава	Истите полиња се прикажани во друг редослед, на пример: start_time, energy_kwh, *EVSE*_id, session_id.	Се добива различна хеш-вредност.	Различната сериализација може да предизвика лажно несовпаѓање при проверка.
C – канонска претстава	Полињата се претставени според однапред дефиниран детерминистички редослед и формат.	Се добива стабилна и повторлива хеш-вредност.	Канонската JSON репрезентација обезбедува истата содржина секогаш да резултира со иста хеш-вредност.

Практично, процесот на генерирање се состои од неколку чекори. Најпрво се прибираат податоците од завршената сесија. Потоа се пресметуваат енергетските и пресметковните вредности, се формира Мерклова коренска вредност *(Merkle root value)* на мерниот тек и се создава структурата на потврдата. Откако потврдата ќе се претстави во канонски формат, се пресметува нејзината хеш-вредност. Таа потоа може да се зачува во заднинскиот систем, да се вклучи во групно закотвување или да се користи при ревизиска проверка [16], [17], [26].

Процесот на генерирање на *Proof-of-Charge* потврда е прикажан на сликата 4.5.



Слика 4.5: Процесот на генерирање на *Proof-of-Charge* потврда

Сликата 4.5 го прикажува редоследот на главните активности: завршување на сесијата, прибирање на релевантните податоци, нормализација, пресметување на Мерклова коренска вредност*(Merkle root value)*, формирање на потврдата, хеширање и подготовка за групирање или закотвување. Ваквиот редослед овозможува секоја потврда да биде создадена на ист начин, што е важно за нејзината подоцнежна проверка.

Целосната потврда може да се чува во заднинскиот или друг доверлив *off-chain* простор. На блокчејн не мора да се запишуваат деталните податоци од сесијата, туку само компактни криптографски вредности што служат како доказ за интегритет. Овој пристап ја намалува количината на изложени информации, а сепак овозможува проверка дали потврдата или мерните записи биле изменети по нивното создавање [15], [18], [23], [26].

Во случаи кога потврдата содржи податоци за увезена, извезена или нето енергија, истата постапка може да се примени и за сесии што се подготвени за идни *V2G* сценарија. Тоа не значи дека моделот целосно го решава управувањето со *V2G* пазар или енергетско балансирање, туку дека структурата на потврдата може да поддржи поширок тип енергетски записи и доверлива проверка на нивната конзистентност [20], [26], [27].

На овој начин, генерирањето на *Proof-of-Charge* потврдата го поврзува оперативниот запис од сесијата со криптографските докази што се користат во понатамошните чекори. Следното потпоглавје го разгледува групирањето на повеќе потврди и нивното закотвување преку групно закотвување (*batch anchoring)*.

4.5 Групирање и закотвување на потврдите

По генерирањето на поединечните *Proof-of-Charge* потврди, следниот чекор е нивно групирање и закотвување. Целта на овој процес е да се обезбеди ефикасна проверливост на поголем број сесии за полнење, без потреба секоја потврда одделно да се запишува на блокчејн. На овој начин се намалуваат трошоците, се подобрува скалабилноста и се задржува можноста за подоцнежна независна проверка [15], [16], [18].

Во предложениот модел, секоја потврда по нејзиното создавање се претставува преку хеш-вредност. Таа вредност претставува дигитален отпечаток на целата потврда и овозможува да се утврди дали потврдата била изменета по финализирањето [22], [26], [27]. Наместо сите потврди да се закотвуваат одделно, нивните хеш-вредности се групираат во дефинирани временски интервали, на пример дневно, неделно или според друг избран период.

Групната криптографска потврда се формира преку Мерклова структура, каде што хеш-вредностите на поединечните потврди се користат како листови на дрвото. Со нивно комбинирање и повторно хеширање се добива заедничка Мерклова коренска вредност, која ја претставува целата група потврди. Ако се промени која било поединечна потврда, се менува нејзината хеш-вредност, а со тоа и крајната Мерклова коренска вредност [17], [24], [26].

Закотвувањето претставува процес во кој групната Мерклова коренска вредност се запишува на блокчејн или во надворешен регистар за интегритет. Притоа, на блокчејн не се зачувуваат деталните мерни податоци, целосните потврди или приватните информации за корисникот. Се зачувува само минимален криптографски доказ, кој подоцна може да се користи за проверка дали конкретна потврда била дел од одредена група и дали таа група постоела во даден временски период [15], [18], [23].

Во табелата 4.2 е прикажана поделбата меѓу податоците што остануваат во *off-chain* слојот и минималните криптографски докази што можат да се закотват *on-chain* или во надворешен регистар за интегритет.

Табела 4.2: Поделба на off-chain податоци и on-chain криптографски докази

Категорија	Се чува *off-chain*	Се закотвува *on-chain* / во регистар
Мерни податоци	Детални временски серии од мерењето	Не се зачувуваат јавно
Потврда за полнење	Целосна *Proof-of-Charge* потврда	Хеш-вредност преку групен доказ
Група потврди	Листа на потврди и нивни хеш-вредности	Групен Мерклов корен
Верификациски податоци	Мерклова патека, *batch ID*, metadata	Референца кон закотвениот доказ
Приватни податоци	Под контрола на операторот	Не се објавуваат

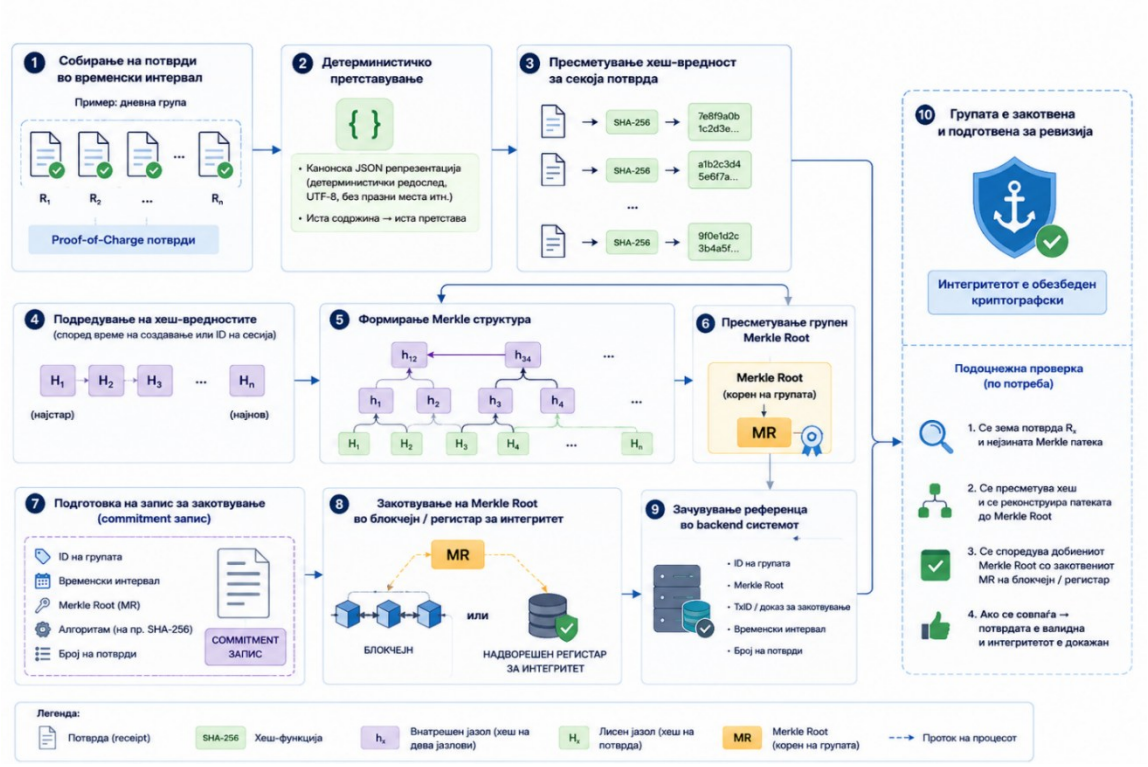
Како што е прикажано во табелата 4.2, деталните податоци од сесиите остануваат надвор од јавниот регистар. Блокчејн или надворешниот регистар се користи само како слој за проверка на интегритетот, преку компактни вредности како *receipt hash*, *Merkle Root* или *batch root*. Ваквата поделба ја намалува изложеноста на чувствителни информации и ја прави архитектурата попрактична за системи со голем број сесии [15], [18], [23].

Овој пристап е во согласност со логиката на проверливи регистри и системи за временско означување, каде што целта е да се обезбеди доказ дека одреден дигитален запис постоел во одреден момент и дека не бил неовластено изменет подоцна [23], [24]. Во контекст на *Proof-of-Charge*, закотвената Мерклова коренска вредност претставува доказ за постоењето и интегритетот на група потврди за полнење, без откривање на содржината на секоја поединечна сесија.

Во зависност од имплементацијата, закотвувањето може да се реализира на јавен блокчејн, приватна мрежа, *consortium blockchain* или друг доверлив регистар за интегритет. Јавните блокчејн мрежи обезбедуваат повисоко ниво на независна проверливост, додека приватните и *consortium blockchain* можат да понудат подобра контрола, пониски трошоци и поголема усогласеност со организациските барања [11], [13], [28].

Покрај блокчејн-закотвувањето, целосните потврди и придружните податоци можат да се чуваат во заднинскиот систем на операторот или во децентрализирани системи за складирање. Во таква поставеност, блокчејн не ја презема улогата на база на податоци, туку служи како регистар за проверка на интегритетот. Слична логика се применува и кај системи со *content-addressed storage*, каде што податоците се адресираат преку нивните криптографски отпечатоци [15], [29].

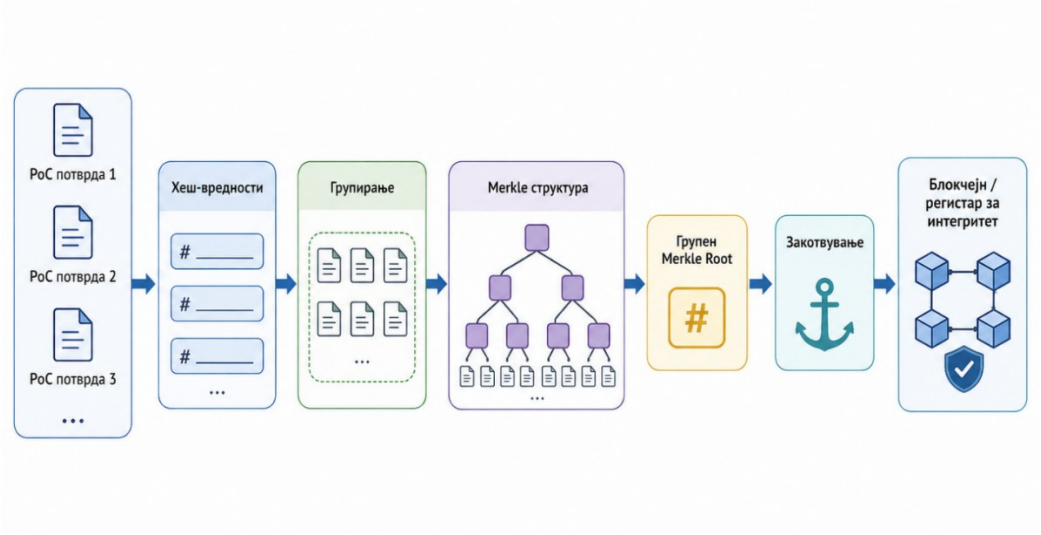
Процесот на групирање и закотвување на *Proof-of-Charge* потврдите е прикажан на сликата 4.6. Во овој процес, поединечните потврди најпрво се претставуваат преку хеш-вредности, потоа се групираат во заедничка Мерклова структура, од која се формира групна Мерклова коренска вредност. Овој корен се користи како компактен доказ за целата група и се закотвува на блокчејн или во надворешен регистар за интегритет.



Слика 4.6: Формирање групен Мерклов корен *(Merkle Root)* и закотвување на *Proof-of-Charge* потврди

Како што е прикажано на сликата 4.6, закотвувањето не бара складирање на целосните потврди или деталните податоци од сесиите на блокчејн. Наместо тоа, се зачувува само групниот криптографски доказ. На овој начин, повеќе сесии за полнење можат да бидат заштитени преку еден закотвен запис, со помали трошоци и без непотребно изложување на чувствителни податоци.

Разликата меѓу проверката на поединечна потврда и проверката на групно закотвени потврди е прикажана на сликата 4.7. Оваа споредба ја објаснува улогата на локалната Мерклова коренска вредност во рамките на една сесија и улогата на вредноста на групниот корен *(batch root)* при проверка на повеќе потврди.



Слика 4.7: Групирање и закотвување на *Proof-of-Charge* потврди

Како што е прикажано на сликата 4.7, локалната верификација се однесува на една конкретна потврда и нејзиниот мерен тек, додека групната верификација проверува дали одредена потврда припаѓа на заедничка *batch root* вредност. Со тоа моделот овозможува проверливост и на ниво на поединечна сесија и на ниво на група сесии.

Процесот на проверка по закотвувањето се состои од неколку чекори. Најпрво, проверувачот ја зема конкретната потврда и ја пресметува нејзината хеш-вредност. Потоа се користи Мерклова патека за да се докаже дека таа вредност била дел од групата. На крај, повторно пресметаната Мерклова коренска вредност се споредува со вредноста што е закотвена на блокчејн или во надворешниот регистар. Доколку вредностите се совпаѓаат, потврдата се смета за дел од валидната група и нејзиниот интегритет е потврден [17], [24], [25].

Во целина, групирањето и закотвувањето претставуваат механизам преку кој моделот *Proof-of-Charge* станува поскалабилен и попримењлив во реални системи за полнење електрични возила. Голем број потврди можат да бидат заштитени преку мал број криптографски докази, при што се задржува можноста за независна проверка ревизија и откривање на неовластени промени. Овој механизам ја поставува основата за процесот на верификација, кој се разгледува во следното потпоглавје.

4.6 Верификација на потврдата и откривање неовластени промени

Верификацијата на *Proof-of-Charge* потврдата претставува процес преку кој се проверува дали финалниот запис за полнење е конзистентен со оригиналните мерни податоци, криптографските отпечатоци и закотвените докази. Овој процес има клучна улога во предложениот модел, бидејќи овозможува независна проверка на записите без потреба сите детални податоци од сесијата да се складираат на блокчејн или да се откриваат на сите учесници во системот [16], [17].

Верификацијата може да се изведува на две нивоа. Првото ниво е проверка на поединечна потврда, при што се пресметува хеш-вредноста на конкретниот запис и се споредува со зачуваната вредност. Второто ниво е групна проверка, при што се пресметува групен Мерклов корен (*batch Merkle Root)* од сите потврди во дадена група и се споредува со закотвениот доказ. Оваа поделба овозможува локално откривање на промени во конкретна потврда, но и глобална проверка дали целата група потврди останала непроменета [16].

Споредбата меѓу локалната и групната верификација е прикажана на сликата 4. 8:

Слика 4.8: Споредба на локална и групна верификација на *Proof-of-Charge* потврди

Постапката за верификација започнува со прибирање на потребните елементи: потврдата за полнење, релевантните мерни вредности, хеш-вредноста на потврдата, Мерклoвиот корен *(Merkle Root)* на мерните податоци, Мерклoвата патеката (*Merkle path*) доколку се проверува поединечен запис, како и закотвениот криптографски доказ во блокчејн или надворешен регистар за интегритет. Овие елементи овозможуваат проверувачот повторно да ги изврши криптографските пресметки и да ги спореди добиените вредности со вредностите зачувани во потврдата или во закотвениот запис [17], [24], [25].

Првиот чекор во верификацијата е проверка на структурата на потврдата. Проверувачот треба да утврди дали потврдата ги содржи потребните полиња, како идентификатор на сесија, идентификатор на полнач, временски ознаки, агрегирана испорачана енергија, ценовен контекст, хеш-вредност на потврдата и Мерклвиот корен *(Merkle Root)* на мерните податоци. Доколку недостасува некое од клучните полиња, потврдата не може целосно да се провери и треба да се смета за невалидна или непотполна.

Вториот чекор е повторна нормализација на податоците. Податоците од потврдата и мерните вредности мора да се претстават во истиот детерминистички формат што бил користен при нивното првично хеширање. Овој чекор е неопходен затоа што криптографските хеш-функции се чувствителни на секоја промена во влезот, вклучувајќи различен редослед на полиња, различен формат на временски ознаки или различна прецизност на бројните вредности [22], [27].

Третиот чекор е пресметување на хеш-вредноста на потврдата. Проверувачот ја зема нормализираната форма на потврдата и врз неа применува ист алгоритам за хеширање што бил користен при создавањето на потврдата. Доколку повторно пресметаната хеш-вредност се совпаѓа со хеш-вредноста зачувана во системот или во групната криптографска потврда, тоа покажува дека содржината на потврдата не била изменета по нејзиното создавање [22].

Четвртиот чекор е проверка на Мерклвиот корен за мерните податоци. Проверувачот повторно ја формира Мерклвата структурата од достапните мерни записи или ја користи соодветната Мерклова патека за селективна проверка. Пресметаниот Мерклов корен потоа се споредува со вредноста зачувана во потврдата. Совпаѓањето на вредностите укажува дека мерните податоци се конзистентни со потврдата за полнење, додека несовпаѓањето може да укаже на промена, бришење или замена на некој од записите [17], [24], [26].

Селективната проверка е особено важна кога не е потребно или не е дозволено откривање на целата низа на мерни податоци. Во таков случај, проверувачот добива конкретна мерна вредност и минимален збир на хеш-вредности потребни за докажување дека таа вредност е дел од оригиналната Мерклова структура. Овој пристап овозможува проверка на поединечни записи без откривање на сите останати мерења, што е значајно за заштита на приватноста и за намалување на количината на податоци што се споделуваат при ревизија [24], [25].

Петтиот чекор е проверка на групната криптографска потврда. Доколку потврдата за полнење била вклучена во група потврди, нејзината хеш-вредност се користи како еден од листовите во групната Мерклова структура. Проверувачот може да ја искористи соодветната Мерклвата патека за да докаже дека конкретната потврда е дел од групата. Потоа, повторно пресметаниот групен Мерклов корен (*Merkle Root)* се споредува со Мерклвиот корен закотвен во блокчејн или во надворешниот регистар за интегритет [16], [17], [24].

Доколку сите пресметки се совпаѓаат, потврдата се смета за валидна, а записот за полнење за конзистентен. Во спротивно, доколку постои несовпаѓање во хеш-вредноста на потврдата, Мерклвиот корен на мерните податоци или групниот Мерклов корен, системот може да укаже на можна неовластена промена, бришење, замена или

неконзистентност во податоците. На овој начин, моделот *Proof-of-Charge* овозможува откривање на манипулации без потреба од целосна доверба во заднинскиот (*backend)* систем на операторот.

Откривањето на неовластени промени може да се однесува на повеќе типови нарушувања. Може да се открие промена во поединечна мерна вредност, како изменета енергија или временска ознака; промена во финалната потврда, како изменет ценовен контекст или различен агрегираниот износ на енергија; или промена во групата потврди, како отстранување или додавање запис што доведува до несовпаѓање со закотвениот Мерклов корен.

Верификацијата е особено значајна во случаи на спор меѓу корисникот и операторот, меѓу оператор и давател на услуги за електрична мобилност, или при надворешна ревизија. Наместо спорот да се решава само врз основа на интерни дневници, страните можат да ја користат потврдата за полнење и закотвените криптографски докази за независна проверка. Ваквиот пристап се надоврзува на концептите за безбедни ревизорски дневници и записи отпорни на неовластени промени, каде што целта е откривање на промени во записите преку криптографски механизми [16], [23], [24], [30], [31].

Во табелата 4.3 се прикажани главните чекори во процесот на верификација на *Proof-of-Charge* потврдата и нивната улога во откривање на можни неовластени промени.

Табела 4.3: Чекори за верификација на Proof-of-Charge потврда

Чекор	Опис	Цел на проверката
Проверка на структурата	Се проверува дали потврдата ги содржи сите потребни полиња, како идентификатор на сесија, идентификатор на полнач, временски ознаки, агрегирана енергија, ценовен контекст, хеш-вредност и Мерклов корен *(Merkle Root).*	Откривање непотполна, неправилно формирана или невалидна потврда.
Нормализација на податоците	Податоците од потврдата и мерните вредности се претставуваат во детерминистички формат.	Обезбедување повторливост на хеш-пресметките и избегнување различни резултати поради различно форматирање.
Проверка на хеш-вредноста на потврдата	Се пресметува хеш-вредност на нормализираната потврда и се споредува со зачуваната вредност.	Откривање промени во финалниот запис за полнење.
Проверка на Мерклов корен (*Merkle Root)*	Се пресметува или проверува Мерклов корен од мерните податоци.	Потврдување дека мерните податоци се

		конзистентни со потврдата за полнење.
Проверка преку Мерклова патека	Се проверува поединечна мерна вредност или конкретна потврда преку минимален збир на хеш-вредности.	Селективна проверка без откривање на целата низа на мерни податоци.
Проверка на закотвениот доказ	Групниот Мерклов корен се споредува со доказот закотвен во блокчејн или надворешен регистар за интегритет.	Потврдување дека групата потврди не е изменета по закотвувањето.
Детекција на несовпаѓање	Се анализираат разликите меѓу повторно пресметаните и зачуваните криптографски вредности.	Откривање можни неовластени промени, бришење, замена или неконзистентност во записите.

На овој начин, верификацијата на *Proof-of-Charge* потврдата обезбедува практичен механизам за проверка на интегритетот на записите за полнење. Таа овозможува откривање на неовластени промени, поддржува независна ревизија и ја зачувува приватноста преку користење на компактни криптографски докази наместо целосно откривање на мерните податоци.

4.7 Ограничувања и претпоставки на моделот *Proof-of-Charge*

Иако моделот *Proof-of-Charge* обезбедува криптографска проверливост на записите за полнење електрични возила, неговата примена се темели на одредени претпоставки и има неколку ограничувања што треба јасно да се разгледаат. Овие ограничувања не ја намалуваат вредноста на моделот, туку ја дефинираат неговата применливост, опсег и условите под кои може да обезбеди доверливи резултати.

Првата претпоставка се однесува на мерната опрема. *Proof-of-Charge* може да докаже дека одредени мерни податоци не биле изменети по нивното создавање, но не може самостојно да гарантира дека физичкото мерење било точно доколку самата мерна опрема е неисправна, погрешно калибрирана или компромитирана. Затоа, моделот претпоставува дека вредностите од мерењето се создаваат од доверлива, правилно конфигурирана или сертифицирана опрема за полнење.

Втората претпоставка се однесува на нормализацијата на податоците. За да биде проверката повторлива, сите податоци што се користат за хеширање мора да бидат претставени во детерминистички формат. Различен редослед на полињата, различен формат на временските ознаки или различна прецизност на енергетските вредности може да доведе до различни хеш-вредности. Поради тоа, нормализацијата претставува критичен чекор во генерирањето и верификацијата на потврдата [22], [27].

Третото ограничување е поврзано со складирањето на деталните податоци надвор од блокчејнот. Моделот не ги складира сите мерни вредности и целосни записи на блокчејн, туку користи хеш-вредности, Мерклов корен и групни криптографски потврди како докази за интегритет [15], [18]. Овој пристап ја подобрува приватноста и скалабилноста, но бара операторот да ги зачува оригиналните податоци во својот заднински *(backend)* систем или во друг соодветен простор за складирање, за да може подоцна да се изврши верификација.

Четвртото ограничување се однесува на трошоците и доцнењето при закотвување. Доколку секоја поединечна потврда се запишува директно на блокчејн, системот може да се соочи со високи трансакциски трошоци и ограничувања во перформансите. Поради тоа, моделот користи групирање на потврдите и закотвување на групен Мерклов корен, што овозможува поголема скалабилност и намалување на бројот на записи на блокчејн [16], [17], [24].

Петтото ограничување се однесува на приватноста. *Proof-of-Charge* го намалува откривањето на детални временски серии од мерењето и не бара јавно објавување на чувствителни податоци. Сепак, моделот не обезбедува целосна анонимност на корисникот. Во реалните системи може да биде потребна дополнителна примена на механизми за заштита на идентитетот, контролирано откривање на податоци или други privacy-preserving техники, особено во сценарија на роаминг и регулаторна проверка [5], [6], [9], [19], [20].

Шестото ограничување се однесува на опсегот на моделот. *Proof-of-Charge* не е целосно решение за сите безбедносни предизвици во инфраструктурата за полнење електрични возила. Тој не ја заменува потребата од безбедна комуникација, автентикација, заштита на заднинските системи, безбедност на полначите или управување со пристап. Наместо тоа, моделот обезбедува дополнителен слој за проверливост на записите за полнење, кој може да се комбинира со постојните OCPP/OCPI процеси и со други безбедносни механизми [4], [7], [8], [21].

Главните претпоставки и ограничувања на моделот *Proof-of-Charge* се систематизирани во табелата 4. 4.

Табела 4.4: Претпоставки и ограничувања на моделот Proof-of-Charge

Категорија	Опис	Влијание врз моделот
Претпоставка за мерна опрема	Моделот претпоставува дека мерните податоци се создаваат од доверлива или сертифицирана опрема.	Ако мерната опрема генерира погрешни податоци, криптографијата може да го докаже интегритетот на записот, но не и физичката точност на мерењето.
Зависност од нормализација	Податоците мора да се претстават во детерминистички формат пред хеширање.	Различен формат може да доведе до различни хеш-вредности и проблеми при проверка.

Складирање надвор од блокчејнот	Деталните мерни податоци и целосните потврди остануваат надвор од блокчејнот.	Потребно е операторот да ги зачува оригиналните податоци за подоцнежна верификација.
Трошоци за закотвување	Закотвувањето на блокчејн може да има трошоци и доцнење.	Потребно е групирање на потврдите за поголема скалабилност.
Приватност, но не целосна анонимност	Моделот го намалува откривањето на детални податоци, но не гарантира целосна анонимност.	Може да бидат потребни дополнителни механизми за заштита на идентитетот.
Компатибилност со постојни системи	Моделот се надградува врз постојните OCPP/OCPI процеси.	Не ги заменува постојните протоколи, туку додава проверлив слој.
Ограничен безбедносен опсег	Моделот не ги решава сите кибербезбедносни ризици на полначите и заднинските системи.	Треба да се комбинира со други безбедносни мерки и политики.

На овој начин, верификацијата на *Proof-of-Charge* потврдата обезбедува практичен механизам за проверка на интегритетот на записите за полнење. Таа овозможува откривање на неовластени промени, поддржува независна ревизија и ја зачувува приватноста преку користење на компактни криптографски докази наместо целосно откривање на мерните податоци.

4.8 Заклучок на поглавјето

Во ова поглавје беше разработен моделот *Proof-of-Charge* како централен механизам за создавање и проверка на криптографски проверливи потврди за сесиите на полнење електрични возила. Моделот има за цел да ја надмине зависноста од доверба само во backend системот на операторот, преку воведување на криптографски докази кои овозможуваат проверка на интегритетот на записите за полнење [16].

Најпрво беше дефинирана структурата на потврдата за полнење, која ги обединува идентификациските податоци, временските ознаки, агрегираниот износ на испорачана енергија, ценовниот контекст, Меркловиот корен (*Merkle Root)* на мерните податоци и податоците за закотвување. Ваквата структура овозможува потврдата да биде доволно информативна за проверка, но истовремено да не открива непотребни чувствителни податоци за корисникот или деталните временски серии од мерењето.

Потоа беше објаснето криптографското поврзување на мерните податоци преку нормализација, хеширање и Мерклови структури. Хеш-функциите овозможуваат создавање дигитален отпечаток на податоците, додека Мерклovите структури овозможуваат компактно претставување на цела низа на мерни записи преку еден Мерклов корен [17], [22], [26]. На тој начин, секоја промена во мерните податоци може да биде откриена преку повторна пресметка и споредба на криптографските вредности.

Во поглавјето беше разработен и процесот на генерирање потврда за *Proof-of-Charge*, кој започнува со прибирање на податоците од сесијата, продолжува со нивна нормализација и криптографска обработка, а завршува со создавање на финален проверлив запис. Овој процес овозможува секоја сесија на полнење да биде претставена преку компактен дигитален запис кој е поврзан со оригиналните мерни податоци и со финалната наплата.

Дополнително, беше анализиран процесот на групирање и закотвување на потврдите. Наместо секоја потврда да се запишува директно на блокчејн, поединечните хеш-вредности се групираат во Мерклова структура, а групниот Мерклов корен *(Merkle Root)* се закотвува во блокчејн или во надворешен регистар за интегритет. Овој пристап овозможува намалување на трошоците, подобрување на скалабилноста и зачувување на приватноста, бидејќи деталните податоци остануваат надвор од блокчејнот [15], [18], [23], [28], [29].

На крај, беше претставена постапката за верификација на потврдата и откривање на неовластени промени. Верификацијата се базира на повторна нормализација, пресметување на хеш-вредности, проверка на Мерклovиот корен, користење Мерклови патеки и споредба со закотвениот криптографски доказ. Ваквиот пристап овозможува откривање на промени, бришење, замена или неконзистентност во записите, што е во согласност со концептите за безбедни ревизорски дневници и записи отпорни на неовластени промени [24], [25], [30], [31].

Со тоа, моделот *Proof-of-Charge* обезбедува рамнотежа меѓу проверливост, приватност, скалабилност и практична применливост. Тој не ја заменува постојната инфраструктура за полнење електрични возила, туку ја надградува со слој за криптографска верификација и независна ревизија. Ова поглавје ја поставува техничката основа за следното поглавје, во кое се разгледуваат офлајн моделите и интеграцијата на предложениот пристап со реални системи за полнење електрични возила.

5. ОФЛАЈН МОДЕЛИ И ИНТЕГРАЦИЈА СО РЕАЛНИТЕ СИСТЕМИ

5.1 Вовед во офлајн моделите и интеграција

Во претходното поглавје беше разработен моделот *Proof-of-Charge* како механизам за создавање проверливи потврди за сесии на полнење електрични возила. Преку хеш-вредностите, Мерклovата коренска вредност и групното закотвување, потврдата се поврзува со мерниот тек и може да се користи како основа за ревизија. За ваквиот пристап да биде применлив во реални услови, потребно е да се разгледа и неговото однесување кога мрежната поврзаност не е постојано достапна.

Во практичната инфраструктура за полнење не може секогаш да се очекува стабилна комуникација меѓу полначот, заднинскиот систем и надворешните сервиси. Полначите можат да работат на локации со ограничена интернет врска, привремени прекини или зависност од локални мрежни услови. Такви ситуации се можни кај јавни паркинзи, рурални средини, кампуси, индустриски објекти или станици поставени на места со нестабилна поврзаност.

Поради тоа, офлајн и полуонлајн моделите имаат важна улога во дизајнот на доверливи системи за полнење. Нивната цел е сесијата да може да продолжи, или барем правилно да се евидентира, и кога директната врска со заднинскиот систем е прекината. Во такви услови, полначот или локалната компонента треба да зачува доволно информации за подоцнежна синхронизација и ревизија.

Интеграцијата на *Proof-of-Charge* во вакви сценарија овозможува локално создадените записи да не останат само привремени оперативни податоци. Тие добиваат криптографска основа преку која може да се утврди дали биле изменети пред да се испратат кон заднинскиот систем. Дури и кога потврдата не може веднаш да се вклучи во групно закотвување, таа може локално да се формира, хешира и поврзе со мерниот тек.

Овој пристап ја намалува зависноста од постојана мрежна достапност. Наместо доверливоста на сесијата да зависи само од моменталната комуникација со централниот систем, дел од доказите за интегритет можат да се создадат локално. Со тоа се добива поотпорен систем, појасна ревизиска трага и подобра основа за решавање можни несогласувања при наплата или синхронизација.

Во ова поглавје се разгледуваат режимите на работа во онлајн, полуонлајн и офлајн сценарија, локалното евидентирање, синхронизацијата, примената на *Proof-of-Charge* при ограничена поврзаност и интеграцијата со реални заднински системи, OCPP и OCPI процеси. На крајот, се дискутираат практичните ограничувања и предизвиците што треба да се земат предвид при реална имплементација.

5.2 Режим на работа: онлајн, полуонлајн и офлајн сценарија

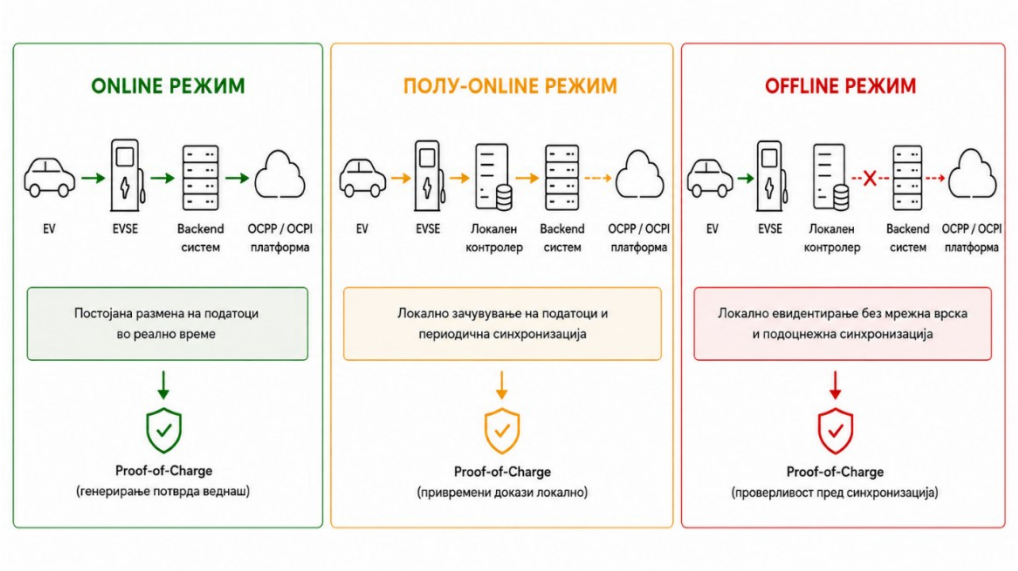
Системите за полнење електрични возила можат да работат во различни услови на мрежна поврзаност. Во идеален случај, полначот има стабилна врска со заднинскиот систем и сите податоци се разменуваат во реално време. Во практична средина, сепак, можни се доцнења, прекини или целосна недостапност на комуникацијата. Поради тоа, предложениот пристап ги разгледува трите основни режими на работа: онлајн, полуонлајн и офлајн сценарио.

Во онлајн режим, полначот постојано комуницира со заднинскиот систем. Автентикацијата, следењето на сесијата, преносот на мерни вредности и обработката на податоците се изведуваат речиси во реално време. Во овој режим, OCPP овозможува размена на оперативни податоци меѓу полначот и заднинскиот систем, додека OCPI може да се користи за размена на податоци во роаминг сценарија [7], [8]. Потврдата *Proof-of-Charge* може да се генерира веднаш по завршување на сесијата, а нејзината хеш-вредност може да се вклучи во групна криптографска потврда за подоцнежно закотвување [16].

Во полуонлајн режим, системот има делумна или повремена поврзаност. Полначот може да започне или да продолжи со работа и кога врската е привремено нестабилна, но дел од податоците се зачувуваат локално до повторно воспоставување на комуникацијата. Овој режим е корисен во ситуации кога прекините се краткотрајни, а системот треба да ја зачува континуираноста на услугата.

Во офлајн режим, полначот или локалната компонента работи без активна врска со заднинскиот систем. Во таков случај, податоците за сесијата мора да се евидентираат локално, со јасен редослед, временски ознаки и механизам за заштита од подоцнежни измени. По повторно воспоставување на врската, овие записи се синхронизираат со заднинскиот систем и можат да се вклучат во процесот на проверка и закотвување. На тој начин, дури и кога системот работи во офлајн услови, се зачувува можноста за последователна верификација [16].

Разликата меѓу трите режими е прикажана на сликата 5.1.



Слика 5.1: Режим на работа во онлајн, полуонлајн и офлајн сценарија

Како што е прикажано на сликата 5.1, главната разлика меѓу режимите е степенот на зависност од мрежната поврзаност. Во онлајн режим, податоците се испраќаат веднаш. Во полуонлајн режим, дел од податоците може привремено да се задржат локално. Во офлајн режим, локалното евидентирање станува основен услов за подоцнежна синхронизација и проверка.

Споредбата на трите режими е систематизирана во табелата 5.1.

Табела 5. 1: Споредба на онлајн, полуонлајн и офлајн режими на работа

Режим на работа	**Мрежна поврзаност**	**Обработка на податоци**	**Улога на *Proof-of-Charge***
Онлајн режим	Постојана врска со заднинскиот систем.	Податоците се испраќаат и обработуваат во реално време или речиси во реално време.	Потврдата се генерира веднаш по завршување на сесијата и може да се вклучи во групна криптографска потврда.
Полуонлајн режим	Повремена, нестабилна или ограничена поврзаност.	Дел од податоците се зачувуваат локално и периодично се синхронизираат со заднинскиот (*backend)* систем.	Се создаваат привремени криптографски докази за локалните записи, кои подоцна се синхронизираат и проверуваат.
Офлајн режим	Нема активна врска со заднинскиот систем за време на сесијата.	Сесијата се евидентира локално, а податоците се синхронизираат по повторно воспоставување на врската.	Се обезбедува проверливост на локално создадените податоци пред нивната синхронизација со заднинскиот систем.

Како што е прикажано во табелата 5.1, секој режим има различни предности и ограничувања. Онлајн режимот обезбедува најбрза размена на податоци, но е најмногу зависен од комуникациската инфраструктура. Полуонлајн режимот овозможува поголема флексибилност бидејќи може да поднесе краткотрајни прекини. Офлајн режимот е најотпорен на прекини, но бара внимателно локално евидентирање, заштита на записите и контролирана синхронизација по повторно воспоставување на врската.

Во контекст на *Proof-of-Charge*, овие режими се важни затоа што проверливоста не треба да зависи само од постојана комуникација со централниот систем. Дури и кога сесијата се изведува во полуонлајн или офлајн услови, потврдата може локално да се формира и да се поврзе со мерниот тек преку криптографски вредности. На тој начин, по синхронизацијата, системот може да провери дали записите останале непроменети и дали можат да се вклучат во понатамошен процес на закотвување [16].

Оваа поделба на режимите претставува основа за следното потпоглавје, каде што подетално се разгледуваат локалното евидентирање и синхронизацијата на податоците.

5.3 Локално евидентирање и синхронизација на податоците

Локалното евидентирање на податоци претставува еден од клучните механизми за поддршка на полуонлајн и офлајн сценарија во системите за полнење електрични возила. Во услови кога полначот нема постојана врска со заднинскиот (*backend)* систем, податоците што се создаваат во текот на сесијата не можат веднаш да се испратат до операторот. Затоа, потребно е тие привремено да се зачуваат локално, во самиот полнач, во локален контролер или во друг доверлив уред во близина на инфраструктурата за полнење.

Локално евидентираните податоци може да вклучуваат идентификатор на сесијата, идентификатор на полначот, време на почеток и завршување, вредности од мерењето, статуси на сесијата, информации за автентикација и применет тарифен контекст. Овие податоци претставуваат основа за подоцнежна обработка, пресметка на испорачаната енергија и создавање финален запис за полнење. Во онлајн режим, ваквите податоци најчесто се испраќаат до заднинскиот *(backend)* систем преку OCPP во реално време, додека во офлајн и полуонлајн режими тие мора да се зачуваат локално до повторното воспоставување на врската [7], [14].

Главниот предизвик кај локалното евидентирање е обезбедување на интегритетот на податоците пред нивната синхронизација. Ако локално зачуваните вредности можат да се изменат без можност за откривање, заднинскиот систем подоцна нема сигурна основа за проверка дали примените податоци се автентични и конзистентни. Поради тоа, локалното евидентирање треба да биде придружено со криптографски механизми, како хеширање, временско означување, поврзување на записите во секвенца и создавање привремен *Proof-of-Charge* [16], [22], [23].

Во предложениот пристап, секој локален запис се претставува во детерминистички формат и се хешира веднаш по неговото создавање. Така се создава дигитален отпечаток кој подоцна може да се спореди со повторно пресметаната вредност при синхронизација. Доколку записот бил изменет, несовпаѓањето на хеш-вредностите овозможува откривање на неконзистентноста. Дополнително, повеќе локални записи

можат да се поврзат преку Мерклова структура или секвенцијално хеширање, со што се намалува можноста за незабележано додавање, отстранување или преуредување на податоците [17], [24], [30], [31].

Синхронизацијата започнува кога полначот или локалниот контролер повторно ќе воспостави врска со backend системот. Во оваа фаза, локално зачуваните податоци се испраќаат до заднинскиот систем за понатамошна обработка. Заднинскиот систем може повторно да ги пресмета хеш-вредностите, да ја провери структурата на податоците и да утврди дали локално создадените записи се конзистентни со *Proof-of-Charge* потврдата. Доколку проверката е успешна, сесијата може да се вклучи во групна криптографска потврда и подоцна да се закотви во блокчејн или надворешен регистар за интегритет [15], [16], [18].

Процесот на синхронизација треба да биде внимателно организиран за да се избегнат дупликати, загуба на записи или конфликт меѓу локалните и заднински податоците. За таа цел, секоја сесија треба да има единствен идентификатор, а секој локален запис треба да биде временски означен и поврзан со конкретна сесија. Доколку backend системот веќе има делумен запис за истата сесија, потребно е да се изврши споредба и усогласување на податоците. Во случај на несовпаѓање, системот треба да го означи записот како спорен и да овозможи дополнителна ревизија.

Во табелата 5.2. се прикажани главните чекори во процесот на локално евидентирање и синхронизација на податоците во офлајн и полуонлајн сценарија.

Табела 5.2: Чекори за локално евидентирање и синхронизација на податоците

Чекор	**Опис**	**Улога во системот**
Создавање локален запис	Полначот или локалниот контролер ги евидентира основните податоци од сесијата, како идентификатор на сесија, време, статус и вредности од мерењето.	Обезбедува привремена евиденција кога мрежната врска е ограничена или недостапна.
Нормализација на податоците	Податоците се претставуваат во детерминистички формат со дефиниран редослед на полиња, формат на временски ознаки и точност на мерните вредности.	Овозможува повторлива криптографска проверка и избегнува различни хеш-вредности поради различно форматирање.
Хеширање на записите	Секој локален запис се претставува преку хеш-вредност.	Овозможува откривање на промени, бришење или неусогласеност пред синхронизација.
Создавање привремен *Proof-of-Charge*	Се создава локален доказ или привремена потврда за сесијата врз основа на мерните податоци и криптографските вредности.	Го поврзува локалниот запис со подоцнежната верификација во заднинскиот систем.

Синхронизација со заднинскиот (*backend)* системот	Податоците се испраќаат до заднинскиот систем по повторно воспоставување на мрежната врска.	Овозможува финална обработка, усогласување и подготовка на записот за полнење.
Верификација и усогласување	Заднинскиот систем ги проверува хеш-вредностите, структурата на записите и конзистентноста со *Proof-of-Charge* потврдата.	Открива дупликати, промени, нецелосни записи или спорни сесии.
Групирање и закотвување	Валидните потврди се вклучуваат во групна криптографска потврда и се подготвуваат за закотвување.	Обезбедува подоцнежна независна ревизија и проверка на интегритетот.

Постапката за локално евидентирање на офлајн сесија може дополнително да се систематизира преку сликата 5.2, каде што се прикажани чекорите од иницијализација на сесијата до создавање привремена *Proof-of-Charge* потврда и подготовка за подоцнежна синхронизација.

Слика 5.2: Дијаграм на процесот за локално евидентирање на офлајн сесија

Сликата 5.2 покажува дека локалното евидентирање не претставува само привремено складирање на податоци, туку контролиран процес во кој мерните записи се проверуваат, нормализираат и криптографски се поврзуваат со привремена потврда. На тој начин се создава основа за подоцнежна синхронизација и верификација во заднинскиот систем.

Овој пристап овозможува офлајн и полуонлајн сценаријата да се вклучат во редовната системска логика, наместо да се третираат како исклучоци при прекин на мрежната поврзаност. Со комбинирање на локално евидентирање, криптографска заштита и последователна синхронизација, моделот *Proof-of-Charge* обезбедува зачувување на интегритетот на записите и можност за нивна подоцнежна верификација дури и во услови на ограничена или привремено недостапна комуникација со заднинскиот систем.

5.4 Примена на *Proof-of-Charge* во офлајн сценарија

Примената на *Proof-of-Charge* во офлајн сценаријата има цел да обезбеди проверливост на сесиите за полнење електрични возила и во услови кога полначот нема активна врска со заднинскиот систем на операторот. Во такви ситуации, автентикацијата, започнувањето на сесијата, евидентирањето на мерните податоци и подготовката на записот за полнење треба да се извршат локално или со ограничена комуникација. Затоа е потребен механизам што ќе овозможи локално создадените записи да останат конзистентни и проверливи при подоцнежна синхронизација [14], [16].

Во класичен онлајн режим, заднинскиот систем има централна улога во управувањето со сесијата, прибирањето на податоците и подготовката на записот за наплата. Во офлајн режим, дел од оваа улога се пренесува на полначот, локалниот контролер или друг доверлив локален модул. Поради тоа, локалниот систем треба да може да ги евидентира основните податоци од сесијата, да ги зачува мерните вредности и да создаде привремен криптографски доказ што подоцна ќе се користи за верификација.

Proof-of-Charge во офлајн сценарио може да се реализира преку неколку последователни чекори. При започнување на сесијата се создава локален идентификатор, кој ја поврзува сесијата со конкретен полнач, кориснички токен или друг метод на автентикација. Во текот на полнењето, полначот локално ги евидентира мерните вредности и временските ознаки. Овие записи се нормализираат и се претставуваат преку хеш-вредности, со цел да се создаде криптографски отпечаток на локалниот запис [16], [22].

По завршување на сесијата, локалниот систем може да формира привремена *Proof-of-Charge* потврда. Таа може да содржи идентификатор на сесијата, идентификатор на полначот, време на започнување и завршување, агрегирана испорачана енергија, локален тарифен контекст и Мерклова коренска вредност на мерните податоци. Доколку сите потребни информации не се достапни во офлајн моментот, потврдата може да се означи како привремена и да се финализира по синхронизацијата со заднинскиот систем.

Клучната вредност на ваквиот пристап е тоа што локално создадените податоци добиваат криптографска заштита уште пред да бидат испратени кон заднинскиот систем. Ако некој се обиде да ги измени мерните вредности, временските ознаки или агрегираниот износ на енергија пред синхронизацијата, повторната пресметка на хеш-вредностите или Мерклова коренска вредноста ќе покаже несовпаѓање. На тој начин, *Proof-of-Charge* овозможува откривање неовластени промени и во периодот кога системот не е поврзан со централната инфраструктура [17], [24], [31].

При повторно воспоставување на мрежната врска, локално зачуваните податоци и привремената потврда се испраќаат до заднинскиот систем. Тој ја проверува структурата на записот, повторно ги пресметува релевантните хеш-вредности и ја споредува добиената вредност со локално зачуваниот доказ. Доколку проверката е успешна, потврдата може да се финализира, да се вклучи во групна криптографска потврда и подоцна да се закотви на блокчејн или во надворешен регистар за интегритет [15], [16], [18].

Во офлајн сценарија, *Proof-of-Charge* не треба да се разгледува како замена за автентикација, платежни механизми или комуникациски протоколи. Тој претставува дополнителен слој за интегритет и проверливост на податоците што се создаваат локално. Овој слој може да се комбинира со офлајн платежни модели базирани на блокчејн, локална автентикација и подоцнежна синхронизација со заднинскиот систем [14], [16].

Особено значајно е раздвојувањето меѓу оперативното извршување на сесијата и криптографската проверка. Сесијата може да се изврши локално, додека нејзиниот интегритет може да се провери подоцна. Ова е важно за реални услови во кои достапноста на мрежата не може секогаш да се гарантира, но системот сепак треба да обезбеди доверлив запис за испорачаната енергија и финалната наплата.

Процесот на примена на *Proof-of-Charge* во офлајн сценарио може да се претстави преку неколку фази: локално започнување на сесијата, локално евидентирање на мерните податоци, создавање привремен криптографски доказ, чување на потврдата до повторно воспоставување на врската, синхронизација со заднинскиот систем, финална верификација и вклучување во групна криптографска потврда. Овој тек овозможува офлајн сесиите да се третираат како дел од редовниот системски процес, а не како исклучок што не може да се провери.

Табела 5.3: Фази на примена на *Proof-of-Charge* во офлајн сценарија

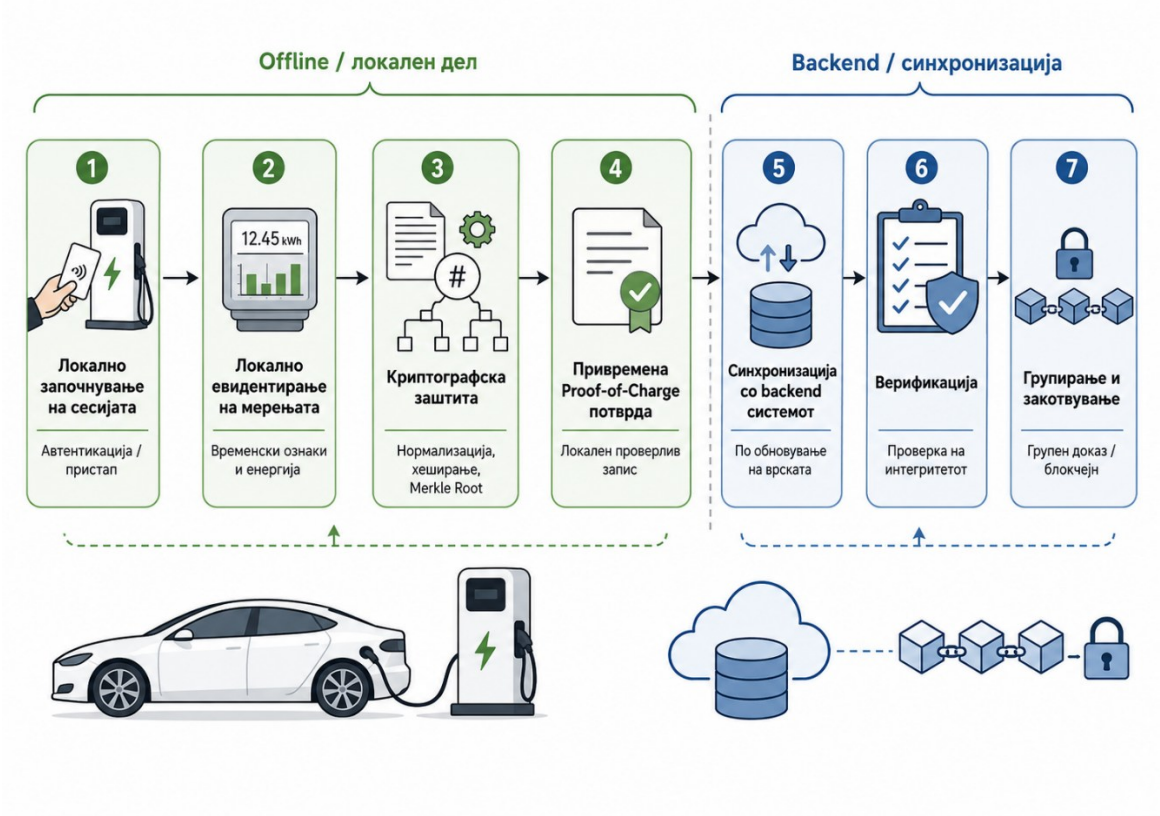
Фаза	**Опис**	**Резултат**
Локално започнување на сесијата	Се создава идентификатор на сесијата и се врши локална автентикација или проверка на пристап.	Сесијата може да започне без активна врска со backend системот.
Локално евидентирање на мерењата	Полначот или локалниот контролер ги зачувува вредностите од мерењето, временските ознаки и основните податоци за сесијата.	Се создава локален запис за текот на сесијата на полнење.
Криптографска заштита на записот	Локалните податоци се нормализираат, хешираат и можат да се поврзат преку Мерклова структура.	Се создава доказ за интегритет на локално создадените податоци.
Привремена потврда за *Proof-of-Charge*	Се создава привремена потврда со агрегирана енергија, временски податоци, ценовен контекст и криптографски доказ.	Сесијата добива проверлив дигитален запис пред синхронизација.
Синхронизација со заднинскиот (*backend*) систем	Податоците и привремената потврда се испраќаат до заднинскиот (*backend)* систем по обновување на мрежната врска.	Заднинскиот систем добива основа за проверка, усогласување и финализација.
Финална верификација	Заднинскиот систем ги проверува хеш-вредностите, Мерклвиот корен *(Merkle Root)* и конзистентноста на потврдата.	Се потврдува дали локално создадените податоци биле изменети или останале конзистентни.
Групирање и закотвување	Валидните потврди се вклучуваат во групна криптографска потврда и се подготвуваат за закотвување.	Сесијата станува дел од проверлива и ревизорски достапна евиденција.

Како што е прикажано во табелата 5.3, процесот започнува со локално започнување на сесијата и евидентирање на мерните податоци, продолжува со создавање привремен криптографски доказ, а завршува со синхронизација, финална верификација и вклучување во групна криптографска потврда. На овој начин, офлајн сесиите стануваат дел од редовниот системски процес, а не исклучок што не може да се провери.

Процесот претставен во табелата 5.3 е прикажан и графички на сликата 5.3. Сликата го визуализира преминот од локално започнување на сесијата, преку

евидентирање на мерните податоци и создавање привремен криптографски доказ, до подоцнежна синхронизација и финализација во заднинскиот систем.

Процесот на примена на *Proof-of-Charge* во офлајн сценарио е прикажан на сликата 5.3.



Слика 5.3: Примена на *Proof-of-Charge* во офлајн сценарио

Како што е прикажано на сликата 5.3, офлајн сесијата не се третира како изолиран или непроверлив настан. Напротив, податоците што се создаваат локално се зачувуваат во структуриран облик и се поврзуваат со криптографски доказ. По повторно воспоставување на врската, тие можат да се синхронизираат со заднинскиот систем и да се вклучат во редовниот процес на проверка и закотвување.

5.5 Интеграција со заднински (*backend*) системи, OCPP и OCPI процеси

Интеграцијата на офлајн и полуонлајн моделите со реални системи за полнење електрични возила бара внимателно усогласување со постојната инфраструктура на операторите. Во практични услови, заднинскиот систем претставува централна компонента која управува со сесиите на полнење, автентикацијата, тарифите, обработката на мерните податоци, наплатата и размената на информации со други учесници во екосистемот. Поради тоа, моделот *Proof-of-Charge* треба да се интегрира како дополнителен слој за проверливост, без да ја наруши основната функционалност на заднинскиот систем и постојните комуникациски процеси [7], [8], [16].

Во онлајн режим, заднинскиот систем ги прима податоците од полначот во реално време и може веднаш да ги обработи за создавање потврда за полнење. Во

полуонлајни офлајн режими, дел од податоците се создаваат и зачувуваат локално, а заднинскиот систем ја презема улогата на точка за синхронизација, верификација и финализација на записите. При повторно воспоставување на мрежната врска, локално зачуваните податоци се испраќаат кон заднинскиот систем, каде што се проверува нивната структура, се пресметуваат хеш-вредностите и се утврдува дали тие се конзистентни со привремената *Proof-of-Charge* потврда [14], [16].

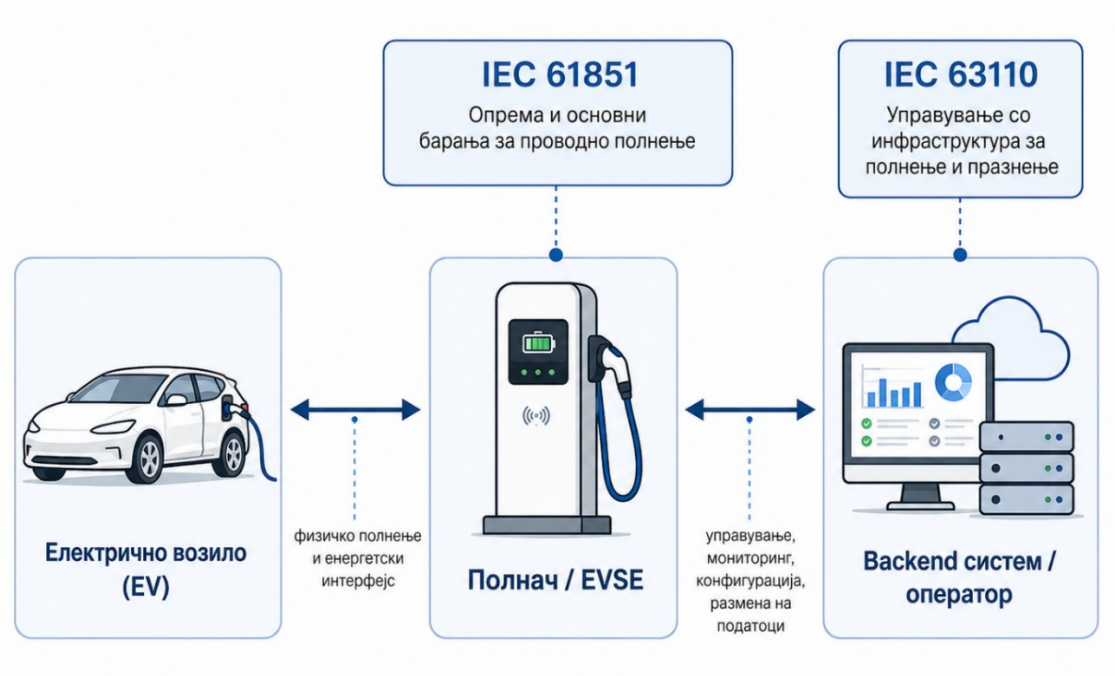
Интеграцијата со OCPP е значајна затоа што овој протокол ја дефинира комуникацијата меѓу полначот и заднинскиот систем на операторот [7]. Во предложениот пристап, OCPP продолжува да ја има својата основна улога во размена на оперативни податоци, како статуси на полначот, почеток и завршување на сесија, вредности од мерењето и други релевантни информации. *Proof-of-Charge* не бара замена на OCPP, туку ги користи податоците што веќе се создаваат во рамките на овој процес за да формира криптографски проверлив запис.

Во практична примена, OCPI CDR записот не мора да ја содржи целосната *Proof-of-Charge* потврда. Доволно е да содржи референца кон потврдата, хеш-вредност на потврдата, идентификатор на групата (*batch)* или референца кон закотвениот групен Мерклов корен (*Merkle Root)*. Со тоа роаминг партнерот добива можност за подоцнежна проверка, без да се наруши приватноста на деталните мерни податоци [16].

Во офлајн и полуонлајн сценарија, одредени OCPP пораки или записи може да бидат испратени со задоцнување, односно по повторното воспоставување на врската. Во такви случаи, заднинскиот систем треба да може да ги прифати локално зачуваните податоци, да ги поврзе со конкретна сесија и да провери дали нивната содржина е конзистентна со криптографските докази создадени локално. Ова е важно затоа што задоцнетата синхронизација не треба автоматски да се третира како невалидна, туку како дел од контролирана офлајн логика.

Покрај OCPP и OCPI, реалната интеграција со инфраструктурата за полнење електрични возила треба да се разгледува и во контекст на поширокиите стандарди за опрема, управување и интероперабилност, како IEC 61851 и IEC 63110 [34], [35].

Поврзаноста меѓу електричното возило, опремата за полнење и заднинскиот систем во контекст на IEC 61851 и IEC 63110 е прикажана на сликата 5.4. IEC 61851 се однесува на основните барања за проводно полнење и физичкиот енергетски интерфејс меѓу електричното возило и полначот, додека IEC 63110 ја опфаќа поширокаата рамка за управување, мониторинг и размена на податоци во инфраструктурата за полнење и празнење електрични возила [34], [35].



Слика 5.4: Улогата на IEC 61851 и IEC 63110 во инфраструктурата за полнење електрични возила

Како што е прикажано на сликата 5.4, предложениот модел се поставува над постојната инфраструктура за полнење. Основните процеси за комуникација, управување со сесии и размена на податоци продолжуваат да се изведуваат преку постојните компоненти, додека *Proof-of-Charge* додава механизам за криптографска проверка. Така, моделот може да се интегрира постепено, без да бара целосно редизајнирање на системот.

Важна предност на ваквата интеграција е тоа што моделот може да работи и во онлајн и во полуонлајн или офлајн сценарија. Во онлајн услови, потврдата може да се создаде веднаш по завршување на сесијата. Во услови на ограничена поврзаност, податоците можат прво да се зачуваат локално, а потоа да се синхронизираат со заднинскиот систем и да се вклучат во процесот на проверка [30], [31].

На овој начин, *Proof-of-Charge* не ја нарушува постојната комуникациска рамка, туку ја надградува со проверлив слој. Таквиот пристап е практично значаен затоа што овозможува операторите да ја задржат постојната инфраструктура, а истовремено да добијат подобра основа за ревизија, интегритет на записите и доверба меѓу различни учесници во системот.

Во табелата 5.4. се прикажани главните компоненти кои учествуваат во интеграцијата на *Proof-of-Charge* со реални заднински системи, OCPP и OCPI процеси.

Табела 5.4: Интеграција со реални системски компоненти

Компонента	**Улога во постојниот систем**	**Улога во *Proof-of-Charge* интеграцијата**
Полнач / *EV*SE	Извршува физичко полнење и создава мерни податоци.	Генерира податоци што се користат за локален или заднински (*backend) Proof-of-Charge* запис.
Локален контролер	Поддржува локална обработка при ограничена или недостапна мрежна поврзаност.	Привремено чува записи, хеш-вредности и локални криптографски докази.
Заднински (*backend*) систем	Управува со сесии, автентикација, тарифи, обработка на податоци и наплата.	Врши синхронизација, верификација и финализација на *Proof-of-Charge* потврдите.
OCPP процеси	Овозможуваат комуникација меѓу полначот и заднинскиот систем.	Обезбедуваат оперативни податоци што се користат за создавање проверлива потврда за полнење.
OCPI процеси	Овозможуваат размена на податоци меѓу оператори и даватели на услуги за електрична мобилност во роаминг сценарија.	Можат да пренесат референца кон потврдата, хеш-вредност или групен криптографски доказ.
***Proof-of-Charge* модул**	Не е дел од класичната инфраструктура за полнење.	Создава, проверува и подготвува криптографски докази за групирање и закотвување.
Блокчејн / регистар за интегритет	Не е задолжителен дел од класичните OCPP/OCPI процеси.	Зачувува минимални криптографски докази за независна проверка.

Како што е прикажано во табелата 5.4, *Proof-of-Charge* може да се постави како дополнителна компонента што ги користи податоците создадени од полначот, заднинскиот систем и комуникациските протоколи. Полначот создава мерни податоци, заднинскиот систем ги обработува и ги поврзува со тарифниот контекст, а компонентата за *Proof-of-Charge* создава криптографски проверлива потврда. Ова овозможува интеграција без потреба од целосна промена на постојната архитектура.

5.6 Практични ограничувања и предизвици при реална имплементација

Иако моделот *Proof-of-Charge* овозможува проверливост и интегритет на записите за полнење електрични возила, неговата реална имплементација во офлајн и полуонлајн сценарија носи одредени практични ограничувања и предизвици. Овие предизвици се поврзани со техничката инфраструктура, доверливоста на мерната опрема, локалното складирање, синхронизацијата, кибербезбедноста, приватноста и усогласувањето со постојните заднински (*backend*), OCPP, OCPI и поширoки стандардизациски процеси.

Првиот предизвик е поврзан со доверливоста на локално создадените податоци. Во офлајн режим, полначот или локалниот контролер ја преземаат улогата на привремен извор на податоци. Доколку локалниот уред е компромитиран, неправилно конфигуриран или физички оштетен, може да се создадат неточни или непотполни записи. *Proof-of-Charge* може да обезбеди доказ дека записите не биле изменети по нивното создавање, но не може самостојно да гарантира дека физичкото мерење било точно ако мерната опрема генерирала погрешни вредности. Поради тоа, моделот треба да се комбинира со доверлива мерна опрема, соодветна конфигурација и безбедносни механизми на ниво на полнач [21], [34].

Вториот предизвик се однесува на локалното складирање. Во полуонлајн и офлајн сценарија, податоците мора привремено да се зачуваат во полначот, локалниот контролер или друг локален систем. Ова бара доволен капацитет за складирање, заштита од бришење или оштетување на податоците и механизми за управување со ситуации кога локалната меморија е исполнета. Ако податоците се изгубат пред синхронизацијата, заднинскиот систем нема да може целосно да ја провери сесијата, дури и ако постојат делумни криптографски докази.

Третиот предизвик е синхронизацијата по повторно воспоставување на врската. Во реални услови, повеќе офлајн сесии може да се акумулираат локално и да се испратат кон backend системот во ист момент. Тоа може да создаде оптоварување, дупликати, конфликти меѓу записи или проблеми со редоследот на обработка. Затоа, потребно е секоја сесија да има единствен идентификатор, јасни временски ознаки и криптографски доказ кој овозможува проверка на конзистентноста при синхронизација [16], [30], [31].

Четвртиот предизвик е поврзан со нормализацијата на податоците. За да може хеширањето и верификацијата да бидат повторливи, податоците мора да се претстават во ист детерминистички формат и во локалниот систем и во заднинскиот систем. Различен формат на временски ознаки, различна точност на енергетските вредности или различен редослед на полињата може да доведе до различни хеш-вредности и до неуспешна верификација. Поради тоа, нормализацијата треба да биде строго дефинирана и имплементирана на сите релевантни компоненти [22], [27].

Петтиот предизвик се однесува на трошоците и доцнењето при закотвување. Доколку секоја офлајн сесија се закотвува поединечно, бројот на записи во блокчејн или во надворешниот регистар за интегритет може значително да се зголеми. Ова може да предизвика повисоки трошоци, подолго време на потврдување и ограничена скалабилност. Затоа, групирањето на потврдите и закотвувањето на групен Мерклов

корен *(Merkle Root)* претставуваат попрактичен пристап за реални инфраструктури со голем број сесии [15], [16], [18].

Шестиот предизвик е приватноста на корисниците. Иако *Proof-of-Charge* не бара објавување на деталните мерни податоци на блокчејн, офлајн и полуонлајн сценаријата може да вклучуваат локално складирање на податоци кои откриваат време, локација, траење на сесијата и навики на користење. Поради тоа, потребно е да се применат мерки за минимизација на податоците, контролирана достапност, енкрипција на локалните записи и ограничување на тоа кои податоци се споделуваат при синхронизација [5], [6], [9].

Седмиот предизвик е интеграцијата со постојните заднински, OCPP и OCPI процеси. Реалните системи за полнење електрични возила често имаат различни имплементации, различни заднински архитектури и различни правила за обработка на сесии. Затоа, модулот *Proof-of-Charge* треба да биде доволно модуларен за да може да се интегрира со постојните процеси без радикални промени во инфраструктурата. Воедно, треба да се дефинира како се обработуваат задоцнети OCPP записи, како се поврзуваат со OCPI записи во роаминг сценарија и како се означуваат спорни или неусогласени сесии [7], [8], [16].

Осмиот предизвик се однесува на усогласувањето со пошироките стандарди за инфраструктурата за полнење електрични возила. Покрај OCPP и OCPI, реалната имплементација треба да се разгледува и во контекст на стандардите што ги дефинираат барањата за опрема, управување и интероперабилност. IEC 61851 е значаен за основните барања за проводно полнење и опремата за полнење, додека IEC 63110 се однесува на управување со инфраструктура за полнење и празнење, употребни случаи и архитектури [34], [35]. Овие стандарди не ја заменуваат потребата од *Proof-of-Charge*, но ја дефинираат техничката и управувачката околина во која таквиот модел треба да се интегрира.

Деветтиот предизвик е поврзан со кибербезбедноста на поширокиот систем. Бидејќи инфраструктурата за полнење електрични возила е дел од *smart grid* екосистемот, безбедносните ризици треба да се разгледуваат не само на ниво на полнач, туку и на ниво на заднински систем, локални контролери, комуникациски канали и интеракција со енергетската мрежа [36]. Дополнително, управувањето со ваквите ризици може да се разгледува и преку поширок рамки за управување со кибербезбедносен ризик, како NIST Cybersecurity Framework 2.0, како и преку пристапи засновани на континуирана проверка, ограничена доверба и контролиран пристап меѓу компонентите [37], [38].

Истражувањата за кибербезбедност и приватност во инфраструктурата за полнење електрични возила покажуваат дека ризиците не се ограничени само на комуникациските протоколи. Тие ги опфаќаат и корисничките податоци, заднинските (*backend)* системи, локалните уреди, платежните процеси и интеракцијата со енергетската мрежа [39]. Во овој контекст, *Proof-of-Charge* треба да се разгледува како еден дел од поширока безбедносна архитектура, кој обезбедува проверливост на записите, но треба да биде придружен со други организациски, технички и регулаторни мерки.

Една од предностите на моделот *Proof-of-Charge* е можноста за постепена имплементација. Бидејќи моделот функционира како дополнителен слој над постојните заднински, OCPP и OCPI процеси, операторите можат најпрво да го применат за внатрешна проверка, а подоцна да го прошират кон роаминг партнери, регулаторни проверки или надворешно закотвување. Ваквиот пристап ја намалува потребата од радикални промени во постојната инфраструктура [16].

Табела 5.5: Практични предизвици и можни механизми за нивно надминување

Предизвик	Опис	Можен механизам
Доверливост на локалните податоци	Локалниот уред може да биде компромитиран, неправилно конфигуриран или физички оштетен.	Сертифицирана мерна опрема, локална заштита и криптографска проверка на записите.
Локално складирање	Податоците може да се изгубат, избришат или локалната меморија може да нема доволен капацитет.	Заштитено локално складирање, резервни записи, управување со меморија и контролирано бришење.
Синхронизација	При повторно воспоставување на врската може да се појават дупликати, конфликти или доцнење при пренос.	Единствени идентификатори на сесии, временски ознаки и проверка на конзистентност при синхронизација.
Нормализација на податоците	Различно форматирање на истите податоци може да доведе до различни хеш-вредности.	Детерминистички формат и заеднички правила за претставување на податоците во локалниот и заднинскиот (*backend)* систем.
Трошоци за закотвување	Поединечно закотвување на сите потврди може да биде скапо и неефикасно.	Групирање на потврдите и закотвување на групен Мерклов корен (*Merkle Root)*.
Приватност на корисниците	Локалните записи може да содржат чувствителни информации за времето, локацијата, траењето и навиките на користење.	Минимизација на податоци, енкрипција, контролирана достапност и ограничено споделување при синхронизација.
Интеграција со постојните системи	Различни заднински (*backend*), OCPP и OCPI имплементации може да создадат технички ограничувања.	Модуларен сервис на *Proof-of-Charge*, јасно дефинирани интерфејси и поддршка за задоцнети записи.
Усогласување со стандардите	Реалната имплементација треба да се усогласи со	Разгледување на IEC 61851, IEC 63110 и релевантни

	поширок стандарди за опрема, управување и интероперабилност.	насоки за *smart grid* кибербезбедност.
Кибербезбедносен ризик	Нападите може да влијаат врз полначите, заднинските (*backend)* системи, локалните уреди, комуникациските канали и корисничките податоци.	Примена на рамки за управување со ризик, *Zero Trust* принципи, континуирана проверка и контролирана доверба меѓу компонентите.

Како што е прикажано во табелата 5.5, предизвиците не се однесуваат само на криптографијата или блокчејн закотвувањето. Тие ги опфаќаат и комуникациските услови, локалното складирање, синхронизацијата, приватноста, трошоците, интероперабилноста и управувањето со податоците. Затоа, предложениот модел треба да се воведува постепено и со јасно дефинирани правила за секоја фаза од процесот.

Постепениот пристап за имплементација на моделот *Proof-of-Charge* е прикажан на сликата 5.4.

Слика 5.5: Постепениот пристап за имплементација на моделот *Proof-of-Charge*

Како што е прикажано на сликата 5.5, имплементацијата може да започне со локално создавање потврди и хеш-вредности, без веднаш да се користи блокчејн закотвување. Во следна фаза, потврдите можат да се групираат преку групни коренски (*batch root)* вредности, а потоа овие вредности да се закотвуваат на блокчејн или во надворешен регистар за интегритет. Ваквиот постепен пристап овозможува системот да се тестира, да се приспособи и да се прошири без нагла промена на постојната инфраструктура [16], [18], [30].

Посебно внимание треба да се посвети и на приватноста. Иако моделот не бара деталните мерни податоци да се запишуваат на блокчејн, тие сепак остануваат чувствителни во заднинскиот или локалниот систем. Затоа, потребни се политики за пристап, складирање, задржување и бришење на податоците. *Proof-of-Charge* може да обезбеди доказ за интегритет, но не ги заменува сите мерки за безбедност, автентикација и заштита на личните податоци [6], [9], [31], [39].

Во целина, реалната имплементација на *Proof-of-Charge* бара рамнотежа меѓу техничката изводливост, трошоците, приватноста и интероперабилноста. Моделот е најпрактичен кога се применува како дополнителен слој над постојните системи, а не како целосна замена за нив. Со внимателна интеграција, тој може да придонесе за подобра ревизија, поголема доверба во записите и посигурно управување со податоците од сесиите за полнење.

5.7 Заклучок на поглавјето

Во ова поглавје беше разгледана примената на моделот *Proof-of-Charge* во услови на различна мрежна поврзаност. Во поглавјето беа поврзани прашањата за онлајн, полуонлајн и офлајн работа, локално евидентирање, синхронизација, интеграција со постојни системи и практични ограничувања при реална имплементација [7], [8], [14], [16].

Главниот заклучок е дека проверливоста на сесиите за полнење не треба да зависи само од постојаната комуникација со заднинскиот систем. Во полуонлајн и офлајн услови, податоците можат локално да се евидентираат, да се поврзат со хеш--вредности и Мерклови структури, а потоа да се синхронизираат и проверат по повторното воспоставување на врската [16], [17], [22], [24].

На овој начин, офлајн сесиите не се третираат како исклучок надвор од редовниот системски процес. Тие можат да добијат привремена *Proof-of-Charge* потврда, која подоцна се верификува, финализира и вклучува во групна криптографска потврда [14], [16].

Интеграцијата со заднински системи, *OCPP* и *OCPI* процесите покажува дека предложениот модел не ја заменува постојната инфраструктура, туку ја надградува со дополнителен слој за проверливост. Тој може да обезбеди криптографска референца кон потврдата, хеш-вредноста или групниот доказ, без да ја наруши основната логика на комуникациските процеси [7], [8], [15], [16].

За реална примена, значајни се и пошироките стандарди и безбедносни насоки. IEC 61851 и IEC 63110 ја дефинираат техничката и управувачката рамка на инфраструктурата за полнење, додека насоките за кибербезбедност на паметните мрежи ја поставуваат оваа инфраструктура во поширок *smart grid* контекст [34]–[36]. Дополнително, рамките за управување со кибербезбедносен ризик и пристапите засновани на континуирана проверка се важни за практична и безбедна имплементација [37], [38].

Практичните ограничувања што беа разгледани во ова поглавје се однесуваат на доверливоста на мерната опрема, локалното складирање, синхронизацијата, нормализацијата на податоците, трошоците за закотвување, приватноста и кибербезбедносните ризици. Овие предизвици покажуваат дека *Proof-of-Charge* треба да се воведува постепено, како дополнителен слој над постојните системи, а не како нивна замена [21], [30], [31], [39].

Со ова, поглавјето ја проширува применливоста на моделот *Proof-of-Charge* од стандардни онлајн услови кон пореални сценарија со ограничена или нестабилна

поврзаност. Следното поглавје ја продолжува анализата преку подетално разгледување на блокчејн технологијата, *on-chain* и *off-chain* моделите, паметните договори (*smart contracts)* и нивната поврзаност со предложениот пристап.

6. УЛОГАТА НА БЛОКЧЕЈН ТЕХНОЛОГИЈАТА ВО ОБЕЗБЕДУВАЊЕ ПРОВЕРЛИВОСТ, ИНТЕГРИТЕТ И ПРИВАТНОСТ ВО СИСТЕМИТЕ ЗА ПОЛНЕЊЕ ЕЛЕКТРИЧНИ

6.1 Вовед во улогата на блокчејн технологијата

Блокчејн технологијата претставува значаен пристап во развојот на современи дистрибуирани системи во кои се бара интегритет на податоците, трајност на записите и можност за независна проверка. Нејзината основна логика се заснова на криптографски поврзана евиденција, во која секој нов запис е поврзан со претходните записи. На тој начин се создава последователна структура во која неовластената промена на претходно зачуван запис може да се открие преку нарушување на криптографската врска [42].

Првично, блокчејн беше претставен преку биткоин (*Bitcoin)* како механизам за децентрализирана електронска готовина без потреба од централна финансиска институција [10]. Подоцна, со развојот на Етериум (*Ethereum)* и концептот на паметен договор (*smart contracts)*, неговата примена се прошири од трансфер на дигитална вредност кон извршување децентрализирани апликации и автоматизирани правила запишани во програмски код [40], [41]. Овој развој овозможи блокчејн да се разгледува не само како финансиска технологија, туку и како поширок механизам за доверба, автоматизација и ревизија.

Во споредба со класичните централизирани бази на податоци, каде што довербата најчесто се поставува во еден заднински систем или во една организација, блокчејн овозможува заедничка евиденција што може да биде проверена од повеќе учесници. Ова е особено важно во системи со повеќе независни страни, различни административни домени и потреба да се докаже дека одреден запис постоел во конкретен временски момент и не бил изменет подоцна [42], [43].

Во инфраструктурата за полнење електрични возила, ваквата потреба е посебно изразена. Податоците за една сесија можат да поминуваат низ повеќе компоненти: полнач, локален контролер, заднински систем на операторот, роаминг платформа, давател на услуги за електрична мобилност и системи за наплата. Во овој процес може да се појават грешки, доцнења, неусогласености или спорови околу испорачаната енергија, применетата тарифа или конечниот запис за наплата. Затоа, блокчејн може да се користи како дополнителен механизам за интегритет и независна проверка на критичните записи [44], [45].

Сепак, тоа не значи дека сите податоци од полнењето треба директно да се зачувуваат на блокчејн. Таквиот пристап би бил непрактичен поради трошоци, ограничена пропусност, јавна видливост на податоците и можни ризици за приватноста. Поради тоа, посоодветен е хибриден пристап: деталните оперативни податоци остануваат *off-chain*, додека на блокчејн или во надворешен регистар за интегритет се

закотвуваат само минимални криптографски докази, како хеш-вредности или Мерклов корен (*Merkle Root)* [43], [44].

Во оваа дисертација, блокчејн технологијата се разгледува во таа насока. Предложениот модел *Proof-of-Charge* ги задржува деталните мерни податоци и целосните потврди за полнење надвор од блокчејн, додека на блокчејн или во надворешен регистар се закотвува групен криптографски доказ. Така може подоцна да се провери дали конкретна потврда припаѓала на одредена група записи и дали таа група постоела во даден временски период.

Во рамките на предложениот модел, блокчејн не ја заменува постојната инфраструктура за полнење. Оперативните процеси, комуникацијата со полначите и размената преку OCPP и OCPI остануваат дел од постојните заднински системи. Блокчејн се додава како ревизорски и криптографски проверлив слој, чија улога е да обезбеди доказ за постоење и непроменетост на група потврди, без да ја наруши основната логика на системот.

6.2 Основни карактеристики на блокчејн системите

Блокчејн системите се разликуваат од класичните централизирани информациски системи по начинот на кој ги организираат, зачувуваат и проверуваат податоците. Наместо една централна база на податоци што е целосно контролирана од еден субјект, блокчејн користи дистрибуирана евиденција во која повеќе јазли можат да учествуваат во одржување на заедничката состојба на системот. Ова е особено важно во средини со повеќе учесници, каде што довербата не треба да зависи само од една организација [42], [43].

Првата важна карактеристика е дистрибуираноста. Записите не се чуваат само на едно место, туку се реплицираат или споделуваат меѓу повеќе јазли во мрежата. Во зависност од типот на мрежата, тие јазли можат да бидат јавни и отворени за секој учесник, или ограничени само на однапред одобрени организации. Со ова се намалува зависноста од една точка на отказ и се создава основа за заедничка проверка на состојбата на системот.

Втора карактеристика е криптографското поврзување на записите. Секој блок содржи хеш-вредност од претходниот блок, со што се формира синџир на меѓусебно поврзани блокови. Ако се измени претходен запис, се менува и неговата хеш-вредност, а со тоа се нарушува врската со следните блокови. На тој начин, неовластените промени не мора секогаш да бидат физички невозможни, но стануваат откривливи преку криптографска проверка [42].

Трета карактеристика е природата на евиденцијата *append-only*. Во типичен блокчејн систем, новите записи се додаваат последователно, додека претходните записи не се бришат или заменуваат како во класична база на податоци. Ова создава историска трага на настани, која може подоцна да се користи за ревизија и анализа. Во системите за полнење електрични возила, ваквиот принцип е значаен затоа што овозможува да се докаже дека одреден криптографски доказ бил создаден и закотвен во конкретен временски период.

Четврта карактеристика е транспарентноста и проверливоста. Во зависност од архитектурата на блокчејн мрежата, учесниците можат да ја проверат валидноста на записите, состојбата на синџирот и криптографските врски меѓу блоковите. Ова не значи дека сите податоци треба да бидат јавно достапни. Напротив, во хибридни модели може да се објавуваат само минимални криптографски докази, додека деталните податоци остануваат *off-chain*. Така се постигнува рамнотежа меѓу проверливост и приватност [43], [44].

Петта карактеристика е консензусот, односно механизмот преку кој учесниците во мрежата се согласуваат за валидната состојба на евиденцијата. Во јавни блокчејн мрежи, консензусот е потребен за координација меѓу голем број независни и потенцијално недоверливи учесници. Во приватни или конзорциумски (*consortium)* мрежи, тој може да биде поедноставен, бидејќи учесниците се однапред познати и имаат дефинирани улоги. За предложениот модел *Proof-of-Charge* не е неопходно сите детали од системот за полнење да се обработуваат преку сложен консензус. Доволно е блокчејн или надворешниот регистар да обезбеди доверлив запис за закотвениот групен криптографски доказ.

Шеста карактеристика е независната ревизибилност. Бидејќи блокчејн записите се криптографски поврзани и временски подредени, тие можат да се користат како основа за подоцнежна проверка од трета страна. Во контекст на полнење електрични возила, ова е значајно при роаминг спорови, регулаторна проверка или несогласување околу наплата. Наместо ревизорот целосно да се потпира на интерната база на податоци на операторот, тој може да ја провери врската меѓу потврдата за полнење, нејзината хеш-вредност, групниот Мерклов корен *(Merkle Root)* и закотвениот доказ.

Основните карактеристики на блокчејн системите се прикажани на сликата 6.1.

Слика 6.1: Основни карактеристики на блокчејн системите

Како што е прикажано на сликата 6.1, блокчејн системите ја комбинираат дистрибуираната евиденција, криптографското поврзување на записите, *append-only* логиката, транспарентноста, консензусот и независната ревизибилност. Токму овие карактеристики ја прават блокчејн технологијата соодветна како слој за интегритет и проверливост во системите за полнење електрични возила.

6.3 Криптографски механизми во блокчејн системите

Криптографските механизми се основа врз која блокчејн системите обезбедуваат интегритет, проверливост и отпорност на неовластени промени. Иако блокчејн често се поврзува со дистрибуираност и консензус, неговата доверливост во голема мера произлегува од начинот на кој податоците се хешираат, поврзуваат и проверуваат. Во оваа група механизми спаѓаат криптографските хеш-функции, дигиталните потписи, Мерклови структури, временското означување и криптографските *commitments* [23], [42].

Првиот значаен механизам се криптографските хеш-функции. Тие земаат влезен податок со произволна должина и создаваат излез со фиксна должина, односно хеш-вредност. Кај добрите криптографски хеш-функции, дури и мала промена во влезниот податок создава целосно различна вредност. Во блокчејн системите, тие се користат за поврзување на блоковите, за идентификација на трансакции и за создавање компактни докази за интегритет. Во контекст на *Proof-of-Charge*, хеш-функциите се користат за пресметување вредности на мерните записи, потврдите за полнење и групните структури за закотвување [16], [22], [46].

Вториот механизам се Мерклови структури, односно Мерклово дрво (*Merkle tree)*. Оваа структура овозможува голем број записи да се претстават преку еден заеднички криптографски корен, познат како Мерклов корен (*Merkle Root)*. Секој поединечен запис прво се хешира како лист во дрвото, а потоа хеш-вредностите се комбинираат по парови сè додека не се добие еден корен. Предноста на овој пристап е тоа што може да се докаже дека одреден запис е дел од поголемо множество без да се откриваат сите останати записи. Ова е особено важно за системите што бараат проверливост, но истовремено треба да ја зачуваат приватноста на деталните податоци [7], [16], [48].

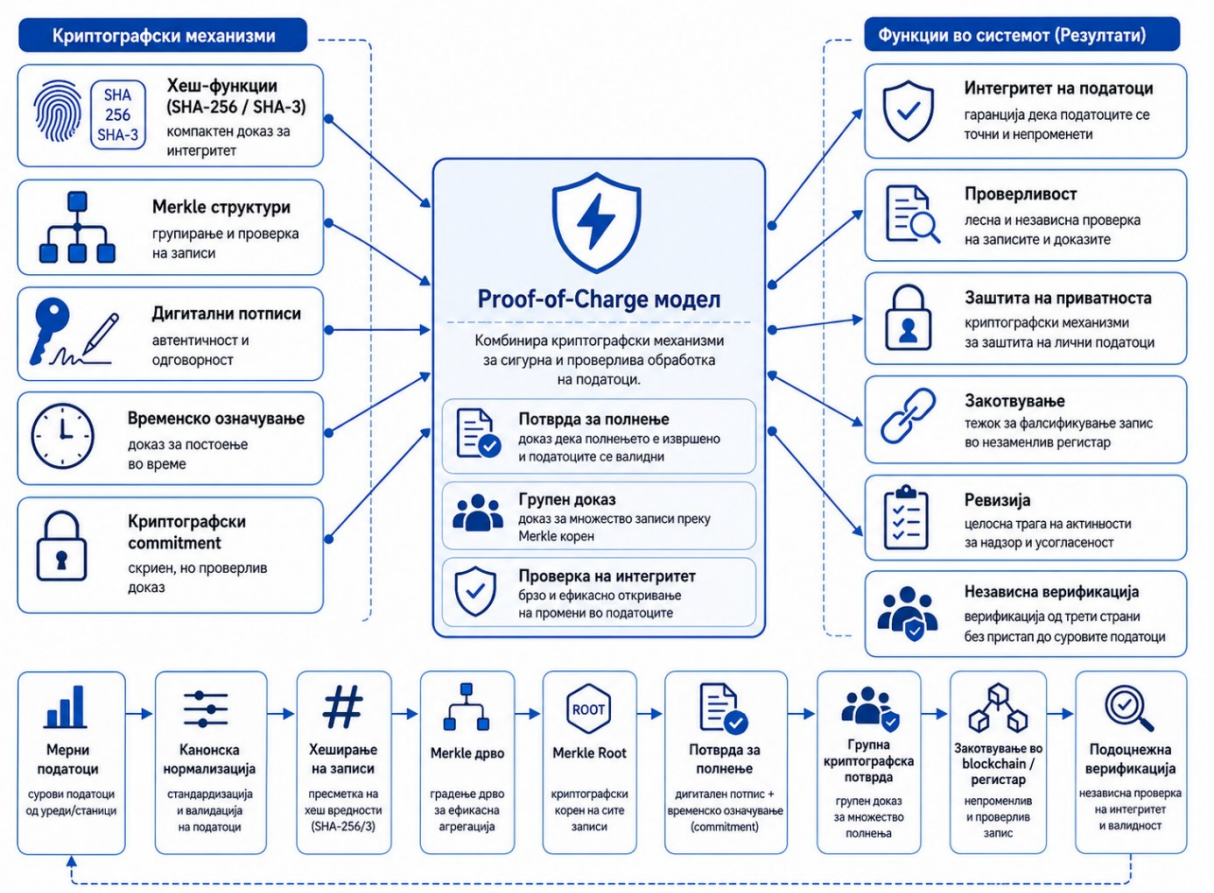
Третиот механизам се дигиталните потписи. Тие овозможуваат потврда на идентитетот на субјектот што креирал, одобрил или испратил одреден запис, како и заштита од негирање на извршено дејство. Во блокчејн системите, дигиталните потписи најчесто се користат за авторизација на трансакции, за поврзување на одредена активност со конкретен криптографски идентитет и за поддршка на проверлива одговорност меѓу учесниците. Во системите за полнење електрични возила, тие можат да се користат за потврдување на улогата на оператор, заднински систем, ревизор или друг доверлив учесник во процесот на закотвување и проверка [47], [49].

Четвртиот механизам е временското означување. Блокчејн записите се додаваат последователно, при што секој блок или запис може да се поврзе со одреден временски период. Ова не значи дека блокчејн секогаш обезбедува апсолутно прецизно време, но овозможува да се докаже дека одреден криптографски доказ постоел пред или во рамките на одреден момент во евиденцијата. За *Proof-of-Charge*, ова е значајно бидејќи

групниот Мерклов корен (*Merkle Root)* може да се закотви во одреден временски интервал, со што се создава доказ дека групата потврди постоела пред подоцнежна ревизија или спор [23].

Петтиот механизам е криптографскиот *commitment*. Тој претставува криптографска вредност што се однесува на одредена содржина, без таа содржина целосно да се открие. Подоцна, доколку е потребно, содржината може повторно да се пресмета и да се спореди со *commitment* вредноста. Во моделот *Proof-of-Charge*, хеш-вредноста на потврдата и групниот Мерклов корен имаат улога на *commitment*: тие не ги откриваат деталните мерни податоци, но овозможуваат проверка дали потврдата и групата записи останале непроменети [50].

Криптографските механизми и нивната улога во предложениот модел се прикажани на сликата 6.2.



Слика 6.2: Криптографски механизми во блокчејн системите и нивната улога во моделот Proof-of-Charge

Како што е прикажано на сликата 6.2, предложениот модел не се потпира на блокчејн за складирање на целосните податоци од сесиите. Наместо тоа, ги користи криптографските својства на хеширање, Мерклови структури, дигитални потписи, временско означување и закотвување за да создаде проверлив доказ за интегритет. Деталните податоци остануваат во заднинскиот систем или во контролирано *off-chain* складиште, додека блокчејн или надворешниот регистар обезбедува минимален, но независно проверлив доказ за постоење и непроменетост на групата потврди.

6.4 On-chain и off-chain модели за складирање и проверливост

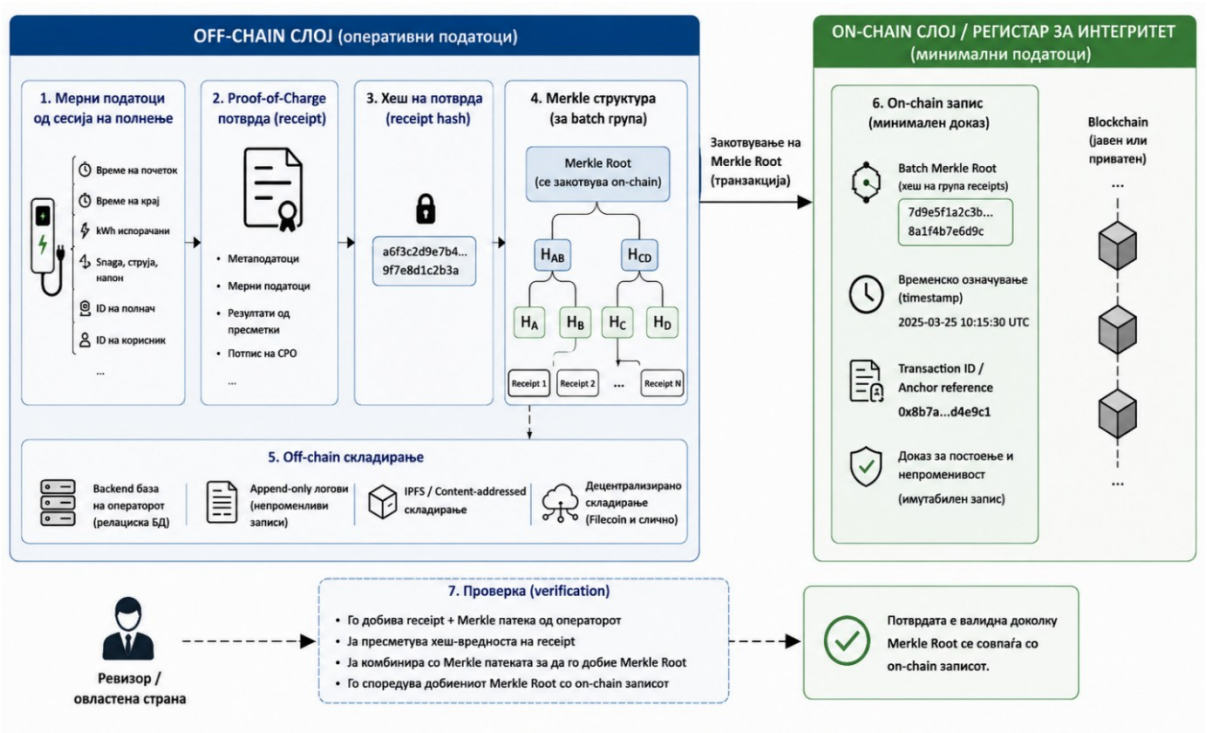
Една од најважните архитектурни одлуки при примена на блокчејн технологија во системи за полнење електрични возила е изборот кои податоци треба да се зачуваат *on-chain*, а кои треба да останат *off-chain*. Ова прашање е значајно затоа што податоците од сесиите за полнење можат да бидат обемни, чувствителни и поврзани со корисничко однесување, локација, време на користење и навики на движење. Доколку сите мерни податоци, потврди и наплатни записи би се зачувувале директно на блокчејн, системот би се соочил со високи трошоци, ограничена скалабилност и ризици за приватноста [43], [44], [55].

Моделот *on-chain* подразбира дека податоците или нивните релевантни записи се зачувуваат директно во блокчејн мрежата. Предноста на ваквиот пристап е транспарентноста и можноста записите да се проверат од овластени или јавни учесници, во зависност од типот на мрежата. Сепак, овој модел е ограничен кога станува збор за големи количини податоци, чести записи или информации што не треба да бидат јавно достапни. Во контекст на полнење електрични возила, деталните временски серии од мерењето, податоците за локацијата, идентификаторите на корисниците и наплатните детали не се погодни за директно *on-chain* складирање.

Моделот *off-chain*, од друга страна, подразбира дека деталните оперативни податоци се чуваат надвор од блокчејн, најчесто во заднинскиот систем на операторот, во контролирано складиште или во децентрализирани системи за складирање. Во овој случај, блокчејн не се користи како примарна база на податоци, туку како слој за интегритет. Наместо целосните податоци, *on-chain* се зачувуваат само криптографски докази, како хеш-вредности, Мерклов корен (*Merkle Root)*, идентификатор на група (*batch)* или референца кон надворешен доказ [51]–[54].

Хибридниот *on-chain/off-chain* пристап претставува најсоодветно решение за системи што треба да обезбедат проверливост, но без непотребно зголемување на трошоците и без јавно изложување на чувствителни податоци. Во ваков модел, податоците потребни за оперативна обработка, пресметка на енергија, наплата и евентуална ревизија остануваат *off-chain*. Од друга страна, блокчејн или надворешниот регистар за интегритет зачувува минимален криптографски доказ што подоцна може да се искористи за проверка дали одреден запис или група записи постоеле во даден временски период и дали биле изменети по нивното создавање.

Хибридниот модел на складирање и проверливост е прикажан на сликата 6.3.



Слика 6.3: *On-chain* и *off-chain* модели за складирање и проверливост

Како што е прикажано на сликата 6.3, *off-chain* слојот ја задржува целосната содржина на потврдите и мерните податоци, додека *on-chain* слојот обезбедува независно проверлива референца преку групен Мерклов корен (*batch Merkle Root)*. На овој начин се постигнува рамнотежа меѓу приватноста, скалабилноста и ревизибилноста.

Во предложениот модел *Proof-of-Charge*, овој хибриден пристап има централна улога. Деталните мерни податоци, целосната потврда за полнење и придружните метаподатоци (*metadata)* се чуваат *off-chain*, под контрола на операторот или во доверливо складиште. За секоја потврда се пресметува хеш-вредност, а повеќе потврди се групираат во Мерклова структура. На блокчејн или во надворешен регистар се закотвува само групниот Мерклов корен *(Merkle Root)*, кој претставува компактен доказ за интегритет на целата група потврди. Така се постигнува проверливост без јавно објавување на деталните податоци од сесиите [16].

Споредбата меѓу *on-chain*, *off-chain* и хибридниот пристап е прикажана во табелата 6.1.

Табела 6. 1: On-chain и off-chain модели

Критериум	***On-chain* модел**	***Off-chain* модел**	**Хибриден пристап во *Proof-of-Charge***
Локација на податоците	Податоците или записите се зачувуваат	Деталните податоци се зачувуваат надвор од блокчејн, во заднински (*backend*)	Деталните мерни податоци и потврдите остануваат off-chain,

	директно на блокчејн.	систем или надворешно складиште.	а on-chain се закотвува само групен доказ.
Тип на зачувани информации	Трансакции, хеш-вредности, метаподатоци или други записи достапни во блокчејн мрежата.	Мерни податоци, потврди за полнење, Мерклови патеки, метаподатоци и оперативни записи.	На блокчејн се зачувува *batch Merkle Root*, *timestamp* и референца кон доказот.
Приватност	Може да биде ограничена ако се објавуваат премногу детали.	Поголема контрола врз пристапот до чувствителни податоци.	Се зачувува приватноста бидејќи не се објавуваат детални податоци од сесијата.
Скалабилност	Ограничена при голем број записи и чести трансакции.	Поголема флексибилност за складирање на големи количини податоци.	Повеќе потврди се групираат во група (*batch)*, а се закотвува само еден Мерклов корен.
Трошоци	Може да бидат високи поради *on-chain* трансакции и складирање.	Пониски трошоци за оперативно складирање, но потребни се механизми за заштита и достапност.	Се намалуваат трошоците преку минимален *on-chain* запис.
Проверливост	Записите можат директно да се проверат преку блокчејн.	Проверливоста зависи од хеш-вредности, Мерклови патеки и зачувани метаподатоци.	Потврдата се проверува преку *receipt hash*, Мерклова патека и закотвениот *batch Merkle Root*.
Ризици	Висока јавна изложеност, трошоци и ограничена пропусност.	Ризик од губење, недостапност или измена на off-chain податоците.	Ризиците се намалуваат преку криптографско закотвување и контролирано складирање.
Применливост во *EB*-полнење	Погоден само за минимални докази, не за целосни мерни податоци.	Погоден за детални податоци од сесии, наплата и ревизија.	Најсоодветен пристап за моделот *Proof-of-Charge*.

Како што се гледа од табелата 6.1, хибридниот пристап овозможува да се искористат предностите на блокчејн технологијата без непотребно оптоварување на мрежата со детални оперативни податоци. На тој начин се постигнува рамнотежа меѓу приватноста, трошоците, скалабилноста и независната проверливост на *Proof-of-Charge* потврдите.

Дополнителна предност на *off-chain* складирањето е можноста за контрола на пристапот до чувствителните податоци. Операторот може да ги зачува деталните записи во заднинскиот систем, додека ревизорот, роаминг партнерот или регулаторот може да добие само оние податоци што се потребни за конкретна проверка. Доколку треба да се провери една потврда, не мора да се открива целата база на сесии; доволно е да се обезбедат конкретната потврда, нејзината хеш-вредност, соодветната Мерклова патека и закотвениот групен Мерклов корен.

Во практични имплементации, *off-chain* складирањето може да се реализира преку класични заднински бази на податоци, *append-only* логови, децентрализирани системи за складирање или *content-addressed* механизми. *Content-addressed* пристапот, како кај *IPFS* и слични системи, овозможува содржината да се идентификува преку криптографска адреса поврзана со нејзиниот хеш (*hash)*. Ова може да биде корисно во сценарија каде што потврдите или придружните записи треба да бидат достапни за повеќе учесници, но без нивно директно запишување на блокчејн [51]–[54].

Сепак, *off-chain* моделите носат и одредени предизвици. Ако податоците се чуваат надвор од блокчејн, потребни се механизми за нивна достапност, резервно складирање, контрола на пристап, заштита од бришење и усогласеност со политиките за приватност. Блокчејн може да докаже дека одредена хеш-вредност или Мерклов корен биле закотвени, но не може самостојно да гарантира дека *off-chain* податоците ќе бидат секогаш достапни или дека операторот ќе ги зачува во целост. Затоа, хибридните модели треба да се комбинираат со организациски правила, технички механизми за складирање и јасни процедури за ревизија.

Од аспект на скалабилност, хибридниот модел значително го намалува бројот на *on-chain* записи. Наместо секоја сесија за полнење да создава посебна блокчејн трансакција, повеќе потврди можат да се агрегираат во група *(batch)*, а на блокчејн да се запише само еден групен Мерклов корен. Ова ја намалува големината на *on-chain* податоците, ги ограничува трошоците и овозможува моделот да биде применлив во инфраструктури со голем број дневни сесии [55].

Затоа, во контекст на проверливи системи за полнење електрични возила, *on-chain* и *off-chain* моделите не треба да се разгледуваат како спротивставени пристапи, туку како комплементарни слоеви. *Off-chain* слојот обезбедува простор за детални, приватни и оперативни податоци, додека *on-chain* слојот обезбедува минимален, траен и независно проверлив доказ за интегритет. Ваквата поделба е основа на моделот *Proof-of-Charge*, бидејќи овозможува приватност, скалабилност и ревизибилност да се постигнат истовремено.

6.5 Паметни договори (smart contracts) и надворешни регистри за интегритет

Паметните договори (smart contracts) претставуваат програмски дефинирани правила што се извршуваат во блокчејн околина. Тие овозможуваат одредени услови, трансакции или записи да се обработат автоматски, според логиката што однапред е запишана во код. Со развојот на Етериумот (*Ethereum)*, паметните договори (*smart contracts)* станаа основа за децентрализирани апликации, но нивната примена постепено

се прошири и кон системи во кои се бара проверливост, автоматизација и транспарентна обработка на критични записи [40], [41].

Покрај јавните блокчејн мрежи, во вакви сценарија можат да се користат и *permissioned* блокчејн системи, каде што учесниците се однапред познати и имаат дефинирани улоги. Овој пристап е релевантен за инфраструктури во кои учествуваат оператори на полначи, даватели на услуги за електрична мобилност, роаминг платформи, регулатори и ревизори. *Permissioned* системите, како *Hyperledger Fabric*, овозможуваат поголема контрола врз пристапот, управување со идентитети, дефинирање канали за комуникација и прилагодување на механизмите за консензус според потребите на организациската мрежа [56].

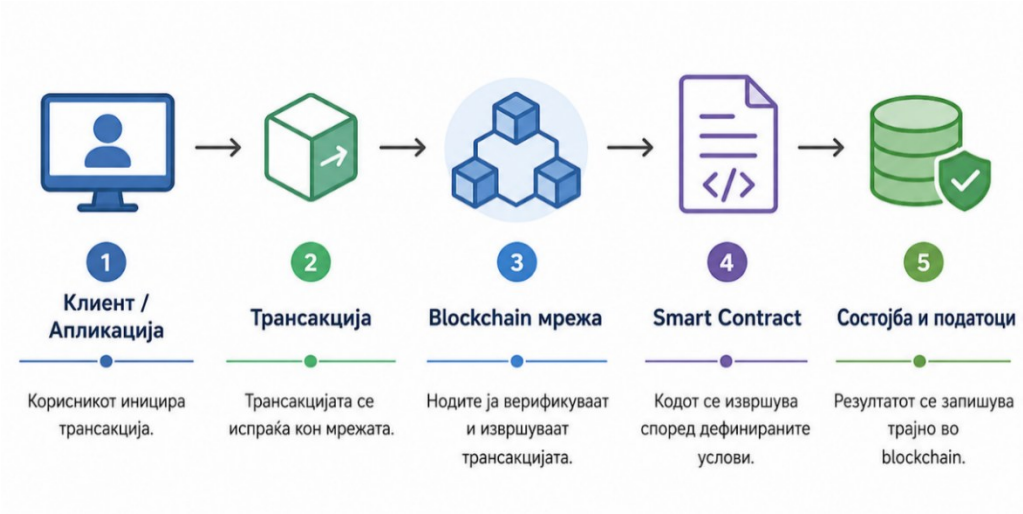
Сепак, паметните договори не треба да се разгледуваат како место каде што се пренесува целата логика на системот. Кодот што се извршува *on-chain* треба внимателно да се дизајнира, бидејќи грешките во договорната логика можат да доведат до неправилно евидентирање, погрешна авторизација или безбедносни пропусти. Дополнително, во јавни блокчејн мрежи секоја операција може да има трансакциски трошок, а објавувањето на премногу метаподатоци може да создаде ризици за приватноста. Поради тоа, во моделот *Proof-of-Charge* паметниот договор се користи ограничено: за закотвување на неопходните криптографски докази, додека деталните податоци и деловната логика остануваат *off-chain* [57], [58].

Начинот на функционирање на паметниот договор е прикажан на сликата 6.4.

Слика 6.4: Како функционира паметниот договор

Како што е прикажано на сликата 6.4, паметниот договор *(smart contract)* се активира кога се исполнети однапред дефинираните услови. По иницирање на трансакцијата, правилата запишани во договорот се извршуваат, се проверуваат влезните параметри и се генерира резултат што се евидентира во блокчејн системот. На тој начин се добива автоматизирана и проверлива обработка на однапред дефинирани правила.

Типичната архитектура на паметниот договорсистем е прикажана на сликата 6.5.



Слика 6.5: Типична архитектура на паметниот договор

Како што е прикажано на сликата 6.5, ваквиот систем обично се состои од корисник или апликација, трансакциски интерфејс, блокчејн мрежа, *smart contract* логика и состојба на договорот. Корисникот или надворешната апликација иницира трансакција, која потоа се обработува според дефинираните правила. Доколку условите се исполнети, состојбата се ажурира и се враќа соодветен резултат. Ова овозможува договорната логика да се извршува автоматизирано и проверливо, без централен посредник.

Покрај финансиските системи, паметните договори можат да се применат и во други области каде што е потребна условно извршлива логика. Дел од овие области се прикажани на сликата 6.6.

Слика 6.6: Примена на паметните договори во различни домени

Сликата 6.6 покажува дека паметните договори не се ограничени само на финансиски трансакции. Тие можат да се користат во договорни процеси, синџири на снабдување, управување со идентитети, јавни услуги и *IoT* системи. Во контекст на полнење електрични возила, оваа логика може да се искористи за евидентирање докази, проверка на услови, поддршка на роаминг процеси и создавање записи што подоцна можат да се ревидираат.

Слика 6.7: Клучни карактеристики на паметните договори

Како што е прикажано на сликата 6.7, паметните договори можат да обезбедат транспарентност, неизменливост, автоматизација и проверливост. Овие карактеристики се корисни само ако договорната логика е јасно дефинирана, безбедносно проверена и ограничена на функции што навистина треба да се извршуваат *on-chain*. Затоа, во моделот *Proof-of-Charge* паметниот договор има помошна улога: тој го поддржува закотвувањето и проверката, но не ја заменува заднинската обработка.

Во системите за полнење електрични возила, паметните договори можат да помогнат при евидентирање криптографски докази, управување со пристап, автоматизирано порамнување, проверка на услови за наплата и поддршка на роаминг процеси. Во предложениот модел *Proof-of-Charge*, сепак, нивната улога е потесно дефинирана. Наместо да ја обработуваат целата сесија или да зачувуваат детални мерни податоци, тие можат да запишат минимални криптографски докази, како групен Мерклов корен (*batch Merkle Root)*, временска ознака, идентификатор на група и референца кон надворешен или *off-chain* запис.

Безбедното користење на паметниот договор бара внимателно дефинирање на договорната логика, тестирање на гранични случаи и избегнување сложени функции што не мора да се извршуваат *on-chain*. Истражувањата покажуваат дека грешките во кодот на паметниот договор можат да доведат до финансиски загуби, неправилно извршување или неочекувано однесување на системот. Поради тоа, се препорачува

постепен развој, формална анализа и ограничување на договорната логика само на неопходните функции [59], [60].

Ова ограничување е важно и од аспект на практична применливост. Колку повеќе деловна логика се префрла *on-chain*, толку поголема е потребата од формална проверка, тестирање и безбедносна анализа на договорниот код. Во моделот *Proof-of-Charge*, паметниот договор не ја пресметува испорачаната енергија, не ја обработува цената и не ја заменува заднинската логика. Неговата функција е да обезбеди проверлив и временски поврзан запис за криптографскиот доказ, додека пресметките, наплатните правила и деталната обработка остануваат во контролираниот заднински систем [61], [62].

Главните функции што паметните договори можат да ги имаат во проверливи системи за полнење електрични возила се систематизирани во табелата 6.2.

Табела 6.2: Функции на паметните договори *во проверливи системи за полнење електрични возила*

Функција	**Опис**	**Применливост во *Proof-of-Charge***
Закотвување на доказ	Запишување на групен Мерклов корен (*batch Merkle Root)* или друг криптографски доказ.	Да, ова е примарната улога.
Временско означување	Поврзување на доказот со конкретен временски момент или блок.	Да, корисно за ревизија.
Идентификација на група (batch)	Поврзување на повеќе потврди со еден групен доказ.	Да, преку batch ID.
Референца кон off-chain запис	Чување минимална врска кон надворешен запис или складиште.	Да, но без откривање на детални податоци.
Автоматизирана наплата	Извршување на наплатна логика директно *on-chain*.	Ограничено, не е примарна улога.
Целосна обработка на сесија	Обработка на мерења, тарифи и целосна сесија во паметен договор (*smart contract)*.	Не се препорачува.

Како што е прикажано во табелата 6.2, паметниот договор во моделот *Proof-of-Charge* има најголема вредност кога се користи за минимални и проверливи функции: закотвување на доказ, временско означување, идентификација на група (*batch)* и референца кон *off-chain* запис. Целосната обработка на сесијата, пресметката на цената и деталната наплата треба да останат дел од заднинскиот систем, бидејќи нивното префрлање *on-chain* би ја зголемило комплексноста, трошоците и безбедносниот ризик.

Надворешен регистар за интегритет е поширок концепт што не мора секогаш да биде јавен блокчејн. Тој може да биде *permissioned* блокчејн, *consortium ledger*, *append-only log*, *notarization service* или друг систем што овозможува независна проверка на закотвените криптографски докази. За *Proof-of-Charge* е важно регистарот да обезбеди трајност на записот, временска поврзаност и можност трета страна подоцна да провери дали одреден *batch Merkle Root* бил закотвен во даден момент. Така регистарот функционира како доверлив слој за проверка, без да ги презема оперативните функции на заднинскиот систем.

Во практична поставеност, заднинскиот систем може периодично да формира група (*batch)* од *Proof-of-Charge* потврди, да го пресмета групниот Мерклов корен и да испрати минимален запис до паметниот договор (*smart contract)* или друг надворешен регистар. Таму се зачувуваат само потребните елементи: идентификаторот на групата, Мерклов корен, временската ознака и идентитетот на субјектот што го извршил закотвувањето. При подоцнежна ревизија, локално пресметаната вредност може да се спореди со вредноста зачувана во регистарот.

Во оваа дисертација, паметниот договор (*smart contracts*) и надворешните регистри за интегритет се разгледуваат како можни механизми за закотвување на доказите, т.е. *Proof-of-Charge*. Нивната улога не е да ја заменат постојната инфраструктура за полнење електрични возила, туку да обезбедат доверлив и проверлив запис за групните криптографски докази. Со ваков пристап, системот ја задржува флексибилноста на заднинските процеси, ја ограничува количината на *on-chain* податоци и создава основа за независна ревизија, роаминг проверка и регулаторен надзор.

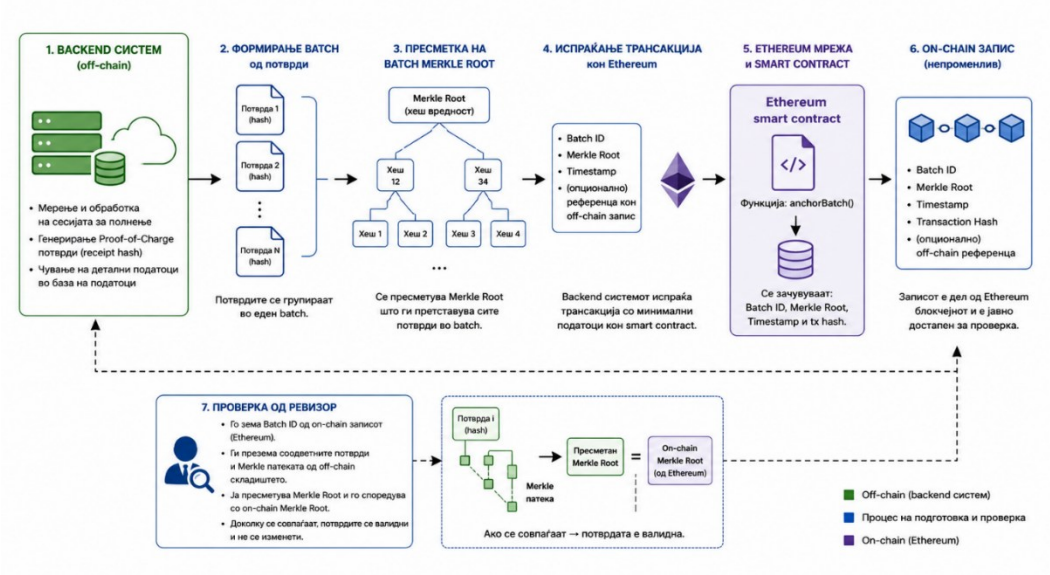
6.6 Етериумот (Ethereum) како платформа за паметни договори (smart contracts)

Етериум *(Ethereum)* претставува една од најзначајните блокчејн платформи за развој и извршување на паметни договори (*smart contracts)* и децентрализирани апликации. За разлика од биткоинот (*Bitcoin)*, кој првично беше дизајниран како систем за децентрализиран пренос на дигитална вредност, Етериумот овозможи блокчејн да се користи како програмска платформа на која може да се дефинираат автоматизирани правила, состојби и трансакциска логика [40], [41].

Основата на Етериумот се состои во тоа што паметните договори се извршуваат во рамките на Етериум виртуелната машина (*Ethereum Virtual Machine)*, односно *EVM*. *EVM* претставува извршна околина во која договорната логика се обработува на детерминистички начин, така што сите јазли што ја верификуваат трансакцијата можат да дојдат до ист резултат. Овој модел овозможува паметните договори да имаат сопствена состојба, да примаат повици преку трансакции и да ажурираат податоци според однапред дефинирани правила [66].

Во контекст на предложениот модел *Proof-of-Charge*, Етериумот може да се користи како можен надворешен слој за закотвување на групни криптографски докази. Наместо паметните договори да ја обработуваат целата сесија на полнење или да зачувуваат детални мерни податоци, неговата улога може да биде ограничена на запишување на групен Мерклов корен (*batch Merkle Root)*, идентификатор на групата, временска ознака и евентуална референца кон *off-chain* запис. На овој начин, Етериумот се користи како регистар за интегритет, додека оперативните податоци и деловната логика остануваат во заднинскиот систем.

Примената на Етериумот како надворешен слој за закотвување на *Proof-of-Charge* е прикажана на сликата 6.8.



Слика 6.8: Етериумот како слој за закотвување на *Proof-of-Charge*

Како што е прикажано на сликата 6.8, паметниот договор на Етериум (*Ethereum smart contract)* не ја обработува целата сесија на полнење. Тој зачувува минимален криптографски доказ што подоцна може да се искористи за независна проверка. Деталните податоци остануваат *off-chain*, додека Етериумот обезбедува проверлив запис за *batch Merkle Root*.

Ваквата примена е погодна за сценарија во кои е потребна независна проверка од ревизор, роаминг партнер или регулатор. Доколку одредена *Proof-of-Charge* потврда треба да се провери подоцна, нејзината хеш-вредност и Мерклова патека можат да се споредат со групниот Мерклов корен (*batch Merkle Root)* запишан преку паметен договор. Со тоа се докажува дека потврдата била дел од конкретна група записи во определен временски период, без да се откриваат сите податоци од сесијата.

Еден од практичните аспекти при користење на Етериум, е трошокот за извршување трансакции, односно *gas*. Секоја операција што се извршува во паметниот договор на Етериумот, има одреден пресметковен трошок, кој се изразува преку *gas*. Поради тоа, сложените паметни договори или честото запишување податоци можат да доведат до повисоки трошоци. Во моделот *Proof-of-Charge*, ова дополнително ја оправдува одлуката *on-chain* да се зачувува само минимален криптографски доказ, наместо детални мерни вредности или целосни потврди [67], [68].

Во табелата 6.3 се прикажани главните компоненти на Етериумот и нивната улога во предложениот модел *Proof-of-Charge*.

Табела 6. 3: Улогата на компонентите на Етериумот во моделот Proof-of-Charge

Компонента	Улога во Етериум (*Ethereum)*	Улога во *Proof-of-Charge*
Ethereum smart contract	Извршува програмски дефинирана логика и зачувува состојба.	Зачувува групен Мерклов корен (*batch Merkle Root)*, *batch ID* и временска ознака.
***EV*M**	Обезбедува детерминистичко извршување на кодот на паметниот договор *(smart contract)*.	Овозможува проверливо извршување на логиката за закотвување.
Трансакција	Активира функција на smart contract и создава *on-chain* запис.	Се користи за запишување на групниот криптографски доказ.
Gas	Го претставува трошокот за извршување на операции.	Го мотивира минималниот *on-chain* запис наместо целосни податоци.
***Transaction* hash**	Референца кон извршената блокчејн трансакција.	Служи како доказ дека *batch Merkle Root* бил закотвен.
Off-chain backend	Не е дел од Етериумот, но комуницира со паметниот договор.	Ги чува деталните потврди, мерните податоци и Мерклови патеките.

Табелата 6.3 покажува дека Етериумот во предложениот модел има ограничена, но значајна функција. Тој обезбедува *on-chain* доказ за интегритет, додека целосната обработка на сесијата за полнење останува во заднинскиот систем.

Од аспект на скалабилност, Етериумот не треба да се користи како база за масовно складирање на сите записи од полнењето. Јавните блокчејн мрежи имаат ограничена пропусност, трансакциски трошоци и специфична динамика на потврдување. Затоа, поефикасен пристап е повеќе потврди да се групираат *off-chain* во Мерклovата структура, а на Етериумот да се запише само еден групен Мерклов корен. Така се намалува бројот на трансакции, се ограничува количината на *on-chain* податоци и се задржува можноста за подоцнежна проверка.

Дополнително, Етериумот помина низ значајна промена со преминот од *proof-of-work* кон *proof-of-stake* консензус. Ова е важно за дискусијата за блокчејн во енергетски и системи за полнење електрични возила, бидејќи ја намалува енергетската потрошувачка на мрежата и го прави Етериумот поприфатлив како инфраструктурна опција за апликации поврзани со одржливост, проверливост и дигитална енергетска трансформација [69].

Сепак, користењето на Етериумот во моделот *Proof-of-Charge* треба да се разгледува како една од можните имплементациски опции, а не како единствено решение. Во зависност од барањата за приватност, трошоци, контрола на пристап и регулаторна усогласеност, истиот концепт може да се реализира и преку други јавни блокчејн мрежи, *Layer-2* решенија, *permissioned* блокчејн системи или надворешни регистри за интегритет. Клучната идеја не е конкретната мрежа, туку принципот: *off-chain* чување на деталните податоци и *on-chain* закотвување на минимален, независно проверлив криптографски доказ.

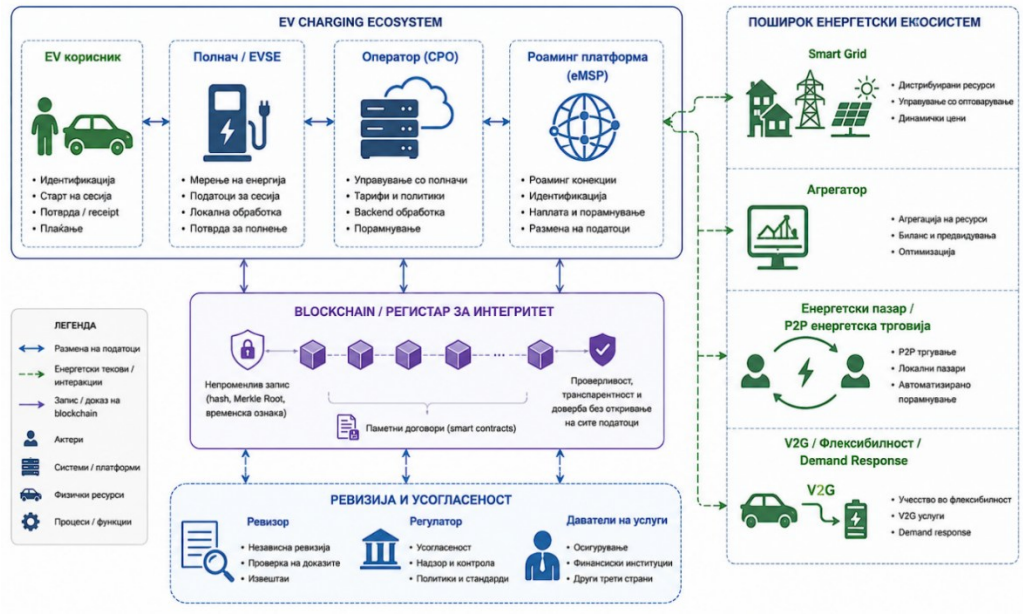
Во рамките на оваа дисертација, Етериумот се разгледува како пример за платформа што овозможува практична реализација на паметни договори за закотвување на *Proof-of-Charge*. Неговата улога е да покаже како блокчејн може да се користи како слој за интегритет, без да ја преземе целосната обработка на процесот на полнење. Со ваков пристап, моделот *Proof-of-Charge* ја задржува флексибилноста на заднинските системи, ја намалува количината на *on-chain* податоци и обезбедува основа за независна криптографска проверка.

6.7 Блокчејн во системите за полнење електрични возила и енергетски системи

Примената на блокчејн технологијата во системите за полнење електрични возила и во пошироките енергетски системи произлегува од потребата за доверлива размена на податоци, проверливи трансакции и координација меѓу повеќе независни учесници. Инфраструктурата за полнење не вклучува само полнач и корисник, туку и оператори на полначи, даватели на услуги за електрична мобилност, роаминг платформи, енергетски компании, агрегатори, регулатори и ревизори. Во таков екосистем, податоците за сесиите, испорачаната енергија, тарифите, плаќањата и порамнувањето често поминуваат низ повеќе системи, што создава потреба од дополнителни механизми за интегритет, проверливост и доверба.

Во литературата, блокчејн се разгледува како технологија што може да поддржи *peer-to-peer energy trading*, автоматизирани плаќања и доверлива размена на податоци во сценарија за полнење електрични возила [70], [74]. Овие пристапи покажуваат дека блокчејн може да обезбеди заеднички слој за доверба меѓу корисници, станици за полнење, енергетски учесници и посреднички платформи, особено кога трансакциите се извршуваат меѓу страни што не припаѓаат на ист заднински систем.

Поврзаноста меѓу блокчејн технологијата, инфраструктурата за полнење електрични возила и поширокиот енергетски екосистем е прикажана на сликата 6.9.



Слика 6.9: Улогата на блокчејн во ЕВ-полнење и енергетски системи

Како што е прикажано на сликата 6.9, блокчејн може да има улога на заеднички проверлив слој меѓу различни учесници во енергетскиот и електромобилниот екосистем. Неговата вредност не е само во евидентирањето трансакции, туку и во можноста критичните записи да се поврзат со временски означен и криптографски проверлив доказ.

Една од важните примени е поврзана со поарамнување и плаќање на сесиите за полнење. Во класични системи, податоците за испорачаната енергија, цената и конечната наплата најчесто се обработуваат во заднинскиот систем на операторот или преку роаминг посредници. Блокчејн може да обезбеди дополнителна проверлива референца, преку која критичните податоци или нивните криптографски докази се поврзуваат со запис што подоцна може да се провери. На тој начин се намалува можноста за спор околу тоа дали одредена сесија била правилно евидентирана, обработена или поарамнета.

Во поширок енергетски контекст, блокчејн се користи и како основа за *peer-to-peer* енергетска трговија, каде што корисниците, производителите и потрошувачите можат директно да разменуваат енергија или поврзани услуги. Овој пристап е значаен за идни сценарија за полнење електрични возила, бидејќи возилата може да се разгледуваат не само како потрошувачи, туку и како флексибилни енергетски ресурси. Во такви услови, блокчејн може да поддржи транспарентна евиденција на трансакции, автоматизирано поарамнување и проверливост на учеството во локални енергетски пазари [76].

Посебно значајна насока е концептот *Vehicle-to-Grid*, односно *V2G*, каде што електричното возило не се разгледува само како потрошувач на енергија, туку и како ресурс што може да враќа енергија кон мрежата или да учествува во услуги за балансирање, флексибилност и управување со оптоварувањето. Во такви сценарија, потребата за проверливост станува уште поизразена, бидејќи треба да се евидентира не само количината на потрошена енергија при полнење, туку и евентуално испорачаната енергија назад кон мрежата, времетраењето на учеството, условите на договорот и

начинот на порамнување. Блокчејн може да обезбеди проверлив слој за ваквите интеракции, додека деталните мерни податоци и оперативната логика остануваат *off-chain*. Во оваа насока, моделот *Proof-of-Charge* може понатаму да се прошири кон концепти како *proof-of-flexibility* или *proof-of-discharge*, каде што криптографските докази би се користеле за потврдување на учество во *V2G* или *demand response* услуги [77].

Блокчејн технологијата се разгледува и во системите *smart grid*, каде што голем број дистрибуирани уреди, корисници, производители, складишта на енергија и агрегатори треба да разменуваат податоци и да учествуваат во координирани процеси. Во вакви системи, дистрибуираната евиденција може да обезбеди поголема транспарентност, отпорност и проверливост на интеракциите, особено кога станува збор за *transactive energy*, *demand response* и управување со дистрибуирани енергетски ресурси [71]–[73], [77].

Од аспект на електромобилноста, важна е и врската меѓу блокчејн, *smart metering* и системите за полнење. Податоците од мерењето се основа за пресметка на испорачаната енергија, наплата, порамнување и потенцијална ревизија. Кога овие податоци се пренесуваат меѓу повеќе системи, потребни се механизми што овозможуваат проверка на нивниот интегритет без секогаш да се открива целосната содржина. Во оваа насока, блокчејн може да се комбинира со *off-chain* складирање, хеширање и Мерклови структури за да се обезбеди проверливост на мерните записи и поврзаните потврди [75].

Блокчејн може да има улога и во роаминг сценарија. Кога корисникот полни возило на полнач што припаѓа на друг оператор или друга мрежа, податоците за сесијата треба да бидат разменети меѓу повеќе страни. Во такви случаи, заедничкиот криптографски доказ или закотвениот запис може да помогне при решавање спорови околу испорачаната енергија, времетраењето на сесијата, ценовниот контекст или валидноста на потврдата. Ова е особено важно кога различни заднински системи треба да се усогласат без целосна меѓусебна доверба.

Главните области на примена се систематизирани во табелата 6.4.

Табела 6.4: Примени на блокчејн технологија во системи за полнење електрични возила и енергетски системи

Област на примена	**Улога на блокчејн**	**Поврзаност со *Proof-of-Charge***
Плаќања за *EB*-полнење	Проверлива евиденција за трансакции и порамнување.	Потврдата за полнење може да служи како криптографски доказ за сесијата.
Роаминг процеси	Заеднички доказ меѓу различни оператори и платформи.	*Receipt hash* или *batch Merkle Root* може да се користи при спор.
Паметно мерење *(Smart metering-*	Интегритет на мерните записи и проверливост на податоците.	Мерните податоци се поврзуваат со Мерклов корен (*Merkle Root)*.

P2P energy trading	Транспарентна евиденција и автоматизирано порамнување.	Записите за ЕВ-полнење можат да бидат дел од локален енергетски пазар.
Demand response / V2G	Овозможува проверка на учество во флексибилност, враќање енергија кон мрежата и енергетски услуги.	*Proof-of-Charge* може да се прошири кон *proof-of-flexibility* или *proof-of-discharge* за проверка на двонасочни енергетски интеракции.
Регулаторна ревизија	Независна проверка на критични записи.	Закотвениот групен доказ овозможува ревизија без откривање на сите податоци.

Како што е прикажано во табелата 6.4, блокчејн може да поддржи повеќе процеси: плаќања, роаминг, *smart metering*, *peer-to-peer* енергетска трговија, *demand response*, *V2G* и регулаторна ревизија. Поврзаноста со *Proof-of-Charge* се гледа во тоа што потврдата, нејзината хеш-вредност или групниот Мерклов корен можат да послужат како криптографски доказ за конкретна сесија или група записи.

Сепак, примената на блокчејн во овие системи треба да се разгледува внимателно. Не сите процеси имаат потреба од *on-chain* извршување, а директното запишување детални податоци на блокчејн може да создаде проблеми со трошоци, приватност, скалабилност и регулаторна усогласеност. Поради тоа, практичните модели најчесто се потпираат на хибридна архитектура: деталните податоци остануваат *off-chain*, додека блокчејн се користи за закотвување на минимални криптографски докази.

Во оваа дисертација, моделот *Proof-of-Charge* ја користи блокчејн технологијата во оваа поширока насока, но со ограничена и практична улога. Наместо блокчејн да ја обработува целата сесија за полнење, тој се користи како слој за закотвување на групни криптографски докази. На тој начин се обезбедува интегритет, ревизибилност и проверливост на критичните записи, додека деталните мерни податоци, корисничките информации и деловната логика остануваат *off-chain*.

6.8 Поврзаност на блокчејн со предложениот модел Proof-of-Charge

Поврзаноста меѓу блокчејн технологијата и предложениот модел *Proof-of-Charge* произлегува од потребата записите за полнење да бидат проверливи, отпорни на подоцнежни измени и погодни за ревизија. Во претходните потпоглавја беа разгледани основните својства на блокчејн системите, криптографските механизми, *on-chain/off-chain* пристапите, *smart contracts*, *Ethereum* и примената на блокчејн во системи за полнење електрични возила и енергетски системи. Во ова потпоглавје тие концепти се поврзуваат со конкретната улога што блокчејн ја има во предложениот модел.

Во *Proof-of-Charge*, блокчејн не се користи како примарно складиште за мерните податоци, ниту како систем што ја обработува целата сесија за полнење. Неговата улога е поограничена, но суштинска: да обезбеди надворешен криптографски доказ за интегритет. Деталните мерни вредности, потврдите за полнење, ценовниот контекст и придружните метаподатоци (*metadata)* остануваат *off-chain*, додека *on-chain* или во

надворешен регистар се зачувува групен Мерклов корен, поврзан со идентификатор на групата, временска ознака и референца кон доказот [16], [51]–[55].

Овој пристап е во согласност со принципот блокчејн да се користи за она што најдобро го обезбедува: траен, проверлив и тешко изменлив запис за критични криптографски вредности. Доколку сите податоци од сесијата би се зачувувале *on-chain*, системот би станал поскап, помалку скалабилен и потенцијално проблематичен од аспект на приватност. Затоа, *Proof-of-Charge* користи хибридна архитектура во која *off-chain* слојот ја задржува деталната оперативна содржина, а блокчејн обезбедува надворешно проверлив доказ за нејзиниот интегритет [43], [44], [55].

Клучната врска меѓу *Proof-of-Charge* и блокчејн се создава преку криптографското поврзување на потврдите. За секоја потврда се пресметува *хеш*-вредност, а повеќе потврди се групираат во Мерклова структура. Добиениот групен Мерклов корен претставува компактна вредност што ја претставува целата група потврди. Доколку подоцна треба да се провери конкретна потврда, доволно е да се обезбедат самата потврда, нејзината хеш-вредност, Мерклова патека и закотвениот групен Мерклов корен [16], [22], [48].

Ваквиот пристап е близок до поширокитe концепти за *transparency overlays* и *key transparency*, каде што проверливоста се додава како дополнителен слој над постојни системи, без тие целосно да се заменат [78], [79]. Слична логика се применува и кај *tamper-evident logs*, каде што записите се организираат така што подоцнежните измени можат да се откријат преку криптографски врски и контролирана историја на промени [80]. Овие идеи се значајни и за *Proof-of-Charge*, бидејќи потврдата за полнење не се проверува изолирано, туку преку нејзината врска со групниот доказ.

Во контекст на блокчејн, механизмите за *audit trail* дополнително ја користат неизменливоста на дистрибуираниот регистар за да обезбедат доверлива трага на настани [81]. Поновите пристапи за *transparency logs* и *verifiable data structures* ја нагласуваат важноста на својствата *append-only*, ефикасните Мерклови докази и независната проверка на логовите [82]–[84]. Овие принципи се надоврзуваат на потребата системот да може да покаже не само дека одреден запис постои, туку и дека тој бил дел од конкретна група записи во определен временски период.

Закотвувањето на групниот Мерклов корен (*batch Merkle Root)* во блокчејн или во надворешен регистар им овозможува на потврдите за полнење да добијат временски поврзан и независно проверлив доказ. Така заднинскиот систем не останува единствениот извор на доверба. Доколку операторот, роаминг партнерот, ревизорот или регулаторот сака да провери одредена потврда, може повторно да ја пресмета хеш-вредноста, да ја провери Мерклovата патека и да ја спореди со вредноста закотвена во блокчејн. На овој начин се обезбедува посилна основа за ревизија и за решавање спорови меѓу различни учесници [23], [56], [85].

Паметните договори можат дополнително да ја систематизираат оваа постапка. Нивната улога во моделот *Proof-of-Charge* не е да ја пресметуваат испорачаната енергија, да ја обработуваат тарифата или да ја заменат заднинската логика. Наместо тоа, паметниот договор може да функционира како минимален регистар за интегритет, во кој се запишуваат *batch ID*, *Merkle Root*, временска ознака и референца кон *off-chain* запис.

Со тоа се создава проверлив *on-chain* запис, додека деталната обработка останува во заднинскиот систем [61], [62].

Во системите за полнење електрични возила и во енергетски системи, ваквата архитектура има практична вредност затоа што овозможува доверба меѓу повеќе учесници. Полначот, операторот, *eMSP* платформата, роаминг посредникот, регулаторот и ревизорот не мора целосно да се потпираат на една интерна база на податоци. Наместо тоа, тие можат да користат заеднички криптографски доказ за проверка на интегритетот на записите. Ова е особено важно во роаминг, *P2P energy trading*, *demand response* и *V2G* сценарија, каде што податоците за енергија, време, тарифа и порамнување можат да имаат финансиско и регулаторно значење [70]–[77].

Од аспект на приватност, предложениот модел го ограничува количеството на податоци што се објавуваат во блокчејн. Наместо кориснички идентификатори, локации, временски серии или наплатни детали, се објавува само криптографски доказ што сам по себе не ја открива целата содржина на сесијата. Ова е важно бидејќи податоците од полнењето можат индиректно да откријат информации за движење, навики на користење и временски модели на корисникот. Затоа, *Proof-of-Charge* го комбинира принципот на проверливост со минимизација на јавно достапните податоци [43], [44], [57].

Поврзаноста со блокчејн е значајна и од аспект на ревизија. Во класичен заднински систем, ревизорот најчесто мора да верува дека операторот ја доставил точната верзија на записите. Кај *Proof-of-Charge*, ревизорот може самостојно да провери дали доставената потврда одговара на претходно закотвениот групен доказ. Ова не ја елиминира потребата од доверливи мерни уреди, правилни тарифни правила и безбедна заднинска инфраструктура, но обезбедува дополнителен криптографски механизам за откривање на *post-hoc* измени.

Процесот на проверка може да се опише преку неколку поврзани чекори. Прво, се зема конкретната *Proof-of-Charge* потврда и се пресметува нејзината *hash*-вредност врз основа на канонска претстава на податоците. Второ, оваа вредност се споредува со вредноста што се користи како лист во Мерклова структура. Трето, преку Мерклovата патека се пресметува групниот Мерклов корен. Четврто, добиениот корен се споредува со вредноста што претходно била закотвена во блокчејн или во надворешен регистар. Доколку сите вредности се совпаѓаат, може да се заклучи дека потврдата припаѓа на конкретната група записи и дека не била изменета по моментот на закотвување [16], [22], [48], [82]–[84].

Позиционирањето на блокчејн технологијата како надворешен слој за доверба, интегритет и проверливост во моделот *Proof-of-Charge* е прикажано на сликата 6.10.

Слика 6.10: Блокчејн како слој за доверба и проверливост во моделот *Proof-of-Charge*

Како што е прикажано на сликата 6.10, *Proof-of-Charge* не ја префрла целата логика на полнењето на блокчејн, туку користи повеќеслоен пристап. Оперативните податоци остануваат *off-chain*, криптографските докази се формираат преку хеширање, Мерклови патеки, групен Мерклов корен и дигитални потписи, додека блокчејн се користи како независен слој за закотвување. На овој начин различни учесници, како корисникот, операторот, роаминг партнерот, ревизорот и регулаторот, можат да ја проверат валидноста на потврдите без директен пристап до сите детални податоци.

Во табелата 6.5, е прикажана споредба меѓу централизирано заднинско складирање, целосно *on-chain* складирање, класични *audit logs* и предложениот хибриден *Proof-of-Charge* пристап.

Табела 6.5: Споредба на пристапи за евидентирање и проверка на сесии за ЕВ-полнење

Критериум	**Централизиран заднински (*backend*) модел**	**Целосно *on-chain* складирање**	**Класични *audit logs***	***Proof-of-Charge* со блокчејн закотвување**
Локација на податоците	Сите податоци се чуваат во заднинскиот (*backend*) систем на операторот.	Деталните податоци се запишуваат директно на блокчејн [43], [44].	Записите се чуваат во системски логови или во посебна *audit* база [80], [83].	Деталните податоци остануваат *off-chain*, а на блокчејн се закотвува групен доказ [16], [51]–[55].
Проверливост	Ограничена, најчесто зависи од доверба во операторот.	Висока, бидејќи податоците или нивните	Средна до висока, доколку логовите се	Висока, бидејќи Мерклвиот корен и

		записи се јавно проверливи [43], [44].	криптографски заштитени и *tamper-EBident* [80], [82]–[84].	Мерклова патека овозможуваат независна проверка на потврдите [16], [22], [48], [82], [84].
Приватност	Податоците не се јавно достапни, но се концентрирани кај операторот.	Ниска, доколку деталните податоци се јавно видливи на блокчејн [43], [44].	Средна, зависно од пристапните политики и начинот на зачувување на логовите [83].	Висока, бидејќи јавно се објавува само криптографск и доказ, а деталните податоци остануваат *off-chain* [16], [43], [44].
Скалабилност	Висока, но со ограничена надворешна проверливост.	Ограничена поради трошоци и обем на *on-chain* податоци [55], [67], [68].	Висока, но со потреба од сигурна лог инфраструктур а [80], [83], [84].	Висока, бидејќи повеќе потврди се групираат во еден *batch Merkle Root* [16], [48], [55].
Трошоци	Ниски оперативни трошоци за складирање.	Високи трошоци поради *on-chain* складирање и gas [67], [68].	Средни, зависно од системот за логирање, потпишување и архивирање [80], [83].	Ниски до средни, бидејќи *on-chain* се зачувува само минимален доказ [16], [55], [67].
Ревизибилнос т	Ограничена, бидејќи ревизијата зависи од доставените податоци од операторот.	Висока, но со ризик од прекумерно јавно откривање на податоци [43], [44].	Средна до висока, доколку логовите се потпишани, редоследно заштитени и проверливи [80], [83]–[85].	Висока, бидејќи ревизорот може да провери конкретна потврда преку Мерклова патека и закотвен Мерклов корен[16], [48], [81], [85].

Ризик од измена на записи	Постојат ризици од post-hoc измени без надворешен доказ.	Многу низок поради неизменливоста на блокчејн [43], [44].	Намален ако логовите се tamper-*EB*ident и криптографски потпишани [80], [83].	Низок, бидејќи измената на потврда ја менува хеш-вредноста, Мерклова патека и групниот Мерклов корен [16], [22], [48].
Практична применливост во ЕВ-полнење (*EV* charging)	Висока, но со ограничена доверба меѓу различни страни.	Ограничена поради приватност, трошоци, скалабилност и регулаторни прашања [43], [44], [55].	Корисна за внатрешна контрола, но не секогаш доволна за меѓусистемска доверба [80], [83], [85].	Висока, бидејќи се комбинираат *off-chain* обработка, приватност, скалабилност и независна проверливост [16], [51]–[55], [70]–[77].

Како што покажува табелата 6.5, предложениот *Proof-of-Charge* пристап не се обидува да го замени заднинскиот систем или да ги префрли сите податоци *on-chain*. Наместо тоа, тој ги комбинира предностите на централизираното оперативно складирање, *tamper-evident* логиката и *blockchain anchoring*. Со ова се добива модел што е практично применлив за инфраструктури за полнење електрични возила, но истовремено обезбедува повисоко ниво на проверливост, ревизибилност и доверба меѓу повеќе независни учесници [16], [70]–[77], [81], [85].

На тој начин, блокчејн во предложениот модел *Proof-of-Charge* има јасно дефинирана и ограничена улога. Тој не ја заменува постојната инфраструктура за полнење електрични возила, не ги заменува *OCPP* и *OCPI* процесите и не ја презема целата деловна логика. Неговата улога е да обезбеди независно проверлив, временски поврзан и криптографски стабилен доказ за група потврди. Ваквата употреба овозможува *Proof-of-Charge* да ги комбинира предностите на обработката *off-chain*, Мерклovите структури и блокчејн закотвување (*blockchain anchoring)* во еден практичен модел за проверливи записи од полнење.

6.9 Заклучок на поглавјето

Во ова поглавје беше разгледана улогата на блокчејн технологијата во развојот на проверливи системи за полнење електрични возила. Анализата покажа дека блокчејн не треба да се разгледува само како технологија за дигитални трансакции, туку и како механизам за создавање трајни, временски означени и криптографски проверливи записи во системи каде што учествуваат повеќе независни страни [40]–[45].

Најпрво беа разгледани основните карактеристики на блокчејн системите, како дистрибуираност, криптографско поврзување на записите, консензус, транспарентност и можност за независна проверка. Овие својства се значајни за системите за полнење електрични возила, бидејќи податоците за сесиите, мерењата, тарифите, наплатата и порамнувањето често се обработуваат од различни учесници и заднински системи [42]–[44].

Потоа беа анализирани криптографските механизми врз кои се заснова блокчејн технологијата. Хеш-функциите, Мерклovите структури, дигиталните потписи, временското означување и криптографските *commitment* механизми претставуваат основа за создавање проверливи записи и за откривање подоцнежни измени [22], [23], [46]–[50]. Овие механизми се директно поврзани со моделот *Proof-of-Charge*, каде што секоја потврда за полнење се претставува преку хеш-вредност, а повеќе потврди се поврзуваат преку групен Мерклов корен (*batch Merkle Root)*.

Во поглавјето беше нагласена и разликата меѓу *on-chain* и *off-chain* пристапите. Целосното *on-chain* складирање може да обезбеди висока проверливост, но создава проблеми со приватност, трошоци и скалабилност. Затоа, за системите за полнење електрични возила е попрактичен хибриден пристап, каде што деталните мерни податоци и потврдите остануваат *off-chain*, додека на блокчејн или во надворешен регистар се закотвува минимален криптографски доказ [51]–[55].

Посебно внимание беше посветено на паметните договори и нивната ограничена, но важна улога во предложениот модел. Тие можат да се користат за запишување на *batch Merkle Root*, *batch ID*, временска ознака и референца кон *off-chain* доказ, но не треба да ја преземат целата логика на сесијата, пресметката на испорачаната енергија или наплатата [61]–[65]. На овој начин се намалува сложеноста на *on-chain* логиката, се ограничуваат трошоците и се намалува безбедносниот ризик.

Етериумот беше разгледан како една од можните платформи за паметни договори (*smart contracts)* и блокчејн закотвување (*blockchain anchoring)*. Неговата улога во моделот *Proof-of-Charge* се состои во можноста да обезбеди проверлив запис за групен криптографски доказ, преку *transaction hash* и *smart contract* функција за закотвување [40], [41], [66]–[69]. Сепак, Етериумот не се третира како единствена можна платформа, туку како пример за практична реализација на надворешен блокчејн слој.

Во поширокиот контекст на системите за полнење електрични возила и енергетските системи, беше покажано дека блокчејн може да има примена во плаќања, роаминг процеси, *smart metering*, *peer-to-peer energy trading*, *demand response* и *V2G* сценарија [70]–[77]. Овие области ја потврдуваат потребата од проверливи записи, доверлива размена на податоци и независна ревизија, особено кога податоците се користат за финансиско порамнување, регулаторна проверка или учество во енергетски услуги.

Завршниот дел од поглавјето ја поврза блокчејн технологијата со предложениот модел *Proof-of-Charge*. Блокчејн во овој модел не ја заменува постојната инфраструктура за полнење, ниту ги заменува OCPP, OCPI или заднинските системи. Неговата улога е да обезбеди независно проверлив, временски поврзан и криптографски стабилен доказ за група потврди. Ова се постигнува преку хеширање, Мерклови структури, *off-chain*

складирање и закотвување на групен Мерклов корен (*batch Merkle Root)* во блокчејн или надворешен регистар [16], [48], [78]–[85].

Врз основа на разгледаното, може да се заклучи дека блокчејн технологијата има најголема вредност во системите за полнење електрични возила кога се користи селективно и целно. Таа не треба да ги замени постојните компоненти, туку да ги надополни со дополнителен слој за интегритет, проверливост и ревизибилност. Таквиот пристап овозможува рамнотежа меѓу практична применливост, приватност, скалабилност и доверба меѓу повеќе независни учесници.

Со ова, поглавјето ја поставува теоретската и техничката основа за понатамошна анализа на моделот *Proof-of-Charge* како практичен механизам за проверливи и *privacy-preserving* потврди за сесии на полнење електрични возила. Во следното поглавје фокусот се насочува кон имплементацијата на предложениот систем и начинот на кој овие концепти се реализираат во прототипна софтверска платформа.

7. ИМПЛЕМЕНТАЦИЈА НА ПРЕДЛОЖЕНИОТ PROOF-OF-CHARGE СИСТЕМ

7.1 Вовед во имплементацијата

Во претходните поглавја беа поставени теоретските, архитектурните и моделските основи на предложениот пристап на *Proof-of-Charge*. Беа разгледани потребата од проверливост во системите за полнење електрични возила, улогата на криптографските механизми, можностите за офлајни полуонлајн- работа, како и примената на блокчејн технологијата како независен слој за потврдување на интегритетот. Ова поглавје не ги повторува тие основи, туку го прикажува начинот на кој предложениот модел е реализиран во форма на прототипен софтверски систем.

Целта на имплементацијата е да се покаже дека моделот *Proof-of-Charge* може практично да се примени преку јасно дефиниран работен тек (*workflow)*. Овој работен тек започнува со прием на податоци за сесија на полнење, продолжува со валидација на структурата на податоците, креирање канонска потврда, пресметување хеш-вредност, поврзување со мерниот тек преку Мерклов корен (*Merkle root)*, групирање на повеќе потврди во групна (*batch)* структура, закотвување на групен корен (*batch root)* во блокчејн околина и последователна проверка на интегритетот. На овој начин, имплементацијата претставува практична проверка на основната идеја на дисертацијата: деталните записи за полнење можат да останат *off-chain,* додека нивниот интегритет се потврдува преку компактни криптографски вредности.

Развиениот прототип е локално ориентирана истражувачка платформа, а не продукциски систем за управување со инфраструктура за полнење електрични возила. Таквата поставеност е избрана со цел процесите на генерирање, закотвување, верификација и ревизија (*audit*) да можат да се тестираат во контролирана и повторлива околина. Во прототипот се реализираат повеќе функционални целини: генерирање синтетички сесии за полнење, креирање потврди за *Proof-of-Charge*, пресметување хеш-вредност на потврдата (*receipt hash)*, формирање Мерклов корен (*Merkle Root)* за мерните податоци, групно закотвување (*batch anchoring)*, локална блокчејн интеграција, верификација и ревизија (*verification* and *audit)*, како и извоз на податоци и резултати за понатамошна анализа [86].

Имплементацијата го следи хибридниот *off-chain/on-chain* пристап. Деталните податоци за сесиите, мерните вредности, потврдите, записите за припадност на групата *(batch membership)* и резултатите од верификацијата се чуваат во *off-chain* база на податоци. Блокчејн-слојот се користи само за закотвување на групен Мерклов корен (*batch Merkle Root)*, односно компактна криптографска вредност што претставува група потврди. Овој пристап ја намалува количината на податоци што се запишуваат на

блокчејн, го избегнува непотребното изложување на чувствителни информации и овозможува независна проверка на интегритетот.

Во практичната реализација, секоја сесија на полнење се обработува преку неколку поврзани чекори. Најпрво се примаат податоците за сесијата и мерните вредности, потоа се креира канонска *Proof-of-Charge* потврда, а врз неа се пресметува *receipt hash*. Дополнително, мерните вредности се поврзуваат преку Мерклов корен *(Merkle root)*, со што потврдата не зависи само од финалната пресметана енергија, туку и од подредениот тек на мерењата од кои таа вредност е добиена. Повеќе *receipt hashes* потоа се групираат во *batch* структура, од која се добива *batch Merkle root* како заеднички доказ за интегритет.

Блокчејн-интеграцијата во оваа фаза е реализирана во локална компатибилна околина на Етериумот (*Ethereum)*. Ваквиот избор овозможува тестирање на функционалностите на паметните договори *(smart contract)* и проверка на процесот на блокчејн закотвувањето без зависност од јавна тест-мрежа (*testnet)* или главна (mainnet) мрежа. Тоа е соодветно за истражувачката фаза на дисертацијата, бидејќи овозможува контролирано тестирање на моделот, повторливост на експериментите и јасна споредба на различни стратегии за закотвување. Во тој контекст, *cost-aware* евалуацијата покажува дека *Merkle batch anchoring* е значително поефикасен пристап од *per-receipt anchoring*, бидејќи повеќе потврди се претставуваат преку една блокчејн трансакција [87].

Покрај генерирањето и закотвувањето на потврдите, прототипот вклучува и механизми за верификација (*verification*) и ревизија/проверка (*audit*). Верификацијата се заснова на повторно пресметување на хеш-вредностите и споредба со зачуваните вредности во базата на податоци и, кога е достапно, со вредноста закотвена во блокчејн-слојот. *Audit*-механизмот овозможува подетална проверка преку реконструкција на потврдата од зачуваните сесиски податоци и споредба со зачуваната *JSON*-структура, нормализираните полиња и претходно пресметаните хеш-вредности. На овој начин може да се откријат промени во содржината на потврдата, мерните податоци, енергетските пресметки или записите за припадност на групата (*batch membership)*.

Бидејќи станува збор за истражувачки прототип, во оваа фаза се користат синтетички генерирани сесии за полнење. Овој пристап овозможува контролирано тестирање, повторливост на експериментите и споредба на различни нивоа работни оптоварувања (*workload*). Сепак, структурата на системот е поставена така што во иднина може да се прошири кон реални OCPP/OCPI податоци, јавни блокчејн тест-мрежни околини, *IPFS* складирање, кориснички контролни табли (*dashboard*) и напредни механизми за заштита на приватноста (*privacy-preserving*).

Во продолжение на ова поглавје се опишуваат технолошката поставеност на прототипот, структурата на податоците и шемата на *Proof-of-Charge* потврдата, процесот на генерирање и хеширање на потврдата, механизмот за групно закотвување *(batch anchoring)*, блокчејн-интеграцијата преку паметни договори (*smart contract)*,

механизмите за верификација *(verification)* и проверка (*audit)*, како и ограничувањата на имплементацијата.

7.2 Технолошка поставеност на прототипот

Прототипот на предложениот систем *Proof-of-Charge* е реализиран како модуларна софтверска платформа, во која секоја компонента има јасно дефинирана улога во процесот на обработка, складирање, закотвување и проверка на податоците за полнење. Ваквата поставеност не е избрана само од програмерски аспект, туку и од истражувачка перспектива: секој чекор од *Proof-of-Charge workflow* може да се набљудува, тестира, повтори и документира одделно. Тоа е особено важно за дисертацијата, бидејќи имплементацијата треба да покаже дека предложениот модел не останува само концептуален, туку може да се реализира како функционален и проверлив прототип [86].

Основниот влез во системот е апликацијата *backend* развиена во *Python*, со користење на *FastAPI*. Во имплементацијата, овој дел е поставен во модулот src/main.py, каде што се дефинираат главните *API endpoints* за работа со системот. Преку овој слој се финализираат сесиите за полнење, се пристапува до зачуваните податоци, се објавуваат *batch anchors* во блокчејн околина и се извршуваат *verification* и *audit*. Главниот *endpoint* е POST /v1/receipts/finalize, преку кој системот прима податоци за завршена сесија на полнење, креира *Proof-of-Charge* потврда, ја пресметува нејзината хеш-вредност и ја зачувува во *persistence* слојот [89].

Структурата на API барањата и одговорите е дефинирана преку моделите *Pydantic*, организирани во модулот src/api_schemas.py. Овој слој има важна улога затоа што потврдата *Proof-of-Charge* мора да се креира од податоци што имаат очекувана структура, валидни типови и задолжителни полиња. На тој начин, уште пред да започне генерирањето на receipt, системот проверува дали доставените податоци се доволно целосни и доследни за понатамошна обработка. Дополнително, ваквата *API*- структура овозможува полесно документирање преку *OpenAPI*-спецификација, што е корисно за тестирање, демонстрација и идно поврзување со други системи [98], [99].

Клучната логика за креирање на *Proof-of-Charge* потврдата е имплементирана во модулот src/receipt_builder.py. Во овој дел се нормализираат мерните вредности, се пресметуваат енергетските параметри и се формира канонската структура на потврдата. Имплементацијата поддржува класични сесии за полнење, но и *V2G*-ready полиња како *import_kwh, export_kwh и net_kwh*. Со тоа прототипот не е ограничен само на еднонасочен тек на енергија, туку е поставен така што може да претстави и сценарија во кои електричното возило враќа енергија назад кон системот. Во рамките на потврдата се вклучуваат идентификатори, временски ознаки, *EVSE*-податоци, *OCPP-transaction identifier*, енергетски пресметки, *pricing*-структура, *settlement*-податоци и *Merkle root* на мерниот тек [86].

На имплементациско ниво, *Proof-of-Charge* потврдата не се третира само како административен запис, туку како детерминистички податочен објект. Откако потврдата ќе се формира во канонска *JSON*-структура, врз него се пресметува криптографска хеш-вредност. За оваа цел се користи *SHA-256* преку библиотеката *Python hashlib* [88]. Пресметката на хеш-вредноста врз детерминистичка *JSON*-претстава е важна затоа што овозможува истата содржина секогаш да произведе иста хеш-вредност. На тој начин,

receipt hash станува компактна и проверлива репрезентација на целата содржина на потврдата.

Криптографското поврзување на мерните вредности е реализирано преку посебен Мерклов модул, поставен во src/merkle.py. Во прототипот Меркловиот корен (*Merkle Root)* се користи на две нивоа. Првото ниво е во рамките на поединечна сесија, каде што мерните вредности се поврзуваат во Мерклов корен што станува дел од *Proof-of-Charge* потврдата. На тој начин, потврдата не се поврзува само со финалната пресметана енергија, туку и со редоследот на мерните примероци од кои таа вредност е добиена. Второто ниво е групното закотвување (*batch anchoring)*, каде што повеќе *receipt hashes* се групираат во една заедничка вредност на Меркловиот корен *(Merkle Root)*.

Складирањето на податоците е реализирано преку *PostgreSQL*-база на податоци, со *SQLAlchemy*-модели дефинирани во src/models.py. Оваа база претставува *off-chain persistence layer* на прототипот. Во неа се чуваат сесиите за полнење, мерните вредности, *Proof-of-Charge* потврдите, групно закотвување (*batch anchors)*, записите за припадност на групата *(batch membership)* и резултатите од верификацијата. Во ваквата поставеност, *Postgres* претставува главен извор на детални податоци за прототипот, додека блокчејн слојот се користи само за закотвување на компактна криптографска вредност. Овој пристап е важен затоа што овозможува деталните записи да останат достапни за пребарување, реконструкција и проверка, без да се запишуваат директно на блокчејн [86], [100].

Во базата се користат повеќе меѓусебно поврзани табели. Табелата *sessions* ги чува основните податоци за сесијата, *meter_values* ги чува поединечните мерни вредности, *receipts* ја чува канонската потврда и нејзиниот *hash*, *batch_anchors* ги чува вредностите на *batch root*, *batch_anchor_receipts* ја поврзува секоја потврда со конкретен *batch anchor*, а *verifications* ги зачувува резултатите од проверките. Ваквата структура овозможува секоја потврда подоцна да се реконструира, да се спореди со зачуваната хеш-вредност и да се провери дали била дел од конкретен *batch anchor*.

Batch anchoring логиката е издвоена од процесот на креирање поединечни потврди. Ова е важна имплементациска одлука, бидејќи генерирањето *receipt* и *blockchain anchoring* не мора да се случуваат во истиот момент. Прво се финализираат и зачувуваат сесиите, а потоа повеќе *receipt hashes* се групираат во *batch* структура. Од таа структура се пресметува *batch Merkle root*, кој служи како заедничка криптографска обврска за повеќе потврди. Овој пристап е во согласност со *cost-aware* евалуацијата, каде што *Merkle batch anchoring* се разгледува како поефикасна алтернатива на *per-receipt anchoring* [87].

Блокчејн интеграцијата е реализирана како локална околина компатибилна на *Ethereum*. За развој и тестирање се користи *Foundry*, додека *Anvil* обезбедува локален *blockchain node* [91], [92]. Компонентата *Smart contract* е имплементирана во *Solidity* и се користи за закотвување на вредностите на *batch root* [93]. Наместо секој *receipt hash* да се објавува како посебна блокчејн трансакција, во блокчејн се запишува само *batch Merkle root*. Со тоа се задржува можноста за независна проверка на интегритетот, но се намалува бројот на *on-chain* операции.

Практичната комуникација со блокчејн околината се реализира преку модулите во src/blockchain/ и преку алатките од екосистемот *Foundry*. Особено важна е алатката

Cast, која овозможува испраќање трансакции, повикување *smart contract* функции и читање податоци преку *Ethereum RPC* интерфејс [90], [94]. Во API-слојот се предвидени *endpoints* за објавување и проверка на *anchor* вредности, како *POST /v1/anchors/{anchor_id}/publish-chain и POST /v1/anchors/{anchor_id}/verify-chain*. На овој начин, прототипот овозможува споредба помеѓу вредноста *off-chain batch root* и вредноста *on-chain anchor*.

Механизмите за верификација и проверка (verification и audit) се реализирани преку посебни модули. Модулот src/verifier.py се однесува на проверка на поединечна потврда, src/verifier_batch.py на проверка на *batch root*, додека src/audit_service.py овозможува подетална проверка преку реконструкција на од зачуваните сесиски податоци. Овој дел е значаен затоа што преку него се покажува практичната вредност на моделот *Proof-of-Charge*. Ако некој дел од *JSON*- receipt, мерните вредности или записите за припадност на групата *(batch membership)* се промени, повторното пресметување на хеш-вредностите или Мерклов корен (*Merkle root*) треба да покаже несовпаѓање.

Покрај главните компоненти *backend, database и blockchain*, прототипот содржи и помошни модули за експериментална работа. Модулот src/synthetic_sessions.py се користи за генерирање контролирани *EV charging* и *V2G-ready* сесии, додека src/run_experiment.py овозможува end-to-end извршување на експериментален workflow. Дополнително, src/export.py и src/charts.py се користат за извоз на datasets и генерирање фигури. Овие модули се важни затоа што имплементацијата не служи само за демонстрација на еден пример, туку и за повторливи експерименти, споредба на нивоата работни оптоварувања (*workload)* и подготовка на резултати за анализа.

Главните модули на прототипната имплементација се сумирани во табелата 7.1.

Табела 7.1: Главни модули на прототипната имплементација

Модул / компонента	**Улога во имплементацијата**
src/main.py	Апликацијата *FastAPI* преку која се реализираат главните API *endpoints* за финализирање на сесии, пристап до зачувани податоци, објавување *anchor* вредности и проверка на интегритет.
src/api_schemas.py	Дефинира *Pydantic* модели за *API* барања и одговори, со што се обезбедува структурна валидација на влезните и излезните податоци.
src/receipt_builder.py	Го креира *canonical Proof-of-Charge receipt*, ги пресметува енергетските и settlement вредностите и ја генерира *receipt hash* вредноста.
src/merkle.py	Имплементира пресметување *Merkle root* за мерните вредности и за *batch* структури составени од повеќе *receipt hashes*.

src/models.py	Ги дефинира *SQLAlchemy* моделите за *Postgres persistence layer*, вклучувајќи сесии, мерни вредности, потврди, *batch anchors* и v*erification* записи.
src/batch_anchoring.py	Групира повеќе *receipt hashes* и формира дневни *batch anchors* што подоцна можат да се проверат или закотват во блокчејн околина.
src/blockchain/	Содржи модули за блокчејн *publish/verify* интеграција, односно за објавување и проверка на batch root вредности.
src/verifier.py	Овозможува проверка на поединечна *Proof-of-Charge* потврда преку повторно пресметување и споредба на хеш-вредностите.
src/verifier_batch.py	Овозможува проверка на *batch Merkle root* преку споредба на локално пресметаната root вредност со зачуваната вредност на *batch anchor*.
src/audit_service.py	Реализира *audit* проверка преку реконструкција на *receipt* од зачуваните сесиски податоци и споредба со зачуваната JSON-структура.
src/synthetic_sessions.py	Генерира синтетички *EV charging* и *V2G-ready* сесии за контролирани и повторливи експерименти.
src/run_experiment.py	Извршува *end-to-end* експериментален *workflow*, од генерирање сесии до извоз на резултати и метрики.
src/export.py и src/charts.py	Се користат за извоз на *datasets* и генерирање фигури потребни за анализа и документација на резултатите.

Како што се гледа од табелата 7.1, прототипната имплементација не е организирана како единствен монолитен програмски блок, туку како збир од поврзани модули. Таквата поделба овозможува секоја фаза од процесот *Proof-of-Charge* да се анализира одделно: приемот и валидацијата на податоците, креирањето на потврдата, криптографското поврзување на мерните вредности, складирањето во off-chain база, процесот на групно закотвување (batch anchoring) и последователната проверка *(verification/audit*).

Од технолошки аспект, оваа поставеност ја покажува практичната реализација на хибридниот пристап *Proof-of-Charge*. Деталните записи се чуваат во *PostgreSQL*, криптографските врски се градат преку *SHA-256* и *Merkle root* структури, а блокчејн се користи како независен слој за закотвување на групен корен (*batch root)*. Со тоа прототипот останува доволно едноставен за локално тестирање, но истовремено ги содржи главните компоненти потребни за проверка на моделот во контролирана истражувачка околина.

Важно е да се нагласи дека оваа технолошка поставеност е избрана според целта на дисертацијата. Прототипот не претставува продукциски *EV charging backend* и не тврди дека ги покрива сите аспекти на реална инфраструктура за полнење. Неговата цел

е поконкретна: да покаже дека *Proof-of-Charge* потврда може детерминистички да се креира, да се складира *off-chain*, да се поврзе со мерниот тек, да се групира во *batch anchor*, да се закотви во блокчејн околина и подоцна повторно да се провери. Токму оваа ограничена, но јасно дефинирана поставеност овозможува резултатите од евалуацијата да бидат повторливи, проверливи и поврзани со реална имплементација.

7.3 Структура на податоци и Proof-of-Charge receipt schema

По дефинирањето на технолошката поставеност на прототипот, следниот важен дел од имплементацијата е структурата на податоците преку која се претставува една сесија за полнење и нејзината *Proof-of-Charge* потврда. Во предложениот систем, потврдата не се третира како обична електронска сметка или текстуален запис, туку како структурирана, детерминистичка и проверлива податочна единица. Неговата задача е да ги поврзе основните податоци за сесијата, мерните вредности, енергетските пресметки, ценовните параметри и криптографските докази во една конзистентна форма.

Во прототипната имплементација, оваа структура е дефинирана преку посебен шема-слој. Тој слој има две главни улоги. Прво, ги дефинира полињата што мора да постојат во секоја *Proof-of-Charge* потврда. Второ, проверува дали односите помеѓу енергетските и финансиските вредности се доследни. Со тоа receipt schema не служи само за формално организирање на податоците, туку и како прв механизам за спречување на нецелосни или неконзистентни записи.

Во кодот, оваа логика е поставена во модулот src/receipt_schema.py. Во него се дефинирани задолжителните top-level полиња на потврдата: version, schema_version, session_type, session_id, user_id, evse_id, ocpp_tx_id, start_ts, end_ts, energy_kwh, energy_summary, pricing, settlement, merkle_root и stream_hash_alg. Ваквата структура е во согласност со целта на моделот Proof-of-Charge: секоја потврда да содржи доволно информации за да може подоцна да се реконструира, хешира, спореди и провери, без целосните податоци да се запишуваат директно на блокчејн [86].

Од практичен аспект, *receipt schema* може да се разгледа како збир од неколку логички групи. Првата група ги опфаќа идентификациските и временските податоци, како session_id, user_id, evse_id, ocpp_tx_id, start_ts и end_ts. Втората група ги содржи енергетските вредности, претставени преку energy_kwh и energy_summary. Третата група се однесува на податоците за *pricing* и *settlement*, додека четвртата група ја претставува криптографската врска со мерниот тек преку *Merkle_root* и stream_hash_alg.

Особено значаен дел од оваа структура е *energy_summary*, каде што се чуваат вредностите import_kwh, export_kwh и net_kwh. Овие полиња овозможуваат потврдата да биде применлива не само за класични *charge-only* сесии, туку и за *V2G-ready* сценарија. Кај стандардното полнење, export_kwh може да биде нула, а net_kwh е еднаков на преземената енергија. Кај двонасочните сценарија, net_kwh ја претставува разликата помеѓу внесената и вратената енергија. На тој начин, истата *receipt schema* може да претстави различни типови сесии без промена на основната структура.

Основната енергетска врска во *receipt schema* може да се претстави со следната равенка:

$$\boldsymbol{net_{kwh} = import_{kwh} - export_{kwh}} \quad (7.1)$$

Дополнително, во прототипот се применува условот финалната вредност energy_kwh да биде еднаква на net_kwh:

$$\boldsymbol{energy_{kwh} = net_{kwh}} \quad (7.2)$$

Овие равенки не се само описни правила, туку се дел од практичната логика за валидација на потврдата. Ако вредностите не се совпаѓаат, потврдата не се смета за конзистентна и не треба да продолжи во следните чекори на *Proof-of-Charge* процесот.

Слична логика се применува и кај финансискиот дел од потврдата. Во структурата *settlement* се чуваат gross_import_cost, gross_export_credit, net_amount и currency. Со тоа се овозможува одделно претставување на трошокот за преземена енергија и кредитот за евентуално вратена енергија. Во прототипот се проверува следната врска:

$$\boldsymbol{net_{amount} = gross_{import_{cost}} - gross_{export_{credit}}} \quad (7.3)$$

Ова е важно бидејќи *Proof-of-Charge* потврдата треба да биде не само криптографски проверлива, туку и внатрешно доследна. Доколку по финализирањето на сесијата се промени некоја енергетска или финансиска вредност, повторната пресметка треба да покаже несовпаѓање во хеш-вредностите или во проверката *(audit)*.

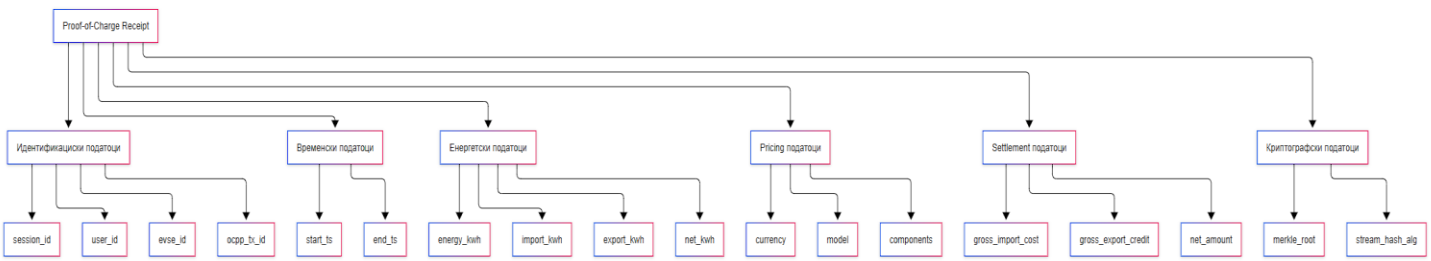
Во имплементацијата, самата потврда се формира во модулот src/receipt_builder.py. Овој модул ги обработува мерните вредности, ги пресметува разликите помеѓу почетната и крајната состојба на енергетските броила, ги изведува import_kwh, export_kwh и net_kwh, ја подготвува *pricing* структурата и ги пресметува settlement вредностите. Потоа се формира *canonical receipt object*, кој ги содржи задолжителните полиња и криптографската врска со мерниот тек. Во рамките на потврдата, Мерклвиот корен (*Merkle_Root)* се запишува како хеш-вредност (*hash value)* со 0x префикс, а stream_hash_alg е поставен на *SHA-256*, со што јасно се означува применетиот хеш-алгоритам (*hash algorithm)* [88].

Табела 7.2: Главните полиња во *Proof-of-Charge receipt schema*

Група	Поле	Улога во потврдата
Верзионирање	version	Формат верзија на структурата на потврдата *(receipt)*
Верзионирање	schema_version	Верзија на шема што се користи за валидација
Тип на сесија	session_type	Означува дали сесијата е *charge_only, discharge_only или bidirectional*

Идентификација	session_id	Единствен идентификатор на сесијата
Идентификација	user_id	Идентификатор на корисникот или учесникот во сесијата
Идентификација	evse_id	Идентификатор на точката за полнење
Идентификација	ocpp_tx_id	*Transaction identifier* поврзан со *OCPP* контекст
Време	start_ts, end_ts	Почеток и крај на сесијата
Енергија	energy_kwh	Финална нето енергетска вредност
Енергија	energy_summary	Структура со import_kwh, export_kwh и net_kwh
Цена	pricing	Валута, ценовен модел и ценовни компоненти
Пресметка	settlement	Трошок, кредит и нето износ
Криптографска врска	merkle_root	Мерклов корен на мерниот тек
Криптографска врска	stream_hash_alg	Алгоритам користен за хеш на мерниот тек

Како што се гледа од табелата 7.2, *Proof-of-Charge* потврдата е составен од оперативни, енергетски, финансиски и криптографски податоци. Оваа комбинација е потребна затоа што проверливоста на една сесија не зависи само од финалната вредност на потрошената енергија. Таа зависи и од тоа дали постои доследна врска помеѓу мерните примероци, пресметаните енергетски вредности, ценовниот модел и финалниот износ.



Слика 7.1. Логичка структура на *Proof-of-Charge* потврда

Во базата на податоци, шемата на потврдата (*receipt schema)* не останува само како *JSON*-документ. Дел од податоците се чуваат и како нормализирани полиња во табелите, што овозможува пребарување, филтрирање и споредба без секогаш да се обработува целата JSON- структура. Така, табелата **receipts** содржи: receipt_hash, merkle_root, schema_version, session_type, energy_kwh, import_kwh, export_kwh, net_kwh, start_ts, end_ts и receipt_json. Оваа комбинација на нормализирани полиња и J*SON payload* е важна за *audit*, бидејќи овозможува и брз пристап до главните вредности и целосна реконструкција на потврдата кога е потребно [100].

Во продолжение е даден краток извадок од оригиналниот код што ги прикажува задолжителните полиња во шемата на потврдата (*receipt schema*). Извадокот е скратен само на делот што е релевантен за структурата на потврдата.

```
REQUIRED_RECEIPT_FIELDS = {
    "version",
    "schema_version",
    "session_type",
    "session_id",
    "user_id",
    "evse_id",
    "ocpp_tx_id",
    "start_ts",
    "end_ts",
    "energy_kwh",
    "energy_summary",
    "pricing",
    "settlement",
    "merkle_root",
    "stream_hash_alg",
}
```

Листинг 7.1: Задолжителни полиња во *Proof-of-Charge receipt schema*

Покрај дефинирањето на задолжителните полиња, валидаторот проверува и дали главните енергетски и финансиски односи се исполнети. Следниот извадок од кодот ја покажува оваа логика.

```
if round(import_kwh - export_kwh, 3) != round(net_kwh, 3):
    raise ValueError("energy_summary.net_kwh must equal import_kwh - export_kwh")

if round(energy_kwh, 3) != round(net_kwh, 3):
    raise ValueError("energy_kwh must equal energy_summary.net_kwh")

if round(gross_import_cost - gross_export_credit, 3) != round(net_amount, 3):
    raise ValueError("settlement.net_amount must equal gross_import_cost - gross_export_credit")
```

Листинг 7.2: Проверка на енергетски и *settlement* инваријанти

Овие извадоци покажуваат дека структурата на податоците не е оставена само како договорена форма, туку е поддржана со конкретни програмски проверки. Тоа е значајно за дисертацијата, бидејќи моделот *Proof-of-Charge* бара секоја потврда да биде не само криптографски хеширана, туку и внатрешно конзистентна пред да стане дел од процесот на групно закотвување *(batch anchoring)*.

На крај, може да се забележи дека *receipt schema* има улога на врска помеѓу концептуалниот модел и практичната имплементација. Таа ги претвора поимите дефинирани во претходните поглавја во конкретни полиња, правила и проверки. Преку оваа структура, секоја сесија добива формален дигитален запис што може да се хешира, да се поврзе со мерниот тек, да се зачува во *off-chain* база и подоцна да се провери преку механизми за верификација или ревизија *(verification* или *audit)*.

7.4 Имплементација на Proof-of-Charge потврда

По дефинирањето на структурата на податоците и *receipt schema*, следниот чекор во прототипот е практичното креирање на *Proof-of-Charge* потврдата. Во оваа фаза, податоците од една сесија за полнење се претвораат во канонски *receipt* o*bject*, кој подоцна може да се хешира, складира, верификува и да стане дел од процесот на групно закотвување *(batch anchoring)*. Овој дел од имплементацијата е особено важен, бидејќи токму тука концептуалниот модел се претвора во конкретен дигитален запис.

Во прототипот, логиката за креирање на потврдата е имплементирана во модулот src/receipt_builder.py. Овој модул ја прима сесијата како структурирани податоци, ги нормализира мерните вредности, ги пресметува енергетските разлики, ја подготвува *pricing* и *settlement* структурата и го формира финалниот *receipt* o*bject*. На тој начин, *Proof-of-Charge* потврдата не се создава рачно, туку се генерира преку детерминистички процес што може повторно да се изврши и провери [86].

Првиот чекор во креирањето на потврдата е обработка на мерните вредности. Мерните примероци се подредуваат според временската ознака, а потоа се проверува дали енергетските бројачи се конзистентни. Во имплементацијата се поддржуваат вредности за преземена енергија, вратена енергија и нето енергија. Ова е важно затоа што истиот механизам може да обработи класична сесија за полнење, но и *V2G-ready* сесија во која енергијата може да тече во двете насоки.

Енергетските вредности се пресметуваат според разликата помеѓу последниот и првиот мерен примерок. На практично ниво, тоа значи дека потрошената или разменетата енергија не се внесува како произволна финална вредност, туку се изведува од мерниот тек. Овој пристап ја засилува проверливоста на потврдата, бидејќи финалниот резултат е поврзан со редоследот на мерните податоци.

Основната пресметка може да се претстави на следниот начин:

$$\boldsymbol{import_{kwh} = import_{kwh}^{last} - import_{kwh}^{first}} \tag{7.4}$$

$$\boldsymbol{export_{kwh} = export_{kwh}^{last} - export_{kwh}^{first}} \tag{7.5}$$

$$\boldsymbol{net_{kwh} = import_{kwh} - export_{kwh}} \quad (7.6)$$

Овие равенки ја покажуваат логиката што се применува во прототипот: потврдата ја користи разликата помеѓу почетната и крајната состојба на мерните вредности, а не само финална агрегирана вредност. Така се добива потврда што може да се реконструира од зачуваните вредности на мерењето (*meter values)*.

Покрај енергетските вредности, во потврдата се пресметува и делот *settlement*. Тој ги претставува финансиските вредности поврзани со сесијата, односно трошокот за преземена енергија, кредитот за евентуално вратена енергија и финалниот нето износ. Во имплементацијата, овие вредности се пресметуваат врз основа на pricing компонентите и времетраењето на сесијата. На тој начин, потврдата ја поврзува енергетската и финансиската страна на сесијата во една заедничка структура.

Откако ќе се пресметаат енергетските и финансиските вредности, се формира *canonical receipt object*. Тој ги содржи основните идентификатори, временските ознаки, типот на сесијата, енергетската сума, *pricing* структурата, *settlement* податоците, Мерклов корен (*Merkle Root)* на мерните вредности и ознаката за користениот хеш-алгоритам. Во оваа фаза, потврдата станува формален дигитален запис што може да се зачува и подоцна повторно да се провери.

Процесот на креирање на *Proof-of-Charge* потврдата може да се прикаже преку следната табела.

Табела 7.3: Главни чекори при генерирање Proof-of-Charge потврда

Чекор	**Опис**	**Резултат**
Прием на сесија	Системот прима структурирани податоци за сесијата и мерните вредности	Влезен *session payload*
Нормализација на мерења	Мерните вредности се подредуваат и се проверува нивната конзистентност	Подготвен *meter stream*
Пресметка на енергија	Се пресметуваат import_kwh, export_kwh и net_kwh	Енергетски *summary*
Пресметка на *settlement*	Се пресметуваат трошок, кредит и нето износ	*Settlement* структура
Мерклов корен *(Merkle root)*	Мерните вредности се поврзуваат во *Merkle root*	Криптографска врска со *meter stream*
Креирање потврда	Се формира канонска *Proof-of-Charge* потврда	Структуриран *receip*t o*bject*

Receipt hash	Потврдата се претвора во детерминистичка JSON-форма и се хешира	receipt_hash

Криптографската идентификација на потврдата се реализира преку *receipt hash*. По формирањето на *receipt* објектот, тој се претставува како *JSON*-структура со сортирани клучеви и врз таа претстава се пресметува *SHA*-256 *hash value* [88], [95], [96]. Ова може да се претстави со равенката:

$$\boldsymbol{h_R = SHA256(CanonicalJSON(R))} \tag{7.7}$$

каде што R ја претставува *Proof-of-Charge* потврдата, а h_R е нејзината хеш-вредност. Оваа хеш-вредност подоцна се користи како компактна репрезентација на целата потврда. Ако се промени кое било поле во потврдата, повторната пресметка треба да даде различна хеш-вредност.

Финализираната потврда и нејзината хеш-вредност се зачувуваат во слојот *off-chain persistence*, кој во прототипот е реализиран преку *PostgreSQL* [100]. Со тоа, системот ја задржува целосната структура на потврдата за подоцнежна реконструкција и проверка, додека за блокчејн закотвување се користи компактната хеш-вредност или групен корен (*batch root)* што произлегува од повеќе *receipt hashes*.

Во продолжение е прикажан скратен извадок од оригиналниот код што ја формира *Proof-of-Charge* потврдата. Извадокот не го прикажува целиот модул, туку само делот каде што се создава финалниот *receipt* објект.

```
receipt = {
    "version": RECEIPT_FORMAT_VERSION,
    "schema_version": session.get("schema_version", DEFAULT_SCHEMA_VERSION),
    "session_type": _derive_session_type(
        session.get("session_type"), import_kwh, export_kwh
    ),
    "session_id": session["session_id"],
    "user_id": session["user_id"],
    "evse_id": session["evse_id"],
    "ocpp_tx_id": session["ocpp_tx_id"],
    "start_ts": session["start_ts"],
    "end_ts": session["end_ts"],
    "energy_kwh": net_kwh,
    "energy_summary": {
        "import_kwh": import_kwh,
        "export_kwh": export_kwh,
        "net_kwh": net_kwh,
    },
    "settlement": {
        "gross_import_cost": gross_import_cost,
        "gross_export_credit": gross_export_credit,
        "net_amount": net_amount,
        "currency": (pricing or {}).get("currency", "EUR"),
    },
    "merkle_root": "0x" + root.hex(),
    "stream_hash_alg": "sha256",
}
```

Листинг 7.3: Креирање *Canonical Proof-of-Charge receipt*

Овој извадок покажува дека потврдата се формира како јасно дефинирана структура, а не како неформален текстуален запис. Секое поле има конкретна улога: идентификација на сесијата, поврзување со полначот и OCPP трансакцијата, пресметка на енергетските вредности, претставување на делот *settlement* и криптографско поврзување со мерните податоци.

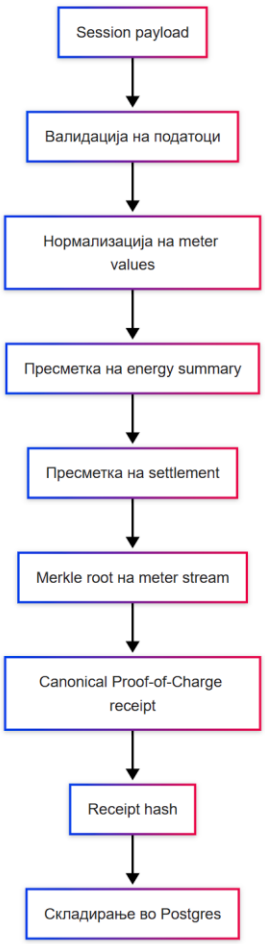
Следниот извадок ја прикажува логиката за пресметување на хеш на потврдата (*receipt hash)*. Овој хеш е клучен за понатамошното групно закотвување (*batch anchoring)*, бидејќи во *batch structure* не се групираат целосните записи на потврдата *(receipt)*, туку нивните хеш-вредности (*hash-value).*

```python
def hash_receipt(receipt: Dict[str, Any]) -> str:
    payload = json.dumps(receipt, sort_keys=True).encode("utf-8")
    h = hashlib.sha256(payload).hexdigest()
    return "0x" + h
```

Листинг 7.4: Пресметување *recept hash*

Со оваа функција, секоја *Proof-of-Charge* потврда добива единствена криптографска репрезентација. Важно е што хеш-вредноста се пресметува по формирањето на целата структура на потврдата. Тоа значи дека хеш ја опфаќа содржината на потврдата како целина, вклучувајќи ги идентификаторите, временските ознаки, енергетските вредности, *settlement* податоците и вредноста на Меркловиот корен (*Merkle Root)*.

Логиката на генерирање може да се прикаже и преку следниот дијаграм.



Слика 7.2: Тек на генерирање *Proof-of-Charge потврда*

Во однос на имплементациската логика, значајно е што генерирањето потврда (*receipt)* и пресметувањето на хеш (*hash)* се одвоени, но поврзани чекори. Прво се формира целосната потврда, потоа се врши валидација на нејзината структура и на крај

се пресметува хеш-вредноста. Ваквиот редослед е важен затоа што спречува невалидни или нецелосни записи да станат дел од понатамошниот процес на групно закотвување (*batch anchoring)*.

Овој *receipt hash* подоцна се користи како влез во процесот *batch anchoring*, каде што повеќе *receipt hashes* се групираат во *Merkle batch root*. Во *cost-aware* евалуацијата, ваквиот пристап се разгледува како поефикасна стратегија од *per-receipt anchoring*, бидејќи повеќе потврди можат да се претстават преку една заедничка *blockchain anchor* вредност [87].

На крај, имплементацијата на *Proof-of-Charge* потврдата покажува дека предложениот модел може да се реализира преку јасен и повторлив работен тек (*workflow)*. Потврдата се креира од структурирани податоци, се поврзува со мерниот тек, се претставува во канонска форма и се хешира. Со тоа се создава основата за следниот чекор во системот: групирање на повеќе *receipt hashes* во *batch* структура и формирање *Merkle root* што може да се закотви во блокчејн околина.

7.5 Групно закотвување и генерирање Мерклови коренски вредности (Merkle Root)

Откако поединечната *Proof-of-Charge* потврда ќе се креира и ќе се претстави преку *receipt_hash*, следниот чекор во прототипот е групирање на повеќе потврди во групна (*batch*) структура. Овој чекор е важен затоа што предложениот систем не се потпира на тоа секоја потврда поединечно да се запишува на блокчејн. Наместо тоа, повеќе *receipt hashes* се комбинираат во една Мерклова структура, од која се добива *batch Merkle root*. Таа вредност на коренот подоцна може да се користи како компактна криптографска обврска за целата група потврди.

Во имплементацијата, *batch anchoring* логиката е организирана во модулот src/batch_anchoring.py [86]. Овој модул ги собира *receipt hash value* за одреден ден или за одреден експериментален *prefix*, ги нормализира, ги подредува во детерминистички редослед и врз нив пресметува *Merkle Root*. На тој начин, истиот сет на *receipt hashes* секогаш треба да произведе иста *batch root* вредност, без разлика на редоследот во кој податоците биле прочитани од базата или од локалните записи.

Основната идеја може да се претстави со следната равенка:

$$\boldsymbol{B = MerkleRoot(h_1, h_2, \dots, h_n)} \tag{7.8}$$

каде што $h_1, h_2, \dots, h_n$се hash-value на поединечните *Proof-of-Charge* потврди, а B е *batch Merkle root*. Во овој модел, блокчејн не мора да ги чува сите *receipt hashes*. Доволно е да се закотви само вредноста B, бидејќи таа претставува криптографска обврска за целата група.

Од имплементациски аспект, *batch root* се формира преку неколку внимателно дефинирани чекори. Најпрво, секоја *receipt hash value* се нормализира, односно се отстранува 0x префиксот ако постои и вредноста се претвора во *lowercase* форма. Потоа

сите *hash values* се сортираат. Овој чекор е важен за повторливост, бидејќи обезбедува истите податоци секогаш да се групираат во ист редослед. Потоа нормализираните *hash values* се претвораат во *bytes* и се проследуваат кон *Merkle helper* функцијата, која ја пресметува root вредноста.

Оваа логика може да се претстави и преку поедноставена формална нотација:

$$\boldsymbol{H = sort(normalize(h_1), normalize(h_2), \dots, normalize(h_n))} \quad (7.9)$$

$$\boldsymbol{B = MerkleRoot(H)} \quad (7.10)$$

каде што *H* го претставува детерминистички подредениот сет од нормализирани receipt hash вредности. Со ова се избегнува ситуација во која исти потврди би дале различна *batch root* вредност само поради различен редослед на читање.

Во прототипот, *batch anchoring* може да се изврши врз основа на датумот на сесијата. Тоа значи дека сите потврди што припаѓаат на еден ден можат да се групираат во еден *batch*. Дополнително, во експерименталните сценарија може да се користи и session_prefix, со што се овозможува одвојување на потврдите што припаѓаат на конкретен експериментален *run*. Овој пристап е корисен за дисертацијата, бидејќи овозможува контролирано генерирање на *batch anchors* за различни нивоа работни оптоварувања (*workload)*.

Во *database-backed* режимот, *receipt hashes* се читаат од табелата *receipts*, при што се избираат записите што припаѓаат на одреден ден. Потоа се формира *batch root* и се зачувува *batch anchor* запис. Покрај самата *root* вредност, системот зачувува и *membership* информации, односно кои сесии и кои *receipt hashes* биле дел од конкретниот *batch*. Ова е важно затоа што подоцнежната верификациска или ревизиска проверка (*verification* или *audit)* треба да може да утврди дали конкретна потврда навистина била вклучена во одреден *batch*.

Табела 7. 4: Главни чекори во процесот групно закотвување *(batch anchoring)*

Чекор	Опис	Резултат
Избор на потврди	Се избираат потврди (*receipts)* за одреден ден или експериментален префикс (*prefix)*	Сет од релевантни хеш-вредности на потврдара (*receipt_hash values*)
Нормализација	Се отстранува 0x префиксот и хеш-вредностите се претвораат во *lowercase* форма	Единствен формат на хеш-вредности (*hash-values)*
Детерминистичко сортирање	Хеш-вредностите се сортираат пред Мерклovата (*Merkle)* пресметка	Повторлив редослед на *leaves*

Merkle root generation	Сортираните хеш-вредности се користат како *leaves*	Групен Мерклов корен *(Batch Merkle root)*
Зачувување на anchor	Групниот корен *(batch root)* и метаподатоците (*metadata)* се зачувуваат во *off-chain* база	Запис во групното закотвување (*batch_anchors)*
Membership запис	Се зачувува врската меѓу *batch anchor* и *receipt hashes*	Записи во *batch_anchor_receipts*

Како што се гледа од табелата 7.4, процесот на групно закотвување (*batch anchoring)* не е само техничко групирање на хеш-вредности. Тој создава проверлива структура во која секој хеш на потврдата (*receipt hash)* има место во конкретна група (*batch)*. Со тоа, подоцна може да се провери дали одредена потврда била дел од групата и дали локално пресметаната вредност на коренот се совпаѓа со зачуваната или закотвената вредност.

Во продолжение е прикажан скратен извадок од оригиналниот код што ја пресметува *batch Merkle root values*. Извадокот го прикажува само делот од функцијата што е најрелевантен за нормализација, детерминистичко сортирање и *Merkle root generation.*

```
def build_batch_root(receipt_hashes: List[str]) -> str:
    normalized = []
    for h in receipt_hashes:
        if h.startswith("0x"):
            h = h[2:]
        normalized.append(h.lower())

    normalized.sort()
    leaves = [bytes.fromhex(h) for h in normalized]

    if not leaves:
        raise ValueError("Cannot build batch root from empty list of hashes")

    root = merkle_root(leaves)
    return "0x" + root.hex()
```

Листинг 7.5: Пресметување *batch Merkle Root од receipt hashes*

Овој извадок покажува дека *batch root* не се формира произволно, туку преку јасно дефиниран и повторлив процес. Прво се обезбедува единствен формат на хеш-вредностите, потоа се наметнува детерминистички редослед, а на крај се пресметува Мерклов корен (*Merkle Root)*. Ваквиот пристап е значаен затоа што *batch root* мора да биде идентичен и при закотвување (*anchoring*) и при подоцнежна проверка.

Покрај вредноста на коренот (*root)*, прототипот зачувува и записи за припадност на групата *(batch membership)*. Во кодот, *membership* листата се формира преку

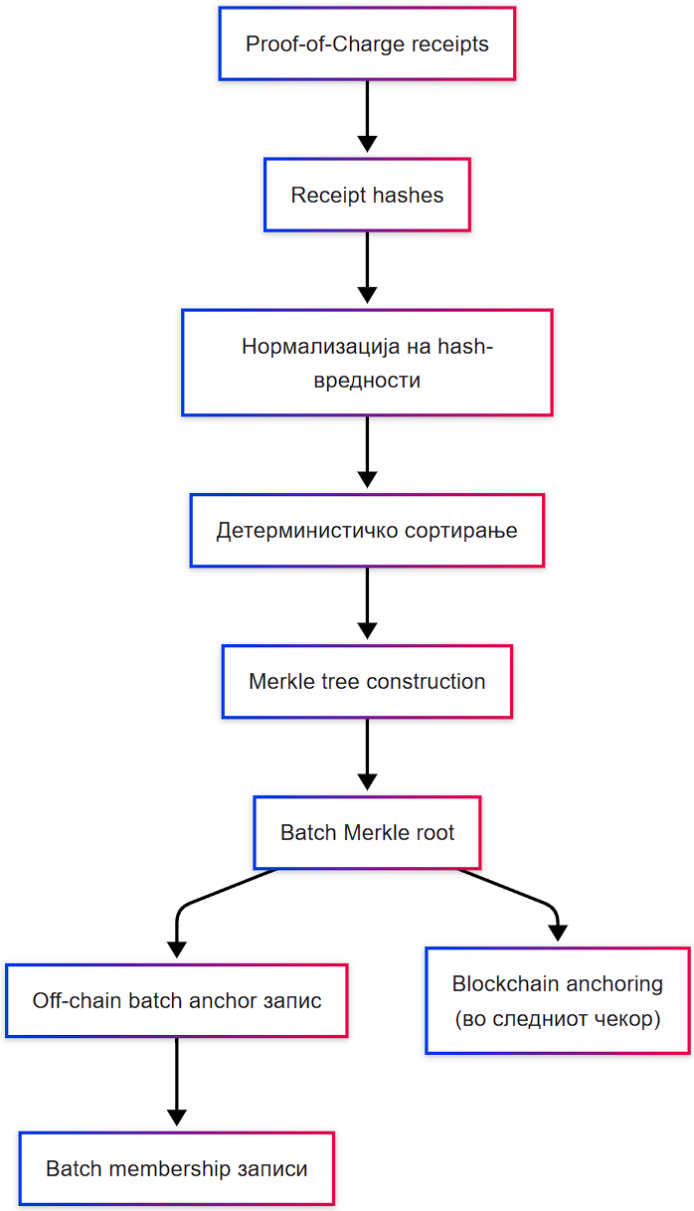
сортирање на паровите (session_id, receipt_hash) според нормализираната хеш-вредност. За секој елемент се зачувуваат session_id, receipt_hash и leaf_index. Овој leaf_index ја претставува позицијата на receipt hash вредноста во batch структурата и е корисен за следење на тоа како поединечните потврди се поврзани со конкретниот *batch anchor*.

```
def _build_anchor_memberships(
    session_ids: List[str],
    receipt_hashes: List[str]
) -> List[Dict[str, Any]]:
    pairs = sorted(
        zip(session_ids, receipt_hashes),
        key=lambda pair: _normalized_hash(pair[1]),
    )
    return [
        {
            "session_id": session_id,
            "receipt_hash": receipt_hash,
            "leaf_index": index,
        }
        for index, (session_id, receipt_hash) in enumerate(pairs)
    ]
```

Листинг 7.6: Формирање записи за *batch membership*

Формирањето записи за припадност ја зголемува ревизиската вредност на системот. Без овие записи, групната коренска вредност би покажувала дека постои одредена група хеш-вредности, но не би било доволно јасно кои конкретни потврди биле вклучени во таа група. Со зачувување на податоците за припадност, системот овозможува подоцнежна проверка на врската меѓу поединечната сесија, нејзината хеш-вредност и соодветниот запис за групно закотвување.

Работниот тек на процесот на групно закотвување може да се прикаже преку следниот дијаграм.



Слика 7.3: Работен тек на групното закотвување

Од аспект на ефикасност, групното закотвување (*batch anchoring)* е значајно затоа што овозможува повеќе потврди да се претстават преку една коренска (*root)* вредност. Ова ја намалува потребата од *per-receipt blockchain* операции и ја прави архитектурата попрактична за поголем број сесии. Во *cost-aware* евалуацијата, токму оваа разлика помеѓу *per-receipt anchoring* и *Merkle batch anchoring* се разгледува како главен фактор за намалување на *blockchain overhead* [87].

Важно е да се нагласи дека *batch root* сам по себе не ги заменува деталните записи. Деталните информации за *receipts*, *meter values* и *membership* остануваат во *off-chain persistence* слојот. *Batch root* служи како компактна криптографска обврска кон тие записи. Ако подоцна се промени некој *receipt hash*, се избрише потврда од *batch membership* или се измени редоследот на *leaves*, повторната пресметка на *batch root* треба

да даде различна вредност. На тој начин, процесот *batch anchoring* ја засилува *tamper-evidence* карактеристиката на системот.

Со ова, *Proof-of-Charge* системот преминува од проверливост на поединечна потврда кон проверливост на група потврди. Овој чекор е основа за следната секција, каде што *batch Merkle root value* се објавува во блокчејн околина преку *smart contract*. Така, *off-chain* податоците остануваат детални и пребарливи, додека блокчејн-слојот обезбедува независна точка за проверка на интегритетот.

7.6 Блокчејн интеграција преку паметен договор

По формирањето на групната вредност на Меркловиот корен *(Merkle root)*, следниот чекор во прототипот е нејзино закотвување во блокчејн околина. Во оваа секција фокусот е ставен на начинот на кој претходно формираниот off-chain batch anchor се поврзува со блокчејн слојот преку паметен договор компонента. Во прототипната имплементација, блокчејн интеграцијата е реализирана во локална компатибилна околина на Етериумот. За таа цел се користи *Foundry* како развојна околина, *Anvil* како локален блокчејн јазол, *Cast* како командна алатка за комуникација со мрежата и *Solidity* за паметен договор компонентата [90]–[93]. Комуникацијата со блокчејн јазолот се извршува преку *Ethereum JSON-RPC* интерфејс [94]. Ваквата поставеност е погодна за истражувачка имплементација, бидејќи овозможува контролирано тестирање без потреба од јавна тест-мрежа или главна мрежа.

Во системот, блокчејн слојот се користи по завршување на процесот на групно закотвување. Прво се креира batch_anchors запис во *off-chain* базата, кој содржи ден, број на потврди, групна Мерклова коренска вредност и дополнителни метаподатоци (*metadata)*. Потоа оваа вредност се испраќа кон компонентата паметен договор. По успешно извршување на трансакцијата, хешот на блокчејн трансакцијата се зачувува назад во базата како chain_tx. На овој начин, *off-chain* записот и *on-chain* доказот остануваат поврзани.

Во *API*-слојот, објавувањето и проверката на блокчејн *anchor* вредностите се реализирани преку посебни *endpoints*: POST /v1/anchors/{anchor_id}/publish-chain и POST /v1/anchors/{anchor_id}/verify-chain. Првиот *endpoint* ја објавува зачуваната групна *root* вредност во блокчејн околината, додека вториот ја чита *on-chain* вредноста и ја споредува со вредноста зачувана во базата на податоци. Овие *endpoints* се дефинирани во апликацијата *backend* и ја поврзуваат апликациската логика со блокчејн модулите.

Процесот на објавување на блокчејн *anchor* вредноста е имплементиран во модулот src/blockchain/publisher.py. Овој модул го пронаоѓа соодветниот *batch anchor* запис, ја испраќа неговата *root* вредност кон блокчејн, ја чита потврдата на трансакцијата и потоа го зачувува chain_tx во базата. Дополнително, како дел од резултатот се враќаат и информации како број на блок, *timestamp*, искористен *gas*, ефективна *gas* цена и статус на трансакцијата.

Формално, процесот на блокчејн закотвување може да се претстави на следниот начин:

$$\boldsymbol{T_x = Publish(B, d, n)} \tag{7.11}$$

каде што B е групната Merkle root вредност, d е денот или временската група на *batch*, nе бројот на потврди во *batch*, а T_x е *hash-value* на блокчејн трансакцијата. Со ова, блокчејн трансакцијата не го претставува целосниот сет на потврди, туку само криптографската обврска кон нив.

Во оваа архитектура, блокчејн записот има улога на надворешна референтна точка. Доколку подоцна се промени некоја потврда, нејзината хеш-вредност ќе се промени. Ако се промени некој член на групата, ќе се промени и групната вредност на Меркловиот корен. Таквата промена нема да се совпаѓа со вредноста што претходно била закотвена во блокчејн, па системот ќе може да открие несовпаѓање при проверка.

Главните елементи на блокчејн интеграцијата се прикажани во табелата 7.5.

Табела 7.5: Главните елементи на блокчејн интеграцијата

Елемент	**Улога во системот**
Групна *Merkle root value*	Компактна криптографска вредност што претставува група потврди *Proof-of-Charge*
batch_anchors	Off-chain запис во базата каде што се чува вредноста на коренот (*root value)* и метаподатоците (metadata) за групата (*batch)*
Smart contract	Блокчејн компонента што ја зачувува или регистрира *root value*
chain_tx	Хеш-вредност *(Hash-value)* на блокчејн трансакцијата преку која е објавена *root value*
publish-chain endpoint	*API* операција за објавување на *root value* во блокчејн околина
verify-chain endpoint	*API* операција за споредба меѓу *off-chain* и *on-chain root value*
Cast / JSON-RPC	Механизам преку кој прототипот комуницира со локалниот блокчејн јазол

Како што се гледа од табелата 7.5, блокчејн интеграцијата е поставена како дополнителен слој над веќе формираниот *off-chain batch anchor*. Тоа значи дека системот може да функционира и да извршува локална проверка на потврдите без блокчејн, но блокчејн закотвувањето обезбедува повисоко ниво на независна проверливост.

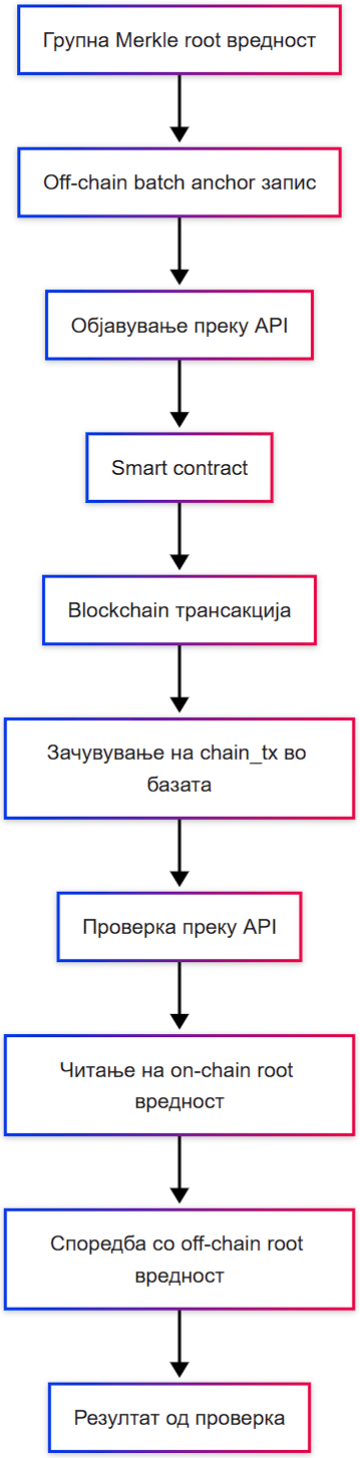
Проверката на *blockchain anchor value* е реализирана во модулот src/blockchain/verifier.py. Овој модул ја чита *root value* од блокчејн, ја споредува со вредноста зачувана во *off-chain* базата и проверува дали се совпаѓа и бројот на потврди во *batch*. Резултатот од проверката содржи expected_root, computed_root, број на потврди, chain_tx, оператор, *timestamp* и полето, match, кое покажува дали проверката е успешна.

Оваа проверка може да се претстави со следната равенка:

$$\boldsymbol{match = (B_{db} = B_{chain}) \wedge (n_{db} = n_{chain})} \quad \textbf{(7.12)}$$

каде што B_{db} е групната *Merkle root value* зачувана во *off-chain* базата, B_{chain} е *root* вредноста прочитана од блокчејн, n_{db} е бројот на потврди зачуван во базата, а n_{chain}е бројот на потврди регистриран во блокчејн. Ако двете споредби се точни, *anchor value* се смета за успешно проверена.

Работниот тек на блокчејн интеграцијата може да се прикаже преку следниот дијаграм.



Слика 7.4: Работен тек на блокчејн закотвување и проверка

Во овој работен тек, податоците се движат од *off-chain* слојот кон блокчејн само во форма на групна коренска вредност (*root value)*. Целосните *Proof-of-Charge* потврди, мерните вредности и записите за *membership* не се објавуваат на блокчејн. Ова е значајно

од аспект на приватност, скалабилност и трошоци, бидејќи блокчејн се користи само за она што е неопходно за проверка на интегритетот.

Дополнителна предност на ваквата поставеност е можноста за повторна проверка. Доколку во иднина се појави спор околу одредена сесија или потврда, системот може повторно да ја пресмета хеш-вредноста на потврдата, потоа да ја пресмета групната Мерклова коренска вредност (*Merkle root value)* и да ја спореди со вредноста што била закотвена во блокчејн. Ако сите вредности се совпаѓаат, тоа покажува дека потврдата и групната (*batch)* структура не биле изменети по моментот на закотвување.

Важно е да се нагласи дека во оваа фаза блокчејн интеграцијата е локална и истражувачка. Таа не претставува продукциска интеграција со јавна блокчејн мрежа. Сепак, локалната околина овозможува проверка на главните функции: објавување на root вредност, зачувување на *transaction hash*, читање на *on-chain* податоци и споредба со *off-chain* записите. Ова е доволно за целите на дисертацијата, бидејќи покажува дека предложениот модел *Proof-of-Charge* може да се поврзе со блокчејн слој преку реална паметен договор логика.

Со ова, блокчејн интеграцијата ја надополнува *off-chain* структурата со надворешна точка за проверка на интегритетот. Следната секција го разгледува процесот на проверка и ревизиска проверка, односно начинот на кој системот открива можни измени во потврдите, *batch* записите или закотвените вредности.

7.7 Механизми за проверка и ревизиска проверка

По креирањето на *Proof-of-Charge* потврдата, формирањето на групната Мерклова коренска вредност (*Merkle root value)* и нејзиното закотвување во блокчејн околина, потребен е механизам преку кој системот може подоцна да провери дали зачуваните податоци останале непроменети. Проверката е клучен дел од предложениот модел, бидејќи *Proof-of-Charge* потврдата има вредност само ако нејзиниот интегритет може повторно да се потврди [86].

Во прототипот се реализирани повеќе нивоа на проверка. Првото ниво се однесува на поединечна потврда, каде што повторно се пресметува хеш-вредноста на зачуваната потврда (*receipt)* и се споредува со претходно зачуваната вредност. Второто ниво се однесува на групна проверка, каде што од повеќе хеш-вредности на потврдата (*receipt_hash values*) повторно се пресметува групната Мерклова коренска вредност (*Merkle root value)* и се споредува со зачуваниот запис за групно закотвување. Третото ниво се однесува на споредба со блокчејн слојот, каде што *off-chain root* вредноста се споредува со вредноста зачувана преку паметниот договор. Дополнително, ревизиската проверка ја реконструира потврдата од оригиналните сесиски податоци и ја споредува со зачуваниот *receipt* запис [86].

Проверката на поединечна потврда е имплементирана во модулот src/verifier.py. Во овој процес, системот ја чита зачуваната потврда, повторно ја пресметува нејзината хеш-вредност и ја споредува со вредноста што била зачувана при финализирањето на

сесијата. Ако двете вредности се исти, потврдата се смета за непроменета. Ако вредностите се разликуваат, тоа укажува дека содржината на потврдата била изменета или дека записот не е конзистентен со претходно пресметаната hash-вредност. Бидејќи пресметката се заснова на *JSON* претстава и *SHA-256* хеш алгоритам, овој чекор ја поврзува структурата на потврдата со нејзината криптографска репрезентација [88], [95], [96].

Оваа проверка може да се претстави со следната равенка:

$$\boldsymbol{match_R = \left(h_{stored} = \ h_{computed}\right)} \tag{7.13}$$

каде што h_{stored}е хеш-вредноста зачувана во базата на податоци, а $h_{computed}$е hash-вредноста повторно пресметана од зачуваната потврда. Доколку двете вредности се совпаѓаат, резултатот од проверката е успешен.

Во практичната имплементација, резултатот од проверката содржи неколку главни полиња: expected_hash, computed_hash, expected_root, computed_root, match и денот на кој припаѓа сесијата. Овие податоци се корисни затоа што не покажуваат само дали проверката е успешна, туку и кои вредности биле споредени. На тој начин, системот обезбедува основа за понатамошна анализа во случај на несовпаѓање.

Покрај проверката на поединечна потврда, прототипот овозможува и проверка на групна root вредност. Оваа логика е имплементирана во модулот src/verifier_batch.py. При групната проверка, системот ги чита хеш-вредностите на потврдите што припаѓаат на конкретен запис за групно закотвување, повторно ја пресметува Мерклovата коренска вредност (*Merkle root value*) и ја споредува со претходно зачуваната вредност на коренот. Ако двете вредности се совпаѓаат, тоа покажува дека групата потврди не била изменета по формирањето на записот за групно закотвување [86].

Формално, групната проверка може да се претстави како:

$$\boldsymbol{match_B = \left(B_{stored} = B_{computed}\right)} \tag{7.14}$$

каде што B_{stored}е зачуваната групна Мерклovата коренска вредност, а $B_{computed}$е root вредноста добиена со повторна пресметка од хеш-вредностите на потврдите. Оваа проверка е важна затоа што овозможува откривање на промени не само во една потврда, туку и во составот на целата група. Во контекст на евалуацијата, ваквиот групен пристап е значаен затоа што овозможува повеќе потврди да се проверуваат преку една заедничка коренскавредност [87].

Проверката со блокчејн слојот се надоврзува на групната проверка. Во овој случај, системот ја споредува root вредноста зачувана во *off-chain* базата со коренската вредност прочитана од блокчејн. Дополнително, се споредува и бројот на потврди во групата. Овој механизам овозможува да се провери дали локално зачуваниот запис за групно закотвување се совпаѓа со вредноста што била закотвена преку паметниот договор [86].

Ова може да се претстави со равенката:

$$\boldsymbol{match_C = (B_{db} = B_{chain}) \wedge (n_{db} = n_{chain})} \quad (7.15)$$

каде што B_{db}е коренската вредност (*root value*) зачувана во off-chain базата, B_{chain}е коренската вредност прочитана од блокчејн, n_{db}е бројот на потврди зачуван во базата, а n_{chain}е бројот на потврди регистриран во блокчејн слојот.

Посебно значаен дел од системот е ревизиската проверка. За разлика од едноставната проверка на хеш-вредност, ревизиската проверка не се ограничува само на повторно хеширање на веќе зачуваниот receipt. Наместо тоа, системот ја зема зачуваната сесија, повторно ја гради *Proof-of-Charge* потврдата и потоа ја споредува со записот за потврдата (*receipt*) што се наоѓа во базата. Ова овозможува да се откријат посложени неконзистентности, на пример промена во сесиските податоци, промена во зачуваната *JSON* структура или разлика помеѓу нормализираните колони и содржината на потврдата [86], [100].

Ревизиската проверка е имплементирана во модулот *src/audit_service.py*. Во овој процес, системот ја реконструира потврдата од зачуваните сесиски податоци, повторно ја пресметува хеш-вредноста, ја споредува со зачуваната вредност и дополнително проверува дали нормализираните полиња во базата се совпаѓаат со вредностите во *JSON* структурата на потврдата. Овој пристап овозможува проверката да не зависи само од еден хеш, туку да ги опфати и односите меѓу зачуваните табеларни податоци и целосниот запис за потврдата (*receipt)* [86], [100].

Главните проверки во ревизиската постапка се прикажани во табелата 7.6.

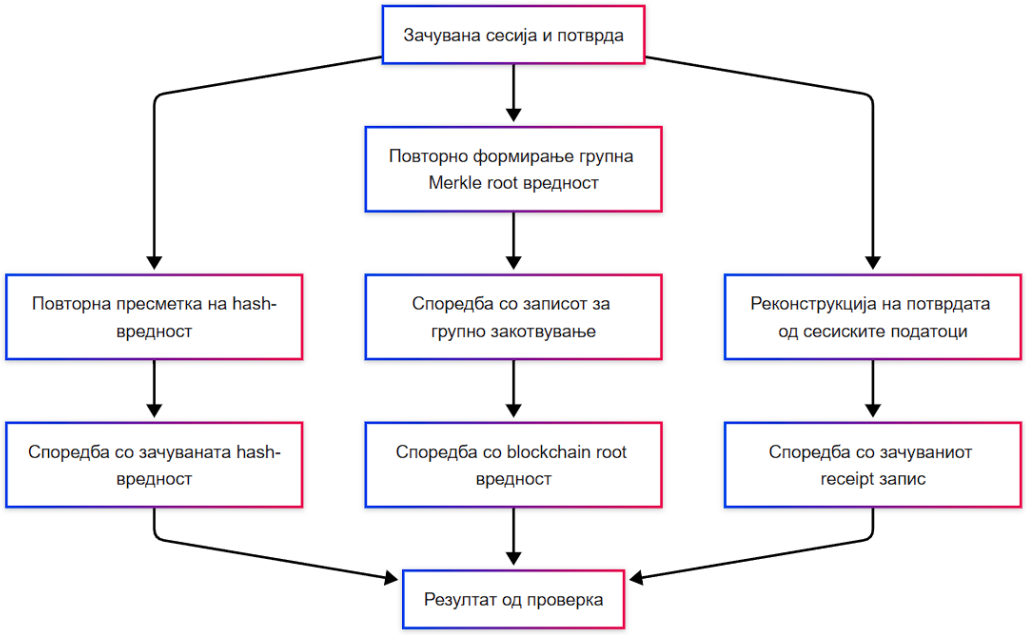
Табела 7.6: Главни проверки во процесот на ревизиска проверка

Проверка	**Опис**	**Цел**
Проверка на потврда	Повторно се пресметува хеш-вредноста на зачуваната потврда (*receip*t)	Откривање промени во поединечна потврда
Групна проверка	Повторно се пресметува групната Мерклова коренска вредност (*Merkle root value*)	Откривање промени во групата потврди
Блокчејн проверка	Се споредува *off-chain root* вредноста со *blockchain root* вредноста	Проверка на надворешната точка за интегритет
Реконструкција на потврда	Потврдата повторно се гради од зачуваните сесиски податоци	Проверка дали потврдата одговара на оригиналната сесија
Проверка на нормализирани полиња	Се споредуваат колоните во базата со вредностите во *JSON*-структурата	Откривање внатрешни неконзистентности

Како што се гледа од табелата 7.6, проверката во прототипот не се сведува на една споредба. Системот комбинира проверка на поединечна потврда, проверка на групна коренска вредност, проверка со блокчејн слојот и подетална ревизиска проверка.

Со тоа се добива повеќеслоен пристап, кој овозможува откривање на различни типови измени.

Работниот тек на проверка и ревизиска проверка може да се прикаже преку следниот дијаграм.



Слика 7.5: Работен тек на проверка и ревизиска проверка

Резултатите од проверките се зачувуваат во посебна структура за верификациски записи. Ова овозможува секоја проверка да остави трага во системот: која сесија или група била проверена, кои вредности биле споредени и дали резултатот бил успешен. На тој начин, системот не обезбедува само моментална проверка, туку и историја на извршени проверки, што е важно за подоцнежен увид и анализа [86], [100].

Во случај на промена на податоците, механизмите за проверка треба да покажат несовпаѓање. На пример, ако се измени содржината на една потврда, повторно пресметаната хеш-вредност нема да се совпадне со зачуваната вредност. Ако се измени составот на групата потврди, повторно пресметаната Мерклова коренска вредност *(Merkle root value)* ќе се разликува од зачуваниот запис за групно закотвување. Ако *off-chain* записот не одговара на блокчејн вредноста, проверката со блокчејн слојот ќе врати неуспешен резултат.

Со овие механизми, предложениот *Proof-of-Charge* систем обезбедува практична проверливост на повеќе нивоа. Поединечната потврда може да се провери преку нејзината хеш-вредност, групата потврди преку Мерклова коренска вредност *(Merkle root value)*, а закотвената вредност преку споредба со блокчејн записот. Ревизиската проверка дополнително ја засилува доверливоста, бидејќи ја реконструира потврдата од основните сесиски податоци и ја споредува со зачуваната состојба во системот [86].

7.8 Ограничувања на имплементацијата

Иако развиениот прототип ја покажува практичната применливост на предложениот модел *Proof-of-Charge*, важно е да се нагласи дека имплементацијата има истражувачки карактер. Таа е наменета за проверка на основната идеја, работниот тек и механизмите за создавање, закотвување и проверка на потврди, а не претставува целосен продукциски систем за јавна инфраструктура за полнење електрични возила.

Првото ограничување се однесува на користените податоци. Во прототипот се користат синтетички генерирани сесии за полнење, што овозможува контролирано тестирање и повторливост на експериментите. Сепак, реалните системи можат да содржат доцнења, прекини, нецелосни записи, комуникациски грешки или неправилности во мерните податоци. Затоа, како следен чекор би било потребно тестирање со реални податоци од OCPP или OCPI околини.

Второто ограничување е поврзано со блокчејн слојот. Во оваа фаза, закотвувањето се извршува во локална компатибилна околина на Етериумот. Таквата поставеност е соодветна за истражувачко тестирање, бидејќи овозможува контролирана проверка на паметниот договор и на процесот на закотвување. Сепак, таа не ги опфаќа сите услови што се јавуваат во јавни блокчејн мрежи, како променливи трансакциски трошоци, оптоварување на мрежата и време на потврдување на трансакциите [86], [87].

Третото ограничување се однесува на надворешното складирање и приватноста. Во прототипот деталните податоци се чуваат во *off-chain* база, а на блокчејн се закотвува само групна root вредност. Овој пристап го намалува изложувањето на чувствителни податоци, но во тековната верзија не е реализирана целосна IPFS-интеграција, ниту напредни механизми за приватност како *zero-knowledge* докази или селективно откривање на податоци. Овие елементи претставуваат можни насоки за понатамошна работа.

Четвртото ограничување е поврзано со продукциската примена. Прототипот е главно *backend* и експериментална платформа. Тој овозможува генерирање потврди, групно закотвување, проверка и ревизиска проверка, но не вклучува целосен кориснички интерфејс, управување со улоги, дигитални потписи на сите учесници или целосна безбедносна анализа за продукциско распоредување. Овие аспекти би биле потребни доколку системот се проширува кон реална примена.

Главните ограничувања се сумирани во табелата 7.7.

Табела 7.7: Главни ограничувања на прототипната имплементација

Ограничување	**Тековна состојба**	**Насока за понатамошна работа**
Податоци	Се користат синтетички сесии	Тестирање со реални OCPP/OCPI податоци
Блокчејн околина	Се користи локална компатибилна околина на Етериумот	Тестирање на јавна тест-мрежа
Надворешно складирање	IPFS-полиња се предвидени, но не се целосно активирани	Реална интеграција со IPFS или сличен систем

Приватност	На блокчејн се објавува само групна *root* вредност	Додавање напредни механизми за заштита на приватноста
Продукциска примена	Прототипот е *backend* и експериментална платформа	Кориснички интерфејс, улоги, потписи и подетално безбедносно тестирање

Овие ограничувања не ја намалуваат вредноста на имплементацијата, туку го дефинираат нејзиниот тековен истражувачки опсег. Прототипот покажува дека P*roof-of-Charge* потврда може да се креира, хешира, складира, групно да се закотви и подоцна да се провери. Истовремено, ограничувањата јасно покажуваат кои компоненти треба да се развијат дополнително за системот да се приближи кон реална примена во јавна инфраструктура за полнење електрични возила.

7.9 Заклучок на поглавјето

Во ова поглавје беше прикажана практичната реализација на предложениот *Proof-of-Charge* систем. Главниот фокус беше ставен на тоа како концептуалниот модел може да се претвори во функционален прототип, во кој податоците од една сесија за полнење се обработуваат, се претставуваат како структурирана потврда и се поврзуваат со криптографски докази за интегритет.

Имплементацијата покажа дека проверливоста не зависи од запишување на сите податоци во блокчејн околина. Напротив, деталните записи остануваат во *off-chain* слојот, додека блокчејн се користи за закотвување на компактна групна вредност. На овој начин се задржува можноста за независна проверка, а истовремено се намалува количината на податоци што треба да се објават на блокчејн [86], [87].

Посебно значење има тоа што прототипот не ја третира потврдата како обичен административен запис, туку како проверлива дигитална структура. Секоја потврда може повторно да се пресмета, да се спореди со зачуваната хеш-вредност и да се поврзе со групна Мерклова коренска вредност (*Merkle root value*). Со тоа системот овозможува откривање на можни измени во потврдите, мерните податоци или записите за групно закотвување.

Иако имплементацијата има истражувачки карактер и одредени ограничувања, таа ја покажува практичната изводливост на предложениот пристап. Прототипот обезбедува основа за понатамошна евалуација на ефикасноста, трошоците и проверливоста на моделот. Затоа, следното поглавје се насочува кон анализа и дискусија на резултатите добиени преку експерименталната поставеност.

8. АНАЛИЗА И ДИСКУСИЈА НА РЕЗУЛТАТИТЕ

8.1 Вовед во евалуацијата

Во ова поглавје се анализираат резултатите добиени од експерименталната проверка на предложениот прототип *Proof-of-Charge*. Фокусот е ставен на практичната применливост на системот, односно на тоа дали потврдите можат доследно да се креираат, групно да се закотват и подоцна повторно да се проверат.

Евалуацијата ги опфаќа главните аспекти на прототипот: генерирање потврди, групно закотвување, блокчејн трошоци и проверка на интегритетот. На овој начин се оценува дали предложениот пристап обезбедува повторлив, проверлив и практично применлив механизам за сесии на полнење електрични возила.

Резултатите во продолжение се користат за да се прикаже ефикасноста на прототипот, предностите на групното закотвување и можноста за откривање промени во зачуваните податоци.

8.2 Експериментална поставеност

Експерименталната поставеност е дефинирана со цел да се провери функционалноста, повторливоста и практичната применливост на предложениот прототип *Proof-of-Charge*. Евалуацијата е организирана како контролирана проверка на системот, при што се анализира дали прототипот може доследно да создава потврди, да ги поврзува со криптографски вредности и да овозможи нивна подоцнежна проверка.

При разгледување на безбедносните аспекти на паметните договори се земаат предвид препораките од *Open Worldwide Application Security Project - OWASP Smart Contract Top* 10 [101]. Квалитетот и тестирањето на софтверскиот систем се разгледуваат во согласност со општите принципи за софтверски квалитет и тестирање [102], [103], додека мерењето на времето на извршување и анализата на перформансите се поврзуваат со општите принципи за евалуација на компјутерски системи [104], [105].

Во експериментите се користат синтетички генерирани сесии за полнење. Овој пристап овозможува контролирани услови, повторливост на резултатите и споредба на различни големини на податочни множества. Иако ваквите податоци не ги заменуваат целосно реалните записи од инфраструктура за полнење, тие се погодни за почетна проверка на моделот и за споредба на различни сценарија во иста експериментална околина.

Главните елементи на експерименталната поставеност се прикажани во табелата 8.1.

Табела 8.1: Главни чекори во експерименталната поставеност

Елемент	Улога во евалуацијата
Синтетички сесии	Овозможуваат контролирано генерирање податоци за различни големини на тестови
Proof-of-Charge потврди	Служат како основни проверливи записи за секоја сесија
Хеш-вредности	Обезбедуваат компактна криптографска претстава на потврдите
Групно закотвување	Овозможува повеќе потврди да се претстават преку една заедничка root вредност
Блокчејн околина	Се користи за проверка на процесот на закотвување во контролирани услови
Механизми за проверка	Овозможуваат споредба на повторно пресметаните вредности со зачуваните записи

Оваа поставеност овозможува резултатите да се анализираат според неколку аспекти: создавање потврди, групно закотвување, трошоци за блокчејн операции и проверка на интегритетот. Деталната анализа на овие аспекти е дадена во следните потпоглавја.

8.3 Анализа на генерирање Proof-of-Charge потврди

Овој дел од евалуацијата се фокусира на генерирањето потврди *Proof-of-Charge* за различни големини на податочни множества. Целта е да се провери дали прототипот може доследно да создава проверливи потврди за секоја сесија и дали тие потврди можат да се користат како основа за понатамошно групно закотвување и проверка [86].

Во анализата се разгледуваат неколку критериуми: успешноста на креирањето потврда, доследноста на хеш-вредноста, поврзаноста со мерниот тек и можноста потврдата подоцна повторно да се провери. Овие критериуми се прикажани во табелата 8.2.

Табела 8.2: Критериуми за анализа на генерирање потврди

Критериум	Опис
Успешно креирање потврда	За секоја валидна сесија се формира *Proof-of-Charge* потврда
Доследна хеш-вредност	Истата содржина треба да произведе иста хеш-вредност
Поврзаност со мерниот тек	Потврдата содржи Мерклова коренска вредност *(Merkle root value)* што ја поврзува со мерните податоци
Зачувување во база	Потврдата и нејзината хеш-вредност се зачувуваат во off-chain слојот
Подоцнежна проверливост	Потврдата може повторно да се пресмета и спореди со зачуваната вредност

Резултатите покажуваат дека прототипот успешно го извршува процесот на креирање потврди кај различни големини на тестови. Кај помали податочни множества се потврдува исправноста на целокупниот работен тек, додека кај поголеми множества

се проверува дали истиот пристап останува стабилен и повторлив при зголемен број сесии.

Посебно значајно е тоа што секоја потврда се сведува на компактна хеш-вредност. Ова овозможува следните чекори, како групно закотвување и проверка на интегритет, да се извршуваат без потреба постојано да се обработува целата содржина на потврдата. На тој начин се задржува проверливоста, а истовремено се намалува количината на податоци што се користи во понатамошните операции.

Од оваа анализа може да се заклучи дека генерирањето *Proof-of-Charge* потврди е функционално и повторливо. Прототипот ја исполнува основната задача: секоја сесија да добие структуриран и проверлив запис, кој потоа може да се користи во процесите на групно закотвување, блокчејн проверка и ревизиска проверка.

8.4 Анализа на групното закотвување

Овој дел од евалуацијата се фокусира на групното закотвување, односно на тоа дали повеќе потврди можат да се претстават преку една заедничка Мерклова коренска вредност *(Merkle root value)* вредност и подоцна повторно да се проверат.

Во контекст на евалуацијата, групното закотвување се разгледува како механизам за намалување на бројот на блокчејн операции. Наместо бројот на трансакции да расте со бројот на потврди, повеќе потврди се претставуваат преку една заедничка root вредност [86], [87].

Критериумите според кои се анализира групното закотвување се прикажани во табелата 8.3.

Табела 8.3: Критериуми за анализа на групното закотвување

Критериум	**Опис**
Формирање група	Повеќе хеш-вредности на потврди се избираат за одреден ден или експериментален сет
Детерминистичко подредување	Хеш-вредностите се подредуваат на ист начин при закотвување и проверка
Пресметување Мерклова коренска вредност *(Merkle root value)*вредност	Од подредените хеш-вредности се добива една групна коренска вредност
Зачувување на записот	Вредноста на коренот (*root value)* и бројот на потврди се зачувуваат во *off-chain* база
Подоцнежна проверка	Истата вредност на коренот (*root value)* може повторно да се пресмета и спореди

Резултатите покажуваат дека групното закотвување успешно се извршува за различни големини на податочни множества. При секој експериментален сет, системот ги собира релевантните хеш-вредности, ги подредува на детерминистички начин и формира групна Мерклова коренска вредност *(Merkle root value)*. Со тоа се обезбедува повторливост на процесот, бидејќи истиот сет на потврди треба секогаш да даде иста вредност на коренот.

Овој пристап е особено значаен кај поголем број сесии. Со групното закотвување, повеќе потврди се претставуваат преку една root вредност, што го прави пристапот попрактичен за сценарија со поголем обем на податоци. Истовремено, деталните податоци остануваат во *off-chain* база, додека root вредноста се користи како компактна криптографска врска со тие записи.

Од оваа анализа може да се заклучи дека групното закотвување е функционално и соодветно за предложениот модел *Proof-of-Charge*. Тоа овозможува повеќе потврди да се поврзат во една проверлива структура, ја намалува потребата од поединечни блокчејн операции и создава основа за поефикасна проверка на интегритетот.

8.5 Анализа на блокчејн трошоци

Овој дел од евалуацијата ја разгледува разликата меѓу поединечно закотвување на секоја потврда и групно закотвување преку една заедничка Мерклова коренска вредност *(Merkle root value)*. Целта е да се покаже дали предложениот пристап го намалува бројот на блокчејн операции и дали останува практичен при зголемување на бројот на сесии.

Кај поединечното закотвување, секоја *Proof-of-Charge* потврда би барала посебна блокчејн трансакција. Тоа значи дека бројот на трансакции расте директно со бројот на сесии. Кај групното закотвување, повеќе потврди се претставуваат преку една коренска вредност, па бројот на блокчејн трансакции останува значително помал [87].

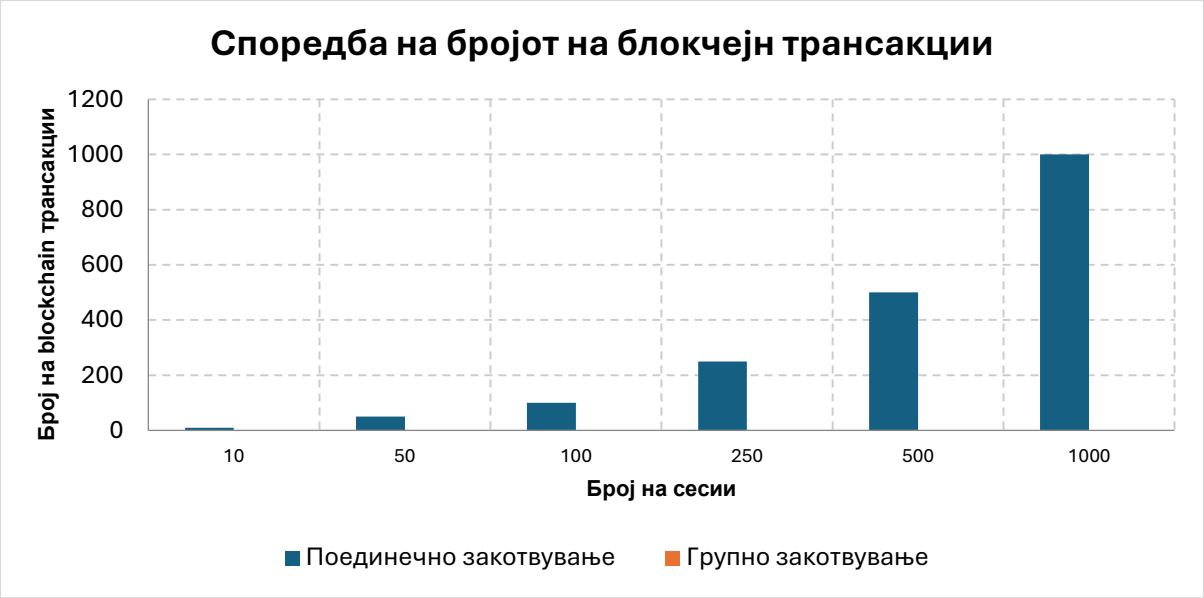
Резултатите од споредбата се прикажани во табелата 8.4.

Табела 8.4: Споредба меѓу поединечно и групно закотвување

Број на сесии	**Поединечно закотвување**	**Групно закотвување**	**Намалување на блокчејн операции**
10	10 трансакции	1 трансакција	90.0 %
50	50 трансакции	1 трансакција	98.0 %
100	100 трансакции	1 трансакција	99.0 %
250	250 трансакции	1 трансакција	99.6 %
500	500 трансакции	1 трансакција	99.8 %
1000	1000 трансакции	1 трансакција	99.9 %

Како што се гледа од табелата 8.4, предноста на групното закотвување станува поизразена со зголемување на бројот на сесии. Кај мал број сесии, разликата е видлива, но кај поголеми множества ефектот е многу позначаен. Наместо секоја потврда да создава посебна блокчејн-операција, целата група може да се претстави преку една заедничка вредност.

Овој резултат е важен затоа што директно ја поддржува архитектурната одлука деталните податоци да останат *off-chain*, а блокчејн слојот да се користи само за закотвување на компактни криптографски вредности. На тој начин, системот ја задржува можноста за проверка на интегритетот, но избегнува непотребно зголемување на бројот на трансакции.



Слика 8.1: Споредба на бројот на блокчејн трансакции кај поединечно и групно закотвување

Од оваа анализа може да се заклучи дека групното закотвување значително го намалува *blockchain overhead* во споредба со поединечното закотвување. Овој резултат ја потврдува практичната вредност на предложениот пристап *Proof-of-Charge*, особено во услови кога системот треба да обработува поголем број сесии за полнење.

Сликата 8.1 го прикажува намалувањето на бројот на блокчејн операции при користење групно закотвување. Кај поединечното закотвување, бројот на трансакции расте пропорционално со бројот на сесии. Наспроти тоа, кај групното закотвување повеќе потврди се претставуваат преку една заедничка коренска вредност, па бројот на блокчејн трансакции останува значително помал.

Овој резултат покажува дека групното закотвување е посоодветно за сценарија со поголем број сесии. Како што се зголемува бројот на потврди, разликата меѓу двата пристапи станува поизразена. На тој начин, предложениот пристап овозможува

зачувување на проверливоста, но без потреба секоја потврда поединечно да се објавува во блокчејн околина.

8.6 Проверка на интегритетот и ревизиска проверка

Овој дел од евалуацијата се однесува на проверката на интегритетот на генерираните *Proof-of-Charge* потврди. Целта е да се покаже дали системот може повторно да ги пресмета релевантните хеш и коренски вредности и да ги спореди со зачуваните записи.

Проверката се изведува на повеќе нивоа. Најпрво се проверува поединечната потврда преку споредба меѓу зачуваната и повторно пресметаната хеш-вредност. Потоа се проверува групната Мерклова коренска вредност *(Merkle root value)*, а дополнително може да се изврши и споредба со вредноста закотвена во блокчејн околина. Ревизиската проверка оди чекор понатаму, бидејќи ја реконструира потврдата од зачуваните сесијски податоци и ја споредува со постојниот запис [86].

Критериумите за оваа анализа се прикажани во табелата 8.5.

Табела 8.5: Критериуми за проверка на интегритетот

Критериум	**Опис**
Проверка на потврда	Се споредува зачуваната хеш-вредност со повторно пресметаната вредност
Проверка на групна коренска вредност	Повторно се пресметува Мерклова коренска вредност *(Merkle root value)*за групата потврди
Блокчејн проверка	Се споредува *off-chain* коренската вредност со закотвената вредност
Ревизиска проверка	Потврдата повторно се гради од зачуваните сесиски податоци
Резултат *match*	Покажува дали споредените вредности се совпаѓаат

Резултатите од проверките покажуваат дека кај валидните експериментални множества повторно пресметаните вредности се совпаѓаат со зачуваните записи. Тоа значи дека потврдите, групните коренски вредности и записите за закотвување можат повторно да се проверат без да се менува основната содржина на податоците.

За појасен приказ, резултатите можат да се претстават преку табелата 8.6.

Табела 8. 6: Резултати од проверка на интегритетот

Број на сесии	**Проверени потврди**	**Групна коренска вредност**	**Резултат од проверка**
100	100	Се совпаѓа	Успешна проверка
500	500	Се совпаѓа	Успешна проверка
1000	1000	Се совпаѓа	Успешна проверка

Како што се гледа од табелата 8.6, системот успешно ја задржува проверливоста и кај поголем број сесии. Ова е значајно бидејќи предложениот модел не треба само да создава потврди, туку и да овозможи нивна подоцнежна проверка.

Овие резултати покажуваат дека механизмите за проверка и ревизиска проверка се функционални во рамките на прототипот. Ако некоја потврда, хеш-вредност или групен запис се измени, повторната пресметка треба да покаже несовпаѓање. На тој начин, системот обезбедува практична основа за откривање промени во податоците и за поддршка на независна проверка на сесиите за полнење.

8.7 Проширена експериментална анализа на прототипот

Покрај основната евалуација на генерирањето потврди, групното закотвување, блокчејн трошоците и проверката на интегритетот, во ова поглавје се вклучува и проширена експериментална анализа на прототипот. Целта на оваа анализа е да се оцени дали предложениот *Proof-of-Charge* систем може повторливо да генерира, закотвува и проверува потврди за сесии на полнење при различни големини на податочни множества.

Во рамките на оваа дисертација, покрај основната проверка на предложениот модел, е спроведена и проширена експериментална анализа на прототипната имплементација [86]. Во анализата, прототипот е разгледан преку повторени извршувања, контролирани податочни множества и проверка на конзистентноста на добиените резултати. На тој начин, евалуацијата не се ограничува само на функционална демонстрација, туку ги опфаќа и стабилноста на извршувањето, времето на обработка, пропусноста и однесувањето на системот при контролирани измени во податоците.

За потребите на проширената анализа се користени податочни множества со различен број *Proof-of-Charge* потврди. Анализирани се тестови со 10, 50, 100, 500 и 1000 потврди, при што за секоја големина се извршени повеќе повторувања. Овој пристап овозможува да се добие пореална слика за стабилноста на прототипот, бидејќи резултатите не се базираат на едно извршување, туку на повторени мерења.

Во анализата се разгледуваат неколку клучни аспекти. Прво, се анализира просечното време потребно за обработка на една *Proof-of-Charge* потврда. Второ, се разгледува пропусноста на системот, односно бројот на потврди што може да се обработат во една секунда. Трето, се анализира потрошувачката на *gas* при групно закотвување на различен број потврди. Четврто, се проверува дали системот може да открие контролирани измени во различни делови од работниот тек, како што се содржината на потврдата, мерните вредности, записите *за* припадност на групата *(batch membership)*, зачуваниот групен корен (*batch roo)t* и надворешната блокчејн вредност.

Главната причина за вклучување на оваа проширена анализа е да се покаже дека предложениот модел не е само концептуален, туку може да се реализира како репродуцибилен прототип со мерливи резултати. На овој начин, евалуацијата овозможува да се процени практичната изводливост на *Proof-of-Charge* пристапот, неговата стабилност при различни големини на тестови и неговата способност за откривање промени во податоците по финализирање и закотвување.

Во продолжение, резултатите од проширената анализа се прикажани преку три главни насоки: анализа на времето на обработка и пропусноста, анализа на *gas* потрошувачката при групно закотвување и проверка на контролирани измени во податоците. Овие резултати ја надополнуваат основната евалуација и обезбедуваат подетален увид во однесувањето на прототипната имплементација.

8.8 Анализа на време на обработка и пропусност

Еден од важните аспекти на проширената евалуација е анализата на времето потребно за обработка на *Proof-of-Charge* потврдите. Овој показател е значаен бидејќи покажува дали предложениот прототип може да генерира и проверува потврди со стабилно однесување при различни големини на податочни множества.

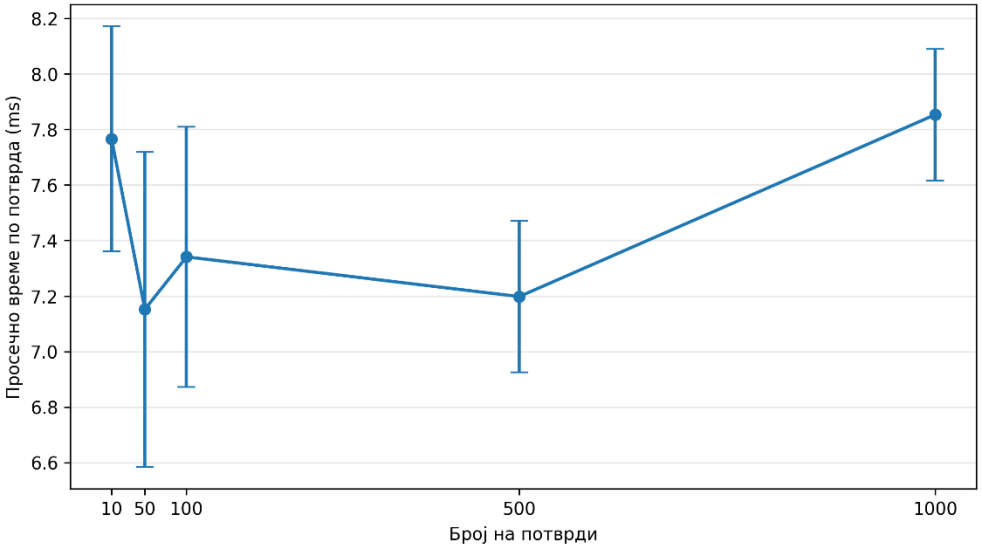
Во анализата се користени податочни множества со 10, 50, 100, 500 и 1000 потврди. За секоја големина се извршени по 10 повторувања, а резултатите се прикажани преку просечно време по потврда, 95 % интервали на доверба, пропусност и резултат од проверките. Овој пристап овозможува резултатите да не се базираат на едно извршување, туку на повторени мерења под контролирани услови.

Табела 8.7: Резултати од повторлива анализа на прототипот Proof-of-Charge

Број на потврди	**Број на извршувања**	**Просечно време по потврда (ms)**	**95 % CI (ms)**	**Пропусност (потврди/s)**	**Проверки**
10	10	7.766	7.362–8.171	129.41	Успешни
50	10	7.152	6.585–7.719	141.23	Успешни
100	10	7.341	6.873–7.810	137.17	Успешни
500	10	7.198	6.925–7.471	139.28	Успешни
1000	10	7.853	7.616–8.090	127.54	Успешни

Како што се гледа од табелата 8.7, просечното време по потврда останува во релативно стабилен опсег кај сите анализирани големини. Најниското просечно време е добиено кај тестот со 50 потврди и изнесува 7.152 ms, додека највисокото просечно време е добиено кај тестот со 1000 потврди и изнесува 7.853 ms [86]. Разликата меѓу овие вредности е мала, што покажува дека зголемувањето на бројот на потврди не доведува до значително влошување на времето на обработка.

Резултатите од табелата се прикажани и графички на сликата 8.2.



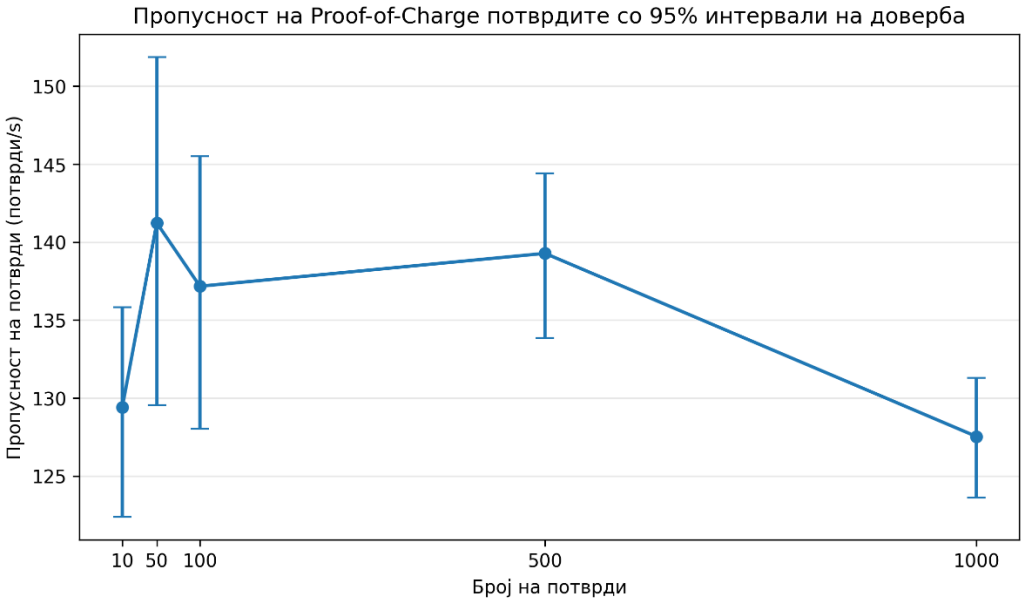
Слика 8.2: Просечно време по *Proof-of-Charge* потврда со 95 % интервали на доверба

Од сликата 8.2, може да се забележи дека линијата на просечното време останува стабилна и дека интервалите на доверба не покажуваат големи отстапувања меѓу различните големини на тестови. Ова укажува дека прототипот има предвидливо однесување при генерирање и проверка на потврди.

Покрај времето на обработка, анализирана е и пропусноста на системот. Пропусноста покажува колку *Proof-of-Charge* потврди може да се обработат во една секунда. Овој показател е важен за практичната применливост на моделот, особено во системи каде што во краток временски период може да се финализираат поголем број сесии на полнење.

Според резултатите, пропусноста се движи од 127.54 до 141.23 потврди во секунда. Највисока пропусност е добиена кај тестот со 50 потврди, додека најниска кај тестот со 1000 потврди. И покрај оваа разлика, резултатите остануваат во стабилен опсег и покажуваат дека прототипот може да обработува поголеми податочни множества без изразено намалување на ефикасноста.

Резултатите за пропусноста се прикажани на сликата 8.3.



Слика 8.3: Пропусност на *Proof-of-Charge* потврдите со 95 % интервали на доверба

Како што се гледа од сликата 8.3, пропусноста останува релативно стабилна кај сите анализирани големини. Малите разлики меѓу тестовите може да се должат на локалната извршна околина, работата со базата на податоци и варијациите при повторените извршувања. Сепак, сите проверки се успешно поминати, што значи дека стабилноста на обработката не е постигната на сметка на точноста или конзистентноста на резултатите.

Во целина, анализата на времето на обработка и пропусноста покажува дека прототипот може повторливо да генерира и проверува *Proof-of-Charge* потврди при различни големини на податочни множества. Просечното време по потврда останува под 8 ms, а пропусноста останува над 127 потврди во секунда [86]. Овие резултати ја поддржуваат практичната изводливост на предложениот модел и претставуваат основа за понатамошна анализа на блокчејн закотвувањето и трошоците во следниот дел.

8.9 Анализа на потрошувачката на gas при групно закотвување

Покрај времето на обработка и пропусноста, важен дел од евалуацијата е анализата на потрошувачката на gas при закотвување на криптографските докази на блокчејн. Овој аспект е значаен бидејќи директно влијае врз практичната применливост на предложениот *Proof-of-Charge* модел, особено во случаи кога системот треба да обработува поголем број сесии на полнење.

Во предложениот модел не се закотвува секоја потврда поединечно. Наместо тоа, повеќе *Proof-of-Charge* потврди се групираат во една група (*batch)*, од нивните хеш-вредности на потврдите (*receipt hash value*) се пресметува една заедничка Мерклова коренска вредност *(Merkle Root value)*, а на блокчејн се запишува само тој компактен криптографски доказ. На овој начин, бројот на блокчејн трансакции значително се намалува, додека можноста за подоцнежна проверка на секоја поединечна потврда се

зачувува преку Мерклова структура (*Merkle structure*) и записите за припадност на групата (*batch membership)*.

Во проширената евалуација се анализира потрошувачката на *gas* за различни големини на групи. Резултатите се прикажани во табелата 8.8.

Табела 8. 8: Резултати од блокчејн закотвување и ефективен трошок по потврда

Број на сесии	Број на потврди	Совпаѓање со блокчејн root	Потрошувачка на *gas* (*gas units*)	Трансакциски трошок (*Wei*)
10	10	Точно	143,329	9,025,384,417,958
50	50	Точно	143,329	7,907,991,390,629
100	100	Точно	143,341	6,929,518,052,149
250	250	Точно	143,341	6,071,605,682,934
500	500	Точно	143,353	5,320,353,068,450
1000	1000	Точно	143,365	4,662,055,038,065

Како што се гледа од табелата 8.8, блокчејн закотвувањето е успешно за сите анализирани големини на податочни множества. Во секој случај, вредноста на групниот корен (*batch root)* зачувана во локалната база се совпаѓа со вредноста прочитана од блокчејн слојот. Ова е означено со резултатот *Точно* во колоната за совпаѓање со блокчејн корен и покажува дека објавената вредност на *batch root* може да служи како надворешна референтна точка за проверка на интегритетот на *off-chain* потврдите.

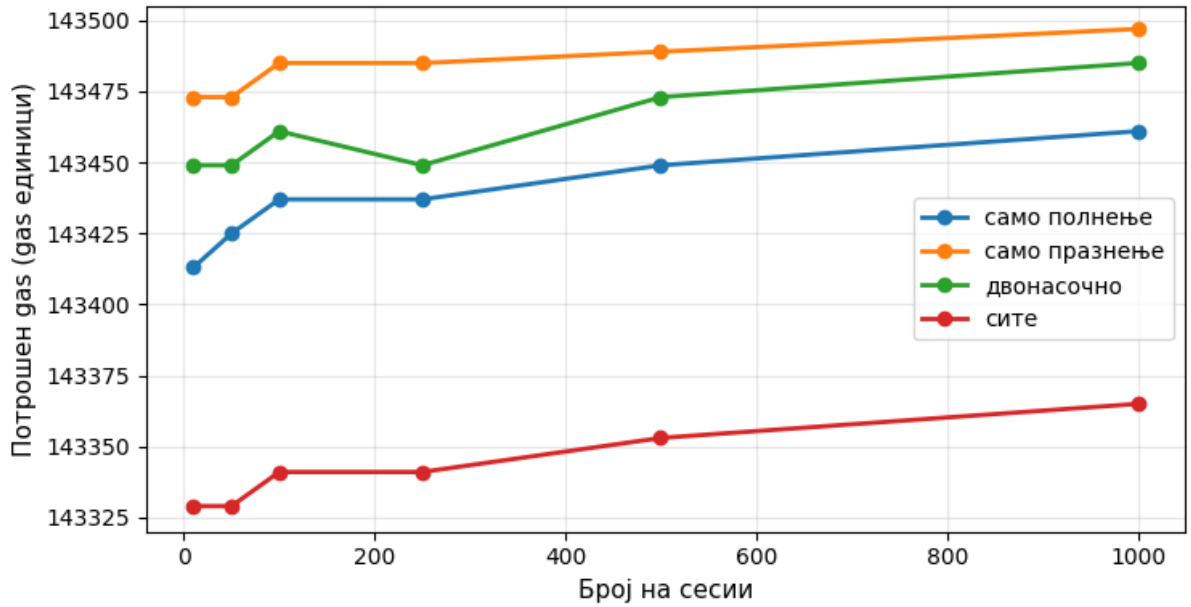
Потрошувачката на gas останува речиси константна кај сите анализирани големини. За 10 сесии таа изнесува 143,329 gas единици, додека за 1000 сесии изнесува 143,365 *gas* единици. Разликата е минимална, иако бројот на сесии се зголемува сто пати. Ова се должи на фактот дека на блокчејн се закотвува само една компактна вредност на *batch root*, а не секоја потврда или секој мерен запис поединечно.

Дополнителна вредност на оваа анализа се гледа преку колоната за трошок по потврда. Иако секоја група (*batch)* се објавува со една блокчејн трансакција, ефективниот трошок по потврда се намалува како што се зголемува бројот на потврди вклучени во групата. Кај 10 потврди, трошокот по потврда изнесува приближно 902.5 милијарди *Wei*, додека кај 1000 потврди се намалува на приближно 4.66 милијарди *Wei*. Ова јасно ја покажува предноста на групното закотвување (*batch anchoring)* во споредба со поединечно закотвување.

Овој резултат е значаен затоа што ја раздвојува комплексноста на *off-chain* податоците од трошокот на *on-chain* закотвувањето. Потврдите може да содржат повеќе полиња, како што се податоци за внесена енергија, испорачана енергија, нето енергија, цена, тарифен контекст и *settlement* вредности, но на блокчејн се запишува само

криптографската обврска што ја претставува целата група (*batch)*. Затоа зголемувањето на бројот на потврди во групата не доведува до пропорционално зголемување на потрошувачката на gas [86].

Резултатите се прикажани и графички на сликата 8.4.



Слика 8.4 :Потрошувачка на gas при една трансакција за групно закотвување

Од сликата 8.4 може да се забележи дека потрошувачката на *gas* останува во многу тесен опсег и при зголемување на бројот на сесии. Ова важи за различните типови сесии, како што се само полнење, само празнење, двонасочни сесии и мешаното податочно множество. Ваквото однесување покажува дека сложеноста на потврдите се обработува во *off-chain* слојот, додека блокчејн слојот зачувува само една компактна root вредност.

Треба да се нагласи дека трансакциските трошоци се добиени во контролирана локална блокчејн околина и не треба директно да се толкуваат како реални трошоци на јавна блокчејн мрежа. На јавни мрежи конечниот финансиски трошок зависи од цената на *gas*, оптоварувањето на мрежата, избраната блокчејн платформа и евентуалната употреба на *Layer-2* решенија. Во оваа евалуација, вредноста на овие резултати е споредбена: тие покажуваат дека бројот на блокчејн операции и ефективниот трошок по потврда се намалуваат кога повеќе потврди се претставуваат преку еден заеднички криптографски доказ.

Во целина, анализата за потрошувачката на gas покажува дека групното закотвување е практичен механизам за намалување на блокчејн трошоците и за подобрување на скалабилноста на *Proof-of-Charge* системот. Со користење на една групна коренска вредност *(batch root value)*, системот може да обезбеди надворешна проверлива референца за голем број потврди, без да ја изложи целосната содржина на потврдите или мерните податоци на блокчејн.

8.10 Проверка на контролирани измени во податоците

Покрај анализата на времето на обработка, пропусноста и *gas* потрошувачката, важен дел од проширената евалуација е проверката на однесувањето на системот при контролирани измени во податоците. Целта на оваа анализа е да се утврди дали предложениот *Proof-of-Charge* работен тек може да открие промени направени по финализирањето на потврдата, по формирањето на групното закотвување или при споредбата со надворешната блокчејн вредност.

Во оваа проверка не се анализира само една точка на контрола, туку повеќе слоеви од системот. Промените може да се појават во содржината на потврдата, во нормализираните мерни вредности, во зачуваната Мерклова коренска вредност *(Merkle root)*, во записите за припадност кон група (*batch)*, во зачуваниот групен корен (*batch root)* или во надворешната вредност добиена од блокчејн слојот. Затоа, системот користи повеќе механизми за повторна пресметка и споредба.

Во проширената анализа се разгледани седум контролирани сценарија, означени како T1–T7. Секое сценарио започнува од валидна основна состојба, по што се прави една контролирана измена во одреден дел од податоците. Потоа системот повторно ги пресметува релевантните вредности и проверува дали измената може да се открие преку соодветниот слој на проверка. Резултатите се прикажани во табелата 8.9 [86].

Табела 8. 9: Резултати по слоеви од контролираните сценарија за измени во податоците

Сценарио	**Изменет објект**	***Receipt Hash***	**Мерен тек**	**Ревизиска проверка на база**	***Batch* проверка**	**Блокчејн споредба**	**Очекувано однесување**	**Успешно враќање**
T1	Поле за енергија во receipt_json	Несовпаѓање	Помина то	Несовпаѓање	Помина то	Помина то	Да	Да
T2	Нормализирана import мерна вредност	Помина то	Несовпаѓање	Несовпаѓање	Помина то	Помина то	Да	Да
T3	Нормализиран мерен запис	Помина то	Несовпаѓање	Несовпаѓање	Помина то	Помина то	Да	Да
T4	Нормализирана потврда	Помина то	Помина то	Несовпаѓање	Помина то	Помина то	Да	Да

	root колона							
T5	Запис за *batch membership*	Помина то	Помина то	Помина то	Несовпаѓање	Помина то	Да	Да
T6	Зачуван *batch root*	Помина то	Помина то	Помина то	Несовпаѓање	Несовпаѓање	Да	Да
T7	Надворешна *root* вредност преку injected reader	Помина то	Помина то	Помина то	Помина то	Несовпаѓање	Да	Да

Во табелата 8.9, вредноста „поминато“ означува дека соодветниот слој останал конзистентен, додека „несовпаѓање“ означува дека контролираното нарушување е откриено во тој слој. На овој начин, табелата не прикажува само дали измената е откриена, туку покажува и преку кој дел од работниот тек е локализирано несовпаѓањето.

Како што се гледа од табелата 8.9, различните сценарија се откриваат во различни слоеви. Измената во содржината на потврдата кај T1 влијае врз *receipt hash* и ревизиската проверка на база. Измените во мерниот тек кај T2 и T3 не го менуваат зачуваниот *receipt hash*, но се откриваат преку реконструкција на мерниот тек и ревизиската проверка. Сценариото T4 покажува дека измена во нормализирана колона на потврдата може да се открие преку ревизиската проверка, додека T5 и T6 ја покажуваат улогата на *batch* проверката. Кај T7 локалните проверки остануваат конзистентни, но блокчејн споредбата открива несовпаѓање со надворешната *root* вредност.

Оваа поцелосна табела е повредна за дисертацијата бидејќи ја покажува слоевитата природа на проверката. *Receipt hash* ја штити канонската содржина на потврдата, реконструкцијата на мерниот тек ја штити секвенцата на нормализирани мерни записи, ревизиската проверка ја споредува реконструираната состојба со зачуваните податоци, *batch* проверката ја штити групната припадност и групниот корен, а блокчејн споредбата ја проверува усогласеноста со надворешно закотвената вредност.

Сите седум сценарија го исполниле очекуваното однесување, а по секоја контролирана измена основната состојба била успешно вратена. Ова покажува дека сценаријата биле изолирани едно од друго и дека резултатите не се последица на претходна измена во базата. Во сценариото T7 не е корумпирана реална *Anvil* трансакција, туку е користена алтернативна надворешна root вредност преку *injected*

reader, со цел да се провери однесувањето на блокчејн споредбата во контролирани услови [86].

8.11 Дискусија на резултатите

Резултатите од евалуацијата покажуваат дека предложениот *Proof-of-Charge* пристап може да се реализира како практичен механизам за проверливост во контролирана експериментална околина. Најзначајниот заклучок е дека интегритетот на сесиите за полнење може да се потврди без деталните податоци да се запишуваат директно на блокчејн. Наместо тоа, деталните записи остануваат во *off-chain* слојот, а блокчејн се користи како надворешна точка за проверка на групна криптографска вредност.

Овој резултат е важен од аспект на ефикасност и приватност. Доколку секоја потврда би се закотвувала поединечно, бројот на блокчејн операции би растел со бројот на сесии. Групното закотвување го избегнува овој проблем, бидејќи повеќе потврди се претставуваат преку една заедничка коренска (*root)* вредност. Со тоа се задржува проверливоста, а истовремено се намалува потребата од голем број блокчејн трансакции [87].

Резултатите од проверката покажуваат дека системот може повторно да ги пресмета релевантните вредности и да открие можни несовпаѓања. Ова ја потврдува практичната вредност на моделот, бидејќи *Proof-of-Charge* потврдата не е само запис создаден по завршување на сесијата, туку доказ што може да се провери и подоцна. Таквата можност е значајна за ревизија, решавање спорови и зголемување на довербата меѓу различните учесници во процесот на полнење.

Од практична перспектива, предложениот модел може да се разгледува како дополнителен слој над постојните системи за полнење електрични возила. Тој не мора да ја замени инфраструктурата за наплата или управување со сесии, туку може да ја надополни со механизам за независна проверка на податоците. Ова е особено важно во средини каде што повеќе страни имаат интерес за точноста на записите, како оператори, корисници, даватели на услуги и регулаторни институции.

Сепак, резултатите треба да се толкуваат во рамките на истражувачката поставеност на прототипот. Евалуацијата е изведена со синтетички податоци и локална блокчејн околина, па затоа резултатите ја потврдуваат техничката изводливост и повторливоста на пристапот, но не претставуваат конечна процена за продукциска примена. За таква примена потребни се тестирања со реални податоци, јавна testnet мрежа, посеопфатна безбедносна анализа и дополнителни механизми за заштита на приватноста.

Во целина, дискусијата покажува дека предложениот модел ги исполнува главните цели на евалуацијата: обезбедува проверлив запис за сесија на полнење, овозможува ефикасно групно закотвување и поддржува подоцнежна проверка на интегритетот. Со тоа, *Proof-of-Charge* пристапот претставува основа за потранспарентни и проверливи процеси во јавната инфраструктура за полнење електрични возила.

8.12 Заклучок на поглавјето

Во ова поглавје беа анализирани резултатите од експерименталната проверка на предложениот *Proof-of-Charge* прототип. Резултатите покажуваат дека системот може да создава проверливи потврди, да ги групира преку Мерклова коренска вредност *(Merkle root value*) и да овозможи нивна подоцнежна проверка.

Посебно значаен резултат е намалувањето на бројот на блокчејн операции преку групно закотвување. Со овој пристап, повеќе потврди се претставуваат преку една заедничка root вредност, со што се задржува проверливоста, а се намалува потребата од поединечно закотвување.

Врз основа на добиените резултати, може да се заклучи дека *Proof-of-Charge* пристапот има практична вредност како дополнителен слој за проверливост во системите за полнење електрични возила. Следното поглавје ги сумира главните придонеси на дисертацијата и ги наведува можните насоки за понатамошно истражување.

9. ЗАКЛУЧОК И ИДНИ НАСОКИ ЗА ИСТРАЖУВАЊЕ

9.1 Заклучни согледувања

Оваа дисертација се фокусираше на проблемот на проверливост и доверливост на податоците во процесот на полнење електрични возила. Во современите системи за полнење, податоците за сесијата најчесто се чуваат и обработуваат во различни off-chain системи, додека корисникот, операторот или друга заинтересирана страна нема секогаш едноставен и независен начин да провери дали финалната потврда навистина одговара на мерните податоци од кои е добиена. Токму оваа празнина ја мотивираше потребата за модел што овозможува криптографски проверливи потврди за сесии на полнење.

Во рамките на истражувањето беше предложен моделот *Proof-of-Charge*, чија главна цел е секоја завршена сесија за полнење да се претстави преку структурирана и проверлива дигитална потврда. Потврдата ги поврзува основните податоци за сесијата, мерниот тек, енергетските вредности, пресметковните податоци и криптографските докази за интегритет. На тој начин, потврдата не претставува само административен запис, туку податочна структура што може повторно да се пресмета, спореди и провери.

Еден од главните заклучоци е дека блокчејн технологијата не мора да се користи за директно складирање на сите податоци од сесиите за полнење. Напротив, поефикасен пристап е деталните податоци да останат во *off-chain* слојот, додека на блокчејн се закотвуваат само компактни криптографски вредности. Со тоа се намалува количината на податоци што се објавуваат во блокчејн околина, а сепак се задржува можноста за независна проверка на интегритетот.

Резултатите од имплементацијата и евалуацијата покажаа дека предложениот пристап е практично изводлив во контролирана експериментална околина. Прототипот овозможува креирање *Proof-of-Charge* потврди, нивно поврзување со мерните вредности, групно закотвување преку Мерклова коренска вредност *(Merkle root value)* и подоцнежна проверка на интегритетот. Ова покажува дека моделот може да служи како дополнителен слој за проверливост во системите за полнење електрични возила.

Иако прототипот има истражувачки карактер и одредени ограничувања, добиените резултати ја потврдуваат основната претпоставка на дисертацијата: податоците за сесија на полнење можат да останат надвор од блокчејн, но нивниот интегритет да биде проверлив преку криптографски докази и групно закотвување. Со тоа се создава основа за потранспарентни, проверливи и доверливи процеси во јавната инфраструктура за полнење електрични возила.

9.2 Главни придонеси на дисертацијата

Главниот придонес на оваа дисертација е дефинирањето на моделот *Proof-of-Charge* за проверливи дигитални потврди во процесот на полнење електрични возила. Моделот овозможува една завршена сесија да се претстави преку структурирана потврда што може подоцна да се провери независно од системот во кој првично била создадена.

Вториот придонес е предложениот хибриден пристап за поврзување на *off-chain* податоци со блокчејн слој. Наместо деталните записи да се објавуваат директно на блокчејн, во моделот се закотвуваат само компактни криптографски вредности. Со тоа се намалува изложувањето на податоци, а се задржува можноста за независна проверка.

Третиот придонес е примената на групно закотвување преку Мерклова структура. Овој пристап овозможува повеќе потврди да се претстават преку една заедничка root вредност, со што се намалува бројот на блокчејн операции и се зголемува практичната применливост на моделот кај поголем број сесии.

Четвртиот придонес е развиениот прототип, преку кој предложениот модел е проверен во контролирана експериментална околина. Прототипот ја покажува практичната изводливост на предложениот пристап и овозможува анализа на неговата повторливост, ефикасност и проверливост.

Петтиот придонес е дефинирањето механизми за проверка и ревизиска проверка. Преку повторна пресметка на криптографските вредности и споредба со зачуваните записи, системот овозможува откривање можни измени во потврдите, групните записи или закотвените вредности.

Со овие придонеси, дисертацијата покажува дека блокчејн технологијата може да се користи како дополнителен слој за доверба и проверливост, без потреба сите податоци од сесиите за полнење да се пренесуваат во блокчејн околина. На тој начин, предложениот пристап создава основа за потранспарентни и посигурни процеси во јавната инфраструктура за полнење електрични возила.

9.3 Идни насоки за истражување

Идните истражувања може да се насочат кон постепено приближување на предложениот модел *Proof-of-Charge* до реални услови на примена. Во оваа дисертација прототипот беше проверен во контролирана експериментална околина, што овозможи јасна анализа на основниот пристап. Како следен чекор, потребно е моделот да се тестира со реални податоци од системи за полнење електрични возила. Таквото тестирање би овозможило да се согледа како моделот се однесува во ситуации со различни типови полначи, прекини во сесијата, задоцнети записи или нецелосни мерни податоци.

Посебно важна насока е поврзувањето со постојни комуникациски протоколи и платформи, како OCPP и OCPI. Со ваква интеграција, *Proof-of-Charge* не би морал да ја замени постојната инфраструктура, туку би можел да функционира како дополнителен слој за доверба. На тој начин, операторите, корисниците и другите засегнати страни би добиле појасен механизам за потврдување на точноста на записите за полнење.

Понатамошното истражување треба да го опфати и блокчејн делот во пореални услови. Тестирањето на јавна тест-мрежа би овозможило подобра процена на трансакциските трошоци, времето на потврдување и стабилноста на системот при различно оптоварување на мрежата. Ова е важно затоа што локалната експериментална околина не ги прикажува целосно сите услови што се јавуваат во јавните блокчејн мрежи.

Друга можна насока е користење надворешни системи за складирање, како IPFS или слични решенија. Со тоа, дел од ревизиските записи би можеле да се чуваат надвор од централната база, додека нивната поврзаност со закотвените вредности би останала зачувана. Ваквиот пристап би ја намалил зависноста од еден единствен систем за складирање и би ја зголемил отпорноста на целокупното решение.

Во иднина треба да се посвети поголемо внимание и на приватноста. Податоците за полнење можат индиректно да откријат информации за движење, навики или локации на корисниците. Затоа е потребно да се разгледаат решенија што овозможуваат проверливост, но без непотребно откривање чувствителни информации. Во оваа насока може да се истражат дополнителна псевдонимизација, селективно откривање на податоци и напредни криптографски техники.

Од практичен аспект, корисно би било да се развие едноставен кориснички интерфејс за проверка на потврди. Таков интерфејс би им овозможил на корисниците, операторите или ревизорите полесно да проверат дали одредена сесија е правилно евидентирана. Со тоа моделот би станал поразбирлив и попристапен и за лица кои немаат подлабоко техничко познавање од блокчејн технологијата.

Како поширока насока, моделот може да се прошири и кон двонасочно полнење, односно *V2G* сценарија. Во такви услови, сесијата не се однесува само на потрошена енергија, туку и на енергија што може да се врати назад кон мрежата. Затоа, идни проширувања би можеле да опфатат проверка на нето-енергетскиот биланс меѓу возилото, полначот и електроенергетскиот систем.

Во целина, идната работа треба да се насочи кон реална интеграција, пошироко тестирање, подобра заштита на приватноста и поголема практична употребливост. Со такви надградби, предложениот модел *Proof-of-Charge* може да прерасне од истражувачки прототип во посеопфатно решение за доверливи и проверливи процеси во инфраструктурата за полнење електрични возила.

10. ТРУДОВИ ОБЈАВЕНИ ОД ДОКТОРСКАТА ДИСЕРТАЦИЈА

1. SEJFULI-RAMADANI, Nexhibe; IDRIZI, Florim; MISIMI, Verda; RAMADANI, Erenis (2018) BLOCKCHAIN: GENERAL OVERVIEW OF THE ARCHITECTURE, SECURITY AND RELIABILIY. Journal of Natural Sciences and Mathematics of UT, 3 (5-6). pp. 64-68. ISSN 2671-3039

2. SEJFULI-RAMADANI, Nexhibe; RISTESKI, Aleksandar; IDRIZI, Florim; SHEMSHI, Vjollca (2021) REVIEWING THE LATEST TRENDS OF IMPLEMENTING BLOCKCHAIN TECHNOLOGY SOLUTIONS IN SEVERAL BUSINESS-RELATED INDUSTRIES. Journal of Natural Sciences and Mathematics of UT, 6 (11-12). pp. 60-69. ISSN 2671-3039

3. SEJFULI-RAMADANI, Nexhibe; POPOVSKI, Borislav; RISTESKI, Aleksandar (2023) INTEGRATION AND IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGIES IN THE AUTOMOTIVE INDUSTRY. Journal of Natural Sciences and Mathematics, Vol. 8, No. 15-16, 2023. pp.(283-291) ISSN: 2545-4072 (Print), ISSN: 2671-3039 (Online)

4. BAHTIRI, Yllka; BYTYCI, Enkelejda; IDRIZI, Florim; ISMAILI, Shpend; SEJFULI-RAMADANI, Nexhibe (2023) CYBER SECURITY IN EDUCATIONAL INSTITUTIONS. Journal of Natural Sciences and Mathematics, Vol. 8, No. 15-16, 2023. pp.(307-314). ISSN: 2545-4072 (Print), ISSN: 2671-3039 (Online)

5. SEJFULI-RAMADANI, Nexhibe; GJORGJEV, Jelena; ANGELKOVSKA, Valentina; IDRIZI, Florim; PORJAZOSKI, Marko; RISTESKI, Aleksandar. SYSTEM PROPOSAL FOR INTEGRATION OF OFFLINE BLOCKCHAIN PAYMENT MODELS IN FULLY OFFLINE EV AUTHENTICATION AND CHARGING PROCEDURE. 7th International Balkan Conference on Communications and Networking (BalkanCom) 2024, Ljubljana, Slovenia.

6. SEJFULI-RAMADANI, Nexhibe; ANGELKOVSKA, Valentina; GJORGJEV, Jelena; IDRIZI, Florim; LATKOSKI, Pero; RISTESKI, Aleksandar. ADVANCEMENTS AND APPLICATIONS OF BLOCKCHAIN TECHNOLOGY IN DIVERSE DOMAIN: A LITERATURE REVIEW. 2024 13th Mediterranean Conference on Embedded Computing (MECO)

7. SEJFULI-RAMADANI, Nexhibe; IDRIZI, Florim; ANGELKOVSKA, Valentina; RISTESKI, Aleksandar. A COMPARATIVE ANALYSIS OF OFFLINE WALLET AND THEIR INTEGRATION WITH NFC FOR PRACTICAL OFFLINE PAYMENTS. International Congress On Natural, Health Sciences And Technology. 15-17 May, 2024.

8. GJORGJEV, Jelena; SEJFULI-RAMADANI, Nexhibe; ANGELKOVSKA, Valentina, RAKOVIC, Valentin; RISTESKI, Aleksandar. REVIEW OF APPROACHES TO

IMPLEMENT SCIENCE-BASED TARGETS FOR REDUCING CARBON FOOTPRINT IN ICT SECTOR. 2024 IEEE International Humanitarian Technologies Conference, Bari, Italy.

9. GJORGJEV, Jelena; SEJFULI-RAMADANI, Nexhibe; ANGELKOVSKA, Valentina, LATKOSKI, Pero; RISTESKI, Aleksandar. USE CASES AND COMPARATIVE ANALYSIS OF BLOCKCHAIN NETWORKS AND LAYERS FOR DAPP DEVELOPMENT. MECO 2024 &CPSIo T'2024 & SS-CPSIoT;2024, Budva, Montenegro,

10. GJORGJEV, Jelena; SEJFULI-RAMADANI, Nexhibe; ANGELKOVSKA, Valentina, RAKOVIC, Valentin; RISTESKI, Aleksandar. AI STRATEGIES FOR REDUCING CARBON FOOTPRINT IN ICT SECTOR AN EVOLUATION THROUGH THE SCIENCE-BASED TARGETS INITIATIVE. 16TH INTERNATIONAL CONFERENCE ETAI 2024, STRUGA, MACEDONIA.

11. SEJFULI-RAMADANI, Nexhibe; GJORGJEV, Jelena; ANGELKOSKA, Valentina; IDRIZI, Florim; POPOVSKI, Borislav; RISTESKI, Aleksandar. AI-POWEWED X-RAY SCANNING AND BLOCKCHAIN-BASED MANAGEMENT: A SYSTEM FOR CORRUPTION PREVENTION AND SECURE LEGA; ACCOUNTABILITY. Journal of Electrical and Engineering and Information Technologies. Vol. 10, No. 1 (2025), Skopje, North Macedonia. https://jeeit.feit.ukim.edu.mk/index.php/jeeit/article/view/417

12. SEJFULI-RAMADANI, Nexhibe; GJORGJEV, Jelena; ANGELKOSKA, Valentina; RAMADANI, Erenis; IDRIZI, Florim; RISTESKI, Aleksandar. IMMUTABLE AUDIT OF EV CHARGING SESSIONS USING BLOCKCHAIN AND IPFS. 6th International Conference on Communications, Information, Electronic and Energy Systems (CIEES). 26-28 November 2025, Ruse, Bulgaria. DOI: 10.1109/CIEES66347.2025.11300048. https://ieeexplore.ieee.org/document/11300081

13. SEJFULI-RAMADANI, N.; RAMADANI, E.; GJORGJEV, J.; ANGELKOSKA, V.; SHEMSHI, V.; RISTESKI, A. PROOF OF CHARGE: AUDITABLE EV-CHARGING RECEIPTS WITH OFF-CHAIN HASHING AND ON-CHAIN ANCHORS. In Proceedings of the 2026 15th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 9–13 June 2026; IEEE: Piscataway, NJ, USA, 2026. https://doi.org/10.1109/MECO70748.2026.11578972

14. N. SEJFULI - RAMADANI, A. RISTESKI, V. ANGELKOSKA, M. PORJAZOSKI, F. IDRIZI. COST-AWARE BLOCKCHAIN ANCHORING FOR AUDITABLE EV CHARGING RECEIPTS: A BATCH-BASED PROOF-OF-CHARGE EVALUATION. Manuscript submitted for peer review, 2026.

15. SEJFULI-RAMADANI, N.; ANGELKOSKA, V.; IDRIZI, F.; RAKOVIC, V.; RAMADANI, E.; RISTESKI, A. A REPRODUCIBLE BLOCKCHAIN-ANCHORED

PROOF-OF-CHARGE PLATFORM FOR AUDITABLE EV CHARGING RECEIPTS. Future Internet 2026, 18, 423. https://doi.org/10.3390/fi18080423

КОРИСТЕНА ЛИТЕРАТУРА

[1] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, A. Peacock, and T. Morstyn, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 100, pp. 143–174, 2019, doi: 10.1016/j.rser.2018.10.014.

[2] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, 2017, doi: 10.1109/TII.2017.2709784.

[3] N. Sejfuli-Ramadani, B. Popovski, and A. Risteski, "Integration and Implementation of Blockchain Technologies in the Automotive Industry," *Journal of Natural Sciences and Mathematics*, vol. 8, no. 15–16, pp. 283–291, 2023.

[4] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, and C. Douligeris, "Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP)," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1504–1533, 2022, doi: 10.1109/COMST.2022.3184448.

[5] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Computer Science – Research and Development*, vol. 33, no. 1–2, pp. 71–79, 2018, doi: 10.1007/s00450-017-0348-5.

[6] S. Xu, X. Chen, and Y. He, "EVchain: An Anonymous Blockchain-Based System for Charging-Connected Electric Vehicles," *Tsinghua Science and Technology*, vol. 26, no. 6, pp. 845–856, 2021, doi: 10.26599/TST.2020.9010043.

[7] Open Charge Alliance, "Open Charge Point Protocol (OCPP) Specification," official documentation. [Online]. Available: https://www.openchargealliance.org/

[8] EVRoaming Foundation, "Open Charge Point Interface (OCPI)," official documentation. [Online]. Available: https://ocpi-protocol.com/

[9] Y. Wu, C. Zhang, and L. Zhu, "Privacy-Preserving and Traceable Blockchain-Based Charging Payment Scheme for Electric Vehicles," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21254–21265, 2023, doi: 10.1109/JIOT.2023.3283415.

[10] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[11] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[12] N. Sejfuli-Ramadani, V. Angelkoska, J. Gjorgjev, F. Idrizi, P. Latkoski, and A. Risteski, "Advancements and Applications of Blockchain Technology in Diverse Domains: A

Literature Review," in *Proc. Mediterranean Conference on Embedded Computing (MECO)*, 2024, doi: 10.1109/MECO62516.2024.10577865.

[13] J. Gjorgjev, N. Sejfuli-Ramadani, V. Angelkoska, P. Latkoski, and A. Risteski, "Use Cases and Comparative Analysis of Blockchain Networks and Layers for dApp Development," in *Proc. MECO & CPSIoT*, Budva, Montenegro, 2024, doi: 10.1109/MECO62516.2024.10577885.

[14] N. Sejfuli-Ramadani, J. Gjorgjev, V. Angelkoska, F. Idrizi, M. Porjazoski, and A. Risteski, "System Proposal for Integration of Offline Blockchain Payment Models in Fully Offline EV Authentication and Charging Procedure," in *Proc. Balkan Conference on Communications and Networking (BalkanCom)*, Ljubljana, Slovenia, 2024.

[15] N. Sejfuli-Ramadani, J. Gjorgjev, V. Angelkoska, E. Ramadani, F. Idrizi, and A. Risteski, "Immutable Audit of EV Charging Sessions Using Blockchain and IPFS," in *Proc. 6th International Conference on Communications, Information, Electronic and Energy Systems (CIEES)*, Ruse, Bulgaria, 2025, doi: 10.1109/CIEES66347.2025.11300081

[16] N. Sejfuli-Ramadani, J. Gjorgjev, V. Shemshi, E. Ramadani, V. Angelkoska, and A. Risteski, "Proof-of-Charge: Auditable EV-Charging Receipts with Off-Chain Hashing and On-Chain Anchors," in *Proc. 15th Mediterranean Conference on Embedded Computing (MECO)*, Budva, Montenegro, 2026. Doi:

[17] R. C. Merkle, "Protocols for public key cryptosystems," in *Proc. IEEE Symposium on Security and Privacy*, 1980, pp. 122–134, doi: 10.1109/SP.1980.10006.

[18] C. Pop, T. Cioara, I. Anghel, M. Antal, and I. Salomie, "Blockchain-Based Scalable and Tamper-Evident Solution for Registering Energy Data," *Sensors*, vol. 19, no. 14, Art. no. 3033, 2019, doi: 10.3390/s19143033.

[19] A. Aldweesh and S. Alangari, "Privacy-Preserving EV Charging Authorization and Billing via Blockchain and Homomorphic Encryption," *World Electric Vehicle Journal*, vol. 16, no. 8, Art. no. 468, 2025, doi: 10.3390/wevj16080468.

[20] M. Danish et al., "A Blockchain-Based Privacy-Preserving Charging Station Reservation and Payment Scheme for Electric Vehicles," *ACM Transactions on Internet Technology*, 2025, doi: 10.1145/3696428.

[21] J. Johnson, J. Berg, B. Anderson, and B. Wright, "Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses," *Energies*, vol. 15, no. 11, Art. no. 3931, 2022, doi: 10.3390/en15113931.

[22] National Institute of Standards and Technology, "Secure Hash Standard (SHS)," FIPS PUB 180-4, 2015, doi: 10.6028/NIST.FIPS.180-4.

[23] S. Haber and W. S. Stornetta, "How to Time-Stamp a Digital Document," *Journal of Cryptology*, vol. 3, no. 2, pp. 99–111, 1991, doi: 10.1007/BF00196791.

[24] B. Laurie, A. Langley, and E. Kasper, "Certificate Transparency," RFC 6962, 2013.

[25] J. Benaloh and M. de Mare, “One-Way Accumulators: A Decentralized Alternative to Digital Signatures,” in *Advances in Cryptology — EUROCRYPT ’93*, 1993, pp. 274–285, doi: 10.1007/3-540-48285-7_24.

[26] R. C. Merkle, “A Digital Signature Based on a Conventional Encryption Function,” in *Advances in Cryptology — CRYPTO ’87*, Lecture Notes in Computer Science, vol. 293, Springer, 1988, pp. 369–378, doi: 10.1007/3-540-48184-2_32.

[27] M. Bellare and P. Rogaway, “Collision-Resistant Hashing: Towards Making UOWHFs Practical,” in *Advances in Cryptology — CRYPTO ’97*, Lecture Notes in Computer Science, vol. 1294, Springer, 1997, pp. 470–484, doi: 10.1007/BFb0052253.

[28] V. Buterin, “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,” White Paper, 2014.

[29] J. Benet, “IPFS - Content Addressed, Versioned, P2P File System,” arXiv:1407.3561, 2014.

[30] B. Schneier and J. Kelsey, “Secure Audit Logs to Support Computer Forensics,” *ACM Transactions on Information and System Security*, vol. 2, no. 2, pp. 159–176, 1999, doi: 10.1145/317087.317089.

[31] S. A. Crosby and D. S. Wallach, “Efficient Data Structures for Tamper-Evident Logging,” in *Proc. 18th USENIX Security Symposium*, Montreal, QC, Canada, 2009, pp. 317–334.

[32] ISO, “ISO 15118-1:2019 Road vehicles — Vehicle to grid communication interface — Part 1: General information and use-case definition,” International Organization for Standardization, 2019.

[33] R. Valdés et al., “Assessment of the potential for edge computing to support smart charging of electric vehicles,” FLOW Project Deliverable D4.4, 2021.

[34] IEC, “IEC 61851-1:2017 Electric vehicle conductive charging system — Part 1: General requirements,” International Electrotechnical Commission, 2017.

[35] IEC, “IEC 63110-1:2022 Protocol for management of electric vehicles charging and discharging infrastructures — Part 1: Basic definitions, use cases and architectures,” International Electrotechnical Commission, 2022.

[36] National Institute of Standards and Technology, “Guidelines for Smart Grid Cybersecurity,” *NISTIR 7628 Rev. 1*, 2014, doi: 10.6028/NIST.IR.7628r1.

[37] National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” *NIST Cybersecurity White Paper 29*, 2024, doi: 10.6028/NIST.CSWP.29.

[38] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” *NIST Special Publication 800-207*, 2020, doi: 10.6028/NIST.SP.800-207.

[39] R. Metere, Z. Pourmirza, S. Walker, and M. Neaimeh, “An Overview of Cyber Security and Privacy on the Electric Vehicle Charging Infrastructure,” arXiv:2209.07842, 2022.

[40] A. M. Antonopoulos and G. Wood, Mastering Ethereum: Building Smart Contracts and DApps. Sebastopol, CA, USA: O'Reilly Media, 2018.-

[41] G. A. Oliva, A. E. Hassan, and Z. M. Jiang, "An Exploratory Study of Smart Contracts in the Ethereum Blockchain Platform," *Empirical Software Engineering*, vol. 25, no. 3, pp. 1864–1904, 2020, doi: 10.1007/s10664-019-09796-5.

[42] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[43] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, 2019.

[44] M. Aoudia, M. B. M. Alaraj, O. Abu Waraga, T. Mokhamed, M. Abu Talib, M. Bettayeb, Q. Nasir, and C. Ghenai, "Toward Better Blockchain-Enabled Energy Trading Between Electric Vehicles and Smart Grids in Internet of Things Environments: A Survey," Frontiers in Energy Research, vol. 12, Art. no. 1393084, 2024, doi: 10.3389/fenrg.2024.1393084.

[45] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing microgrid energy markets: A case study: The Brooklyn Microgrid," Applied Energy, vol. 210, pp. 870–880, 2018.

[46] M. J. Dworkin, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," NIST FIPS PUB 202, National Institute of Standards and Technology, 2015, doi: 10.6028/NIST.FIPS.202.

[47] National Institute of Standards and Technology, "Digital Signature Standard (DSS)," FIPS PUB 186-5, 2023, doi: 10.6028/NIST.FIPS.186-5.

[48] M. Szydlo, "Merkle Tree Traversal in Log Space and Time," in Advances in Cryptology—EUROCRYPT 2004, Lecture Notes in Computer Science, vol. 3027, pp. 541–554, Springer, 2004, doi: 10.1007/978-3-540-24676-3_32.

[49] E. Barker, "Recommendation for Key Management: Part 1 – General," NIST Special Publication 800-57 Part 1 Revision 5, National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-57pt1r5.

[50] T. P. Pedersen, "Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing," in Advances in Cryptology — CRYPTO '91, Lecture Notes in Computer Science, vol. 576, pp. 129–140, Springer, 1992, doi: 10.1007/3-540-46766-1_9.

[51] Protocol Labs, "Filecoin: A Decentralized Storage Network," 2017.

[52] E. Daniel and F. Tschorsch, "IPFS and Friends: A Qualitative Comparison of Next Generation Peer-to-Peer Data Networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 31–52, 2022.

[53] D. Trautwein et al., “Design and Evaluation of IPFS: A Storage Layer for the Decentralized Web,” in *Proc. ACM SIGCOMM 2022 Conference*, pp. 739–752, 2022, doi: 10.1145/3544216.3544232.

[54] C. Rahalkar and D. Gujar, “Content Addressed P2P File System for the Web with Blockchain-Based Meta-Data Integrity,” arXiv:1912.10298, 2019.

[55] K. Croman et al., “On Scaling Decentralized Blockchains,” in *Financial Cryptography and Data Security*, LNCS, vol. 9604, pp. 106–125, Springer, 2016, doi: 10.1007/978-3-662-53357-4_8.

[56] E. Androulaki et al., “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains,” in *Proc. 13th EuroSys Conference*, 2018, pp. 1–15, doi: 10.1145/3190508.3190538.

[57] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts,” in *Proc. IEEE Symposium on Security and Privacy*, 2016, pp. 839–858, doi: 10.1109/SP.2016.55.

[58] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, “SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies,” in *Proc. IEEE Symposium on Security and Privacy*, 2015, pp. 104–121, doi: 10.1109/SP.2015.14.

[59] M. B. Mollah et al., “Blockchain for Future Smart Grid: A Comprehensive Survey,” *IEEE Internet of Things Journal*, 2021.

[60] A. Laszka, A. Dubey, M. Walker, and D. Schmidt, “Providing Privacy, Safety, and Security in IoT-Based Transactive Energy Systems using Distributed Ledgers,” in *Proc. 7th International Conference on Internet of Things*, 2017, Article 13, doi: 10.1145/3131542.3131562.

[61] S. Rouhani and R. Deters, “Security, Performance, and Applications of Smart Contracts: A Systematic Survey,” IEEE Access, vol. 7, pp. 50759–50779, 2019, doi: 10.1109/ACCESS.2019.2911031.

[62] P. Tolmach, Y. Li, S.-W. Lin, Y. Liu, and Z. Li, “A Survey of Smart Contract Formal Specification and Verification,” ACM Computing Surveys, vol. 54, no. 7, pp. 1–38, 2021, doi: 10.1145/3464421.

[63] H. Chen et al., “A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses,” ACM Computing Surveys, vol. 53, no. 3, pp. 1–43, 2020, doi: 10.1145/3391195.

[64] N. Atzei, M. Bartoletti, and T. Cimoli, “A Survey of Attacks on Ethereum Smart Contracts (SoK),” in Principles of Security and Trust, LNCS, vol. 10204, pp. 164–186, Springer, 2017, doi: 10.1007/978-3-662-54455-6_8.

[65] Z. A. Khan and A. S. Namin, “A Survey on Vulnerabilities of Ethereum Smart Contracts,” arXiv:2012.14481, 2020.

[66] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” Ethereum Yellow Paper, 2014. Available: Ethereum Foundation / Ethereum Yellow Paper repository.

[67] C. Li, B. Palanisamy, R. Xu, J. Wang, L. Xu, and Y. Tang, “Gas Estimation and Optimization for Smart Contracts on Ethereum,” in *Proc. 36th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, 2021, pp. 1082–1086, doi: 10.1109/ASE51524.2021.9678932.

[68] A. Di Sorbo, S. Laudanna, A. Vacca, C. A. Visaggio, and G. Canfora, “Profiling Gas Consumption in Solidity Smart Contracts,” arXiv:2008.05449, 2020.

[69] Ethereum Foundation, “The Merge,” Ethereum.org.

[70] P. W. Khan and Y.-C. Byun, “Blockchain-Based Peer-to-Peer Energy Trading and Charging Payment System for Electric Vehicles,” *Sustainability*, vol. 13, no. 14, Art. no. 7962, 2021, doi: 10.3390/su13147962.

[71] T. Alladi, V. Chamola, J. J. P. C. Rodrigues, and S. A. Kozlov, “Blockchain in Smart Grids: A Review on Different Use Cases,” *Sensors*, vol. 19, no. 22, Art. no. 4862, 2019, doi: 10.3390/s19224862.

[72] M. K. Hasan, A. Alkhalifah, S. Islam, N. B. M. Babiker, A. K. M. A. Habib, A. H. M. Aman, and M. A. Hossain, “Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations,” Wireless Communications and Mobile Computing, vol. 2022, Art. no. 9065768, 2022, doi: 10.1155/2022/9065768.

[73] A. Jindal, G. S. Aujla, N. Kumar, and M. Villari, “GUARDIAN: Blockchain-Based Secure Demand Response Management in Smart Grid System,” IEEE Transactions on Services Computing, vol. 13, no. 4, pp. 613–624, 2020, doi: 10.1109/TSC.2019.2962677.

[74] C. Liu, K. K. Chai, E. T. Lau, and Y. Chen, “Blockchain Based Energy Trading Model for Electric Vehicle Charging Schemes,” in *Smart Grid and Innovative Frontiers in Telecommunications*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 203, pp. 64–72, Springer, 2018, doi: 10.1007/978-3-319-94965-9_7.

[75] J. C. Olivares-Rojas, E. Reyes-Archundia, J. A. Gutiérrez-Gnecchi, and I. Molina-Moreno, “A Survey on Smart Metering Systems Using Blockchain for E-Mobility,” arXiv:2009.09075, 2020.

[76] H. T. Doan, J. Cho, and D. Kim, “Peer-to-Peer Energy Trading in Smart Grid Through Blockchain: A Double Auction-Based Game Theoretic Approach,” *IEEE Access*, vol. 9, pp. 49206–49218, 2021, doi: 10.1109/ACCESS.2021.3068730.

[77] A. Sadiq, M. U. Javed, R. Khalid, A. Almogren, M. Shafiq, and N. Javaid, “Blockchain Based Data and Energy Trading in Internet of Electric Vehicles,” IEEE Access, vol. 9, pp. 7000–7020, 2021, doi: 10.1109/ACCESS.2020.3048169.

[78] M. Chase and S. Meiklejohn, “Transparency Overlays and Applications,” in Proc. 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS), Vienna, Austria, 2016, pp. 168–179, doi: 10.1145/2976749.2978404.

[79] M. S. Melara, A. Blankstein, J. Bonneau, E. W. Felten, and M. J. Freedman, “CONIKS: Bringing Key Transparency to End Users,” in Proc. 24th USENIX Security Symposium, 2015, pp. 383–398.

[80] R. T. Snodgrass, S. S. Yao, and C. S. Collberg, “Tamper Detection in Audit Logs,” in Proceedings of the 30th International Conference on Very Large Data Bases (VLDB), Toronto, Canada, 2004, pp. 504–515, doi: 10.1016/B978-012088469-8.50046-2.

[81] A. Ahmad, M. Saad, and A. Mohaisen, “BlockAudit: A Scalable and Tamper-Proof Blockchain-Based Audit System,” arXiv:1907.10484, 2019.

[82] B. Laurie, E. Messeri, and R. Stradling, “Certificate Transparency Version 2.0,” RFC 9162, 2021.

[83] M. Gerhards and B. Pehrson, “Signed Syslog Messages,” RFC 5848, 2010.

[84] Google, “Trillian: Verifiable Data Structures,” Transparency.dev. [Online]. Available: https://transparency.dev/verifiable-data-structures/. Accessed: Jun. 8, 2026.

[85] C. Regueiro, I. Seco, J. E. Muñoz, and J. A. Álvarez, “A Blockchain-Based Audit Trail Mechanism: Design and Implementation,” Algorithms, vol. 14, no. 12, Art. no. 341, 2021, doi: 10.3390/a14120341.

[86] Sejfuli-Ramadani, N.; Angelkoska, V.; Idrizi, F.; Rakovic, V.; Ramadani, E.; Risteski, A. A Reproducible Blockchain-Anchored Proof-of-Charge Platform for Auditable EV Charging Receipts. *Future Internet* 2026, **18**, 423. https://doi.org/10.3390/fi18080423

[87] N. Sejfuli-Ramadani, A. Risteski, V. Angelkoska, M. Porjazoski, and F. Idrizi, “Cost-Aware Blockchain Anchoring for Auditable EV Charging Receipts: A Batch-Based Proof-of-Charge Evaluation,” manuscript submitted for peer review, 2026.

[88] Python Software Foundation, “hashlib — Secure hashes and message digests,” Python 3 Documentation. [Online]. Accessed: Jun. 11, 2026.

[89] S. Ramírez, “FastAPI Documentation,” FastAPI. [Online]. Accessed: Jun. 11, 2026.

[90] Paradigm, “Cast: Command-line Ethereum RPC tool,” Foundry Documentation. [Online]. Available: https://www.getfoundry.sh/cast. Accessed: Jun. 11, 2026.

[91] Paradigm, “Foundry: Ethereum Development Framework,” Foundry Documentation. [Online]. Accessed: Jun. 11, 2026.

[92] Paradigm, “Anvil Reference,” Foundry Documentation. [Online]. Accessed: Jun. 11, 2026.

[93] Solidity Team, “Solidity Documentation.” [Online]. Accessed: Jun. 11, 2026.

[94] Ethereum Foundation, “JSON-RPC API,” Ethereum Developer Documentation. [Online]. Accessed: Jun. 11, 2026.

[95] T. Bray, Ed., “The JavaScript Object Notation (JSON) Data Interchange Format,” RFC 8259, Dec. 2017, doi: 10.17487/RFC8259.

[96] A. Rundgren, B. Jordan, and S. Erdtman, “JSON Canonicalization Scheme (JCS),” RFC 8785, Jun. 2020, doi: 10.17487/RFC8785.

[97] A. Y. Shafranovich, Ed., “JSON Type Definition,” RFC 8927, Nov. 2020, doi: 10.17487/RFC8927.

[98] OpenAPI Initiative, “OpenAPI Specification,” ver. 3.1.1, Oct. 2024. [Online]. Accessed: Jun. 11, 2026.

[99] Pydantic Services Inc., “Pydantic Documentation,” ver. 2. [Online]. Accessed: Jun. 11, 2026.

[100] PostgreSQL Global Development Group, “JSON Types” and “JSON Functions and Operators,” PostgreSQL 18 Documentation. [Online]. Available: PostgreSQL Documentation. Accessed: Jun. 11, 2026.

[101] OWASP Foundation, “OWASP Smart Contract Top 10: 2026,” 2026. [Online]. Accessed: Jun. 11, 2026.

[102] ISO/IEC 25010:2023, Systems and Software Engineering—Systems and Software Quality Requirements and Evaluation (SQuaRE)—Product Quality Model. Geneva, Switzerland: International Organization for Standardization, 2023.

[103] ISO/IEC/IEEE 29119-1:2022, Software and Systems Engineering—Software Testing—Part 1: General Concepts. Geneva, Switzerland: International Organization for Standardization, 2022.

[104] R. Jain, The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling. New York, NY, USA: John Wiley & Sons, 1991.

[105] D. J. Lilja, Measuring Computer Performance: A Practitioner’s Guide. Cambridge, U.K.: Cambridge University Press, 2000.