



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



Јован Карамачоски

ОПТИМИЗАЦИЈА НА ЈАВЕН ЗДРАВСТВЕН СИСТЕМ БАЗИРАН НА BLOCKCHAIN ТЕХНОЛОГИЈА

Докторски труд

Скопје, 2022

Докторанд:

Јован Карамачоски

Тема:

Оптимизација на протоколи во телекомуникациите – поле на примена телемедицина

Ментор:

Проф. д-р Лилјана Гавриловска,

Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за Електротехника и Информациони Технологии

Комисија за одбрана:

Проф. д-р Александар Ристески, претседател

Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за Електротехника и Информациони Технологии

Проф. д-р Лилјана Гавриловска, ментор

Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за Електротехника и Информациони Технологии

Проф. д-р Тони Јаневски, член

Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за Електротехника и Информациони Технологии

Проф. д-р Перо Латкоски, член

Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за Електротехника и Информациони Технологии

Вонр. проф. д-р Валентин Раковиќ, член

Универзитет „Св. Кирил и Методиј“ во Скопје, Факултет за Електротехника и Информациони Технологии

Научна област:

Телекомуникациско инженерство

Датум на одбрана:

ОПТИМИЗАЦИЈА НА ЈАВЕН ЗДРАВСТВЕН СИСТЕМ БАЗИРАН НА BLOCKCHAIN ТЕХНОЛОГИЈА

– А п с т р а к т –

Присутноста на Blockchain технологиите во различни сегменти од животот на луѓето, преку широк спектар на апликации, ја потврдува нивната универзалност и високата доверливост. Двоеценискиот развој на Blockchain технологиите и зголемената имплементација во индустријата, здравството, транспортните системи и управувањето со пристапот, го покажуваат нивниот капацитет за овозможување доверливи сервиси со висока достапност во присуство на недоверливи и малициозни корисници. Успехот на Blockchain технологиите се должи на користењето на едноставни криптографски механизми кои, во спој со соодветен консензус механизам, овозможуваат долготрајност на записите, сеприсутност на записите, неможност за промена или бришење и неможност за одрекување на било каква активност во системот.

Многубројните сервиси кои се нудат преку Интернет и се почестите проблеми кои се појавуваат со злоупотребата на приватните податоци даваат простор за развој на механизми за заштита на личните податоци. Особено чувствителни се податоците кои циркулираат во здравствените системи што претставува предизвик за дефинирање на систем кој ќе овозможи управување со личните здравствени записи од страна на пациентите. Blockchain технологијата има потенцијал да овозможи решение за проблемите со приватноста.

Спроведената анализа на перформансите за тековните Blockchain технологии ја издвојуваат Tendermint Blockchain технологијата како најнадежна Blockchain технологија за јавни здравствени системи. За таа цел, во емулирана мрежа на валидатори е спроведена темелна и обемна анализа на максималниот капацитет на Tendermint консензус механизмот и на неговиот потенцијал да опслужи глобален здравствен систем. Заклучокот од анализата на перформансите укажува на потребата за дефинирање на дедицирано решение со поголемо ниво на скалабилност, со цел да послужи како глобален здравствен систем базиран на Blockchain технологија.

Во рамките на оваа дисертација се дефинирани BloHeS системската архитектура и соодветниот BloHeS консензус механизам кои се дел од дедицираното решение за Blockchain базиран јавен здравствен систем. BloHeS консензус механизмот има повеќенивова организација за постигнување на консензус и е оптимизиран за сообраќајните карактеристики на јавните здравствени системи. Овој консензус механизам има значително подобрена комуникациска комплексност и асимптотски се доближува до капацитетот на заштита кој го постигнува Tendermint консензус механизмот. Ова допринесува кон зголемена скалабилност на BloHeS системот, со незначително намалување на безбедноста што ја обезбедува консензус механизмот.

Повеќенивовската организација на BloHeS консензус механизмот се постигнува со кластерирање. Валидаторите во мрежата се поделени во два домени: единичен архивски кластер од повисоко ниво и повеќе независни и само-организирачки острови од пониско ниво. Островите се организирани во непреклопени кластери со помош на само-организациски протоколи за управување на острови, воведени во рамките на оваа дисертација. Дополнително, BloHeS системот воведува подобрување во организацијата на складирање на податоци при што значително помал складишен простор се користи кај агентите на пациентите, споредено со традиционалното организирање на складирањето на податоци кај класичните Blockchain технологии. Овој систем исто така овозможува пациент-центрична контрола на привилегиите за пристап до личните податоци на пациентот. Тоа значи дека пациентот има можност да управува кој и какви привилегии има за да пишува или чита податоци од неговото лично здравствено досие. Овој пристап прави BloHeS концептот да биде усогласен со GDPR и HIPAA стандардите за заштита на лични податоци.

Со новиот пристап за управување со лични податоци, може да се развијат нови бизнис решенија кои ќе им овозможат на осигурителните компании и фармацевтските компании да понудат нови производи. Користењето на стандардизиран формат за електронски здравствени записи ќе овозможи употреба на алгоритми со Вештачка интелигенција за попрецизна дијагностика на болести, подобра ефикасност на лековите и подобрување на здравствената состојба на популацијата.

Клучни зборови: Оптимизација, архитектура, телемедицина, здравствен систем, Blockchain технологија, Tendermint, консензус механизам, BloHeS систем

OPTIMIZATION OF A PUBLIC HEALTHCARE SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY

– Abstract –

The presence of Blockchain technologies in different segments of people's lives, within a wide spectrum of applications, confirms their universality and high reliability. Two decades of development of Blockchain technologies and increased implementation in industry, healthcare, transport systems and access management, show their capability of delivering reliable services with high availability in presence of trustless and malicious users. The success of the Blockchain technologies is due to the implementation of simple cryptographic mechanisms, in conjunction with appropriate consensus mechanism, enables durability of the records, omnipresence of the records, impossibility of modification or deletion, and impossibility of repudiation of any activity in the system.

The numerous services offered through the Internet and more frequent problems arising with misuse of personal data give room for development of mechanisms for protection of personal data. Especially sensitive are the data that circulate in the healthcare systems, which poses a challenge to define a system that will enable management of personal healthcare records by the patients themselves. The Blockchain technology is considered as a potential solution provider for privacy problems.

The conducted performance analysis of the current Blockchain technologies highlights the Tendermint Blockchain technology as the most promising Blockchain technology for a public healthcare system. For that reason, in an emulated network of validators it is conducted a thorough and extended analysis of the maximal capacity of the Tendermint consensus mechanism and its potential to serve a global healthcare system. The conclusion from the performance analysis suggests that it needs a definition of a dedicated solution with a higher level of scalability in order to serve a global healthcare system based on Blockchain technology.

This dissertation defines the BloHeS system architecture and the corresponding BloHeS consensus mechanism, which are part of the dedicated solution for a Blockchain-based public healthcare system. The BloHeS consensus mechanism has a multi-level organization for consensus achievement, optimized to the traffic characteristics of the public healthcare systems. This consensus mechanism has significantly better communication complexity and asymptotically approaches the protection capacity achieved by the Tendermint consensus mechanism. This contributes to the increased scalability of the BloHeS system with an insignificant drop in the security provided by the consensus mechanism.

The multi-level organization of the BloHeS consensus mechanism is achieved by clustering. The validators in the network are divided into two domains: the single higher-level Archiving cluster, and multiple independent and self-organized lower-level Islands. The Islands are organized in disjoint clusters using self-organizing Island management protocols, introduced in this dissertation. Furthermore, the BloHeS system introduces an improvement of the storage organization where significantly less storage is used in the patient agents, compared to the traditional storage organization of the classical Blockchain technologies. This system also enables patient-centric control of the privileges for access personal data of the patients. This means that it will enable the patients to manage who and what privileges will have to write or read data from their personal healthcare files. This approach makes BloHeS concept to be compliant with the GDPR and HIPAA standards for personal data protection.

The new approach for managing personal data enables development of new business solutions that will allow insurance companies and pharmaceutical companies to offer new products. The usage of standardized electronic healthcare records format will enable implementation of Artificial intelligence algorithms for more precise diagnostics of illnesses, better efficacy of medications and improvement of the general population health condition.

Keywords: Optimization, architecture, telemedicine, healthcare system, Blockchain technology, Tendermint, consensus mechanism, BloHeS system

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	9
Листа на табели	11
Листа на кратенки	12
1. Вовед	13
1.1. Мотивација за изработка на докторската дисертација	15
1.2. Предмет на истражување и хипотеза	15
1.3. Цели и придобивки од истражувањето	16
1.4. Структура на докторската дисертација	17
2. Јавни здравствени системи – карактеристики и предизвици, генерации на јавни здравствени системи, рамка за јавен здравствен систем базиран на Blockchain технологија	19
2.1. Прва генерација на е-здравствени системи	20
2.2. Втора генерација на е-здравствени системи	20
2.3. Трета генерација на е-здравствени системи	21
2.4. Четврта генерација на е-здравствени системи	22
2.4.1. Рамка за четвртата генерација е-здравствени системи	24
2.4.2. Специфики на четвртата генерација е-здравствени системи	25
3. Blockchain – историја, технички карактеристики, предности и недостатоци	28
3.1. Типови на Blockchain технологии	29
3.2. Blockchain дистрибуирана мрежа	31
3.3. Blockchain податочна структура	32
3.4. Консензус механизам	34
3.4.1. Proof-of-Work и Proof-of-Elapsed-Time (PoW без рударење)	35
3.4.2. Proof-of-Stake и негови варијанти	37
3.4.3. Practical Byzantine Fault Tolerant	38
3.4.4. Tendermint	39
3.4.5. Swirlds Hashgraph	41
3.4.6. Tangle	43
3.4.7. Споредба на консензус механизмите	43
3.5. Најпознати Blockchain технологии и споредба на нивните карактеристики	45
3.5.1. Bitcoin	45
3.5.2. Ethereum	46
3.5.3. Cosmos	47
3.5.4. Hedera Hashgraph	48

3.5.5.	IOTA	49
3.5.6.	Hyperledger	49
3.5.7.	Споредба на карактеристиките на Blockchain технологиите	50
4.	Евалуација на подобноста на Tendermint консензус механизмот како основа за следната генерација јавни здравствени системи базирани на Blockchain технологии...	53
4.1.	Емулациска околина за анализа на перформансите на Tendermint.....	54
4.2.	Основни емулациски резултати	56
4.2.1.	Проток на трансакции во Tendermint мрежата за основни конфигурациски поставки.....	56
4.2.2.	Влијание на конективноста, предавателната и приемната брзина врз протокот на трансакции	57
4.2.3.	Влијание на големината на трансакциите врз протокот на трансакции	59
4.2.4.	Влијание на големината на пакетот со трансакции врз протокот на трансакции.....	61
4.2.5.	Влијание на интервалот за предлагање на трансакции врз протокот на трансакции.....	62
4.2.6.	Влијание на делта интервалот за предлагање на пакети, делта интервалот за пред-гласање и делта интервалот за пред-извршување врз протокот на трансакции.....	63
4.2.7.	Влијание на периодот на испраќање на група од трансакции врз протокот на трансакции	64
4.2.8.	Влијание на латентноста во мрежата врз протокот на трансакции	64
4.2.9.	Влијание на пакетските загуби врз протокот на трансакции	68
4.2.10.	Заклучок за влијанието на конфигурациските поставки врз протокот на трансакции.....	69
4.3.	Перформанси на Tendermint консензус механизмот за големи документи.....	69
4.4.	Естимација на покриеност на пациенти.....	73
5.	Blockchain технологија за јавен здравствен систем – BloHeS	75
5.1.	Архитектура на BloHeS системот	76
5.2.	BloHeS консензус механизам	78
5.2.1.	Дијаграм на размена на пораки кај Tendermint и BloHeS консензус механизмите	80
5.2.2.	Капацитет на заштита	83
5.2.3.	Евалуација на перформанси	84
5.2.4.	Предности и недостатоци на BloHeS консензус механизмот	87
5.3.	Организација на складирањето на податоците во BloHeS системот	88
5.3.1.	Структура на Личен Blockchain поток и организација на базата на податоци за пациентите и заедничката база на податоци.....	88

5.3.2. Анализа на скалабилноста на складирањето податоци	93
5.4. Податочна блок структура.....	99
5.5. Протоколи за управување со островите.....	101
5.5.1. Детекција на валидатори	102
5.5.2. Додавање на нови валидатори во остров	104
5.5.3. Делење на остров	105
5.5.4. Спојување на остров	107
5.5.5. Предности и недостатоци на протоколите за управување со острови.....	107
5.6. Личен трезор и паричник.....	108
5.7. Процедура за контрола на пристап до личните податоци.....	109
5.8. Усогласеност со GDPR и HIPAA регулативите.....	110
Заклучок	112
Користена литература.....	115
Листа на изработени трудови	121

ЛИСТА НА СЛИКИ

Слика 2.1. Симплифициран приказ на првата генерација на е-здравствени системи	20
Слика 2.2. Симплифициран приказ на втората генерација на е-здравствени системи ..	21
Слика 2.3. Симплифициран приказ на третата генерација на е-здравствени системи...	22
Слика 2.4. Симплифициран приказ на комуникациска процедура за основно корисничко сценарио кај четвртата генерација на е-здравствени системи	23
Слика 2.5. Симплифициран приказ на комуникациски процедури за специфични кориснички сценарија кај четвртата генерација на е-здравствени системи	24
Слика 2.6. Нивовска структура на четвртата генерација на е-здравствени системи.....	24
Слика 3.1. Структура на Blockchain базата на податоци	33
Слика 3.2. Merkle дрво	33
Слика 3.3. Процедура за решавање на сложувалката кај PoW консензус механизмот ..	36
Слика 3.4. Една рунда од процесот на гласање кај Tendermint консензус механизам ...	40
Слика 3.5. Временска линија од Swirlds Hashgraph консензус механизмот	42
Слика 3.6. Tangle консензус механизмот	43
Слика 3.7. Рамковна структура на Cosmos апликација базирана на Tendermint консензус механизмот.....	48
Слика 4.1. Основна конфигурација	57
Слика 4.2. Проток на трансакции за влезни и излезни соработници еднакви на 5	58
Слика 4.3. Проток на трансакции за влезни и излезни соработници еднакви на 5, предавателна и приемна брзина еднаква на 1024000B/s	59
Слика 4.4. Проток на трансакции за влезни и излезни соработници еднакви на 65, предавателна и приемна брзина еднаква на 1024000B/s	59
Слика 4.5. Проток на трансакции за големина на трансакција од 1KB	60
Слика 4.6. Проток на трансакции за големина на трансакција од 100KB	60
Слика 4.7. Проток на трансакции за големина на трансакција од 1MB.....	61
Слика 4.8. Проток на трансакции за големина на трансакција од 5MB.....	61
Слика 4.9. Проток на трансакции за максимална големина на пакет од 4096B	62
Слика 4.10. Проток на трансакции за интервал за предлагање пакети еднаков на 1s....	63
Слика 4.11. Проток на трансакции за интервал за предлагање пакети еднаков на 5s....	63
Слика 4.12. Проток на трансакции за делта интервал на предлагање пакети 0ms, делта интервал на пред-гласање 0ms, делта интервал на пред-извршување 0ms.....	64
Слика 4.13. Проток на трансакции за интервал на група од трансакции поставен на 10s	65
Слика 4.14. Проток на трансакции за мрежна латентност од 20ms	65
Слика 4.15. Проток на трансакции за мрежна латентност од 50ms	66
Слика 4.16. Проток на трансакции за мрежна латентност од 100ms	66
Слика 4.17. Проток на трансакции за мрежна латентност од 200ms	67
Слика 4.18. Проток на трансакции за мрежна латентност со случајни вредности со униформна распределба во интервал [0ms, 300ms]	67
Слика 4.19. Проток на трансакции за поставки на пакетски загуби од 10%	68
Слика 4.20. Проток на трансакции за поставки на пакетски загуби од 20%	68
Слика 5.1. BloHeS мрежна организација.....	77
Слика 5.2. BloHeS консензус механизам.....	79
Слика 5.3. Нивовска организација на BloHeS системот.....	79
Слика 5.4. Временска линија на BloHeS консензус механизмот	80

Слика 5.5. Дијаграм на размена на пораки кај Tendermint консензус механизмот	81
Слика 5.6. Дијаграм на размена на пораки кај BloHeS консензус механизмот	82
Слика 5.7. Споредба на број на разменети пораки кај Tendermint и BloHeS консензус механизмот	85
Слика 5.8. Споредба на капацитет на заштита помеѓу Tendermint и BloHeS консензус механизмите	86
Слика 5.9. Споредба на односот разменети пораки/капацитет на заштита кај Tendermint и BloHeS консензус механизмот	87
Слика 5.10. Структура на PBS	90
Слика 5.11. База на пациенти	91
Слика 5.12. Заедничка база на податоци, островска база на податоци и федерална база на податоци	92
Слика 5.13. Вкупен зафатен складишен простор за цела здравствена мрежа	96
Слика 5.14. Вкупен зафатен складишен простор кај пациентот	97
Слика 5.15. Вкупен зафатен складишен простор кај здравствениот работник	97
Слика 5.16. Вкупен зафатен складишен простор кај владиниот агент	98
Слика 5.17. Блок структура на островскиот консензус механизам.....	100
Слика 5.18. Блок структура на архивскиот консензус механизам	101
Слика 5.19. Протокол за додавање на јазол	105
Слика 5.20. Протокол за делење на остров	106
Слика 5.21. Протокол за спојување на остров	107
Слика 5.22. Личен трезор.....	109
Слика 5.23. Процедура за контрола на пристап.....	110

ЛИСТА НА ТАБЕЛИ

Табела 3.1. Разлика помеѓу јавните, приватните и конзорциум Blockchain системите .	31
Табела 3.2. Споредба на карактеристики помеѓу консензус механизмите.....	44
Табела 3.3. Споредба на карактеристиките на Blockchain технологиите	51
Табела 4.1. Карактеристики на сообраќајот кај општа Tendermint апликација и јавен здравствен систем	54
Табела 4.2. Симулациски параметри, нивните основни вредности и краток опис.....	56
Табела 4.3. Сценарија за големина на трансакција.....	70
Табела 4.4. Просечен проток на трансакции за различни големини на трансакции и различна брзина на генерирање на трансакции поголема од 128 трансакции во секунда	71
Табела 4.5. Коефициент на ефикасност за различни големини на трансакции и различна брзина на генерирање на трансакции поголема од 128 трансакции во секунда.....	71
Табела 4.6. Просечен проток на трансакции за различни големини на трансакции и различна брзина на генерирање на трансакции помала од 64 трансакции во секунда ..	73
Табела 4.7. Коефициент на ефикасност за различни големини на трансакции и различна брзина на генерирање на трансакции помала од 64 трансакции во секунда	73
Табела 4.8. Покриеност на пациенти.....	74
Табела 5.1. Симулациски параметри.....	95
Табела 5.2. Споредба на големината на Blockchain базата на податоци за период од 1 и 10 години за мрежа од 10^6 и 10^9 пациенти во класична и BloHeS архитектура	99

ЛИСТА НА КРАТЕКИ

ABCI – Application BlockChain Interface

BaaS – Blockchain-as-a-Servis

BFT – Byzantine Fault Tolerance

BloHeS – Blockchain Healthcare System

CDS – Common Database Storage

DAG – Directed Acyclic Graph

DAO – Decentralized Autonomous Organization

DHT – Distributed Hash Table

DoS – Denial of Service

EHR – Electronic Healthcare Record

EVM – Ethereum Virtual Machine

GDPR – General Data Protection Regulation

HIPAA – Health Insurance Portability and Accountability Act

IBC – Inter-Blockchain Communication

IoT – Internet of Things

IPFS – InterPlanetary File System

P2P – Peer-to-peer

PBFT – Practical Byzantine Fault Tolerance

PBS – Personal Blockchain Stream

PoA – Proof-of-Authority

PoET – Proof-of-Elapsed-Time

PoS – Proof-of-Stake

PoW – Proof-of-Work

SGX – Software Guard Extension

SHA – Secure Hash Algorithm

SSI – Self-Sovereign Identity

UTXO – Unspent Transaction Output

ZKP – Zero-knowledge proof

1. ВОВЕД

Во последните две децении значаен дел од ИТ системите се базирани на Blockchain (Синцир од блокови) технологии. Ветувачките особини на Blockchain технологиите, како и постигнатиот успех, се основната причина за се поголемото прифаќање на овие технологии. Најголем придонес кон етаблирањето на Blockchain технологиите како доверливи технологии има Bitcoin [1] Blockchain технологијата, која овозможува градење на децентрализиран систем во кој корисниците кои учествуваат, немаат взаемна доверба и не се познаваат меѓу себе, но сепак успеваат да градат универзална заедничка вистина во системот. Заеднички особини на сите Blockchain технологии се: висок степен на синхронизираност на записите во системот, лесна проверливост на податоците, неможност истите да се фалсификуваат и неможност да се негира било какво внесување на запис во системот. Основни елементи кои ја дефинираат една Blockchain технологија се: временски сервер, хаш функција, консензус механизам, складишен простор и протокол за мрежна организација на корисниците. Како дополнителна алатка која овозможува напредни функционалности на Blockchain технологијата е паметниот договор.

Клучна алатка за успехот кој го постигнуваат Blockchain технологиите е имплементираниот консензус механизам [2]. Консензус механизмите овозможуваат дистрибуирани корисници во мрежата да постигнат коректен став околу дадена содржина, во услови кога во мрежата може да има и малициозни односно недоверливи корисници. Со екстензивна размена на пораки се овозможува корисниците да донесат правилен заклучок околу коректноста на предложената содржина. Постојат голем број на консензус механизми кои нудат различни перформанси по однос на број на трансакции кои се потврдуваат во системот, заштита од малициозни корисници, времетраење на интервалот за финализирање на трансакциите, скалабилност на системот како и други параметри кои ги карактеризираат консензус механизмите. Некои од најпознатите консензус механизми се: Proof-of-Work (PoW) [3], [4], Proof-of-Stake (PoS) [5], Practical Byzantine Fault Tolerance (PBFT) [6], Tendermint [7], Swirlds Hashgraph [8] и Tangle [9].

Најзастапени консензус механизми се PoW и PoS, кои нудат воедно и највисок степен на заштита од малициозни корисници, и покриваат околу 80% од крипто пазарот [10]. Истите се основа на Blockchain технологиите имплементирани во Bitcoin [1] и Ethereum [11]. Големата доверливост која се гарантира од страна на Bitcoin Blockchain технологијата како и воведувањето на истоимената дигитална валута, ја издигнува Bitcoin мрежата на ниво на банкарски систем. Овој успех дава импулс за креирање на нови дигитални валути во рамките на други Blockchain технологии. Од иницијалното имплементирање на Bitcoin во 2009 година, голем број на слични проекти се обидуваат да го постигнат неговиот успех, преку воведување на нови дигитални валути, но и нови протоколи кои овозможуваат имплементација на Blockchain технологиите во нови области на имплементација. Како најдобра алтернатива на Bitcoin се смета Ethereum мрежата која се појавува во 2015 година. Нејзиното воведување донесува значајно рedefинирање на ентитетите кои учествуваат во мрежата, преку имплементација на Ethereum виртуелната машина (Ethereum Virtual Machine – EVM). Овој нов концепт овозможува воведување на таканаречените паметни договори (Smart contracts) [11] што претставуваат самоизвршни кодови кои овозможуваат автоматизација на процеси во мрежата. Со паметните договори се овозможува развој на Blockchain технологии што ќе можат да се употребат надвор од финансискиот сектор. Перформансите на Bitcoin и Ethereum Blockchain технологиите покажуваат висок степен на заштита на мрежите од

малициозни корисници, но ограничен капацитет за имплементирање на истите во масовни системи.

Како главна алтернатива на PoW и PoS се консензус механизмите од групата на Byzantine Fault Tolerant (BFT) консензус механизми, меѓу кои најпознати се Practical Byzantine Fault Tolerance (PBFT), Tendermint и Swirlds Hashgraph. Истите овозможуваат помало ниво на заштита од малициозни корисници, па затоа се погодни за имплементација во системи каде може да се додаде дополнително ниво на заштита со контрола на пристап за корисниците. Овие консензус механизми овозможуваат неколкукратно зголемен проток на трансакции низ системот и нивно финализирање во период од неколку секунди [12].

Tendermint е најразвиен PBFT базиран протокол кој нуди високо ниво на скалабилност по однос на проток на трансакции низ системот. Корисниците во системот кои активно се вклучени во процесот на контрола и верификација на исправноста на податоците, уште познати и како валидатори, користат три-фазен протокол на гласање со кој постигнуваат консензус околу исправноста на податоците. Финализирањето на трансакциите е во рамките на неколку секунди, што дава простор да се постигне проток од десетици илјади трансакции во секунда. Предноста на овој консензус механизам во однос на останатите BFT протоколи е создадена преку воведувањето на механизмите за заклучување на глас и воведувањето на таканаречениот nil (нулти) глас. Поради високиот степен на конективност меѓу валидаторите, со разменувањето на гласовите за постигнување на консензус, се создава голема редундантност на пораците за гласање и на тој начин неретко се загушува мрежата. Оваа „бура“ од пораки значително влијае кога бројот на валидатори наближува 1000, после што перформансите на Tendermint консензус механизмот значително деградираат [13]. Како оптимална бројка се смета 100 валидатори во мрежата, со што се постигнува значаен степен на децентрализирање на гласачката моќ и воедно се постигнува висок проток на трансакции [14]. Овој консензус механизам, како и останатите PBFT базирани консензус механизми овозможуваат заштита од 1/3 малициозни валидатори.

Карактеристиките кои ги нудат Blockchain технологиите, како што се робустност, анонимност, приватност, заштита од измами и заштита од промени на содржините на универзалната вистина во системот, се овозможени преку користењето на хаш функции. Овие функции се еднонасочни функции кои овозможуваат повторливост на излезните податоци при внес на исти влезни податоци, но не овозможуваат да ја реконструираат влезната содржина кога се употребуваат во обратната насока. Оваа карактеристика се користи за да се постигне меѓусебно поврзување на блоковите од трансакции преку референцирање на хаш вредности од претходните во тековните блокови. На тој начин се формира синцирестата структура на Blockchain базите на податоци, која не може да биде променета со директна интервенција во било кој блок од трансакции. Предностите кои ги има токму оваа податочна структура претставуваат главен проблем за усогласување на сервисите кои се нудат на Blockchain базирани системи и General Data Protection Regulation (GDPR) [15] законските прописи. Оваа некомпатибилност ги става Blockchain технологиите во инфериорна позиција кога истите би се употребиле во сценарија во кои се користат лични податоци.

Во последните неколку децении од технолошкиот развој на здравствените системи има особен напредок во дигитализирањето на истите, како и отворање на истите кон Интернет. Голем дел од услугите се нудат преку Интернет мрежата, што ги прави ранливи здравствените системи од надворешни напади. Во [16] е даден преглед на развојните етапи на здравствените мрежни системи. Моментално, здравствените

системи се високо централизирани во облак-базирани решенија што ги изложува личните податоци на потенцијални кражби. Таквата поставеност на системите, ги става личните податоци на пациентите, надвор од нивна контрола. Потенцијално решение е имплементација на Self-Sovereign Identity (SSI) [17] механизам за складирање на податоците, каде пациентите би имале поголема контрола врз личните податоци.

Дизајнот на глобално решение за јавен здравствен систем за масовна употреба базирано на моменталните Blockchain решенија покажува ограничени можности [18] поради малиот проток на трансакции, големата редундантност на записи и проблемот со имплементацијата на GDPR правилата. И покрај ограничувањата кои постојат, во литературата може да се најдат решенија кои вршат интеграција на Blockchain технологиите и здравствените системи. Најзрели решенија се FHIRChain [19], MedRec [20], Healthcare Data Gateway[21], HIE of One [22], Patientory [23] и MedicalChain [24]. Генерално решенијата се базирани на Ethereum паметни договори или Hyperledger [25] приватниот Blockchain систем. Кај решенијата кои се изработени врз Ethereum платформата главен проблем е скалабилноста на решението кое зависи од скалабилноста на самиот Ethereum Blockchain, додека решенијата кои се изработени врз Hyperledger платформата имаат поголем проблем при заштитата на приватноста на податоците поради тоа што Hyperledger Blockchain системот е облак-базирано решение. Поради ваквите ограничувања, дефинирање на дедицирано Blockchain базирано решение за јавен здравствен систем би овозможило надминување на овие проблеми, преку оптимизација на консензус механизмот, стандардизирање на здравствените записи, намалување на редундантноста на записите и управување на пристапот до лични податоци од страна на пациентите.

1.1. Мотивација за изработка на докторската дисертација

Ветувачките карактеристики на Blockchain технологиите и се почестите проблеми кои ги имаат луѓето со запазување на приватноста на личните податоци е главен мотив за изработка на оваа дисертација. Јавното здравство како посебно атрактивна област во која приватноста на личните податоци има голема улога, би можела да понуди поле за развој на систем каде практично би се примениле решенијата за заштита на приватните податоци преку имплементацијата на Blockchain технологија. На тој начин Blockchain технологијата би била главниот овозможувач за управување со приватноста на податоците, но дополнително би се овозможила трајност на записите, достапност во секое време и на секое место, неможност за бришење или менување на минати записи, како и развој на нови бизнис парадигми. Новиот систем би овозможил управувањето со пристапот кон личните податоци да биде во рацете на пациентите, кои преку користење на мобилна апликација би имале целосен увид во тоа кој има пристап до нивните личните податоци.

1.2. Предмет на истражување и хипотеза

Предмет на истражување на докторската дисертација е дизајн на јавен здравствен систем базиран на Blockchain технологија која ќе имплементира оптимален консензус механизам за да може да одговори на потребите за зголемена скалабилност на системот, а притоа да обезбеди висок степен на приватност на личните податоци на пациентите. Преку определување на перформансните карактеристики на постоечките консензус механизми, издвојување на нивните позитивни и негативни карактеристики, како и нивна анализа во контекст на јавните здравствени системи, определена е јасна насока за дизајн на нов јавен здравствен систем базиран на Blockchain технологија. За да се избере најсоодветен консензус механизам кој во контекст на јавните здравствени системи ќе

понуди доволен капацитет за валидирање на трансакции, споредени се поголем број на постоечки консензус механизми. За избраниот консензус механизам извршени се и дополнителни испитувања, за да се определат перформансите во услови на максимална оптовареност, како и можноста да се изврши негова оптимизација.

Генерално, Blockchain технологиите имаат репутација на мала скалабилност по однос на бројот на трансакции во системот и голема редундантност на податоците, што отвора простор за дефинирање на ново оптимално решение наменето за јавните здравствени системи. Од најпознатите консензус механизми, како најнадежен се смета Tendermint консензус механизмот, кој има висок степен на скалабилност по однос на проток на трансакции, а овозможува и финализирање на трансакциите во рамките на неколку секунди. Поради недостатокот на перформансни карактеристики за Tendermint консензус механизмот во контекст на карактеристиките на јавните здравствени системи, дополнително се спроведени анализи за да се определи однесувањето на овој консензус механизам во услови на максимална оптовареност и големи трансакции.

Главна хипотеза на истражувањето кое е спроведено е: Може да се дизајнира јавен здравствен систем базиран на Blockchain технологија, кој ќе овозможи глобализирање на здравствените сервиси преку унифициран јавен здравствен систем, кој инхерентно би ги наследил високиот степен на доверливост и приватност кои ги овозможува Blockchain технологијата, а воедно би ги надминал проблемите на скалабилност кои се појавуваат кај Blockchain технологиите.

Како посебни тези се поставуваат:

- Постоечките Blockchain технологии не можат да одговорат на волуменот и посебноста на сообраќајот кој би циркулирал во глобалниот јавен здравствен систем.
- Може да се дефинира протокол што ќе овозможи зголемена скалабилност на Blockchain технологијата, која ќе се користи за дизајн на глобалниот јавен здравствен систем и притоа ќе го задржи високиот степен на доверливост на Blockchain технологиите.
- Може да се дефинираат протоколи кои ќе овозможат пациент-центричен механизам за управување со пристапот кон приватните податоци.

1.3. Цели и придобивки од истражувањето

Основна цел на докторската дисертација е да се испита можноста за дизајнирање на јавен здравствен систем базиран на Blockchain технологија која ќе имплементира оптимизиран консензус механизам, кој би ги максимизирал перформансите на јавниот здравствен систем. Дополнително со истражувањето се испитуваат и можностите на постоечките технологии да одговорат на специфичниот тип на податоци кои циркулираат во здравствените системи, притоа обезбедувајќи доверлив систем со високо ниво на приватност и безбедност на податоците. Исто така целта на ова истражување е да се определи можноста за оптимизација на некоја од постоечките Blockchain технологии во насока на дизајн на Blockchain базиран јавен здравствен систем со високи перформанси. Како важна цел е дефинирањето на архитектурата на нов јавен здравствен систем која ќе овозможи пациент-центрична контрола на пристап и целосно управување со личните податоци, кое би било во согласност со General Data Protection Regulation (GDPR) законските прописи. Императивот е да се дефинира дизајн на јавен здравствен систем кој би можел да биде имплементиран на глобално ниво и би овозможил здравствени услуги за пациентите преку границите на матичната држава.

Оваа дисертација дава решение кое е комплемент на големото множество на Blockchain технологии притоа надминувајќи го проблемот со скалабилноста кој го има кај Blockchain технологиите преку искористување на посебноста и карактеристиките на јавните здравствени системи. Придонесот на оваа докторска дисертација е во насока на понудување на глобално решение за јавен здравствен систем кое е Blockchain базирано, притоа овозможувајќи поголема мобилност на пациентите, децентрализирање на здравствените услуги, а централизирање на управувањето со лични податоци во доменот на самите пациенти. Дизајниран е нов, оптимален консензус механизам со кој се овозможува поголема скалабилност на системот, а преку имплементација на само-организирачки протоколи се придонесува кон максимизирање на перформансите на консензус механизмот.

Како дополнителен придонес, во рамките на оваа дисертација се направените екстензивни анализи на перформансите на постоечкиот консензус механизам Tendermint, при што е определен максималниот капацитет на пропустливост на трансакции во системот, во услови кога се користат документи со стандардна големина, но и во сценарија кога во системот се испраќаат слики и видео содржини.

Зголемената мобилност на луѓето како и глобализацијата која се спроведува во светот, ќе биде потпомогната од систем кој нуди универзални услуги на секаде во светот. Со глобалниот јавен здравствен систем ќе се овозможи пациентите да добиваат здравствени услуги надвор од границите на матичната држава и притоа да имаат пристап до здравствените податоци во секое време и на секое место каде и да се движат. Користењето на универзални шифри за опис на дијагнозите, како и автоматизирани системи за преведување, би овозможиле непречено да се даваат здравствени услуги и во држави каде постои јазична бариера. Сето тоа е овозможено од стандардниот формат на записите кои се предвидени во системот.

Со централизирањето на управувањето за пристап до личните податоци се отвораат нови можности за развој на нови бизнис идеи од страна на осигурителните компании, фармацевтските компании како и маркетинг агенциите. Осигурителните компании би имале можност да нудат нови осигурителни пакети базирани на целосната здравствена слика на пациентите, а воедно би имале целосен увид во тековната здравствена состојба на пациентите. Фармацевтските компании би можеле многу поточно да ја испитуваат ефикасноста на нивните производи, како и да имаат подобар увид во потенцијални несакани последици од истите. Преку имплементација на агенти со Вештачка интелигенција дополнително би се подобриле постапките за дијагноза на одредени здравствени состојби.

1.4. Структура на докторската дисертација

Докторската дисертација е организирана во 5 глави.

Првата глава од докторската дисертација е воведна глава која ги содржи мотивацијата за изработка на докторската дисертација, предметот на истражување и хипотезите кои се поставени во рамките на докторската дисертација, како и целите и придобивките од спроведеното истражување на избраната тема.

Во втората глава најпрво е даден осврт на развојот, карактеристиките и предизвиците на јавните здравствени системи, каде покрај традиционалните телемедицински системи се разгледани и новите генерации на е-здравствени системи кои започнуваат да се развиваат со воведувањето на Интернет сервисите во рамките на здравствените институции. Притоа издвоени се четири генерации на развој на е-

здравствените системи меѓу кои е тешко да се постави остра граница поради преклопувањето на развојните етапи на поедини сегменти од здравствениот систем. Нивните општи карактеристики се дадени во оваа глава. На крај од втората глава е дадена рамка за развој и специфики на четвртата генерација на е-здравствени системи.

Во третата глава е направен осврт кон техничките карактеристики на Blockchain технологиите, нивните предности и недостатоци. За еден од најважните сегменти на Blockchain технологиите, консензус механизмот, даден е преглед на општите карактеристики и извршена е детална анализа на структурата, типовите и перформансите на консензус механизмите кои можат да се најдат во литературата. За истите е направена и сублимација на карактеристиките и изведен е заклучок за најнадежен консензус механизам кој има потенцијал да се користи во следната генерација на јавни здравствени системи базирани на Blockchain технологии. Исто така во рамките на оваа глава даден е опис на некои од најпознатите Blockchain технологии како и споредба на нивните карактеристики.

Во глава четири се дадени резултатите од евалуацијата на перформансите на Tendermint консензус механизмот, за сообраќај со општи карактеристики и за сообраќај кој е карактеристичен за јавните здравствени системи. Исто така е извршена и апроксимативна анализа на можноста Tendermint консензус механизмот да опслужи глобален јавен здравствен систем. Во оваа глава се дадени и резултатите од оваа анализа.

Во рамките на петтата глава даден е дизајнот на новиот BloHeS систем, а направена е и анализа на перформансите за истиот. Покрај архитектурата на BloHeS системот, даден е и дизајнот на BloHeS консензус механизмот, организацијата на складишниот простор во системот, податочната структура, протоколите за управување со острови како и други елементи и процедури кои придонесуваат кон овозможување на пациент-центрично управување со личните податоци. Во оваа глава дадени се и резултатите од анализата на комуникациската комплексност и капацитетот за заштита на системот кај Tendermint и кај BloHeS консензус механизмот, како и анализата спроведена за зафатнината на складишниот простор кај класичните Blockchain технологии и BloHeS начинот на складирање на податоците.

2. ЈАВНИ ЗДРАВСТВЕНИ СИСТЕМИ – КАРАКТЕРИСТИКИ И ПРЕДИЗВИЦИ, ГЕНЕРАЦИИ НА ЈАВНИ ЗДРАВСТВЕНИ СИСТЕМИ, РАМКА ЗА ЈАВЕН ЗДРАВСТВЕН СИСТЕМ БАЗИРАН НА BLOCKCHAIN ТЕХНОЛОГИЈА

Здравствена заштита и нега на дистанца се практикува повеќе векови, но развојот на телемедицината каде се користат и првите уреди за телекомуникација датира од крајот на 19-тиот век, кога се појавува првиот телефон [16], [26]. Позначаен напредок во развојот на телемедицината се забележува во втората половина на 20-тиот век откако е развиен телемедицински систем за следење на здравствената состојба на астронаутите, кој бил вграден во ракетниот систем и во облеката на космонаутите. Првите телемедицински решенија биле телевизиски и телефонски базирани двонасочни комуникациски системи кои биле користени за консултативна намена. Генерално гломазни, скапи и многу комплексни, овие системи не претставувале успешни телемедицински проекти. Откако се увидел недостатокот кај овие системи, целта на истражувачите била намалување на зафатнината на системите и упростување на процесот за нивно имплементирање. Позначаен скок во развојот на телемедицинските системи е направен кон крајот на 20-тиот век со појавата на компјутерските и мрежните системи, при што истите започнуваат да се вградуваат во локални мрежи. Примарна цел на овие системи била да се замени дотогашното водење на здравствените записи кое се вршело со повеќекратно внесување на истите информации на повеќе места преку рачно запишување на рецепти и извештаи во амбулантски дневник и во здравствени легитимации. Со градењето на компјутерски мрежи во рамките на болниците се овозможува дигитализација на податоците од пациентите. Ваквите системи се колоцирани во самите болници, а се градат со главна цел да го подобрат текот на работата и внатре-секторската комуникација. Овие системи се изолирани, без пристап на Интернет, што ги прави да бидат безбедни од надворешни мрежни безбедносни напади. Згора на тоа ваквите институции овозможуваат висок степен на физичка заштита, со што загриженоста за приватноста и безбедноста на личните податоци од пациентите е сведена на минимум. Згора на тоа во периодот на постоење на овие системи, свесноста за приватноста на личните податоци кај пациентите била на ниско ниво.

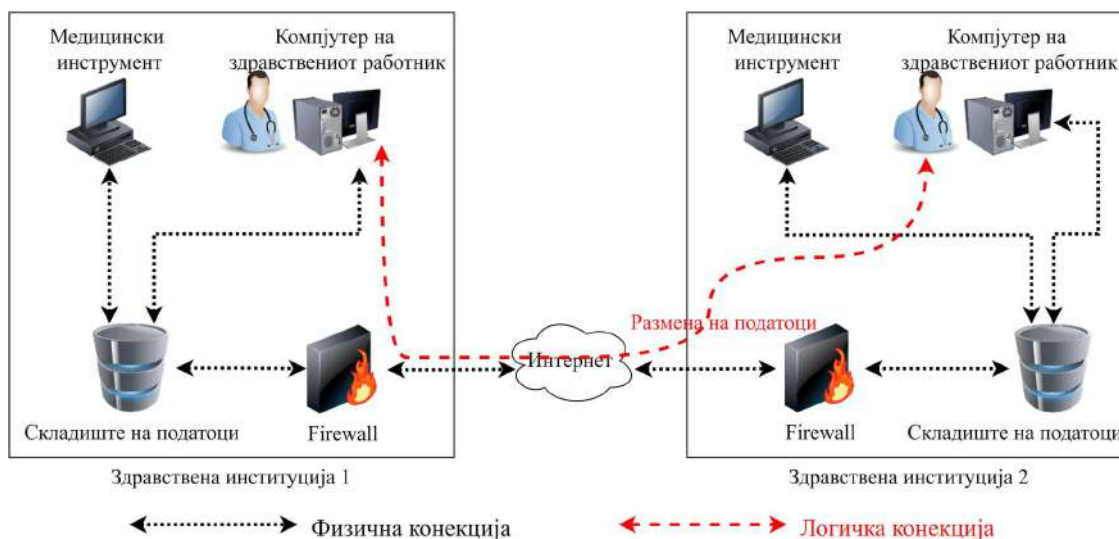
Со развојот и распространувањето на Интернетот, се појавува и нов телемедицински систем [27], денеска познат како е-здравствен систем. Е-здравствените системи се Интернет-базирани системи со постојан пристап кон Интернет, каде ентитетите од различни здравствени институции се поврзуваат и имаат можност да споделуваат информации, соработуваат во реално време или да пристапуваат до информации за пациентите од дистанца. Сеприсутноста на Интернет пристапот овозможи лесен пристап до здравствени услуги од секоја болница, секоја канцеларија па дури и од мобилни уреди. Со овозможувањето на болничките компјутерски мрежи да пристапат до Интернет во секое време, се остава простор за сигурносни напади на истите. Поради омасовувањето на Интернет услугите зголемена е и свесноста на пациентите за приватноста на нивните лични податоци.

Генерално не постои остра граница помеѓу генерациите на здравствени системи бидејќи нивниот развој е инкрементален и во различни сегменти од здравствениот систем. Унапредувањето на е-здравствените системи се забележува во делот на дигитализирање на медицинската опрема и нејзино поврзување со мрежните системи, развој на услуги во реално време на растојание преку мрежно поврзани медицински центри, нега на лица во домашни услови од здравствени работници на растојание и друго.

2.1. Прва генерација на е-здравствени системи

Првата генерација на е-здравствени системи е изградена од комплетно независни и изолирани корпоративни мрежи, со податочни центри кои се наоѓаат во самите болници, како што е прикажано на Слика 2.1. Овие системи се димензионирани да овозможат складирање на медицински податоци за пациентите кои ја посетуваат болницата. Истите може да бидат лесно проширени со дополнителен капацитет за складирање на податоци преку додавање на нови сервери во системот. Ширењето на болниците со нови оддели многу лесно може да биде следено со надградба на болничката мрежа со нови компјутери, свичеви како и сервери. Тоа е овозможено бидејќи ваквите системи ја следат генералната клиент-сервер архитектура.

Со овозможувањето на Интернет пристап на системите од првата генерација, безбедноста на целокупната мрежа се изложува на потенцијални напади од надвор, а со тоа се изложуваат личните податоци од пациентите на потенцијални кражби. Управувањето и одржувањето на ваквите корпоративни мрежи се голем финансиски товар за болниците бидејќи е потребен висококлучен инженерски кадар и скапа опрема која ќе овозможи доверливост на целокупната мрежа. Управувањето со личните податоци го вршат болниците, а пациентите немаат никаква контрола врз своите лични податоци.

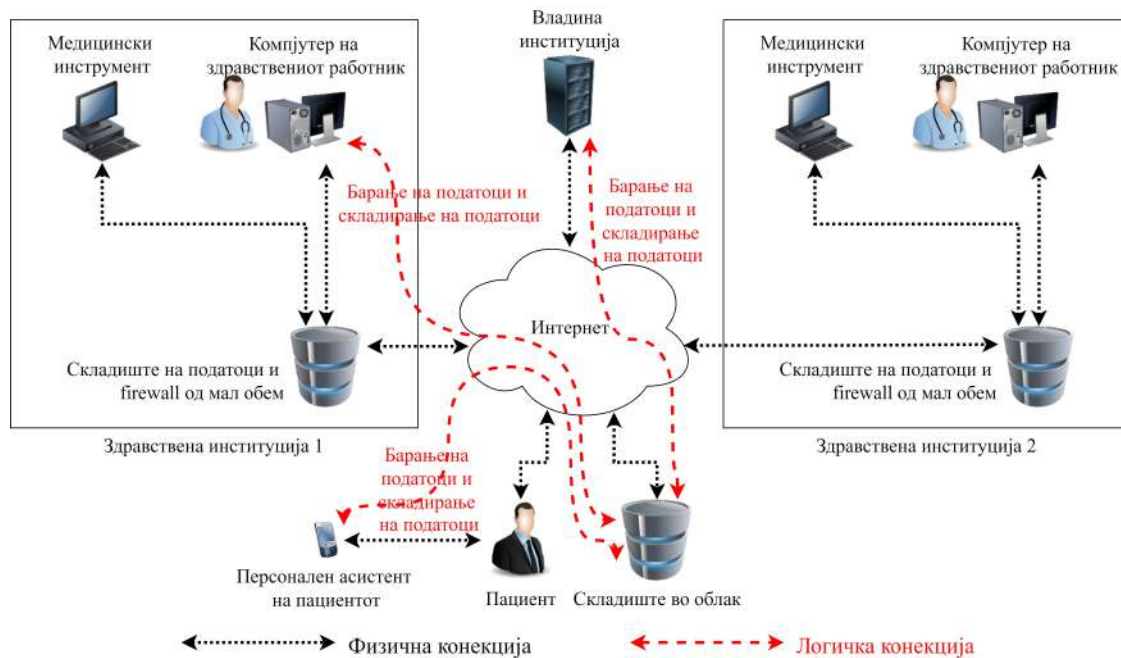


Слика 2.1. Симплифициран приказ на првата генерација на е-здравствени системи

2.2. Втора генерација на е-здравствени системи

Втората генерација на е-здравствени системи се карактеризира со воведување на сервиси во облак и Internet-of-Things (IoT, Интернет-на-нешта) уреди. Симплифицираната организација на е-здравствените системи од втората генерација е прикажана на Слика 2.2. На овој начин болничките системи постануваат облак-центрични решенија. Со тоа се намалуваат трошоците кои болниците ги плаќаат за управување и одржување на корпоративните мрежи. Централизирањето на е-здравствените решенија, ја зголемува загриженоста за приватноста и безбедноста на здравствените податоци. Дополнително, со централизирањето се создава и тесно грло во системското решение поради кое може болничкиот кадар да искуси лоши перформанси на системот. Затоа доброто димензионирање на системот и високото ниво на безбедност

преку користење на најнови сигурносни механизми се есенцијални при развојот на ваквите е-здравствени системи. Главни предности на ваквите системи се намалените трошоци за градење и одржување на истите, можност за синхронизирање на здравствените записи и пристап кон истите од било каде, потоа можност на владините институции да имаат подобар увид во здравствениот статус на пациентите, како и можност за изготвување на финансиски анализи од работата на целокупниот државен здравствен систем.



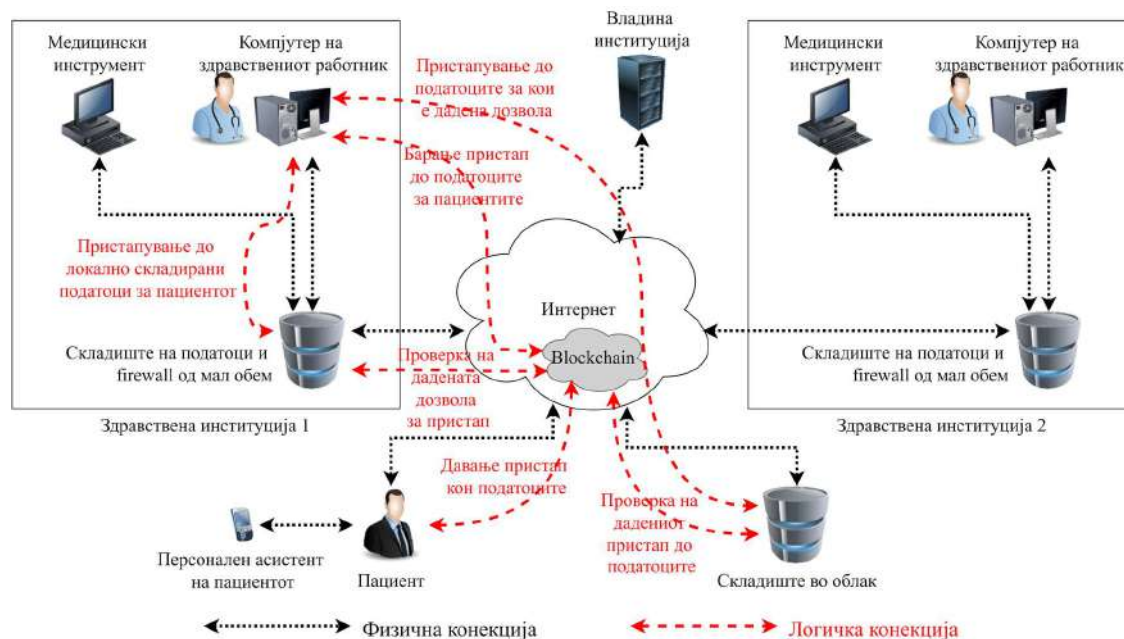
Слика 2.2. Симплифициран приказ на втората генерација на е-здравствени системи

Со воведувањето на IoT уреди кај втората генерација на е-здравствени системи се овозможува пациентите, но и здравствените работници да имаат подобри алатки за надгледување на здравствената состојба на пациентите во реално време и со подобра прецизност, но и со поголем комфор за пациентите [28], [29]. Воведувањето на подобри податочни целуларни решенија од страна на телекомуникациските оператори овозможува надгледувањето на здравствената состојба на пациентите да се изведува и при поголема мобилност на пациентите, надвор од болничките простории и домовите, во реално време. Сеприсутноста на Интернет пристапот со големи брзини придонесува и кон овозможување на сервиси како изведување оперативни зафати на терен, домашна помош за повозрасните лица, дијагностика на оддалеченост итн.

2.3. Трета генерација на е-здравствени системи

Со воведувањето на третата генерација на е-здравствени системи, се прави обид да се реши проблемот на приватноста на податоците преку воведување на Blockchain технологии во системот. Симплифицираната организација на системите од третата генерација е прикажана на Слика 2.3. Паралелно со развојот на третата генерација на е-здравствени системи има и зголемен број на мобилни уреди. Пристапот кон Интернет е овозможен насекаде преку Wi-Fi или 4G технологии, што овозможува дизајн на мобилни апликации и зголемен развој на мобилни здравствени сервиси. Со воведувањето на Blockchain технологиите, пациентите имаат целосна контрола врз нивните лични податоци. Тие можат да дадат времено или постојано авторизирање за користење на

нивните податоци на здравствени работници или трети лица, преку едноставна мобилна апликација која ќе биде поврзана на Blockchain базираниот систем. Во ваквите системи, Blockchain технологијата има улога на независен ентитет или база на податоци каде се запишуваат правата и привилегиите за пристап до приватните податоци. Со тоа Blockchain технологиите претставуваат комплементарен дел на централизираните облак-базирани архитектури. Повеќе различни решенија се елаборирани во [20], [23], [24], [30]. Главна предност на оваа генерација е-здравствени системи е овозможувањето на корисник-центричен пристап за управување со приватноста врз личните податоци кои се поврзани со здравствената состојба. Воведувањето на Blockchain технологиите ја решава приватноста на податоците, но само во крајната точка на користење. Сепак останува нерешен проблемот со заштита на приватноста на податоците кои се чуваат во облакот, но и можноста за крадење на привилегиите и податоците, директно од самите корисници.



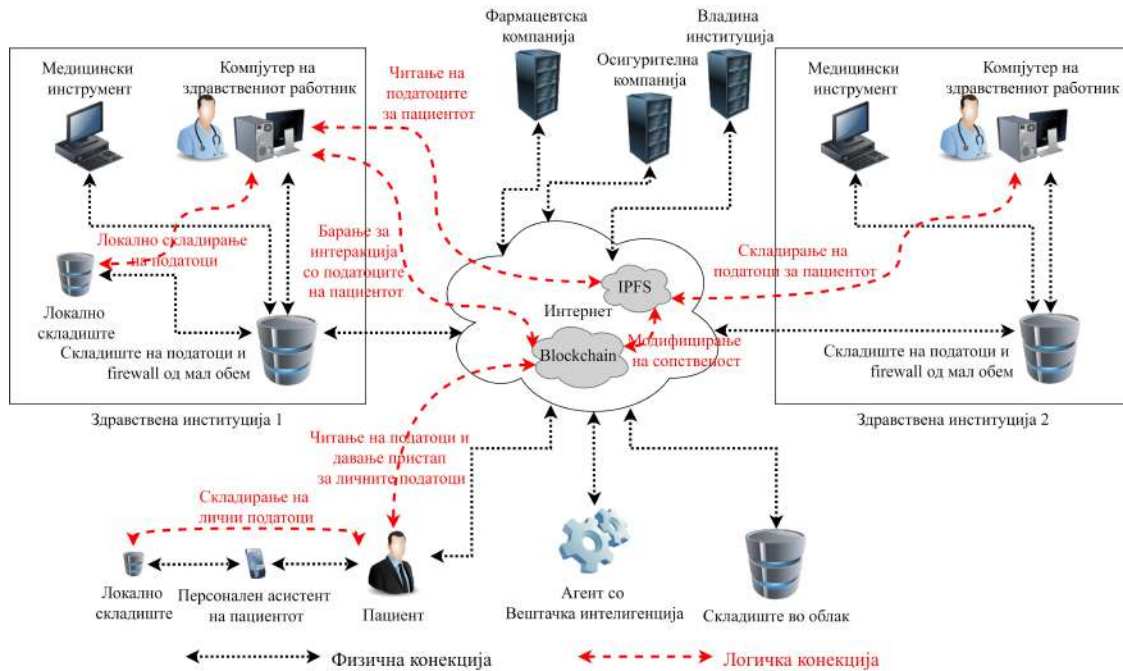
Слика 2.3. Симплифициран приказ на третата генерација на е-здравствени системи

2.4. Четврта генерација на е-здравствени системи

Четвртата генерација на е-здравствени системи треба да воведо дополнителни подобрувања во начинот на обезбедување приватност на податоците, подобрување во управувањето со складирање податоци, подобрен пристап до нови сервиси, зголемен опсег на параметри за надгледување, нови бизнис модели, предиктивна анализа преку имплементација на нова архитектура [16]. На Слика 2.4 е прикажана симплифицирана организација на е-здравствените системи од четвртата генерација и симплифицирана комуникациска процедура за основно корисничко сценарио.

Главен носител на Интернет пристап за овие е-здравствени системи се целуларните 5G решенија кои овозможуваат значително зголемен податочен проток но и намалена латентност. Кај оваа генерација на е-здравствени системи се предвидува децентрализиран пристап за складирање на податоците преку користење Фрагментирани Blockchain (Blockchain Shard) [31] решенија или InterPlanetary File System (IPFS) [32] базирани решенија со што се избегнува потребата од централизирање

на базите на податоци. Се предвидува и воведување на алгоритми со Вештачка интелигенција преку соодветни агенти кои ќе можат да вршат надгледување на здравствената состојба на популацијата и предвидување на епидемии. Со минијатуризирањето на IoT уредите, ќе се подобри спектарот на надгледувани параметри, можноста за постојано следење на пациентите, надгледување на здравствената состојба не само од дома туку и на работното место.

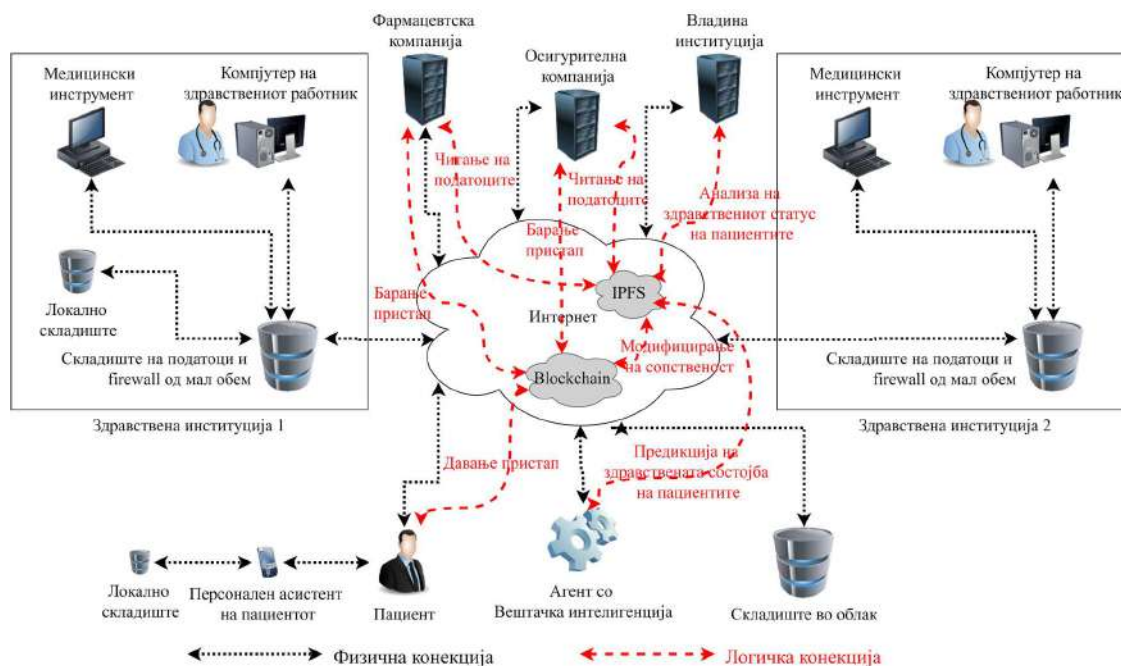


Слика 2.4. Симплифициран приказ на комуникациска процедура за основно корисничко сценарио кај четвртата генерација на е-здравствени системи

Многу владини институции, фармацевтски компании, осигурителни компании и други независни истражувачки тела би имале можност да вршат дополнителни анализи на податоците кои се поврзани со здравствената состојба на пациентите, со претходна дозвола дадена од самите пациенти. На овој начин се отвора можност пациентите лично да управуваат со пристапот до нивните податоци. На Слика 2.5, покрај прикажаната симплифицирана организација на е-здравствените системи од четвртата генерација дадени се и симплифицирани комуникациски процедури за други специфични кориснички сценарија.

Системите од четвртата генерација на здравствени системи би овозможиле имплементација на самоуправувачки механизми преку употреба на паметни договори [11] со кои може да се автоматизираат законски процедури во системот. Се овозможува и поголем спектар на производи за пациентите и повозрасните лица, со што би се поедноставило користењето на апликациите, но и би се подобрило искуството од користење на истите. Најважна придобивка би била подобрувањето на општото здравје на целата популација.

Како основен недостаток се смета високата комплексност на системот во фазата на имплементирање поради очекуваната мала стапка на прифаќање како и потешкотијата за разбирање на Blockchain технологиите.



Слика 2.5. Симплифициран приказ на комуникациски процедури за специфични кориснички сценарија кај четвртата генерација на е-здравствени системи

2.4.1. Рамка за четвртата генерација е-здравствени системи

Се предлага рамка за четвртата генерација на е-здравствени системи која ќе обезбеди подобрување на управувањето со складирање на личните податоци преку имплементирање на повеќесегментно складирање на податоци. Предложената рамка за четвртата генерација на здравствени системи е дадена на Слика 2.6. и истата е базирана врз најновите мрежни и компјутерски технологии, со што би овозможила подобрена приватност, безбедност на податоците, трајност на податоците, корисничко-центрично управување со пристапот до лични податоци, предиктивна здравствена анализа и нови бизнис модели. Сегментирањето на нивоа се прави со цел да се обезбеди независност помеѓу техниките и технологиите кои се користат во секое ниво. Ваквата структура би придонела и за полесно надградување на системот.



Слика 2.6. Нивовска структура на четвртата генерација на е-здравствени системи

Главниот фокус на рамката е ставен на пациентот или сопственикот на податоците во системот, кој преку мобилна апликација ќе има целосна контрола врз дадените привилегии за неговите лични податоци. Покрај пациентот, рамката предвидува и други ентитети како што се здравствени работници, владини институции, осигурителни компании, фармацевтски компании и агенти со вградени алгоритми за Вештачка интелигенција. Сите ентитети имаат различни привилегии и степени за пристап до податоците. Идентитетот на корисниците во системот се определува со помош на персонален паричник (wallet), кој се генерира како комбинација од јавен и приватен енкриптиски клуч. Со помош на паметен договор кој ќе биде поставен во Blockchain базата на податоци, пациентите ќе можат да дадат или одземат привилегии за пристап по потреба. Сите податоци кои ќе бидат генерирани или собрани за пациентот ќе бидат енкриптирани.

Здравствените работници се ентитети кои се предвидени да имаат главна улога во пружањето на здравствена нега, па затоа практично би било истите да добијат постојан пристап до личните податоци на пациентот, но секако би постоела опција за давање времен пристап до личните податоци во зависност од желбата на пациентот. За да се избегне ситуација во која здравствен работник би внесувал податоци во досието на пациентот без негово знаење, рамката предвидува секој запис на здравствени податоци од страна на здравствениот работник да биде одобрен лично од пациентот.

Дополнително се предвидени да се користат IoT уреди, кои постојано ќе собираат податоци за пациентите, па затоа истите би се ставиле во листа на корисници со постојани привилегии за читање и пишување. Бришењето на тие привилегии би било едноставно откако тие уреди не би се користеле повторно.

2.4.2. Специфики на четвртата генерација е-здравствени системи

Зголемената приватност, која претставува примарна вредност на е-здравствените системи од четвртата генерација ќе овозможи развој на голем спектар на нови бизнис идеи. Како основна предност би била можноста, владините институции да можат да ги користат овие системи како алатка за надгледување на здравствената состојба на популацијата. Тоа би овозможило да се зголеми ефикасноста на целокупниот здравствен систем. Со додавањето на агент со Вештачка интелигенција, владините институции би можеле да вршат предиктивна анализа за трошоците кои би ги имала државата по однос на здравствениот систем. Исто така овие агенти со Вештачка интелигенција би можеле да вршат предиктивна анализа за пациентите индивидуално или како група, како и да сугерираат третмани или да предвидуваат епидемии. Пациентите преку соодветна апликација ќе може да дадат пристап кон сите или одреден дел на лични податоци, зависно од постоечката легислатива.

Приватниот сектор, особено осигурителните компании, би можеле да воведат нови бизнис решенија преку персонализирање на осигурителните планови или адаптирани осигурителни планови во зависност од финансиските можности на пациентите. Со взаемен договор би се поставиле меѓусебните односи, при што пациентите би требало соодветно да овозможат пристап до бараните лични податоци. Со тоа осигурителната компанија би можела во реално време да го следи статусот на пациентот или да има увид во минати здравствени состојби на пациентот па со тоа да понуди персонализиран осигурителен план. Пациентот ќе има можност да даде времен пристап на осигурителната компанија со времетраење на постигнатиот договор.

Фармацевтската индустрија исто така би имала бенефит. Двојно-слепите студии кои се спроведуваат од страна на истражувачите се од голема важност за фармацевтските компании. Овие системи би овозможиле фармацевтските компании да имаат многу поголемо множество на испитани пациенти без ни малку да се открие идентитетот на пациентот. Со тоа ќе се добиваат многу подобри резултати за ефективностa на испитуваните лекови. Дополнително, навиките и здравствената состојба на пациентите може значително да помогнат во определувањето на ефикасноста на лековите. За да се поттикнат пациентите да учествуваат во ваквите испитувања, системот би овозможил фармацевтските компании да плаќаат за добиените податоци и со тоа пациентите да имаат можност да ги монетаризираат собраните податоци.

Паметните договори претставуваат есенцијален дел на Blockchain технологиите. Овие унифицирани кодови може да имаат функционалност на агенти со Вештачка интелигенција, со што може да се зголеми потенцијалот на целокупниот систем. Со помош на ваквите агенти би можеле да се предвидат епидемии, би овозможиле и да се следат здравствената состојба и секојдневните навики на одредени пациенти, а со тоа и да се прави предиктивна анализа за потенцијални заболувања. Пациентите кои анонимно би сакале да учествуваат во работата на ваквите агенти со Вештачка интелигенција би дале времена дозвола за користење на личните податоци, кои преку механизми за анонимизација би биле споделувани со агентите. Во зависност од понудениот сервис, за истиот би била извршена наплата или би се дала награда на пациентот за користењето на неговите лични податоци. На ваков начин, агентите со Вештачка интелигенција би можеле да бидат самоодржливи.

За да се изгради систем кој би имал можност да се развива и прилагодува на следните генерации мрежни решенија, потребно е истиот да биде изграден врз Blockchain технологија која ги има надминато проблемите со скалабилност. Скалабилноста по однос на складишниот простор како еден од проблемите кај моменталните Blockchain технологии, би можел да се надмине преку користење на локален складишен простор, фрагментирани Blockchain решенија и IPFS базирани решенија или во крајна линија користење на облак-базиран складишен простор.

Поради големиот податочен товар кој се создава како резултат на користењето слики и видео записи во здравствените системи, но и големиот број на податоци кои се собираат од IoT уредите, потребно е да се направи пренасочување на складирањето на податоците надвор од Blockchain базата на податоци. Со користењето на локален складишен простор, пациентите и здравствените работници би имале брз пристап до потребните податоци. Исто така, податоците кои би ги собрале IoT уредите периодично би можеле да се складираат во локалното складиште на пациентот. Моменталната верзија на IPFS има бавен но доверлив пристап до податоците, па затоа овој систем би се користел за да се овозможи редундантност на податоците, притоа да не се оптоварува Blockchain базата на податоци. Дополнително со фрагментираните Blockchain решенија ќе се овозможи главната база на податоци да се подели на сегменти и на тој начин да се намали интензитетот на размена на податоците во системот. Како опционално решение би постоел и облак-базиран складишен простор кој би се користел за трајно архивирање на податоците кои претходно би биле неколкукратно заштитени.

Значајна поддршка за брзиот развој и прифаќање на новите технологии е постоењето на мрежна технологија која би овозможила лесен и брз пристап до Интернет. Рамката за четвртата генерација е-здравствени системи предвидува користење на најновите текови во мобилните комуникациски технологии меѓу кои најпознати се 5G и WiFi, но и оптичките широкопојасни технологии. Моменталното распространување на

5G мрежите обезбедува пристап кон Интернет со големи проточни брзини и мала латентност, што би значело висок степен на сатисфакција кај пациентите кои треба да добијат медицинска помош на дистанца или пристап кон здравствени параметри во реално време.

3. BLOCKCHAIN – ИСТОРИЈА, ТЕХНИЧКИ КАРАКТЕРИСТИКИ, ПРЕДНОСТИ И НЕДОСТАТОЦИ

Зачетоците на Blockchain технологијата датираат уште од 1991 година, со воведувањето на криптографски обезбедениот синџир од блокови кој се користел за временско обележување и сертифицирање на дигиталните содржини [33]. Во [34] и [35] исто така се објаснува механизмот за криптографско поврзување на блокови кои подоцна станува основен механизам за градење на податочната структура која се користи кај Blockchain технологиите. Првиот чекор кон дефинирање на децентрализирана архитектура за систем во кој би се користеле децентрализирани дигитални валути е претставен во 1998 година [36], [37]. Воедно тоа е и прв пат да се спомне дигиталната валута која се нарекува bit gold. Предложеното решение имало основен недостаток што не можело да обезбеди синхронизираност на записите за дигиталната валута во системот кога во мрежата постојат малициозни корисници. Решението за проблемот на одржување синхронизација помеѓу записите кај децентрализираните корисници е користење на консензус механизам.

Комплетното решение за децентрализиран систем кој го решава проблемот на синхронизација на записите во децентрализирана околина го предлага Сатоши Накамото во 2008 година [1], а истото практично е имплементирано наредната година како Bitcoin платформа со сопствена дигитална валута. Blockchain технологијата имплементирана во Bitcoin платформата претставува основа за подоцнежнo развивање на илјадници други слични системи кои покрај тоа што ја имаат основната намена да бидат алтернативен банкарски систем, истите воведуваат и нови иновативни алатки за да ја надградат основната функција на Blockchain технологијата и овозможат нови имплементациски сценарија кои немаат финансиска природа. Така со воведувањето на Ethereum Blockchain технологијата во 2015 година, поточно со воведувањето на Ethereum Virtual Machine (EVM), Ethereum мрежата прераснува во глобален компјутер. Со тоа се прави драстичен скок во концептот на градење на Blockchain системот, бидејќи се овозможува воведување на паметни договори, со кои Blockchain технологијата може да се имплементира не само во финансиски апликации туку и во апликации од нефинансиска природа. Со тоа се овозможило отпочнување на развој на широк спектар на други апликации, како и примена на Blockchain технологијата во многу други сфери. Како најчесто развивани апликации од нефинансиска природа врз Blockchain технологија се: IoT [38], [39], [40], логистичка поддршка [41], здравствени системи [42], недвижности [43], нотарски услуги [44], индустрија за игри [45] и на многу други места каде може Blockchain технологијата да замени трети лица во процесот на интеракција меѓу два ентитети.

Покрај Bitcoin и Ethereum, како посебен концепт е Hyperledger [46] проектот кој започнува да се развива кон крајот на 2016 година. Истиот нуди приватни, односно затворени решенија со кои може да се изградат апликации на индустриско ниво. Овие апликации имаат голем дел од предностите кои ги нуди Blockchain технологијата како концепт, а притоа нудат и целосна поддршка на корпорациите за управување на системското решение, со која дополнително се зацврстува довербата во Blockchain технологијата. Апликациите развиени во рамките на Hyperledger проектот покрај техничката поддршка, нудат и поставување на техничкото решение во рамките на Hyperledger складишниот простор, со што значително се намалува оптовареноста на корпорациите со мрежни и софтверски решенија, како и нивно одржување.

3.1. Типови на Blockchain технологии

Постоечките Blockchain технологии имаат голем број сличности, но и разлики кои потекнуваат од принципот на градење на Blockchain технологијата, како и од пристапот до софтверскиот код и податоците на апликациите. Основната поделба на Blockchain технологиите базирана на отвореноста на податоците, мрежата и технологијата е на: *јавни* и *приватни* Blockchain технологии. Во зависност од процедурите кои се применуваат за да се пристапи кон Blockchain системот, истите може да се поделат на Blockchain системи *без дозвола* (permissionless) и *со дозвола* (permissioned). Во принцип, Blockchain технологиите може да бидат јавни без дозвола, јавни со дозвола, приватни без дозвола и приватни со дозвола. На граница меѓу јавните и приватните Blockchain системи се наоѓаат *конзорциум* Blockchain технологиите кои може да бидат со дозвола и без дозвола. Истите имаат карактеристики кои се наоѓаат и кај јавните и кај приватните Blockchain системи.

Јавните Blockchain технологии се јавно достапни Blockchain мрежи со јавно достапни отворени податоци, при што секој корисник на мрежата може да ги отчитува податоците од Blockchain системот. Корисниците на јавните Blockchain системи имаат дозвола да учествуваат во донесување на консензус во мрежата, со тоа поддржувајќи го целиот Blockchain екосистем. Јавните Blockchain системи се смета дека се целосно децентрализирани, поради целосно децентрализираното управување со мрежата и целосно децентрализираната база на податоци што претставува универзалната вистина за целиот систем.

Спротивно на јавните Blockchain системи се приватните Blockchain системи, кои се системи управувани од еден централен ентитет. Учесниците во приватните Blockchain системи се додаваат на покана на носителот на Blockchain системот или по претходен договор. За коректноста на податоците се грижи сопственикот на системот или друго авторизирано тело во Blockchain системот.

Кај Blockchain технологиите кои се без дозвола, практично корисниците може да пристапат кон системот без притоа да имаат посебна дозвола за пристап, односно корисниците нема потреба да бидат авторизирани и автентифицирани. Основно барање за интеракција со мрежата на Blockchain системите без дозвола е да се поседува паричник кој може лесно да се создаде анонимно, а исто така може и да се верифицира. Спротивно на овој пристап, кај Blockchain системите со дозвола, секој корисник во мрежата добива сметка од авторизирано тело, притоа обезбедувајќи лични податоци за идентификација.

Најзастапени се јавните без дозвола Blockchain технологии, претставени со најпознатите платформи Bitcoin и Ethereum. Отвореноста на мрежата и неограничениот пристап овозможи овие технологии да бидат брзо и широко прифатени. Овој тип на Blockchain технологии е соодветен за употреба во сценарија каде анонимноста на податоците е доволна за заштита на приватноста на корисниците. Други познати Blockchain технологии од овој тип се Litecoin [47], Monero [48], Dash [49] и други.

Јавни со дозвола Blockchain системи се отворени мрежи каде учесниците треба да покажат информација за единствен идентитет. Со цел да се заштити реалниот идентитет, корисниците може да пристапат кон ваквиот тип на систем со помош на трети страни кои се авторизирани за обезбедување на приватност на личните податоци или преку користење на Zero-knowledge proof (ZKP) [50] алгоритам за да се докаже уникатноста на учесниците. Најпознати решенија од овој тип на Blockchain технологии се: Sovrin [51], EOS [52], Ripple [53] и други.

Следен тип се приватни со дозвола Blockchain технологии. Овие Blockchain технологии овозможуваат да се изгради мрежа од добро познати учесници притоа овозможувајќи заштита на инфраструктурата и податоците во системот. Најпознат Blockchain од овој тип е Hyperledger Fabric [54]. Централизираноста на оваа мрежа фрла сенка на транспарентноста на процесите во мрежата и дава можност сопственикот на мрежата да ги злоупотреби податоците кои циркулираат во мрежата.

Помалку познат тип на Blockchain системи се приватните без дозвола Blockchain системи. Овие системи дозволуваат учесниците да градат приватни мрежи (најчесто ад-хок мрежи), а притоа истите да не бидат авторизирани и автентифицирани при интеракцијата помеѓу себе. Учесниците во овие системи соработуваат на краткорочни задачи од заеднички интерес (на пример, учење на околината, креирање на заедничко знаење) и на тој начин ја одржуваат коректноста на системот. Најпознати решенија од овој тип на Blockchain технологии се: Holochain [55], LTO Network [56] и Monet [57].

Конзорциум Blockchain системите се парцијално децентрализирани системи, каде учесниците може да бидат вклучени во процесите преку механизми слични на оние кои се наоѓаат во јавните Blockchain системи. Поради концентрирањето на моќта за верификација на податоците во помал број на учесници, конзорциум Blockchain системите се доближуваат до перформансите на приватните Blockchain системи. Во литературата постојат повеќе дефиниции за конзорциум Blockchain системите. Според Бутерин [58] конзорциум Blockchain системите се посебен тип на Blockchain системи кои делат карактеристики и со јавните и со приватните Blockchain системи, но се незначително поблиски до приватните Blockchain системи бидејќи делат повеќе карактеристики со нив. Според други извори [59] конзорциум Blockchain системите може да се сметаат за јавни, со дозвола системи, поради отвореноста на Blockchain технологијата, мрежата и податоците кои циркулираат во неа, но се јавува потреба учесниците да бидат автентифицирани за да можат да стапат во интеракција со Blockchain системот. Заеднички за овие дефиниции е фактот дека конзорциум Blockchain технологиите се Blockchain технологии со дозвола, а другите делови од системот може да бидат дефинирани и како јавни и како приватни, во зависност од имплементациското сценарио.

Ограничениот пристап кај конзорциум Blockchain системите само за авторизирани корисници, е овозможен со имплементација на дополнителни механизми за подобрување на безбедноста во мрежата. На таков начин овие решенија би овозможиле оптимизирање на внатрешните процеси во мрежата, особено преку дефинирањето на правилата за пристап до информациите и ограничувањето на пристапот на учесниците. Контролата на пристапот може да биде управувана од еден ентитет или да биде дистрибуирана кај сите партнери во мрежата. Нови учесници во мрежата може да се додаваат преку механизам на покани или преку усогласување на соодветни карактеристики од Self-Sovereign Identity (SSI) [60] на учесниците или пак користење на Zero-knowledge proof (ZKP) [50] алгоритми. Во конзорциум мрежата препорачливо е да се имплементира ентитет за контрола на пристап до мрежата кој ќе треба да го контролира пристапот на учесниците во мрежата како и нивното однесување.

Учесниците во конзорциум мрежата може да имаат една од двете основни улоги: *валидатор* или *корисник*. Улогата на валидаторот е да предлага нови податочни блокови, но и да учествува во одржувањето на консензус механизмот. Спротивен на валидаторот е корисникот, кој има можност само да ги чита податоците и да создава нови трансакции.

Конзорциум Blockchain системите имаат слична податочна структура како и другите Blockchain технологии, со соодветни измени за да се прилагоди податочниот блок кон консензус механизмот кој се применува. Карактеристиките кои ги нудат конзорциум Blockchain технологиите ги прават најдобар избор за градење на јавен здравствен систем базиран на Blockchain технологија.

Во Табела 3.1 дадена е разликата помеѓу јавните, приватните и конзорциум Blockchain системите.

Табела 3.1. Разлика помеѓу јавните, приватните и конзорциум Blockchain системите

	Јавни	Приватни	Конзорциум
Управување со пристап	Без дозвола/со дозвола	Без дозвола/со дозвола	Без дозвола/со дозвола
Дозвола за читање	Секој	Само поканети корисници	Поканети корисници/Секој
Дозвола за запишување	Секој	Авторизирани корисници	Авторизирани корисници/Секој
Сопственост	Ничија	Еден ентитет	Повеќе ентитети
Анонимност на учесниците	Да	Не	Да/Не
Проток на трансакциите	Мал	Голем	Голем
Архитектура	Целосно децентрализирана	Целосно централизирана	Парцијално децентрализирана
Пристап	Секој корисник	Со покана	На барање
Консензус механизми	PoW или PoS	PoS или BFT-базирани	PoS или BFT-базирани
Непроменливост на податоците	Тешко менливи	Со договор	Со договор
Цена на користење	Скапа	Евтина	Евтина
Скалабилност	Мала	Голема	Умерена

3.2. Blockchain дистрибуирана мрежа

Прагмата за дистрибуираните компјутерски мрежи во кои треба да се понудат високодоверливи сервиси, бара при дизајнирањето на ваквите системи да се воведат редундантност на сервисите. Покрај редундантноста на сервисите, истата предвидува и редундантност на серверите како и редундантност на податоците. Притоа серверите може да бидат колоцирани во иста просторија, но може и да бидат дистрибуирани на поголема територија, за да се обезбеди повисок степен на заштита дури и во услови на природни непогоди. Овој пристап на распоредување на идентични сервери во истата мрежа за да се обезбеди редундантност и отпорност на испади на системот се нарекува репликација на состојбата на машините (state machine replication) [61]. Главна цел е да се постигне високо ниво на достапност на сервисите и податоците.

Градењето на дистрибуирани компјутерски мрежи и сервиси, има потреба од синхронизираност помеѓу јазлите во мрежата. При синхронизацијата треба да се обезбеди доволен број на реплики од истите сервиси и податоци и тие да бидат дистрибуирани низ серверите во мрежата, за да се обезбеди коректна работа на системот и во услови на испад на некој од серверите. Податоците кои се запишуваат и реплицираат низ серверите потребно е да бидат исти во секој сервер, реплицирани на време и универзални за целиот систем.

Во основа под поимот испад на серверот се смета хардверска неисправност на делови од серверот, грешки во меморијата, испади на тврди дискови во серверите или во крајна линија целосен испад на серверот. Покрај ваквите основни грешки кои може

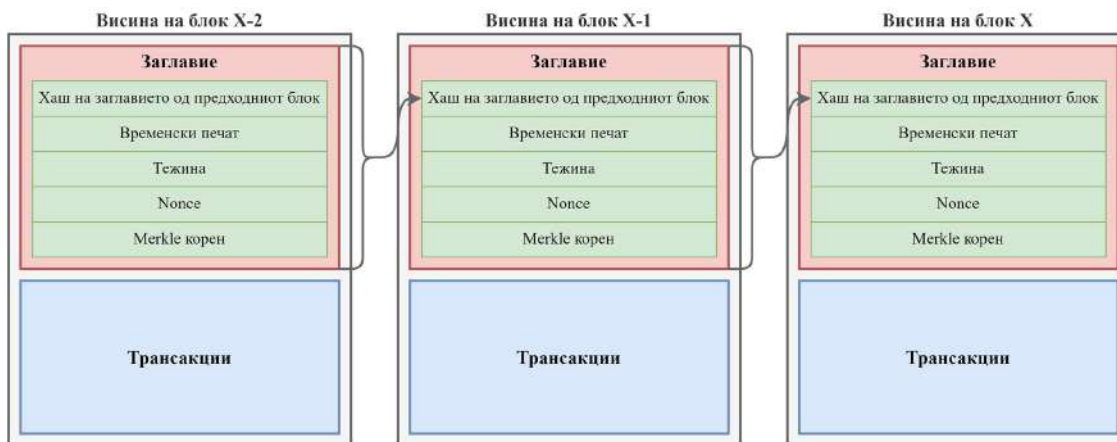
да се појават во системот, постојат и таканаречени Византиски грешки (Byzantine faults) кои за прв пат се дефинирани во [62]. Во овој труд за прв пат е воведен и проблемот на Византиските генерали (Byzantine generals problem). Византиските грешки се малициозни грешки кои се генерираат со намера преку испраќање на двојбени информации во системот до различни корисници, истите да се доведат во заблуда за фактичката состојба на системот и на тој начин да се добие одредена корист. Со генерирањето на вакви грешки во еден дистрибуиран систем, се дава погрешна слика за состојбата на одреден сервер. Детекцијата на Византиска грешка е голем предизвик поради непредвидливоста на однесувањето на серверот. За да може останатите учесници во мрежата да одлучат дали даден сервер е малициозен, тие треба да се согласат најпрво на тоа што е општа вистина, но тоа е проблем кога во системот има малициозни сервери.

Истражувања поврзани со репликација на состојба на машините датираат уште од раните 80ти години на минатиот век, но повторно истите го привлекуваат вниманието откако Bitcoin Blockchain технологијата доби висока популарност. Практично Bitcoin е првата глобална дистрибуирана компјутерска мрежа која користи механизам за репликација на состојбата на машините и е изградена од целосно непознати учесници, во услови на недоверливост меѓу учесниците и асинхрон пристап во внесувањето записи во мрежата. Таа е првата мрежа каде успешно се имплементира јавен механизам за Толеранција на Византиски грешки (Byzantine Fault Tolerance mechanism) [63]. Основна цел на овој механизам е индивидуалните учесници во мрежата кои имаат сопствено складиште за податоци, да овозможат градење на универзална вистина во системот преку активно синхронизирање на податоците од системот, на тој начин креирајќи заедничка Blockchain база на податоци, која ќе биде зачувана во секое индивидуално складиште.

3.3. Blockchain податочна структура

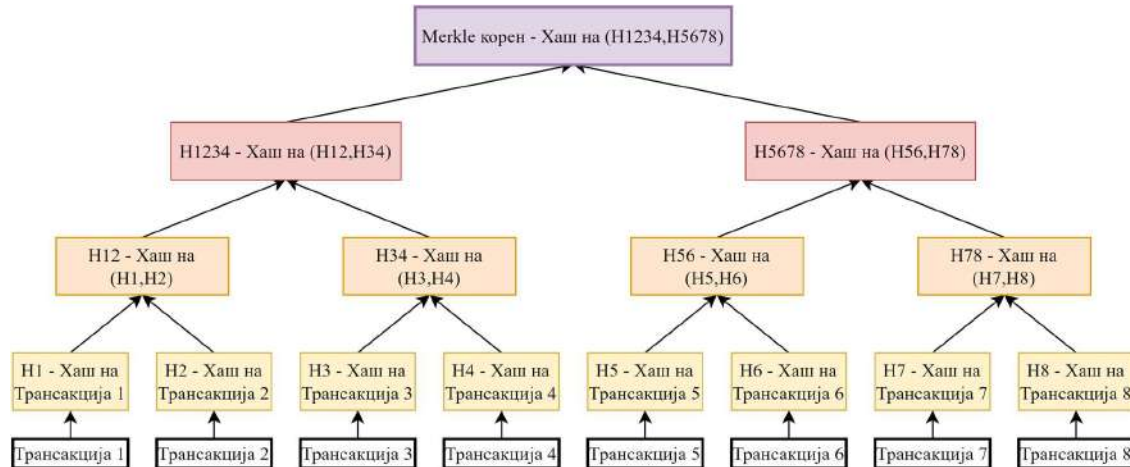
Складирањето на податоците во заедничката Blockchain база на податоци се врши преку имплементација на новата податочна структура која има формат кој е прикажан на Слика 3.1. При формирањето на Blockchain податочната структура се користи криптографска хаш функција [64]. Хаш функциите се еднонасочни функции каде за блок од влезни податоци на излез од функцијата се добива хаш вредност која претставува уникатен отпечаток за влезниот блок податоци, а притоа на никаков начин не ја открива корелираноста на влезните и излезните податоци. Главна карактеристика на хаш функциите е тоа што за исти влезни податочни блокови, секогаш генерираат иста хаш вредност. Доколку два влезни податочни блокови се разликуваат, па макар и само во еден бит информација, хаш вредноста која ќе се добие, ќе има значителна разлика, поради што не е возможно да се направи корелација помеѓу влезните и излезните податоци.

Секој податочен блок е составен од заглавие и листа со трансакции. Во зависност од тоа како дадена Blockchain технологија е дефинирана, полињата во заглавието се разликуваат кај различните Blockchain технологии. Генерално во заглавието задолжителен дел е хаш вредноста од претходниот податочен блок, висина и/или временска информација за дадениот блок што претставува информација со која се потврдува редоследот на блоковите, како и Merkle корен [65] за тековниот блок.



Слика 3.1. Структура на Blockchain базата на податоци

Merkle корен претставува последната хаш вредност за дадено Merkle дрво [65] кое се гради преку рекурзивно имплементирање на хаш функција врз даден блок од трансакции. Процесот на градење на Merkle дрво започнува со поделба на податочниот блок на помали сегменти, за кои се пресметува хаш вредност, потоа тие хаш вредности повторно се групираат и за нив се пресметува хаш вредност. Ваквата постапка се продолжува додека не се добие единечна хаш вредност која понатака не може да се комбинира со друга хаш вредност. Конечната хаш вредност е Merkle корен хаш вредност за податочниот блок. На Слика 3.2 е дадена Merkle дрво структурата за даден податочен блок.



Слика 3.2. Merkle дрво

Blockchain податочната структура е составена од поединечни меѓу себе зависни последователни податочни блокови. Поврзувањето на последователните податочни блокови се прави преку генерирање на референтна точка во тековниот податочен блок кој ќе го поврзува со претходниот податочен блок, кој што веќе е запишан во Blockchain базата на податоци. Со референцирањето на претходниот блок се прави цврста врска помеѓу тековниот и претходниот податочен блок и структура на записите налик на синџир, па од таму е и англискиот назив Blockchain (Синџир од блокови). Постапувањето на хаш вредноста од претходниот податочен блок во тековниот податочен блок, овозможува проверливост на коректноста на блоковите со информации. Проверката за

коректност на хаш вредностите, односно поврзувањето меѓу блоковите се прави од почетниот (genesis) блок се до тековниот податочен блок. Доколку при проверката се добие дадена хаш вредност која не се вклопува во синцирот од блокови, тоа значи дека има обид за промена на содржината на блоковите. Токму механизмот на поврзување на податочните блокови и можноста за проверливост на податоците ги прави Blockchain технологиите да бидат високо доверливи.

Записите во Blockchain базата на податоци, треба да ги следат правилата за градење Blockchain податочната структура. Есенцијално за Blockchain технологиите е тоа што Blockchain базата на податоци покрај тоа што треба да ја има истата податочна структура кај сите корисници, таа треба да има содржина која е синхронизирана кај сите корисници. Тоа значи дека во Blockchain системот сите корисници треба да градат една универзална вистина за содржината на Blockchain базата на податоци. Неминовен факт е дека во системите може да учествуваат и малициозни корисници кои би сакале да ги злоупотребат истите за лична корист преку воведување на Византиски грешки. За да се оневозможи малициозни корисници да ја менуваат содржината на записите како и да вметнуваат неточни информации, потребно е сите корисници на Blockchain системот да имаат увид во новите трансакции, за истите да извршат верифицирање на фактите и на крај да го дадат своето мислење преку потврда за точноста на податочниот блок. Оваа постапка е овозможена преку користење на дистрибуирани протоколи за постигнување консензус околу предложените податочни блокови, познати како консензус механизми.

3.4. Консензус механизам

Механизмите за толеранција на Византиски грешки, уште попознати како *консензус механизми* [66], претставуваат процедури кои се спроведуваат помеѓу дистрибуираните јазли во мрежата за да обезбедат усогласување на ставовите или содржините меѓу учесниците во мрежата, преку повеќекратна размена на пораки со кои се потврдува коректноста на записите од страна на сите учесници во мрежата. Консензус механизмите треба да бидат способни во услови на било какви напади од страна на малициозните корисници да успеат да ги усогласат ставовите на корисниците и коректноста на записите кај сите корисници.

При постигнувањето на консензус во мрежата, голем предизвик е да се натераат учесниците во мрежата, кои не се познаваат меѓу себе, да се однесуваат чесно. Постојат неколку пристапи со кои може да се поттикнат учесниците, при процесот на постигнување консензус да играат фер. Генерално чесните учесници очекуваат стабилна мрежа или систем и некаква форма на награда за нивната лојалност. Во зависност од тоа со што и на каков начин се поттикнуваат учесниците, постојат повеќе консензус механизми. Основни начини на поттикнување на фер игра се решавање на сложувалка, обложување, заработување поени, добивање привилегии и други. Врз основа на тоа, во литературата се дефинирани повеќе консензус механизми, меѓу кои најпознати се Proof-of-Work (PoW) [1], [3], [4], Proof-of-Stake (PoS) [5], Proof-of-Authority (PoA) [67], Proof-of-Elapsed-Time (PoET) [68], Practical Byzantine Fault Tolerant (PBFT) [6], Tendermint [7], Swirlds Hashgraph [8], Tangle [9] и други.

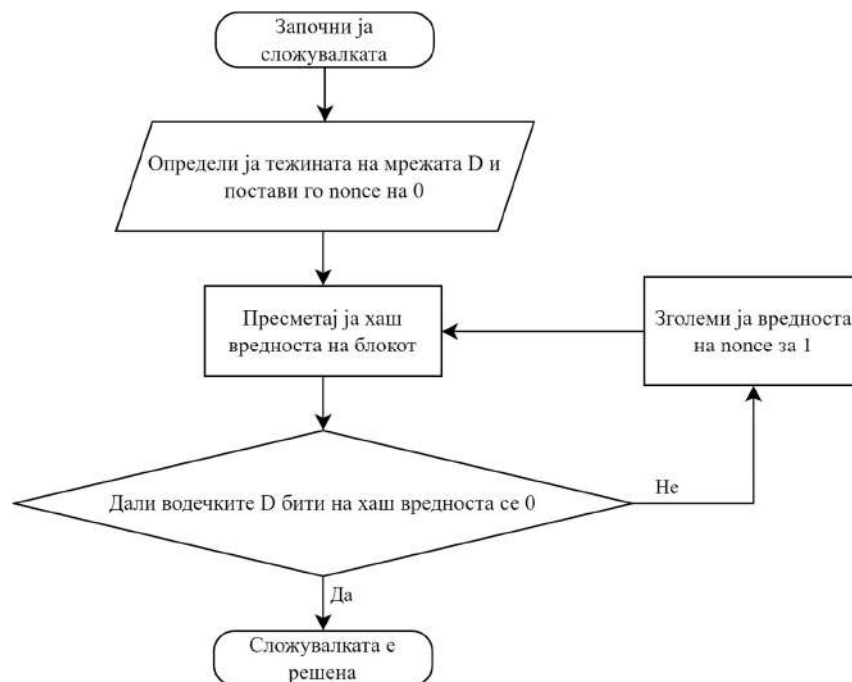
Иницијалниот развој на консензус механизмите бил за приватни или корпоративни средини, каде треба да се изградат мрежи со висока доверливост (во авионите, нуклеарните центри и друго). Главна цел од имплементацијата на консензус механизмите била, во дистрибуираните компјутерски системи да се обезбеди синхронизираност на записите во базите на податоци и да се обезбеди отпорност на испади и детекција на грешки. Првите решенија за консензус механизми [69] имале

општа употребна вредност и одлични теоретски карактеристики, но тешко применливи во пракса. Првиот консензус механизам кој бил припремен за практична употреба бил Practical Byzantine Fault Tolerance (PBFT) [6] консензус механизмот, чија дефиниција се појавува кон крајот на 90тите години од минатиот век. Првите консензус механизми обезбедувале заштита од 1/3 малициозни учесници во мрежата, но со развојот на првата Blockchain технологија, односно Bitcoin мрежата, креираниот систем овозможувал робусност и капацитет да го заштити системот од 1/2 малициозни учесници. Успехот на Bitcoin системот во целина, претставува иницијална искра за нов циклус на истражувања и развој на консензус механизми.

3.4.1. Proof-of-Work и Proof-of-Elapsed-Time (PoW без рударење)

За прв пат Proof-of-Work консензус механизмот е воведен во 2008 година како дел од Bitcoin технологијата [1], воедно истиот претставува прв консензус механизам кој го решава проблемот за децентрализирано постигнување договор во околина каде нема доверба меѓу учесниците. Покрај во Bitcoin, PoW консензус механизмот се користи и во Litecoin (2011) и Ethereum (2015) платформите. PoW е најраспространетиот консензус механизам меѓу Blockchain технологиите со оглед на фактот што Bitcoin, Litecoin и Ethereum делат повеќе од 80% од крипто пазарот, а тоа се должи на високото ниво на заштита што ја нуди овој консензус механизам. Blockchain технологиите кои се базирани на PoW, овозможуваат заштита од 1/2 малициозни јазли односно заштита од 51% нападот, што во пракса би значело дека се додека повеќе од половината јазли се однесуваат коректно во системот, истиот секогаш ќе може да носи коректни одлуки. Со други зборови, за да може група од напаѓачи односно малициозни учесници да обезбеди неточни податоци да циркулираат во системот, истите треба да обезбедат 51% процесирачка моќ во системот.

Влогот за високото ниво на заштита е високата цена за одржување на консензусот во системот поради интензивната процесирачка работа што континуирано треба да се извршува за да се реши предизвикот кој е во форма на сложувалка. Процедурата за решавање на сложувалката е дадена на Слика 3.3. Главен начин на поттикнување на корисниците за да ја решат сложувалката е наградата што се добива за успешно решавање на истата. Учесниците кои ја решаваат сложувалката, уште познати како *рудари* (miners), се во трка кој побрзо да ја реши сложувалката, бидејќи тие што ќе бидат први ја делат наградата. Решавањето на сложувалката во пракса претставува интензивен процес на пробување на различни вредности за полето наречено *nonce* (види Слика 3.1). Кога рударот ќе ја најде бараната вредност, ја споделува најдената информација со останатите корисници на мрежата за да ја добие наградата. Вредноста на полето *nonce* се определува преку постојано пробување на различни вредности за *nonce* полето почнувајќи од 0, се додека рударот не најде вредност која треба да даде хаш вредност за тековниот податочен блок така што започнува со однапред договорен минимален број на нули. Бројот на нули кој е дефиниран со алгоритмот ја дефинира тежината на мрежата. Поради користење на хаш функција во процесот на определување на *nonce* полето, не е возможно истото да се најде преку имплементација на хаш функцијата во обратна насока, туку истата може да се најде само преку процедура на пробување. Како хаш функции во Bitcoin и Litecoin се користи SHA-256 [70], а во Ethereum се користи KECCAK-256 [71] (или SHA-3).



Слика 3.3. Процедура за решавање на слојувалката кај PoW консензус механизмот

Механизмот на слојувалка се активира кога се генерира нов блок во мрежата, а тоа е на секои 10 минути кај Bitcoin мрежата и на секои 12-15 секунди кај Ethereum мрежата. Трансакции во системите може да се генерираат во секое време, но верификација на трансакцијата се прави кога истата се вметнува во блок. За да се обезбеди висока веројатност дека податочниот блок е безбеден од потенцијални малициозни напади и модификации кои би ги правеле малициозните јазли, потребно е истиот да има доволен број на потврдени блокови кои доаѓаат после него. Така кај Bitcoin мрежата потребни се 6 потврдени блокови за да се каже дека даден податочен блок е финализиран, додека кај Ethereum потребни се 12 потврдени блокови. Финализирањето на трансакциите кај PoW е од пробабилистичка природа и само натпреварувачки сет од јазли кои имаат повеќе од половина од вкупната процесирачка моќ во мрежата, може да ги обработат сите податочни блокови преку креирање на нова Blockchain линија и на тој начин да вметнат фалсификувани податоци. За да се зголеми веројатноста дека блокот кој е потврден нема да биде модифициран, потребно е да има поголем број на последователни потврди, но тоа би го зголемило времето потребно за чекање да една трансакција биде финализирана. Дефинираниот број на потврди кај Bitcoin и Ethereum мрежите е баланс помеѓу времето потребно да се чека за блокот да се финализира и веројатноста да се создаде нова алтернативна линија која би ја променила фактичката состојба. Така кај Bitcoin мрежата потребни се 60 минути за да се финализира блок од трансакции, додека кај Ethereum потребни се само 3 минути. Поради големите интервали на создавање нови податочни блокови, технологиите што го користат PoW имаат помал проток на трансакции низ системот што не можат да го следат трендот на растење на самите Blockchain технологии.

Поради големата потрошувачка на електрична енергија за одржување на PoW базираните Blockchain технологии, се бараат алтернативни консензус механизми кои би можеле да обезбедат исто ниво на робусност, но би имале помала потрошувачка на енергија. Како енергетски ефикасна алтернатива на PoW е Proof-of-Elapsed-Time (PoET)

консензус механизмот [68]. PoET консензус механизмот е мимикрија на PoW консензус механизмот, каде наместо скапото рударење преку кое се избира најбрзиот пронаоѓач на попсе вредноста, кај PoET се користи принципот на лотарија. Учесниците во PoET базирана мрежа користат алгоритам за случаен избор на време во кое тие треба да спијат или да бидат деактивирани. Откако ќе помине периодот на спиење, првиот кој ќе се разбуди ќе биде среќниот добитник на наградата во консензус процесот. PoET консензус механизмот користи комерцијално базирано решение на Intel, Software Guard Extension (SGX) [72] кое овозможува да се имплементира процесот на случајно заспивање и будење кај јазлите. Зависноста на PoET од комерцијални решенија, фрлаат сенка на транспарентноста на консензус механизмот. Дополнително SGX инструкцискиот сет е подложен на напади, а постои и потенцијален ризик за протекување на клучеви преку SGX инструкциите. Најзначајна примена на PoET е во Hyperledger Sawtooth проектот [73].

3.4.2. *Proof-of-Stake и негови варијанти*

Екстремните трошоци за електрична енергија поврзани со процесот на рударење кај PoW консензус механизмот, ги мотивира дизајнерите да бараат алтернативни консензус механизми. Една од алтернативите која овозможува високо ниво на заштита против малициозни јазли е Proof-of-Stake (PoS) консензус механизмот [5]. PoS го заменува компетитивниот механизам што се наоѓа кај PoW, со метод на обложување, но притоа го задржува високиот степен на заштита во системот кој овозможува отпорност од 51% нападот.

Консензус механизмот кај PoS се управува од одбран сет на учесници, наречени валидатори. Генерално идејата кај PoS е да се мотивираат валидаторите да одржуваат коректен консензус во мрежата што е особено важно за оние валидатори кои имаат складирано дигитални средства во мрежата. Таа мотивација не е доволна бидејќи секогаш ќе постојат валидатори што ќе сакаат да извршат малициозни активности, а згора на тоа самиот процес на валидација е брз и економичен па секој би можел да направи напад. Затоа потребно е да се воведат механизам на казна за малициозните валидатори. За таа цел секој валидатор депонира средства кои ќе бидат замрзнати во системот за подоцна ако изврши малициозна активност истите да му бидат одземени. Механизмот на казна е потребен бидејќи ако валидаторите не депонираат средства кои ќе бидат замрзнати во системот, тие може да ги валидираат сите трансакции кои се генерираат во системот, што многу лесно може да доведе до делби на мрежата. Ова однесување го дефинира проблемот „Ништо за влог“ (Nothing-at-stake). За да се надмине проблемот, учесниците кои се избираат за валидатори заложуваат дел од нивните средства кои може да бидат во форма на дигитални крипто валути, жетони (tokens), идентитет и друго. Според количината на заложени средства се определува и тежината на нивниот глас во процесот на валидирање на трансакциите. На овој начин тие ја потврдуваат нивната намера дека сакаат да учествуваат во процесот на валидирање и се повлекуваат од идејата да го извршат нападот „Ништо за влог“. Средствата кои се вложени се заклучуваат и не можат да се користат се до моментот додека валидаторот не посака да истапи од процесот на валидирање. За успешно валидирање валидаторите добиваат награда, но за малициозно валидирање она што е вложено ќе биде целосно одземено, а валидаторот може да биде блокиран за учество во мрежата.

Во зависност од процесот и параметрите за селекција на валидатори, постојат повеќе типови на PoS консензус механизми. Некои од попознатите варијанти на PoS [74] се:

- Делегиран (Delegated) PoS што претставува варијанта на PoS каде учесниците во мрежата гласаат за другите учесници од мрежата да бидат избрани за валидатори. Количината на вложени средства ја определуваат тежината на неговиот глас. Учесниците кои добиваат најмногу гласови се избираат за делегати. Делегатите се должни да го обезбедат консензусот за што добиваат и награда, но доколку изведат малициозна активност добиваат казна.
- Во Течниот (Liquid) PoS валидаторите може да делегираат други валидатори да учествуваат во консензус механизмот, но тоа е само опционо право, бидејќи делегирањето на малициозен делегат ќе го казни и валидаторот кој го предложил тој малициозен делегат.
- Врзан (Bonded) PoS е сличен на Течниот PoS каде покрај валидаторот, санкции за малициозни активности добива и самиот делегат.

Покрај основниот PoS механизам, постојат и хибридни варијанти, каде PoS се комбинира со други консензус механизми. Така PoS/PoW е консензус механизам кој имплементира PoW консензус механизам на однапред определен временски интервал за да ги осигура PoS валидираните податочни блокови кои се генерирани помеѓу два PoW интервали. На ваков начин се користат бенефитите од двата консензус механизми.

Посебен тип на PoS консензус механизам е Proof-of-Authority (PoA) консензус механизмот каде учесниците го вложуваат својот идентитет како дигитално средство и гарантираат за фер процес на валидирање. Впрочем главниот мотив за учество во PoA базирана мрежа е да се издигнува репутацијата на учесникот во PoS базирана мрежа каде изборот на валидатори не зависи од вложените средства. Најпозната Blockchain технологија која го употребува овој консензус механизам е VeChain [75].

3.4.3. *Practical Byzantine Fault Tolerant*

Прво практично решение на проблемот на Византиските генерали (Byzantine Generals problem) е Practical Byzantine Fault Tolerance (PBFT) консензус механизам кој за прв пат е воведен во 1999 [6]. Со овој консензус механизам може да се обработат голем број на трансакции во неколку секунди, што е ветувачки параметар за Blockchain решенија кои имаат потреба од голем проток на трансакции и со тоа е компетитивен консензус механизам на PoW и PoS консензус механизмите. Една негативна страна е тоа што обезбедува помала заштита од малициозни јазли споредено со PoW и PoS. PBFT консензус механизмот е способен да ја заштити мрежата од 1/3 малициозни јазли. За да се управува консензус механизмот, валидаторите во мрежата разменуваат голем број пакети меѓу себе со кои се врши гласање по однос на коректноста на предложените податочни блокови. Со тоа се прави голем мрежен сообраќај, со што PBFT е непрактичен да се имплементира во мрежи со голем број валидатори. Овој консензус е имплементиран во рамките на Hyperledger Sawtooth PBFT [76] решението.

PBFT консензус механизмот дефинира еден учесник во мрежата да биде предлагач, додека другите учесници се таканаречени реплики. Предлагачот формира податочен блок од трансакции кои треба да бидат валидирани и го започнува консензус алгоритмот кој се одвива во три фази: пред-подготвителна (pre-prepare), подготвителна (prepare) и извршна (commit) фаза. Трансакциите се процесираат преку прегледи (views). За секој преглед има процедура од циклична (round robin) селекција на предлагачи на преглед. Секој предлагач на преглед, познат како примарен (primary) предлагач, собира трансакции од клиентите, им припишува секвенциски број и креира пред-подготвителна порака. Пред-подготвителната порака се испраќа до сите процеси кои имаат преглед и секвенциски број. Репликите ја прифаќаат пред-подготвителната порака ако претходно

немаат прифатено друга порака со ист преглед и секвенциски број, притоа претпоставувајќи дека пораката е за моменталниот преглед и е потпишана од моменталниот примарен предлагач.

Кога пред-подготвителната порака е прифатена од репликите, се креира подготвителна порака која се потпишува од репликите и се испраќа до сите корисници во мрежата. Откако репликите ќе добијат доволен број подготвителни пораки со ист преглед и секвенциски број, се вели дека репликата е подготвена да одговори на даден клиент. Секвенцискиот број на пред-подготвителната и подготвителната порака осигурува целосен ред во еден преглед од барања. Откако репликата ќе биде подготвена, составува извршна порака, ја потпишува и ја испраќа до сите учесници во мрежата. Извршната порака се прифаќа само ако потписот и прегледот за податочниот блок се коректни. Кога ќе се прими извршна порака од страна на сите реплики, тие го спроведуваат барањето на клиентот и ги спроведуваат инструкциите што се дадени на машините за состојба (state machine instructions).

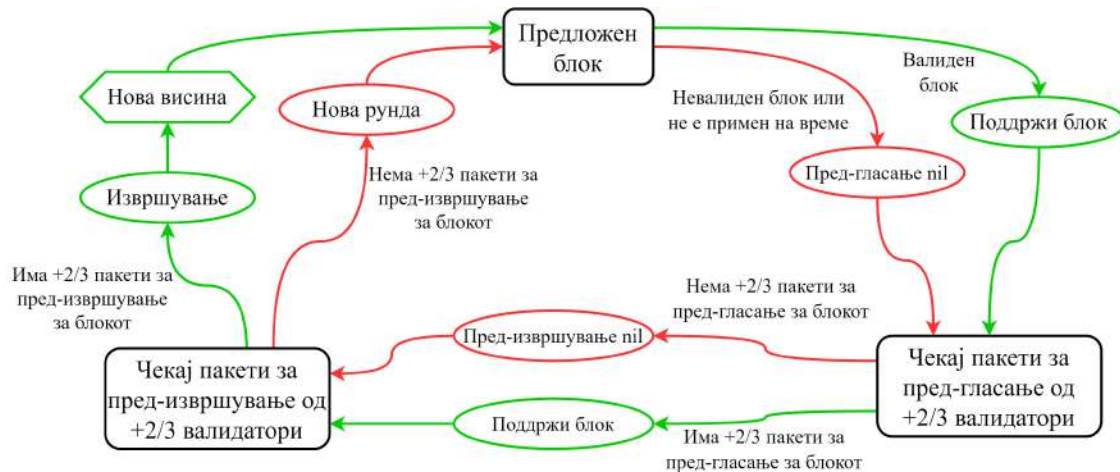
Процедурата за креирање на порака се заснова на еден ентитет (еден предлагач по преглед, кој е статички избран) кој може да дејствува малициозно. За да се надмине проблемот ако примарниот предлагач се однесува малициозно, PBFT имплементира процедура за промена на преглед (view-change). Процедурата за промена на преглед е комплексна процедура за која е потребно да се постигне консензус за да може да се покрене. Новиот преглед треба да биде составен од сите барања на клиентите кои се примени со последната извршна порака. Репликите во мрежата користат интервали за пауза (timeout intervals) за да можат да ја набљудуваат пред-подготвителната порака од примарниот предлагач, при што можат да детектираат малициозен примарен предлагач. Доколку интервалот на пауза истече и притоа не се прими пред-подготвителна порака, се покренува процедура за промена на преглед. Интервалот за пауза се враќа на иницијалната вредност откако би се добило клиентско барање.

Комплексниот механизам на промена на преглед, е главна причина за неприфаќањето на овој консензус механизам во Blockchain решенијата, што може да доведе до целосно блокирање на консензус механизмот кога во неколку последователни промени би се одбрале малициозни примарни предлагачи.

3.4.4. Tendermint

Tendermint [7] е уште еден PBFT базиран консензус механизам со високи перформанси, но со значително побрзи, побезбедни и поробусни процедури за постигнување на консензус. Главна предност на Tendermint над PBFT е исфрлањето на процедурата за промена на преглед и имплементирањето на процедура за избор на предлагач за секој нов податочен блок со што се придонесува кон подобра стабилност на мрежата и се избегнуваат потенцијални ситуации во кои би се блокирал консензус механизмот. Други подобрувања споредено со PBFT се воведувањето на механизам за заклучување на глас и nil (нулти) глас. Со заклучувањето на глас се присилува валидаторот да гласа само за еден податочен блок и притоа да се однесува коректно, односно да не може да се предомисли во следната фаза од гласањето. Предноста на употребата на nil гласот е тоа што со користење на истиот се известува мрежата дека валидаторот е активен и се однесува коректно со ситуации кога истиот испуштил некој од интервалите за гласање или не може да гласа за или против за даден податочен блок. Практично со nil гласот, валидаторот покажува воздржаност од дејствување во услови кога не е целосно сигурен за точноста за дадена процедура или податок.

Консензусот во Tendermint се спроведува во рунди [7], за кои претходно е определен предлагач чија улога е да ги собира трансакциите кои треба да се постават во нов податочен блок и истиот да се испрати до валидаторите. За предложениот податочен блок валидаторите гласаат во три фази: пред-гласање (pre-vote), пред-извршување (pre-commit) и извршување (commit). Една рунда од процесот на гласање за даден податочен блок е претставена на Слика 3.4.



Слика 3.4. Една рунда од процесот на гласање кај Tendermint консензус механизам

Трансакциите кај Tendermint се организираат во податочни блокови, а секој нареден податочен блок има поголема висина (height) од претходниот. За секоја висина во Blockchain структурата се извршува најмалку една рунда на гласање во три фази. Во случај на недоволен број на собрани коректни гласови за предложениот податочен блок во било која од фазите, се спроведува нова рунда на гласање. Кога валидаторите ќе соберат доволен број на пред-извршни гласови, рундата се финализира и се извршува, после што се зголемува висината на следниот податочен блок.

Tendermint нуди исто ниво на заштита од малициозни валидатори како и повеќето PBFT базирани консензус механизми, што значи дека може да го заштити системот од 1/3 малициозни валидатори. За да може да се обезбеди таа заштита при процесот на гласање, во секоја од фазите потребно е да се соберат 2/3 потврдни гласови од страна на сите валидатори во мрежата. Како што е прикажано на Слика 3.4, рундата започнува со предлагање на податочен блок. Притоа предложениот блок треба да има подредена структура од трансакции претходно собрани во динамичката меморијата mempool на предлагачот. Во фазата за пред-гласање, претходно одбрани валидатори гласаат со поддршка за податочниот блок или со nil глас. Откако ќе се соберат 2/3 гласови во фазата за пред-гласање (независно дали се валидациски гласови или nil гласови), се преминува во пред-извршната фаза. Доколку во фазата за пред-гласање се собрал 2/3 гласови, се преминува во фаза на пред-извршување, но доколку не се соберат 2/3 гласови рундата се продолжува со пред-извршен nil глас. И во двата претходни случаи, валидаторите треба да испратат пред-извршен глас со цел да се продолжи тековната рунда на гласање. Откако ќе се соберат 2/3 гласови во пред-извршната фаза се преминува во извршна фаза, после што се зголемува висината на податочниот блок. Доколку не се соберат 2/3 гласови во пред-извршната фаза, започнува нова рунда на гласање со нов предлог за податочен блок. Интервалите за фазата за пред-гласање, пред-извршување и извршување се во рангот на неколку стотина милисекунди (500-3000ms) со што се овозможуваат мали интервали за комплетирање на рундите за гласање како и за

постигнување на консензус. Со тоа финализирањето на консензусот е во опсегот од 1-3 секунди.

Овој едноставен процес на гласање овозможува брзо финализирање на блоковите, а воедно и големи протоци на трансакции, што е потврдено во [77], [78], [79]. Tendermint консензус механизмот може да ја заштити мрежата од 1/3 малициозни јазли, што бара бројот на валидатори во мрежата да биде $n=3*f+1$ каде f е максимален број на малициозни јазли за дадениот број на валидатори [80].

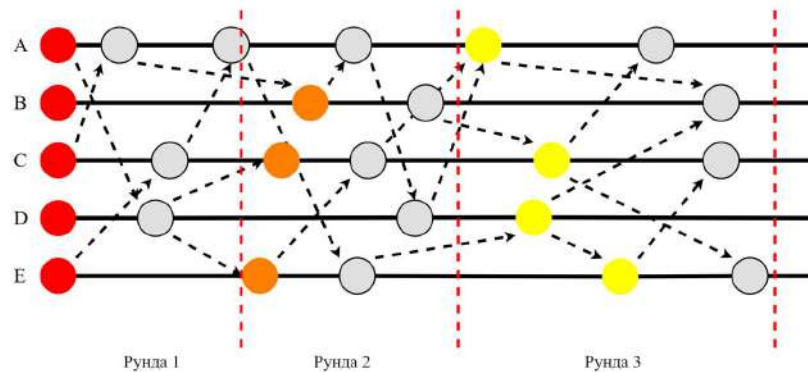
Валидаторите во мрежата интензивно разменуваат пораки со гласови за да постигнат консензус, со што се создава бура од пораки меѓу валидаторите во мрежата. Валидаторите гласаат позитивно за коректен податочен блок, при што порака со гласање се испраќа до сите валидатори во мрежата. Дури и да биде податочниот блок некоректен или задоцнет, валидаторот гласа со nil глас, што исто така придонесува кон создавањето бура од пораки во мрежата. Бројот на разменети пораки се зголемува експоненцијално со зголемувањето на валидатори во мрежата. Со тоа се влијае на мрежниот опсег што е особено изразено во сценарија на големи мрежи. Во [14] и [81] се посочува на проблемот што Tendermint консензус механизмот го има во мрежи со голем број валидатори. Генерално проблемот во сценаријата со голем број валидатори е последица на ограничената процесорска моќ на валидаторите, ограничениот мрежен опсег и зголемената комплексност за постигнување на консензус поради зголемениот број на разменети пораки. Поради овие ограничувања препораката е максималниот број на валидатори во мрежата да биде околу 100, но тој број варира во зависност од перформансите на валидаторите, мрежниот опсег и бројот на трансакции што се генерира во мрежата. Препорачаниот максимален број на валидатори во мрежата е апроксимативен, но експериментално може да се определи поконкретна вредност во зависност од имплементациското сценарио и перформансите на валидаторите.

3.4.5. *Swirls Hashgraph*

Малку поинаков пристап во градење на дистрибуиран регистри (distributed ledgers) е со помош на податочната структура наречена Насочени Ациклични Графови (Directed Acyclic Graph – DAG) [82] што во принцип може да се смета како мрежеста Blockchain структура која не поседува единечна линија на синцирот. Swirls Hashgraph [8] е едно од најпознатите решенија кои користат DAG податочна структура која се користи само во Blockchain технологијата позната како Hedera Hashgraph [83]. Наместо како кај останатите консензус механизми, кај кои консензус се постигнува на однапред формиран податочен блок, кај Swirls Hashgraph трансакциите се организираат преку настани (events). Настан претставува листа од трансакции претходно споделена помеѓу соседите, која содржи хаш вредности (дигитални потписи) од други корисници. Временската линија на Swirls Hashgraph консензусот механизмот е претставена на Слика 3.5.

Главна цел на Swirls Hashgraph консензус механизмот е да ги натера учесниците да постигнат договор за подреденоста на трансакциите, што се прави во неколку рунди. За успешно постигнување на консензус, учесниците треба добро да се познаваат меѓу себе. Секој учесник во мрежата може во било кое време да создаде трансакција и истата да ја испрати до другите учесници. Трансакцијата треба да биде потпишана, на тој начин се покажува кој учесник ја генерира трансакцијата, но може и да се следи трагата по кој пат трансакцијата се испраќа кон другите учесници. За да се распространи трансакцијата во мрежата, се користи оговарачки (gossip) протокол, со чија помош трансакциите се споделуваат со случајно одбрани учесници од соседството преку насочен точка-точка

пристап, на кој начин сите учесници се запознаваат со трансакцијата и учат за мрежната активност.



Слика 3.5. Временска линија од Swirlds Hashgraph консензус механизмот

Со цел да се оптимизира оговарачкиот протокол, се пристапува кон користење на механизмот трач за трач (gossip about gossip), што значи дека учесникот создава настан кој покрај неговата трансакција содржи и претходно научени трансакции кои биле споделени со оговарачкиот протокол. Новиот настан се проследува понатака во мрежата. Со ваков пристап на создавање на Swirlds Hashgraph податочната структура практично се формира историја на трансакции, каде заглавието е многу мало, а самиот процес не ја оптоварува мрежата.

Друг механизам кој се користи е виртуелното гласање. Преку механизмот на оговарање се шири информацијата низ мрежата, а самото проследување на трансакциите кон соседите значи дека учесникот кој ја проследил информацијата гласа за истата и потврдува дека истата е коректна. Финалниот настан има целосна листа од трансакциите како и временски печат за редот по кој се појавиле трансакциите.

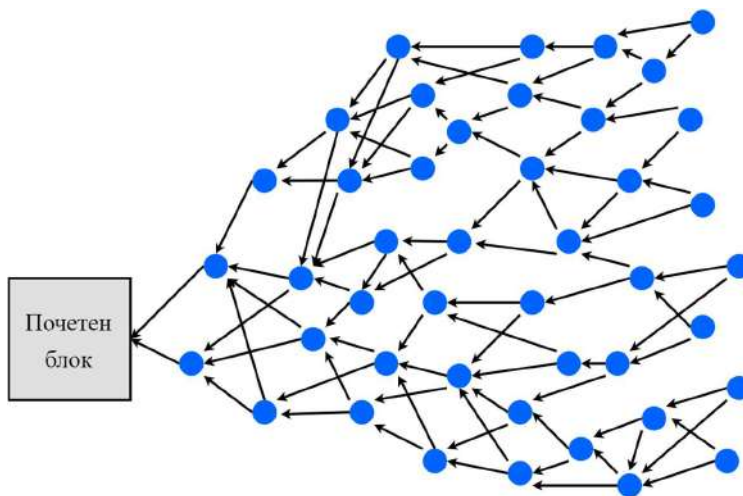
Со имплементирањето на двата механизми, трач за траг и виртуелно гласање, консензусот се постигнува на следниот начин. Прв чекор е определување на почеток на нова рунда. Новата рунда започнува кога еден настан во тековната рунда е поврзан со повеќе од $2/3$ од првите настани преку повеќе патеки од $2/3$ од бројот на учесници во мрежата. Оваа спецификација гарантира дека еден настан цврсто е поврзан со друг настан, кој дозволува два учесници независно да го определат виртуелниот глас од трет учесник и на таков начин тие би го добиле истиот одговор без притоа директно да комуницираат туку само анализирајќи ја патеката на настаните.

Следен чекор во постигнувањето на договор е проверката на гласањето, притоа првиот настан во новата рунда треба да се согласува со коректноста на податоците од првиот настан во претходната рунда. Практично гласањето се верифицира преку потврда на поврзаноста на првиот настан во новата рунда и првиот настан во претходната рунда.

Последен чекор е собирањето на гласови. Во тековната рунда, нов настан се обидува да собере $2/3$ од гласовите на учесниците за настани што биле генерирани во претходните две рунди пред тековната рунда. Новиот настан од тековната рунда треба цврсто да е поврзан со новиот настан од претходната рунда. Тоа значи дека консензусот кај Swirlds Hashgraph се постигнува во три рунди, но должината на рундите не е определена и зависи од бројот на учесници и брзината на генерирање трансакции. Потребата од собирање $2/3$ гласови од учесниците го прави Swirlds Hashgraph да биде способен да ја заштити мрежата од $1/3$ малициозни учесници.

3.4.6. Tangle

Друг консензус механизам кој користи DAG податочна структура е Tangle [9] кој се користи кај IOTA [84] Blockchain технологијата. Овој консензус механизам е брз и енергетски ефикасен, што воедно овозможува да биде имплементиран и без да се наплаќаат такси за негово користење. За да се потиснат несоодветни активности, при генерирањето на трансакцијата, потребно е да биде решена едноставна сложувалка од типот на PoW консензус механизмите. Оваа сложувалка е далеку поедноставна и енергетски ефикасна во споредба со традиционалната PoW сложувалка. Доколку се имплементираат многу мали такси за генерирање на трансакција, дополнително може да се потиснат несоодветните активности.



Слика 3.6. Tangle консензус механизмот

Процесот на гласање кај Tangle консензус механизмот е прикажан на Слика 3.6. За еден учесник да генерира трансакција во мрежата, потребно е истиот да верифицира две трансакции во мрежата кои претходно биле поднесени. Како што трансакцијата влегува се подлабоко во процесот на потврдување, таа добива се повеќе и повеќе потврди од другите учесници, со што се зголемува веројатноста за финализирање на трансакцијата. Дури и во присуство на малициозни учесници, останатите учесници ќе успеат да постигнат консензус над коректните трансакции, но ќе е потребно повеќе време за да се добијат доволен број потврди за коректност на трансакцијата. За време на процесот на потврдување, некои од учесниците може да потврдат лажни трансакции, но како што минува времето се повеќе коректни учесници ќе ги потврдуваат точните трансакции, со тоа лажните трансакции нема да добијат доволно потврди за да постигнат финализирање на трансакцијата.

Вака поставениот Tangle консензус механизам овозможува голема мрежна скалабилност по однос на бројот на трансакции и бројот на учесници во мрежата. Згора на тоа заштитата од малициозни јазли кај Tangle е на ниво од останатите PBFT базирани консензус механизми. Практично консензусот кај Tangle е заштитен од $1/3$ малициозни учесници.

3.4.7. Споредба на консензус механизмите

Генерално не постои перфектен консензус механизам. Изборот на консензус механизам треба да биде соодветен на имплементациското сценарио, барањата за

скалабилност, барањата за безбедност во мрежата и други параметри поврзани со перформансите на консензус механизмот. Во Табела 3.2 е дадено резиме на карактеристиките од погоре опишаните консензус механизми.

Табела 3.2. Споредба на карактеристики помеѓу консензус механизмите

	PoW	PoS	PBFT	Tendermint	Swirlds Hashgraph	Tangle
Синхронизираност	Мала синхронизираност	Мала синхронизираност	Мала синхронизираност	Мала синхронизираност	Асинхрони	Асинхрони
Заштита од Византиски грешки	51%	51%	1/3	1/3	1/3	1/3
Скалабилност	Мала	Мала	Средна	Средна	Голема	Голема
Проток на трансакции	Мал	Мал	Голема	Голема	Голема	Голема
Финализирање на трансакции	Пробабилитетичко	Во неколку секунди	Инстантно (1-3s)	Инстантно (1-3s)	Пробабилитетичко (конвертира во неколку секунди)	Пробабилитетичко (конвертира во неколку секунди)

Од Табела 3.2 е очигледно дека PoW и PoS нудат највисоко ниво на заштита од малициозни корисници, но имаат мал проток на трансакции со што не би било можно да бидат опслужени сите корисници кога истите би биле користени во масовни сценарија. Другите консензус механизми нудат помала заштита од малициозни учесници во мрежата, но затоа пак овозможуваат поголем проток на трансакции во системот како и побрзо финализирање на трансакциите. За да се зголеми безбедноста на системот во кој се користат PBFT, Tendermint, Swirlds Hashgraph и Tangle, потребно е да се додаде дополнително ниво на безбедност за автентикација на корисниците.

3.5. Најпознати Blockchain технологии и споредба на нивните карактеристики

Големиот спектар на консензус механизми дава можност да се изградат голем број разновидни Blockchain технологии. Кога истите ќе бидат искомбинирани со други напредни компјутерски техники, може да се изградат Blockchain технологии со најразлични перформанси и за најразлична примена. Како најпознати Blockchain технологии кои се изградени врз основа на погоре споменатите консензус механизми се: Bitcoin [85], Ethereum [86], Cosmos [87], Hedera Hashgraph [83], IOTA [84], Hyperledger [88] и други.

3.5.1. Bitcoin

Првиот целосно функционален дистрибуиран систем кој овозможува синхронизирање на записите во индивидуални, независни и недоверливи јазли во мрежата е Bitcoin. Техничките карактеристики на Bitcoin системот за прв пат биле објавени во [1] во 2008 година од личност со псевдоним Сатоши Накамото. Првата верзија на софтверската апликација за пристап до Bitcoin мрежата била објавена во 2009. Bitcoin впрочем ја претставува првата успешна Blockchain технологија.

Bitcoin Blockchain технологијата користи традиционален механизам на поврзување на последователните блокови од трансакции, преку референцирање на хаш вредностите од претходниот блок во тековниот блок, како на Слика 3.1. Консензус механизмот кој се користи е PoW.

За приклучување кон Bitcoin мрежата се користи клиентски софтвер, кој најнапред потребно е да ја симне целата база на податоци од Bitcoin мрежата, потоа истата треба да ја провери за коректност на информации и на крај да се синхронизира со останатите учесници во мрежата. Клиентот за поврзување кон Bitcoin мрежата може да служи за генерирање на трансакции, но може да се користи и како рудар за учество во PoW консензус механизмот. Поради намерни или ненамерни промени во софтверскиот код на клиентскиот софтвер, од првичната и основна Blockchain линија може да се формираат повеќе Bitcoin алтернативни мрежи, притоа сите имаат сопствени поддржувачи кои и понатака рударат за да ја поддржат најдолгата линија на Blockchain запис. Најпознати алтернативи на основниот Bitcoin се: Bitcoin Gold [89], Bitcoin Cash [90] и Bitcoin SV [91].

Покрај основниот механизам на синхронизирање на записите во јазлите, кај Bitcoin мрежата за прв пат е воведена целосно функционална крипто валута, Bitcoin. Единствената улога на Bitcoin е да биде дистрибуиран регистар на трансакции без поддршка од паметни договори со кои би се дефинирале напредни функции во рамките на мрежата.

За да се избегне создавањето на посебен регистар на корисници од цела мрежа во кој би се зачувувале салдата на корисниците, во Bitcoin мрежата принципот на следење

на салдата е преку Unspent Transaction Output (UTXO) што претставува количина на Bitcoin средства која корисникот не ја има потрошено при извршен трансфер. За да се провери салдото на даден корисник потребно е да се изврши проверка на сите влезни и излезни трансакции за дадениот корисник од почетокот на мрежата. На тој начин ќе се увиде фактичката состојба на сметката без притоа да треба да се помни конкретна вредност како салдо.

3.5.2. *Ethereum*

Еден од поголемите скокови во развојот на Blockchain технологиите е направен со развојот на Ethereum Blockchain технологијата. Основниот концепт на Ethereum Blockchain технологијата за прв пат е опишан во 2013 година од страна на Виталик Бутерин во [11], а развојот на софтверската имплементација започнува во 2014 година. Првиот официјален софтвер за пристап до Ethereum мрежата е пуштен во употреба во 2015 година, кога е генериран и почетниот блок.

Со воведувањето на новата Blockchain технологија, се воведува и нова дигитална валута Ether (ETH). Оваа валута како и кај Bitcoin потребно е да биде рударена за да може да биде ставена во оптек. За разлика од UTXO начинот на следење на салда на корисниците кај Bitcoin, кај Ethereum клиентските софтвери имаат регистар на кориснички адреси во системот и за нив има целосен увид на тековното салдо преку зачувување на фактичката состојба на сметката. Исто така при трансферот на средства помеѓу корисниците, се прави експлицитен трансфер на средствата преку фактичко префрлање на посакуваното количество од една на друга адреса.

Воведувањето на Ethereum Blockchain технологијата донесува значајно редефинирање на ентитетите кои учествуваат во мрежата, преку имплементација на Ethereum виртуелната машина (Ethereum Virtual Machine – EVM). Со воведувањето на EVM, Ethereum мрежата прераснува во еден глобален компјутер кој покрај основните придобивки од воведувањето на дигиталната валута и другите дигитални средства, овозможува воведување на нов концепт на креирање дистрибуирани апликации и паметни договори (Smart contracts) [11]. Дистрибуираните апликации се јавно достапни апликации без централен серверски дел и без сопственик, притоа истите имаат интеракција со Blockchain структурата преку автоматизирани процедури односно паметни договори. Паметните договори во рамките на Ethereum мрежата претставуваат непроменливи само-извршни кодови кои овозможуваат автоматизација на процеси во мрежата. Практично EVM претставува ниво на апстракција со кое се овозможува кодовите кои се пишуваат за дистрибуираните апликации и паметните договори, да може да се извршуваат независно од околината во која се имплементира Ethereum клиентот. Извршниот бинарен код на паметните договори се поставува во самата Blockchain база на податоци која треба да биде синхронизирана кај сите корисници, поради што не постои механизам за истиот тој код да биде променет или надграден. Паметните договори може да бидат повикани и извршени преку нивната уникатна адреса. Со паметните договори се овозможува развој на Blockchain технологии што ќе бидат надвор од финансискиот сектор. Автоматизирањето на процесите во Blockchain системите преку користење на паметни договори, ги мотивира истражувачите да развиваат системи кои би биле целосно автономни и универзални во области како што се IoT [39], логистика [41], здравство [42] како и други области од нефинансиска природа.

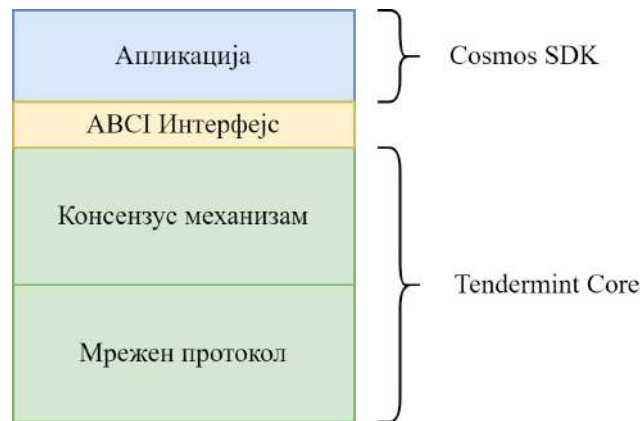
Покрај дигиталните апликации кои овозможуваат интерактивност меѓу корисникот и паметниот договор, дефинирани се и таканаречени Децентрализирани

Автономни Организации (Decentralized Autonomous Organization – DAO). Идејата на DAO е да се овозможи автономно управување со ресурси во рамките на мрежата преку имплементација на стриктни, транспарентни и однапред дефинирани правила. Во DAO корисниците може да партиципираат по различни основи, зависно од корисничкото сценарио, но за да учествуваат потребно е да се користат жетони (tokens) преку кои се определува гласачката моќ за корисникот во рамките на DAO. Преку организирањето во DAO корисниците би имале можност индивидуално да придонесат кон идните одлуки кои треба да се носат во рамките на системот.

Поради големиот успех на Ethereum платформата, нејзиното омасовување, големиот број на развиени алатки, апликации и сервиси, истата многу често се соочува со загушување во процесот на потврдување на трансакции. За да се подобри протокот на трансакции низ системот предвидена е надградба на Ethereum платформата преку имплементација на повеќе механизми. Во новата Ethereum 2.0 [92] платформа ќе се имплементира нов консензус механизам кој ќе биде заснован на PoS и на тој начин Ethereum ќе премине од PoW на PoS консензус механизам. Една од основните предности на оваа промена е значителната енергетска ефикасност која ја имаат PoS консензус механизмите споредено со PoW, а со тоа Ethereum ќе се наметне како систем прифатлив за околината. Покрај таа промена, со цел да се подобри скалабилноста на складишниот простор кај Ethereum, во новата верзија ќе се имплементира Фрагментиран Blockchain (Blockchain Shard). Фрагментирањето на Blockchain складирањето би се извело преку креирање на 64 дополнителни Blockchain синџири каде би се распределил товарот за валидирање на трансакциите меѓу корисниците.

3.5.3. *Cosmos*

Cosmos мрежата [14] започнува да се развива во 2016 година како значајна надградба на Tendermint Blockchain технологијата. Во рамките на Cosmos екосистемот се дефинирани повеќе механизми со кои се проширува спектарот на Blockchain технологии со кои е овозможена директна интеракција. Tendermint Blockchain технологијата е основниот двигател на Tendermint базираните апликации во Cosmos екосистемот, но исто така може да се дефинира и како самостојна апликација вон рамките на Cosmos екосистемот. Основна градбена единица на Tendermint Blockchain технологијата е Tendermint Core сегментот (Слика 3.7), кој се состои од Tendermint консензус механизмот и сегментот за вмрежување. Модуларноста на Tendermint апликацијата е овозможена благодарение на Application BlockChain Interface (ABCI) [93]. ABCI служи како ниво во кое се дефинира начинот на кој комуницираат процедурите дефинирани во Tendermint Core сегментот и делот на апликацијата. Овој интерфејс овозможува Tendermint консензус механизмот да се поврзе со Blockchain апликации од други Blockchain технологии. Особено значајна апликација е Ethermint [94] која практично претставува спој на Tendermint консензус механизмот и Ethereum апликациското ниво. На овој начин може многу лесно да се изгради Ethereum базирана апликација врз Tendermint консензус механизам. Ваквата апликација од една страна ќе може да ги искористи предностите кои ги нудат паметните договори дефинирани кај Ethereum Blockchain технологијата притоа без никаква измена да се искористат сосема истите паметни договори и во новата апликација, а од друга страна ваквата апликација ќе ја искористи предноста на Tendermint консензус механизмот при што ќе се овозможат големи протоци на трансакции и нивно брзо финализирање.



Слика 3.7. Рамковна структура на Cosmos апликација базирана на Tendermint консензус механизмот

Cosmos претставува еден од најуспешните проекти базирани на Blockchain технологија [95]. Cosmos мрежата започнува да се развива како пионерски концепт кој ќе овозможи комуникација помеѓу различните Blockchain технологии. Истиот е познат и како “Internet of Blockchains”. Со користење на Inter-Blockchain Communication (IBC) [96] протоколот се овозможува интеракција на различните Blockchain технологии во еден Cosmos екосистем. Овие поединечни Blockchain технологии, кои функционираат независно во таканаречени зони (zones), преку IBC се поврзуваат на Cosmos Hub, со цел да овозможат комуникација и размена на трансакции помеѓу различните зони. Cosmos Hub е централен ентитет на Cosmos мрежата. Во рамките на Cosmos Hub се користи Tendermint консензус механизмот за координација на валидаторите во мрежата.

Cosmos екосистемот воведува сопствена крипто валута наречена АТОМ. Валутата АТОМ се користи во рамките на Cosmos Hub како платежно средство, но и како средство за вложување во процесот на управување на механизмот за гласање.

3.5.4. Hedera Hashgraph

Hedera Hashgraph е Blockchain технологија која се развива од средината на 2017 година. Таа се издвојува од останатите Blockchain решенија преку користењето на патентирианиот Swirld Hashgraph консензус механизам. Поради користењето на овој консензус механизам, кој е затворен преку патентирање на решението, многу често се смета дека Hedera Hashgraph Blockchain технологијата има потенцијал да биде злоупотребена од страна на креаторите, поради што е најчесто избегнувана.

Во рамките на Hedera Hashgraph се користи сопствената крипто валута HBAR. Истата се користи за плаќање на таксата за верификација на трансакциите, за плаќање на мрежните сервиси и за спречување на малициозни активности во мрежата. Дополнително преку количината на вложени HBAR се определува тежината на гласот во процесот на валидација на трансакциите.

Hedera Hashgraph дефинира користење на паметни договори за автоматизирање на процесите во системот. Паметните договори во системот се извршуваат по принципот „прв повикан, прв извршен“ со што се овозможува фер подредување на процесите во системот. Голема предност на паметните договори кои се дефинирани во Hedera Hashgraph е можноста опционално да се дефинира дали еден паметен договор ќе биде трајно непроменлив или ќе се остави можност за транспарентни надградби и корегирање на грешки во паметниот договор преку дефинирање на администраторски клуч. При

развојот на апликации базирани на паметни договори, сите потребни документи, привилегии и самите бинарни форми на паметните договори, може да бидат складирани во самата Hedera Hashgraph мрежа.

Фазата на развој во која моментално се наоѓа Hedera Hashgraph ја дефинира како Blockchain технологија со дозвола [97]. Тоа се прави со цел да има поголема контрола врз коректноста на консензус механизмот и да се дозволи доволен број на HBAR да бидат распределени низ мрежата што би овозможило премин во следната фаза. За Hedera Hashgraph да премине во Blockchain технологија без дозвола, покрај потребата од зголемена распространетост на HBAR низ мрежата, потребно е и бројот на јазли во мрежата да биде поголем од 39.

3.5.5. IOTA

IOTA [84] е Blockchain технологија која се појавува во 2016 година. Пред се е наменета за користење во IoT системските решенија, во кои треба да се овозможи брза валидација на трансакциите, лесен консензус механизам со цел да не се оптоварат IoT јазлите и притоа да има многу мали такси за валидирање на трансакциите (или воопшто да нема никакви такси). За да се овозможат овие барања IOTA го користи Tangle консензус механизмот. Воведува сопствена крипто валута MIOTA која се користи за плаќање на таксата за валидирање на микротрансакциите кои ги прават јазлите во мрежата.

Моментално IOTA мрежата работи во централизиран мод, наречен период на координатор. Генерираните трансакции се потврдуваат од централен ентитет кој е управуван од IOTA фондацијата, а е познат како Координатор. Оваа централизирана точка во мрежата е точка на испад и мета за хакерски напади, што во периодот на развој на IOTA мрежата се покажал како важен фактор за забавен развој и незначително прифаќање на оваа технологија. Основна цел на постоењето на Координатор во мрежата е да се осигура исправноста на трансакциите во мрежата се додека во истата не почнат да се генерираат доволен број трансакции за да биде мрежата самоодржлива односно Tangle консензус механизмот да биде отпорен на напади. Покрај основната мрежа пуштена е во употреба и тестна мрежа во која има целосно децентрализиран мод на работа без Координатор во мрежата, со што IOTA фондацијата го припрема системот за да го исклучи Координаторот.

Концептот кој се користи во IOTA мрежата ветува голема скалабилност на мрежата по однос на бројот на трансакции и бројот на корисници во мрежата, но поради централизираниот пристап за потврда на трансакциите во фазата во која моментално се наоѓа IOTA мрежата, истата не може да го потврди тоа. Покрај постојаните хакерски напади и испади на Координаторот, исто така IOTA мрежата има напади и врз процесот на потпишување на трансакциите и на корисничките новчаници. Поради овие проблеми, IOTA фондацијата ги рedefинира сите процедури за потпишување на трансакции и генерирање на новчаници. IOTA фондацијата има потешкотии да ја развие мрежата до посакуваното ниво, притоа успевајќи да ги постигне планираните цели поради големиот број на проблеми со кои се среќава од самиот почеток.

3.5.6. Hyperledger

Hyperledger [25] претставува проект на Linux фондацијата кој започнува да се развива кон крајот на 2015 година и почетокот на 2016 година. Иницијално е поддржан од IBM [98], Intel [99] и SAP Ariba [100] со цел создавање на Blockchain технологија со отворен софтвер на корпоративно ниво. Во рамките на Hyperledger проектот главна цел

е да се развиваат повеќе поединечни и помали проекти во кои ќе се користат веќе етаблирани консензус механизми, притоа кодот кој се развива овозможува лесно менување на консензус механизмите во зависност од потребите на финалното решение. Оваа опција е овозможена како резултат на иницијалниот пристап во градење на решенијата, односно дефинирање на модуларност на системот. Hyperledger проектите се Blockchain-as-a-Servis (BaaS) базирани решенија.

Генерално системите кои се градат во рамките на Hyperledger проектите треба да бидат приватни Blockchain системи со дозвола за чија цел е развиен сервис за управување со членови (membership service) во системот. На тој начин се затвора Blockchain решението кое би се изградило само во рамките на предвиденото вмрежување помеѓу контролирана група на корисници. Како и другите Blockchain технологии од поновите генерации, кај Hyperledger решенијата се предвидува користење на паметни договори, кои се нарекуваат кодови во синџирот (chaincodes). Овие кодови се реискористливи и можат да се имплементираат во повеќе реализации на одредено решение, а згора на тоа овозможуваат автоматизација на процесите во рамките на една имплементација од дадено Blockchain решение. Поради затвореноста на системот во помали корпоративни мрежи и постоењето на ниво за контрола на пристап, во решенијата на Hyperledger проектите може да се користат и консензус механизми кои имаат понизок степен на безбедност. Поради тоа низ Blockchain сегментот на решението, поточно консензус механизмот, може да бидат валидирани голем број на трансакции.

Два најпознати проекти во рамките на Hyperledger се: Hyperledger Fabric [54] и Hyperledger Sawtooth [73]. Покрај овие два проекти постојат низа други проекти и алатки со кои се дефинира сет од производи кои може да бидат користени на корпоративно ниво и овозможуваат модуларност и лесна надградба на системите кои се поставени во облак. Практично, решенијата кои се нудат во рамките на Hyperledger проектите се облак базирани решенија кои имплементираат функционалности од Blockchain технологиите со цел да се олеснат одредени процеси во рамките на корпоративните мрежи. Ваквата архитектура фрла сенка на приватноста на податоците иако истите се енкапсулираат во енкриптирани тунели помеѓу членовите на системското решение.

Hyperledger Fabric [54] е проект кој е продолжение на OpenBlockchain проектот на IBM. Во рамките на овој проект се развива Blockchain технологија со дозвола, која како консензус механизам најчесто го користи PBFT консензус механизмот, но има развиени модули и за други консензус механизми.

Hyperledger Sawtooth [73] е проект за кој главен придонес има Intel. Кај овој проект основен консензус механизам е PoET. Покрај овој консензус механизам, во рамките на проектот се предвидени и други консензус механизми. Во рамките на овој проект предвидена е можност за користење на Ethereum паметни договори, што би овозможило брзо имплементирање на паметните договори кои се веќе развиени во рамките на Ethereum мрежата.

3.5.7. Споредба на карактеристиките на Blockchain технологиите

Карактеристиките на Blockchain технологиите воглавно зависат од консензус механизмот кој се користи. Но покрај консензус механизмот, постојат и други протоколи кои се дефинираат во рамките на една Blockchain технологија, со што секоја Blockchain технологија се издвојува во однос на другите. Во Табела 3.3 даден е сублимат на некои од поважните карактеристики на Blockchain технологиите кои се анализирани во

рамките на оваа докторска дисертација, како потенцијални решенија за следната генерација на глобални јавни здравствени системи.

Табела 3.3. Споредба на карактеристиките на Blockchain технологиите

Тип на технологија	Bitcoin	Ethereum	Cosmos	Hashgraph	IOTA	Hyperledger
Поддржува паметни договори	Јавна, без дозвола	Јавна, без дозвола	Јавна/Приватен, без дозвола	Јавна, со дозвола/без дозвола	Јавна, без дозвола	Приватна, со дозвола
Протокок на трансакции	Рудиментирана форма	Да	Да	Да	Да	Да
Скалабилност по број на корисници	Мал	Мал	Голем	Голем	Голем	Голем
Скалабилност по број на валидатори	Голема	Голема	Голема	Голема	Голема	Голема
Чинење на една трансакција	Голема	Голема	Средна	Мала	Голема	Мала
Нефинансиски апликации	Скапо	Скапо	Евтино	Евтино	Бесплатно	Бесплатно
Отвореност на софтвер	Не	Да	Да	Да	Да	Да
Инфраструктура на корисничкото решение	Отворен	Отворен	Отворен	Лиценциран	Отворен	Отворен
	Јавна	Јавна	Јавна	Јавна	Приватна/Јавна	Приватна

Bitcoin и Ethereum се отфрлаат како можни Blockchain технологии врз кои би се градел глобален јавен здравствен систем, поради проблемот кој го имаат овие технологии со скалабилноста по однос на протокот на трансакции, но и високата цена на чинење на трансакциите во рамките на двете Blockchain технологии.

Hedera Hashgraph нуди карактеристики кои би овозможиле скалабилно глобално решение за јавен здравствен систем, но затвореноста на консензус механизмот со лиценца, не остава простор за дополнително оптимизирање на било какво решение кое би се изградило врз негова основа.

IOTA Blockchain технологијата нуди одлични карактеристики кои би овозможиле градење на глобален здравствен систем, но проблемот со кој се соочува IOTA фондацијата да изгради стабилна IOTA мрежа, претставува проблем поради кој IOTA

Blockchain технологијата е отфрлена како можна основа за градење на глобален јавен здравствен систем.

Hyperledger има прифатливи карактеристики по однос на перформансите на скалабилност, но тоа што решението има приватна инфраструктура, поставена во рамките на облакот на Hyperledger фондацијата, фрла сенка на приватноста на податоците и можноста за нивна злоупотреба.

Од карактеристиките на Blockchain технологиите прикажани во Табела 3.3 може да се заклучи дека Cosmos (соодветно Tendermint консензус механизмот) е најдоброто решение врз кое може да се започне да се гради глобален јавен здравствен систем. Предноста на Cosmos и Tendermint е тоа што овозможуваат градење на јавен и приватен Blockchain, со и без дозвола, овозможуваат користење на паметни договори, нудат висока скалабилност по однос на протокот на трансакции, а и задоволителна скалабилност по однос на бројот на валидатори. Исто така голема предност е ниската цена на чинење на трансакциите што би овозможило масовност во употребата на системот.

4. ЕВАЛУАЦИЈА НА ПОДОБНОСТА НА TENDERMINT КОНСЕНЗУС МЕХАНИЗМОТ КАКО ОСНОВА ЗА СЛЕДНАТА ГЕНЕРАЦИЈА ЈАВНИ ЗДРАВСТВЕНИ СИСТЕМИ БАЗИРАНИ НА BLOCKCHAIN ТЕХНОЛОГИИ

Преку екстензивна анализа на достапната литература може да се забележи дека најголем дел на решенијата за здравствени системи се базирани на Ethereum или на Hyperledger Blockchain технологијата. Покрај нив, има и решенија кои се изградени врз целосно независна платформа дедицирана само за здравствениот систем. Најпознати решенија на здравствени системи базирани на Blockchain технологија се Patientory [23], MedRec [20], FHIRChain [19], MedicalChain [24], Healthcare Data Gateway [21] и др. Покрај дизајнот на архитектурата и објаснувањето за функционалноста на системот, во истите недостасува анализа на перформансите на овие здравствени системи, независно од Blockchain технологијата врз која се изградени.

Резултати од испитување на перформанси на здравствен систем базиран на Blockchain технологија се дадени во [101], каде исто така може да се најде детален преглед на дизајнот на PBFT базиран здравствен систем. Во [101] дадени се и резултати од анализата на целокупната скалабилност на системот, кои потврдуваат дека капацитетот на PBFT базиран здравствен систем може да опслужи мал број на пациенти.

Во литературата не е пронајдена анализа на Tendermint базиран јавен здравствен систем, па затоа во рамките на оваа дисертација најнапред е спроведена екстензивна анализа на општите перформанси на Tendermint консензус механизмот, а подоцна е спроведена и специфична анализа на перформансите на Tendermint консензус механизмот за сообраќај кој е карактеристичен за здравствените системи.

Извршен е детален преглед на достапните трудови во кои се посочени резултати од истражувања за реалните перформанси на Tendermint консензус механизмот за општи употребни сценарија. Една од најопсежните и најдеталните анализи е дадена во [77]. Авторот на тезата дава целосен опис на Tendermint протоколот и врши анализа на протокот на трансакции и на латентноста во процесот на финализирање на трансакциите при различни мрежни услови и топологии. Дополнително може да се најдат и резултати од истражувањето на перформансите на Tendermint протоколот во услови кога има испади во системот, случајни мрежни доцнења и Византиски грешки. Според [77], Tendermint консензус механизмот може да постигне проток на трансакции од 30000 трансакции во секунда, со што ветува големо ниво на скалабилност и широк спектар на сервиси. Во рамките на истиот труд се потврдува можноста мрежата да се справи со Византиски грешки и притоа сеуште да овозможи одредено ниво на сервис со прифатлива латентност.

Во [78] е дадена теоретска анализа помеѓу различните типови на Blockchain технологии, нивните предности и недостатоци. Дополнително се дадени и резултати од евалуацијата на перформансите на Ethermint [94] Blockchain технологијата. Ethermint е Blockchain технологија која прави синергија на Tendermint консензус механизмот и Ethereum како апликациско ниво. Евалуацијата во [78] ги покрива анализите на перформанси на Tendermint консензус механизмот поврзани со протокот на трансакции, влијанието на мрежната топологија врз протокот на трансакции и времето на валидација.

Во [102] се дадени резултатите од анализата на перформанси спроведена врз повеќе различни Blockchain технологии, притоа определувајќи ги тесните грла и жешките точки на процесот на постигнување консензус. Во анализата се посочува дека Tendermint консензус механизмот се соочува со тесно грло во делот на серијализацијата на пораките, но не и во мрежниот опсег.

Авторот во [103] изложува резултати од анализата на проблемот поврзан со екстензивната размена на пораки во рамките на Tendermint протоколот за време на процесот на споделување на трансакциите со корисниците и процесот на постигнување на консензус. Евалуацијата е насочена само кон оптимизација на процесот на споделување на трансакциите помеѓу корисниците, но не и определување на перформансите како што е протоколот на трансакции. Авторот предлага решенија кои ќе го намалат притисокот врз мрежата преку паметно препраќање на пораките меѓу корисниците, со што би се овозможиле и поголеми протоци на трансакции во системот.

Од анализата на овие трудови може да се забележи дека Tendermint консензус механизмот има потенцијал да валидира илјадници трансакции во секунда, притоа соочувајќи се со проблемите на тесно грло во доменот на серијализацијата на трансакциите и споделувањето на пораките меѓу корисниците. Евалуацијата на перформансите кај погоре наведените трудови е врз општи апликации на Tendermint консензус механизмот. Треба да се има во предвид дека сообраќајот што циркулира низ здравствените системи има различна природа од сообраќајот што циркулира низ општите апликации на Tendermint консензус механизмот, за што е потребна дополнителна анализа.

Главен фокус на Tendermint протоколот се финансиските апликации, каде трансакциите потребно е да се валидираат во реално време, со што корисниците ќе имаат позитивно искуство од користењето на апликацијата. Од друга страна јавните здравствени системи имаат сообраќајни карактеристики кои се разликуваат од оние кај финансиските системи. Записите за здравствените наоди и терапија кај пациентите се генерираат додека тие се во посета на здравствениот работник и неретко се големи документи, како слики и видео документи. Процесот на валидација на записот кај ваквите системи не мора да биде завршен во реално време, но потребно е целиот процес да обезбеди високо ниво на приватност. Поради есенцијалната разлика на податоците кои циркулираат кај општите Tendermint апликации и оние кои циркулираат во јавните здравствени системи, потребно е дополнително да се испитаат можностите на Tendermint консензус механизмот во поглед на обезбедување на голем проток на валидирани трансакции, не само во услови на мали трансакции туку и во услови на големи трансакции. Во Табела 4.1 се сумирани сообраќајните карактеристики на општи Tendermint апликации и на јавни здравствени системи.

Табела 4.1. Карактеристики на сообраќајот кај општа Tendermint апликација и јавен здравствен систем

	Општа Tendermint апликација	Јавен здравствен систем
Големина на трансакција	Мали трансакции (околу 250B)	Големи трансакции (500KB до 10MB)
Содржина	Текст (финансиски информации)	Текст, слики, звуци, видео записи
Ургентност на сервисот	Трансакции што треба да се валидираат во реално време	Трансакции што треба да се валидираат скоро во реално време
Отвореност на податоците	Јавни или приватни	Стриктно приватни

4.1. Емулациска околина за анализа на перформансите на Tendermint

Направена е екстензивна евалуација на перформансите на Tendermint консензус механизмот во емулирана околина која се состои од 64 Tendermint јазли. Tendermint јазлите се индивидуални виртуелни машини кои извршуваат Tendermint софтвер и на тој начин ја формираат Tendermint мрежата. Покрај Tendermint јазлите има и две

дополнителни виртуелни машини, од кои едната е наменета за генерирање на сообраќај, а другата за набљудување на Tendermint мрежата. Сите виртуелни машини се управувани преку Hyper-V [104] софтвер.

Tendermint јазлите имаат 1GB меморија и 10GB тврд диск за складирање на податоци и користат готов Tendermint софтвер [105] преку кој се вклучуваат во Tendermint мрежата. Tendermint јазлите го активираат Tendermint сервисот при иницијалното стартување и на тој начин се вклучуваат во Tendermint мрежата со однапред поставена основна конфигурација. Со цел јазлите да учествуваат во иста мрежа, конфигурацијата потребно е да биде синхронизирана во дел од параметрите како што е Blockchain идентификациски број и сет на валидатори кои учествуваат во мрежата. За синхронизирање на потребните параметри се користи софтвер за генерирање на конфигурација, што е дел од основниот Tendermint софтверски пакет. Дополнително на секоја виртуелна машина има инсталиран софтвер tcconfig [106] со чија помош се емулира мрежно доцнење, загуби на пакети и други мрежни карактеристики.

Виртуелната машина за генерирање на сообраќај има 2GB меморија и 10GB тврд диск за складирање на податоци. На оваа машина е имплементиран софтвер за тестирање tm-load-test [107], кој е развиен од Tendermint заедницата за евалуација на перформансите на Tendermint мрежата. Некои од параметрите кои може да бидат прилагодени се: големината на трансакцијата, бројот на трансакции во група од трансакции, бројот на конекции до секој краен корисник во мрежата, времето на тестирање и периодот на генерирање на трансакции.

Машината за набљудување има 2GB меморија и 20GB тврд диск за складирање на податоци. За набљудување на перформансите на мрежата се користи InfluxDB [108] за складирање на податоци, Grafana [109] за визуелизација на податоците и Prometheus [110] за собирање на податоци од јазлите, кој како сервис е активиран на сите Tendermint јазли.

На сите виртуелни машини е инсталиран Ubuntu оперативен систем, а оркестрирањето на задачите помеѓу машините се прави со користење на Ansible playbook [111] скрипти и Linux Bash [112] скрипти.

Спроведените емулации ги следат насоките дадени во [77]. Дополнително се спроведени емулации кои го прошируваат множеството на евалуирани параметри кои се прикажани во [77]. Една екстензија е во насока на зголемување на бројот на генерирани трансакции во системот над 32768 трансакции во секунда. Покрај тоа, направена е евалуација на поголемо множество на параметри кои би можеле да го оптимизираат Tendermint консензус механизмот. Некои од параметрите по однос на кои се испитува оптималноста на Tendermint консензус механизмот се: предавателната и приемната брзина, бројот на влезни и излезни соработници (peers) и големината на трансакцијата. Целосната листа на параметри по однос на кои се испитува оптималноста на Tendermint консензус механизмот, нивните основни поставки и краток опис за секој параметар, се дадени во Табела 4.2. Основните поставки се дел од основната конфигурација со која доаѓа однапред конфигуриран Tendermint софтверот.

Табела 4.2. Симулациски параметри, нивните основни вредности и краток опис

Параметри	Основни поставки	Опис на параметрите
Предавателна брзина	5120000 B/s	Брзина со која се испраќаат пакетите
Приемна брзина	5120000 B/s	Брзина со која се примаат пакетите
Број на влезни соработници	40	Број на соработници од кои се добиваат трансакции
Број на излезни соработници	10	Број на соработници кон кои се испраќаат трансакции
Товар на пакетите со трансакции	1024B	Максимална големина на товарот за пакетите со трансакции
Интервал за предлагање на блок	3s	Временски интервал за собирање на трансакции за следната консензус рунда
Делта интервал за предлагање на блок	500ms	Вредност за која се зголемува интервалот за предлагање на блок во секоја наредна рунда, кога има неуспешен циклус на гласање
Делта интервал за пред-гласање	500ms	Вредност за која се зголемува интервалот за пред-гласање во секоја наредна рунда, кога има неуспешен циклус на гласање
Делта интервал за пред-извршување	500ms	Вредност за која се зголемува интервалот за пред-извршување во секоја наредна рунда, кога има неуспешен циклус на гласање
Големина на трансакција	250B	Големина на генерирана трансакција
Период на група на трансакции	1s	Период на генерирање на група од трансакции во јазолот
Дополнителна мрежна латентност	0ms	Дополнителна мрежна латентност која се внесува за да се емулираат реалистични услови во мрежата
Загуба на пакети	0%	Воведени загуби на пакети за да се емулираат реалистични услови во мрежата

Однесувањето на целокупната Tendermint мрежа и анализата на перформансите се изведуваат преку набљудување на протокот на трансакции во мрежата во сценарија со 4, 8, 16, 32 и 64 активни Tendermint јазли во мрежата. Една целосна емулација се состои од спринт-сетови, каде секој спринт-сет е емулација на Tendermint мрежата со однапред дефиниран број на активни Tendermint јазли во времетраење од 60 секунди. Во еден спринт-сет сите валидатори внесуваат ист број на трансакции во мрежата. Кумулативниот број на трансакции кои се внесуваат во мрежата од страна на сите валидатори во една секунда е 2^n каде $n = [7, 8, \dots, 19]$.

4.2. Основни емулациски резултати

Испитана е зависноста на протокот на трансакции низ Tendermint консензус механизмот за повеќе поставки на конфигурацијата на Tendermint софтверот и различни мрежни карактеристики во системот.

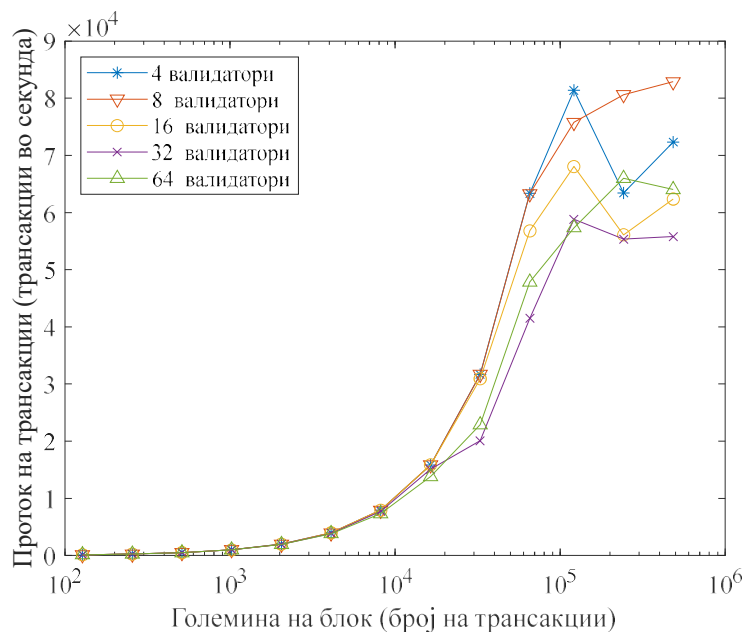
4.2.1. Проток на трансакции во Tendermint мрежата за основни конфигурациски поставки

На Слика 4.1 се претставени резултатите добиени од емулација со основни поставки на конфигурацијата кај Tendermint јазлите, кои се прикажани во Табела 4.2. Резултатите добиени за основните поставки на мрежата може да ги споредиме со резултатите прикажани за големи мрежни сценарија во [77]. Добиените резултати

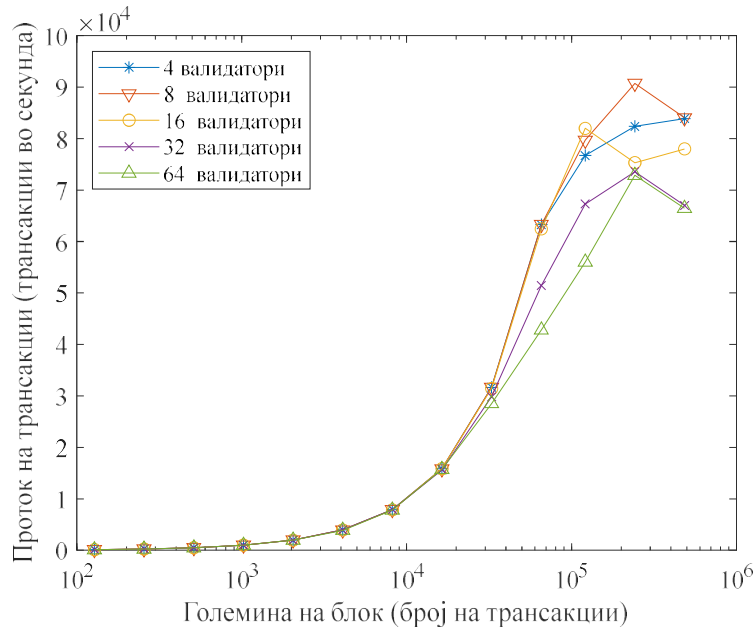
покажуваат максимален проток на трансакциите од околу 70000 трансакции во секунда, што е значително повеќе од резултатите прикажани во [77] за големи мрежни сценарија. Една од причините за постигнатите поголеми вредности за протокот на трансакции е зголемениот опсег на евалуирани трансакциски брзини, но и нееднаквоста на топологијата кај двете мрежи. Емулациите се направени во висококонективна топологијата, што значи дека мнозинството од соработниците се директно поврзани со останатите соработници во мрежата, притоа латентност во мрежата е помала од 1ms, додека во [77] валидаторите се организирани во мрежа која е распространета на 5 континенти во 7 податочни центри со мрежна латентност и цитер соодветни на интерконтинентални линкови. Добиените емулациски резултати покажуваат голема сличноста со резултатите кои се прикажани во [77] за сценарио каде Tendermint мрежата е лоцирана во еден податочен центар.

4.2.2. Влијание на конективноста, предавателната и приемната брзина врз протокот на трансакции

На Слика 4.2 може да се забележат мали подобрувања на мрежните перформанси, поточно зголемување на протокот на трансакции. Конфигурацијата на јазлите се разликува од основната конфигурација по бројот на влезни и излезни соработници. Бројот на влезни соработници е намален од 40 на 5, а бројот на излезни соработници е намален од 10 на 5. Очигледно е дека големиот степен на конективност помеѓу валидаторите ги намалува перформансите на мрежата поради мрежно преоптоварување. Ова намалување на конективноста практично ја намалува децентрализираноста на системот во целина.



Слика 4.1. Основна конфигурација

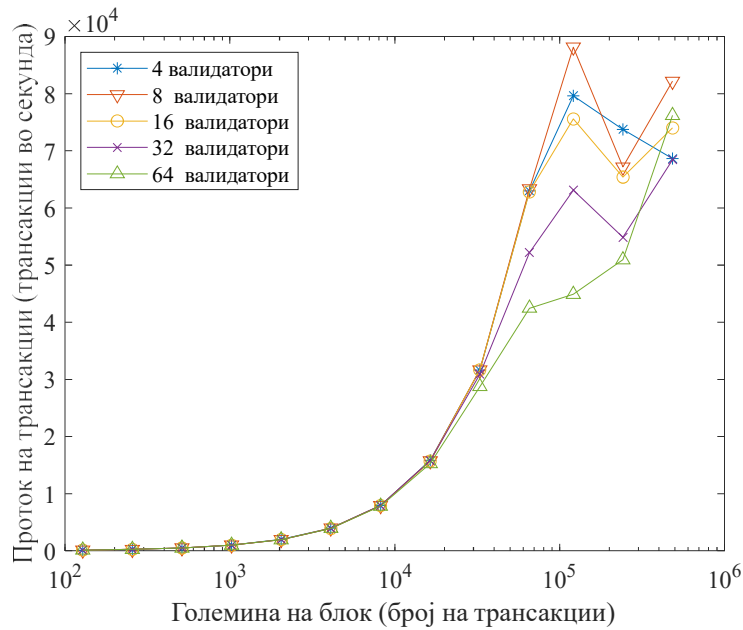


Слика 4.2. Проток на трансакции за влезни и излезни соработници еднакви на 5

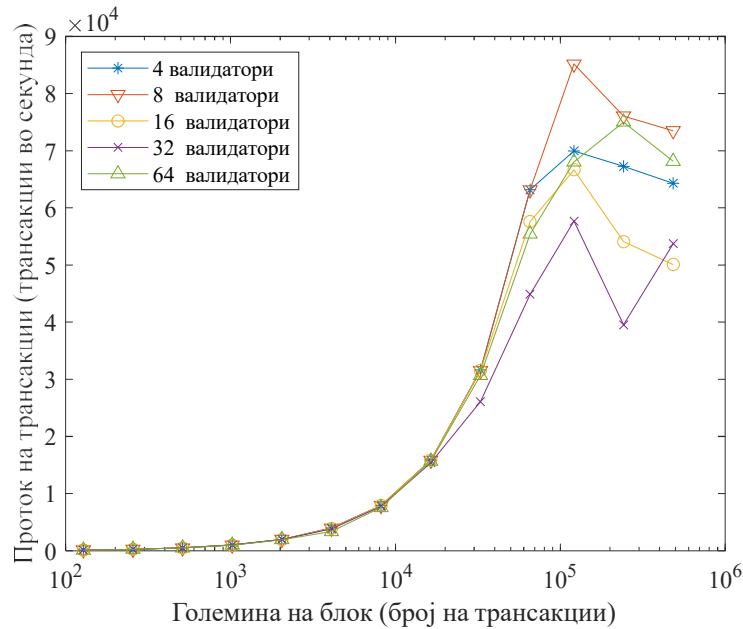
На Слика 4.3 се дадени резултатите од емулацијата за конфигурација на јазли кај која има зголемена предавателна и приемна брзина од основната 5120000B/s на 10240000B/s и намалување на влезните соработници од 40 на 5 и на излезните соработници од 10 на 5. Резултатите не покажуваат особено подобрување на протокот на трансакции во системот кога се споредуваат со основната конфигурација и покрај намалениот број на поврзани соработници. Ваквите резултати се последица на мрежното преоптоварување кое се создава со дуплирањето на предавателната и приемната брзина, но ефект може да има и од емулираната околина поради поделените мрежни ресурси.

Следните резултати се однесуваат на емулација на конфигурација во која е дуплирана предавателната и приемната брзина во однос на основната конфигурација и изнесува 10240000B/s, но зголемен е и бројот на влезни и излезни соработници на 65 со цел да се создаде целосно поврзан сет на валидатори. На Слика 4.4 се гледа намалување на перформансите на протокот на трансакции низ системот, кога истите ќе се споредат со резултатите прикажани на Слика 4.2 и Слика 4.3. Со овие резултати уште еднаш се потврдува ограничувачкиот фактор на расположливиот мрежен опсег. Резултатите на Слика 4.4 се во рангот на оние прикажани на Слика 4.1, односно оваа конфигурација е споредлива со основната конфигурација. Со тоа се потврдува дека зголемениот број на влезни и излезни соработници и тоа како влијае на перформансите на мрежата поточно на самиот консензус механизам.

Од досега прикажаните резултати може да се забележи дека протокот на информации доаѓа до точка на заситување кога консензус механизмот практично и го постигнува максималниот проток на трансакции. После таа точка, перформансите на системот се намалуваат и многу трансакции остануваат невалидирани или одбиени поради пренатрупувањето на консензус механизмот со пораки.



Слика 4.3. Проток на трансакции за влезни и излезни соработници еднакви на 5, предавателна и приемна брзина еднаква на 1024000B/s

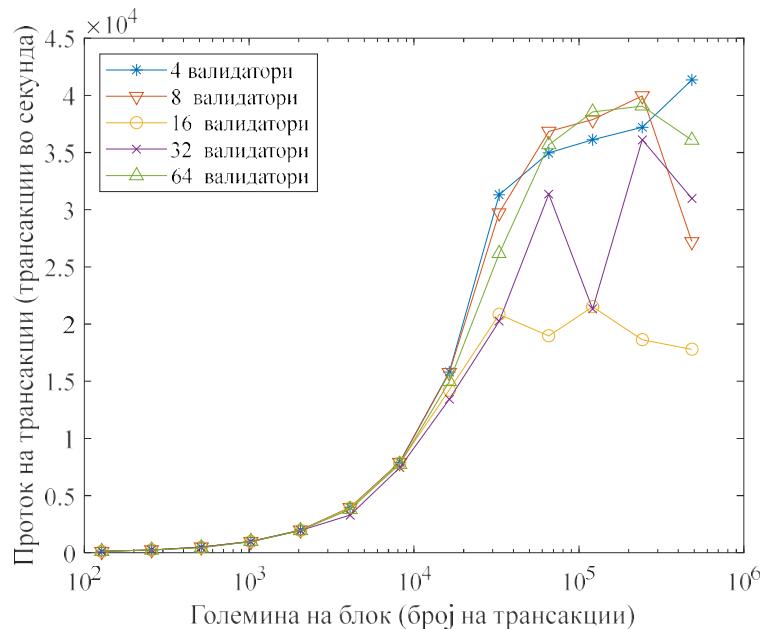


Слика 4.4. Проток на трансакции за влезни и излезни соработници еднакви на 65, предавателна и приемна брзина еднаква на 1024000B/s

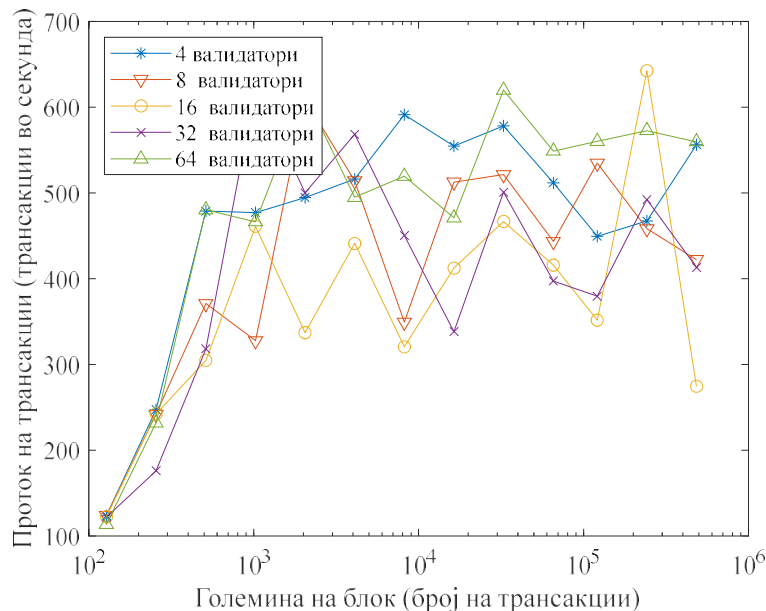
4.2.3. Влијание на големината на трансакциите врз протокот на трансакции

Следниот сет на емулации се однесува на влијанието што големината на трансакциите го има врз протокот на трансакции во системот. Евалуацијата е извршена за големина на трансакциите од 250B што претставува основна поставка за големина на трансакција и е претставена на Слика 4.1. Дополнително се евалуирани перформансите

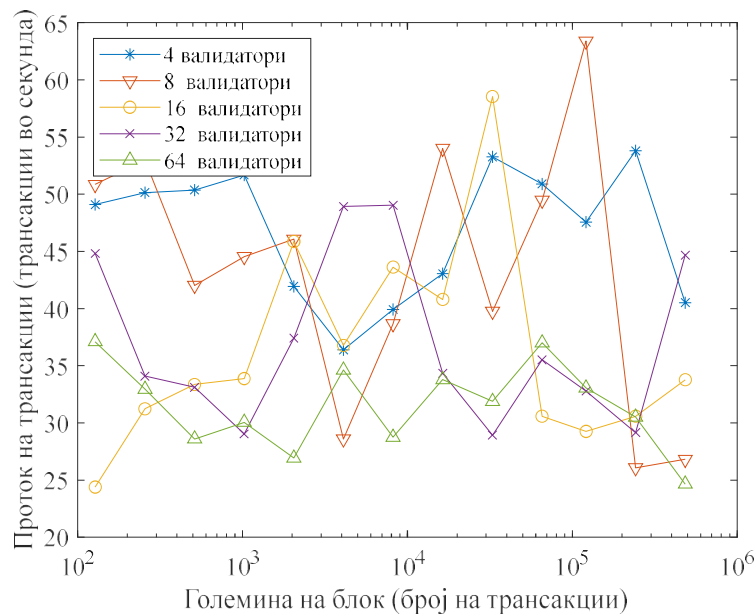
за големини на трансакции од 1KB, 100KB, 1MB и 5MB, а добиените резултати се дадени на Слика 4.5, Слика 4.6, Слика 4.7 и Слика 4.8, соодветно. Од споредбата на сликите очигледен е трендот на намалување на протокот на трансакции со зголемувањето на големината на трансакцијата. Особено големо влијание имаат најголемите трансакции поради потребата истите да бидат препратени низ мрежата до сите валидатори за што е потребно повеќе време. На Слика 4.8 е очигледно дека за големина на трансакциите од 5MB, протокот на трансакции е еднаков на нула поради тоа што трансакциите треба да се испратат до сите валидатори, но процесот на испраќање не може да заврши за интервалите кои се дефинирани со консензус механизмот.



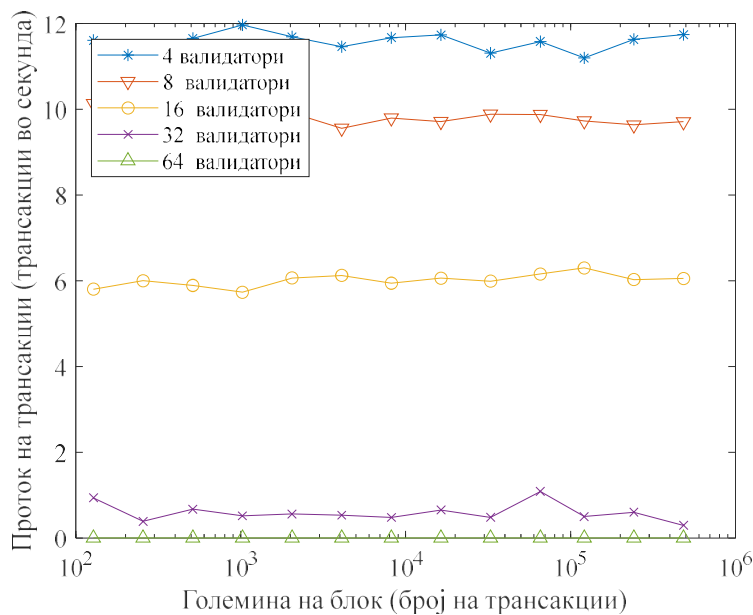
Слика 4.5. Проток на трансакции за големина на трансакција од 1KB



Слика 4.6. Проток на трансакции за големина на трансакција од 100KB



Слика 4.7. Проток на трансакции за големина на трансакција од 1MB

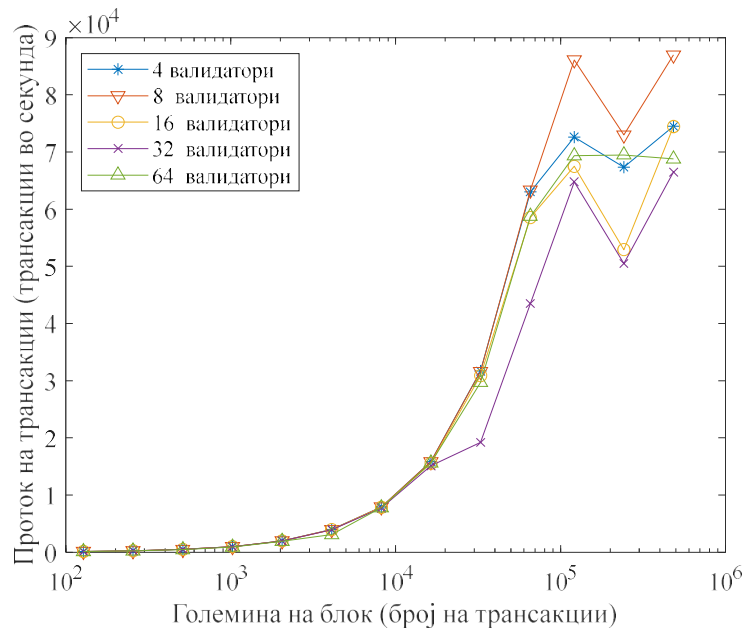


Слика 4.8. Проток на трансакции за големина на трансакција од 5MB

4.2.4. Влијание на големината на пакетот со трансакции врз протокот на трансакции

На Слика 4.9 се прикажани резултати од емулацијата за конфигурација на Tendermint јазли кај кои е променета големината на пакетите со трансакции кои се испраќаат во мрежата, притоа е зголемен параметарот од 1024B на 4096B. Споредбата

на добиените резултати со оние кои се добиваат за основната конфигурација се незначително подобрени. Најголем придонес се остварува кај сценаријата на 32 и 64 валидатори во мрежата.

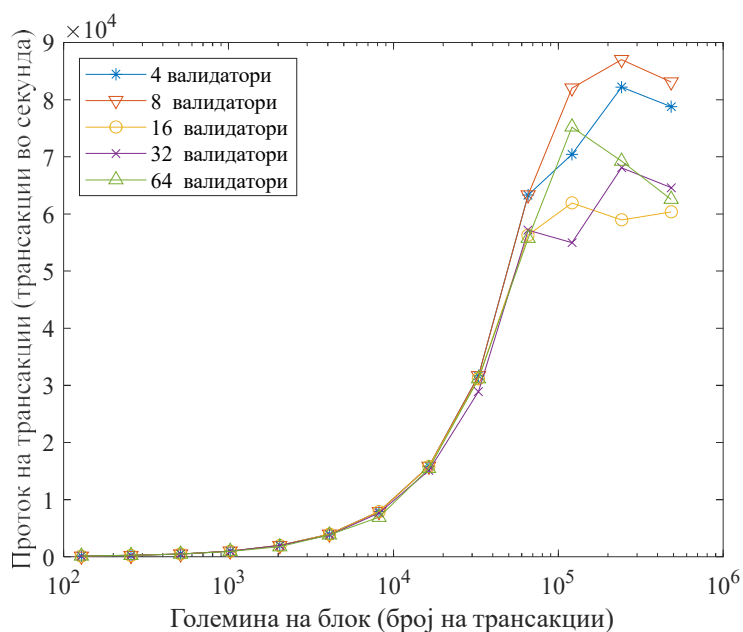


Слика 4.9. Проток на трансакции за максимална големина на пакет од 4096B

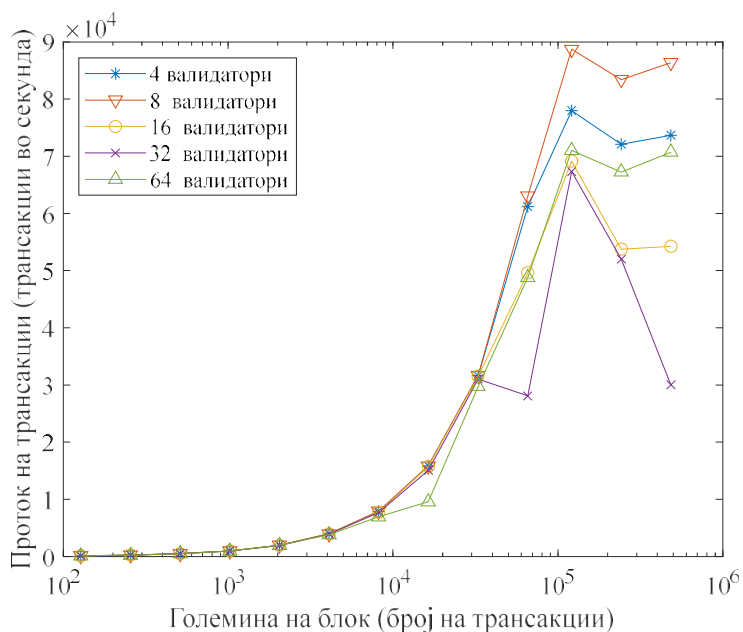
4.2.5. Влијание на интервалот за предлагање на трансакции врз протокот на трансакции

Следните резултати се однесуваат на влијанието на интервалите за предлагање на трансакции врз протокот на трансакции. На Слика 4.10 се дадени резултати од емуляција во која параметарот за интервал за предлагање пакет е намален од 3s на 1s. Со намалувањето на интервалот за предлагање на пакет се постигнува мало подобрување на протокот на трансакции споредено со основната конфигурација. Зголемувањето на протокот на трансакции е поради почестите циклуси на предлагање на пакети кои се постигнуваат поради намалениот интервал. На долг рок, помалиот интервал за предлагање пакет би овозможил подобри перформанси по однос на остварен максимален проток на трансакции во системот, но со почестите циклуси на предлагање пакети значително ќе се зголеми просторот кој ќе го зафаќаат заглавијата на пакетите. На тој начин би имале неоптимално искористување на складишниот простор.

На Слика 4.11 се дадени резултати од зголемувањето на интервалот за предлагање на пакет од 3s на 5s. Со зголемувањето на интервалот за предлагање на пакет се забележува намалување на протокот на трансакции споредено со основната конфигурација, што е резултат на поретките циклуси на предлагање на пакети.



Слика 4.10. Проток на трансакции за интервал за предлагање пакети еднаков на 1s

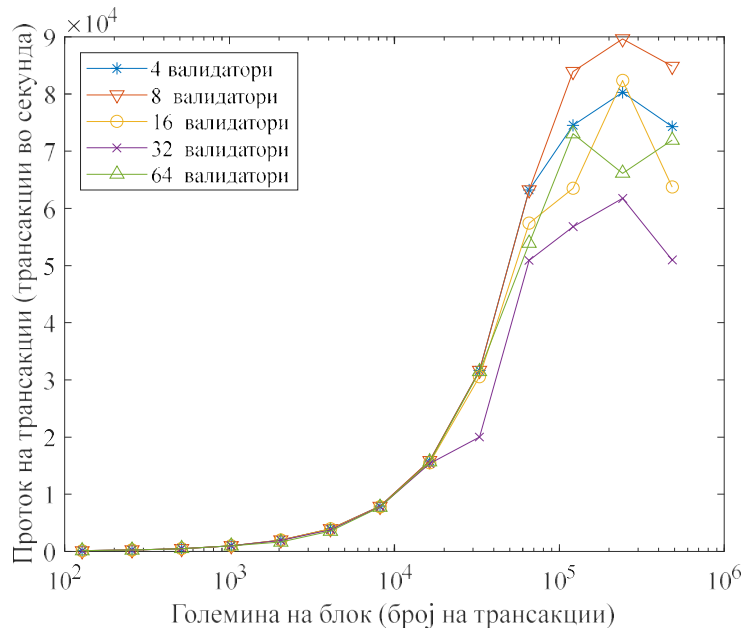


Слика 4.11. Проток на трансакции за интервал за предлагање пакети еднаков на 5s

4.2.6. Влијание на делта интервалот за предлагање на пакети, делта интервалот за пред-гласање и делта интервалот за пред-извршување врз протокот на трансакции

За да се види влијанието на промената на делта интервалот за предлагање на пакет, делта интервалот за пред-гласање и делта интервалот за пред-извршување врз протокот на трансакции, спроведен е емулациски циклус во кој вредностите за овие интервали се намалени од 500ms на 0ms. Резултатите се прикажани на Слика 4.12. Со

зададената вредност на делта интервалот се зголемува должината на соодветната фаза во консензус циклусот во случај на неуспешна рунда од консензус механизмот. На тој начин се дозволува во секоја наредна рунда да се релаксира консензус механизмот во услови кога потенцијален проблем на непостигнувањето на консензус околу предложен пакет би била мрежната латентност и цитер. Резултатите покажуваат незначително подобрување на протокот на трансакции, што е резултат на контролираната мрежна околина, малата мрежна латентност и малиот мрежен цитер.



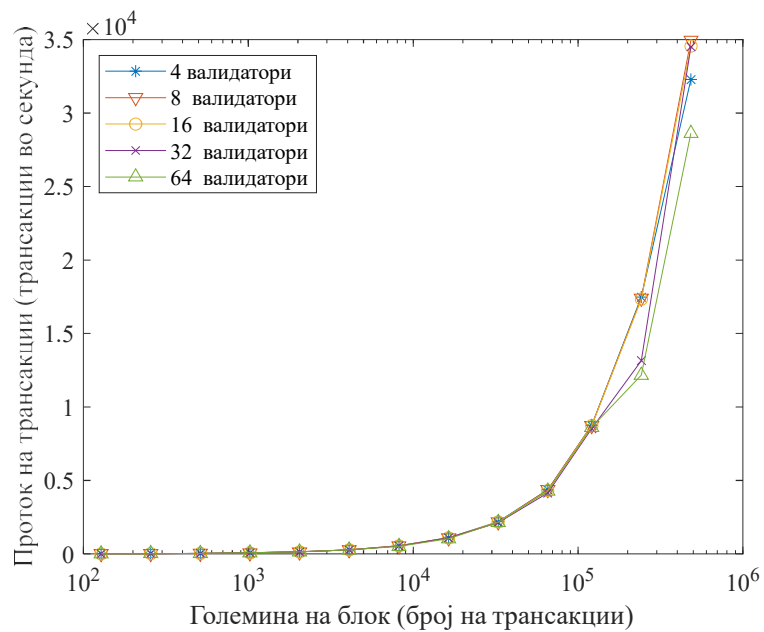
Слика 4.12. Проток на трансакции за делта интервал на предлагање пакети 0ms, делта интервал на пред-гласање 0ms, делта интервал на пред-извршување 0ms

4.2.7. Влијание на периодот на испраќање на група од трансакции врз протокот на трансакции

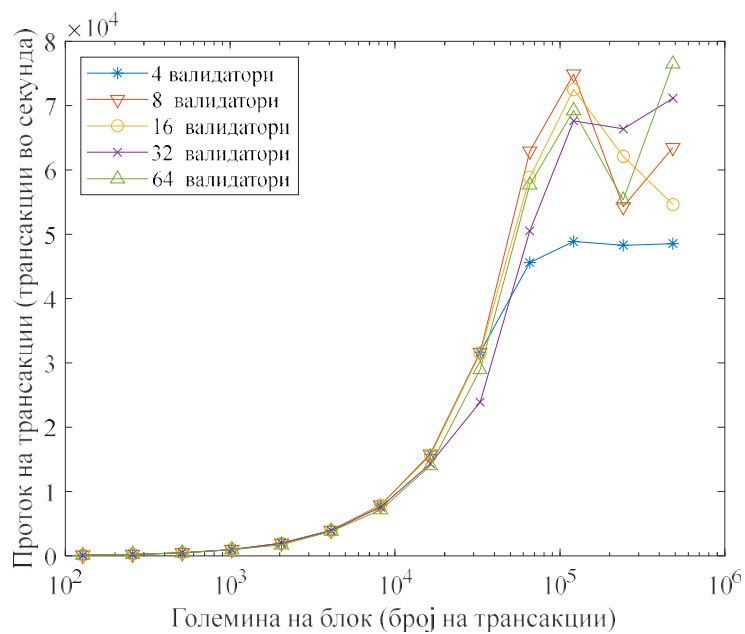
Само за комплетност на емулираните параметри спроведена е евалуација на влијанието на периодот на испраќање на група од трансакции. Промената на вредноста од 1s на 10s покажува значително намалување на протокот на трансакции што е резултат на воздржувањето за испраќање трансакции. Резултатите од овој емулациски циклус се прикажани на Слика 4.13.

4.2.8. Влијание на латентноста во мрежата врз протокот на трансакции

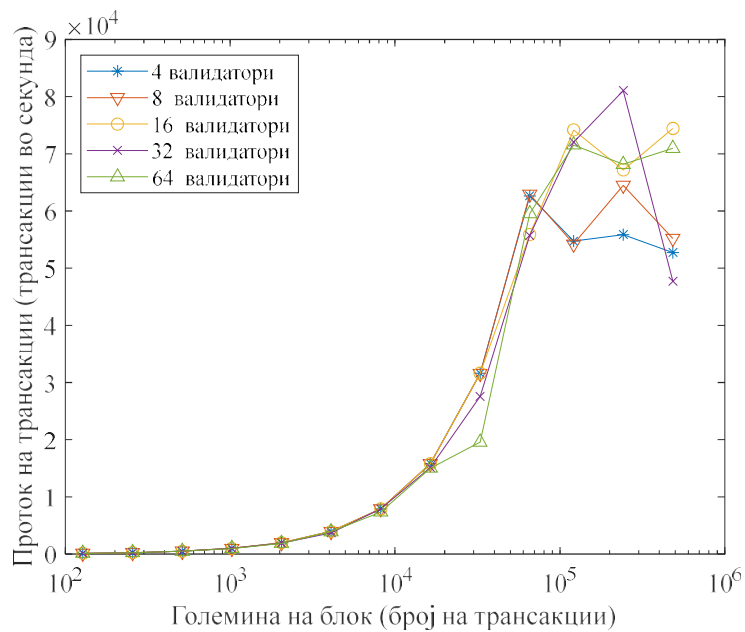
Претходно прикажаните резултати се постигнати во идеални мрежни услови каде нема губење на пакети а латентноста помеѓу две машини е помала од 1ms. Поради поврзаноста на консензус механизмот со однапред дефинирани интервали, се очекува неговите перформанси да зависат од мрежните услови. За таа цел се користи софтвер кој на ниво на мрежен интерфејс воведува дополнителна латентност и цитер по однапред дефинирани услови. Спроведени се емулациски циклуси со параметри на мрежен интерфејс за латентност од 20ms, 50ms, 100ms, 200ms и случајни вредности на латентност со униформна распределба во интервал [0ms, 300ms], како и пакетска загуба од 10% и 20%. На Слика 4.14, Слика 4.15, Слика 4.16, Слика 4.17, се дадени резултати од емулациските циклуси за воведена латентност од 20ms, 50ms, 100ms и 200ms соодветно, а на Слика 4.18 е даден резултатот од емулацискиот циклус за случајни вредности на латентност со униформна распределба во интервал [0ms, 300ms].



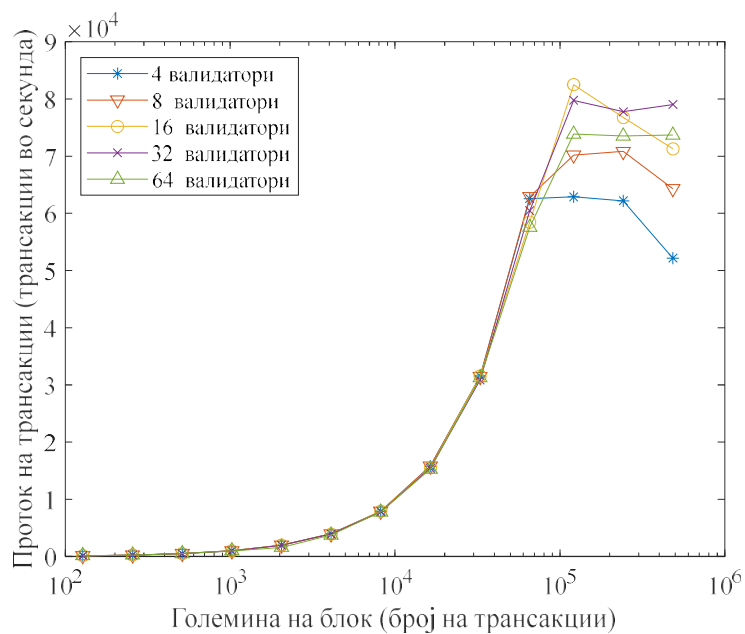
Слика 4.13. Проток на трансакции за интервал на група од трансакции поставен на 10s



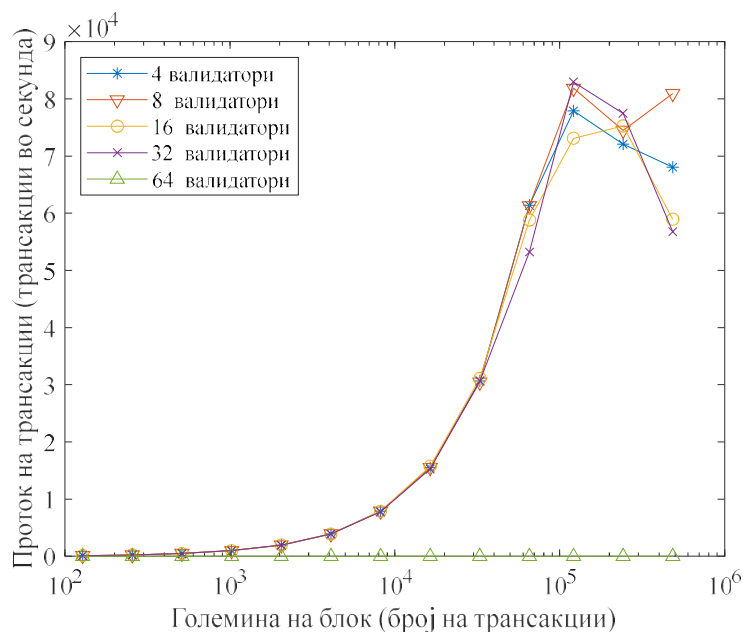
Слика 4.14. Проток на трансакции за мрежна латентност од 20ms



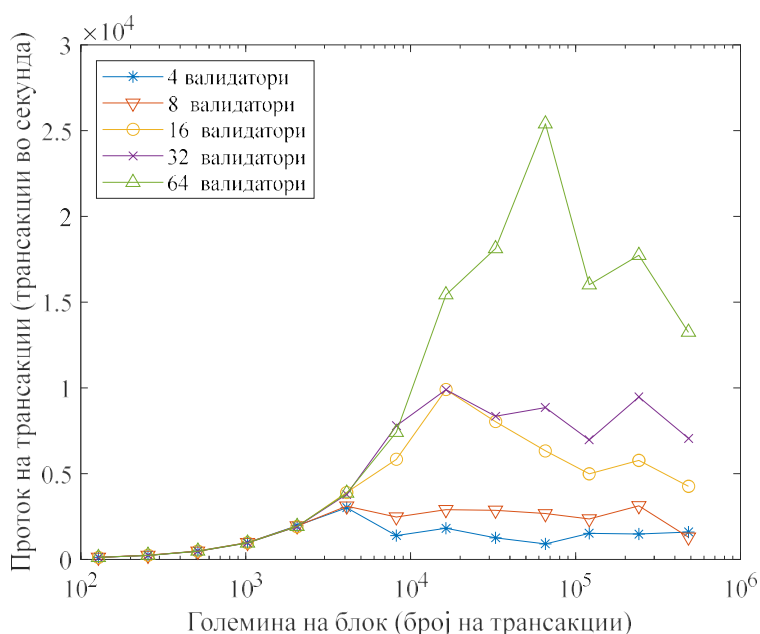
Слика 4.15. Проток на трансакции за мрежна латентност од 50ms



Слика 4.16. Проток на трансакции за мрежна латентност од 100ms



Слика 4.17. Проток на трансакции за мрежна латентност од 200ms



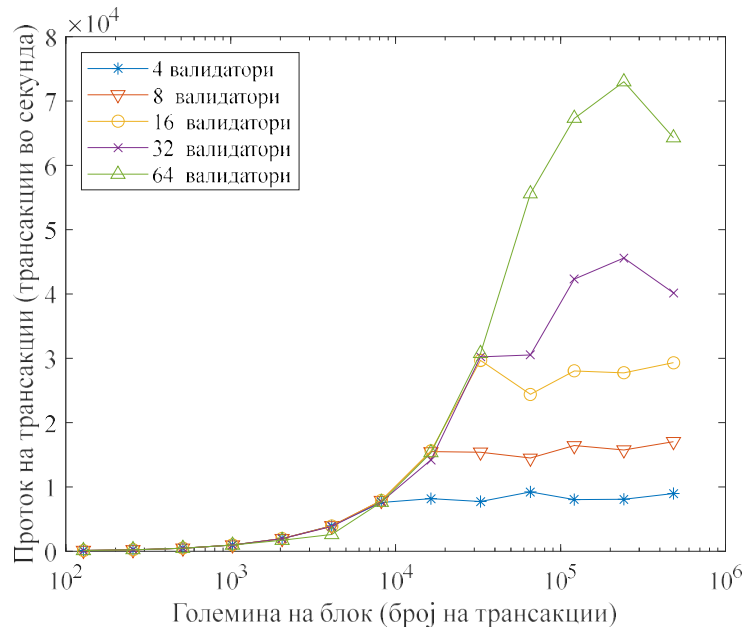
Слика 4.18. Проток на трансакции за мрежна латентност со случајни вредности со униформна распределба во интервал [0ms, 300ms]

Добиените резултати покажуваат незначително влијание на протокот на трансакции во сценаријата со фиксна латентност во мрежата, додека во случајот на променлива латентност со униформна распределба се забележува значително намалување на протокот на трансакции. Фиксното зголемување на латентноста на мрежата не влијае на протокот на трансакции бидејќи тоа воведува константно поместување на консензус интервалите кај сите валидатори, додека променливата латентност поради својата случајна природа може да доведе дел од валидаторите да се

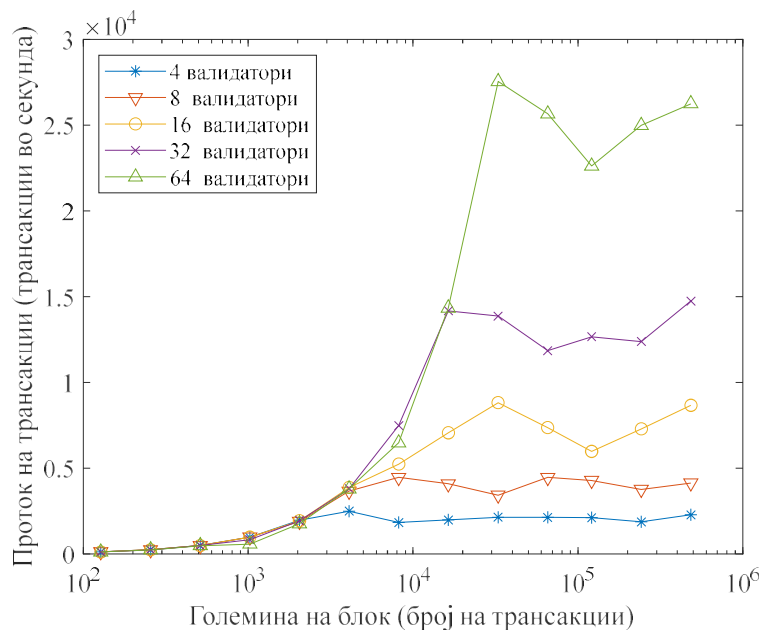
најдат во ситуација да не можат да учествуваат на време во гласањето, на тој начин целиот процес на валидирање да не може да испорача доволен број на валидации во мрежата.

4.2.9. Влијание на пакетските загуби врз протокот на трансакции

Со поставките за загуби на пакети од 10% и 20% се внесуваат рафални загуби на пакети кои значително го намалуваат протокот на трансакции низ мрежата. Резултатите од евалуационите циклуси се дадени на Слика 4.19 и Слика 4.20 соодветно за 10% и 20% на пакетски загуби.



Слика 4.19. Проток на трансакции за поставки на пакетски загуби од 10%



Слика 4.20. Проток на трансакции за поставки на пакетски загуби од 20%

4.2.10. Заклучок за влијанието на конфигурациските поставки врз протокот на трансакции

Од добиените резултати може да се заклучи дека перформансите на основната конфигурација на Tendermint мрежата се блиску до оптимумот за општи сценарија. Најголемо влијание на перформансите има бројот на конекции кон другите валидатори, односно конективност на валидаторите меѓу себе. Висококонективните мрежи имаат послаби перформанси поради натрупувањето на мрежните ресурси со пакети. Спротивно на тоа со нискоконективните мрежи има подобри перформанси на мрежата, но потребно е незначително поголемо време за споделување односно препраќање на пакетите за да стигнат до сите учесници во мрежата.

Друг важен параметар кој влијае на протокот на трансакции е предавателната и приемната брзина. Максимизирањето на овие параметри ќе влијае на намалување на протокот на трансакции поради загушувањето со трансакции кое би се појавило кога би користеле големи брзини. Особено влијание овие параметри имаат во висококонективните мрежи.

Интервалите за предлагање на пакети исто така влијаат на протокот на трансакции. Со намалување на интервалот за предлагање на пакети, во системот се зголемува протокот на трансакции, но тоа ќе го зголеми и мрежниот сообраќај поради зголемениот број на пакети за кои треба да се гласа, но и би се зголемило заглавието поради зачестеноста на пакетите.

Големината на трансакциите исто така има влијание на протокот на трансакции. Како што се очекува поголемите трансакции доведуваат до помали протоци на трансакции во мрежата. Поради дистрибуираната природа на Blockchain технологиите и потребата за дистрибуција на големите трансакции низ мрежата, потребно е и поголемо време за да се завршат тие процеси, што доведува до намалување на протокот на трансакции во мрежата.

Од резултатите може да се забележи дека мрежниот цитер има особено влијание на протокот на трансакции, додека константната латентност нема особено влијание. Важно е да се забележи дека мрежниот цитер има произразено влијание кај мрежите со помалку валидатори каде се забележува значително намалување на протокот на трансакции.

4.3. Перформанси на Tendermint консензус механизмот за големи документи

Со цел да се добие подобра претстава за перформансите на Tendermint консензус механизмот во услови на големи документи во системот и да се определи подобноста за негово користење во систем за јавно здравство, спроведени се сет на емуляции со поголема грануларност на големини на трансакции [113]. Покрај основната големина од 250B, дефинирани се сценарија кои треба да симулираат документи што би циркулирале во јавните здравствени системи. Во Табела 4.3 се претставени сценаријата кои се емулираат и соодветната големина на трансакција за дадениот тип на документи.

Tendermint мрежата се состои од 64 валидатори при што кај секој од нив е активирано подесување за мрежно доцнење од 50ms и цитер од 10ms со униформна распределба. Емуляциите се изведуваат во услови каде се претпоставува дека нема малициозни јазли во системот и сите валидатори се обидуваат максимално да ги опслужат корисниците.

Табела 4.3. Сценарија за големина на трансакција

Сценарио	Големина на трансакција
Основна големина на трансакција	250 Bytes
Краток текст документ	1024 Bytes
Голем текст документ (од една страна)	10240 Bytes
Слика со мала резолуција и мали димензии	102400 Bytes
Слика со мала резолуција и големи димензии	1024000 Bytes
Слика со средна резолуција	3072000 Bytes
Слика со голема резолуција и мали димензии	4096000 Bytes
Слика со голема резолуција и големи димензии	5120000 Bytes

Во Табела 4.4 се дадени резултатите од емулациите за различните сценарија кои се дефинирани со Табела 4.3. Од Табела 4.4 може да се видат вредностите на просечниот проток на трансакции во мрежата за различни брзини на генерирање на трансакции во системот. Се забележува дека процесот на валидација постигнува различни максимални вредности за просечниот проток на трансакции кај различните сценарија. Истакнатите резултати се максимални вредности за просечен проток на трансакции при различните големини на трансакции.

Воведен е нов параметар, *коэффициент на ефикасност*, за да може да се добие подобра слика за ефикасноста со која се верифицираат трансакциите во системот и на тој начин да се определи и искористеноста на системот. Коэффициентот на ефикасност е однос помеѓу бројот на валидирани трансакции во системот и бројот на генерирани трансакции во системот. Поради условите во мрежата, капацитетот за валидирање на валидаторите и протокот на трансакции кај консензус механизмот, бројот на валидирани трансакции е помал, или во идеални услови, еднаков на бројот на генерирани трансакции.

Разликата помеѓу генерираните и валидираните трансакции во системот ни го покажува степенот на искористеност на мрежата, односно колкав број на трансакции не се валидирани заради истечени интервали на консензус механизмот или чекаат во динамичката меморија за да бидат валидирани. За да се постигне подобра искористеност на мрежата, бројот на валидирани трансакции треба да биде што поблизок до бројот на генерирани трансакции.

Во Табела 4.5 се дадени вредностите за коэффициентот на ефикасност за евалуираните сценарија. Истакнатите вредности за коэффициентот на ефикасност се максималните вредности што за дадено сценарио може да се постигнат. Впрочем за истакнатите вредности на коэффициентот на ефикасност, при дадено сценарио може да се определи брзината на генерирање трансакции за која може да се постигне максимално искористување на системот. Со споредување на Табела 4.4 и Табела 4.5 може да се забележи дека максималните вредности за просечен проток на трансакции во системот не соодветствуваат со највисокиот коэффициент на ефикасност за даденото сценарио. Доколку сакаме да го користиме консензус механизмот на тој начин што би го форсирале системот да ја постигне максималната вредност за проток на трансакции, тогаш би дошле до ситуација да голем број од трансакциите кои се генерираат во мрежата, не бидат валидирани, а оние што би се валидирале би ги оставиле корисниците да чекаат долго време за да се финализираат. За да работи системот со што е можно помалку невалидирани трансакции и со прифатливо долги периоди на чекање за валидација на трансакциите, потребно е системот да работи во мод на висок коэффициент на ефикасност.

Табела 4.4. Просечен проток на трансакции за различни големини на трансакции и различна брзина на генерирање на трансакции поголема од 128 трансакции во секунда

Големина на трансакција	Брзина на генерирање трансакции (број на трансакции во секунда генерирани во мрежата)														
	128	256	512	1024	2048	4096	8192	16384	32768	65536	121072	242144	484288		
250 B	116.11	245	445.66	981.41	1921.3	3856.1	7263.7	15580	31038	62887	78277	76493	65696		
1024 B	122.04	218.68	480.64	966.98	1911.8	3333.5	7712	14212	29236	40731	40143	36094	37843		
10240 B	119.58	150.55	447.62	604.15	1925.6	3758.2	5805.6	5901.1	5740.6	5290.9	5151.1	5750.8	5357.7		
102400 B	111.08	178.53	436.13	653.75	600.71	512.48	619.49	502.56	377.43	631.61	549.46	565.7	481.86		
1024000 B	47.831	38.609	33.279	35.027	35.458	35.868	37.492	36.54	37.615	30.988	40.198	36.581	39.281		
3072000 B	1.7364	2.2941	2.2008	2.7886	2.513	2.7311	3.436	2.1986	1.826	1.9918	2.4562	2.6284	3.026		
4096000 B	1.1366	0.76111	1.4067	0.57513	0.85265	1.0181	0.92325	1.4741	0.99508	1.2617	0.99465	0.75897	0.80036		
5120000 B	0.34989	0.52303	0.35393	0.65771	0.34143	0.26216	0.49608	0.52301	0.32678	0.39037	0.52871	0.21459	0.31243		

Табела 4.5. Коэффициент на ефикасност за различни големини на трансакции и различна брзина на генерирање на трансакции поголема од 128 трансакции во секунда

Големина на трансакција	Брзина на генерирање трансакции (број на трансакции во секунда генерирани во мрежата)														
	128	256	512	1024	2048	4096	8192	16384	32768	65536	121072	242144	484288		
250 B	0.91	0.96	0.87	0.96	0.94	0.94	0.89	0.95	0.95	0.96	0.65	0.32	0.14		
1024 B	0.95	0.85	0.94	0.94	0.93	0.81	0.94	0.87	0.89	0.62	0.33	0.15	0.08		
10240 B	0.93	0.59	0.87	0.59	0.94	0.92	0.71	0.36	0.18	0.08	0.04	0.02	0.01		
102400 B	0.87	0.70	0.85	0.64	0.29	0.13	0.08	0.03	0.01	0.01	0.00	0.00	0.00		
1024000 B	0.37	0.15	0.06	0.03	0.02	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00		
3072000 B	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		
4096000 B	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		
5120000 B	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		

Од резултатите во Табела 4.5 може да се согледа дека за големини на трансакции над 102400B коефициентот на ефикасност е низок. Големите документи се значаен дел од јавните здравствени системи, па затоа е потребно подетално да се определи дали постојат брзини на генерирање трансакции за кои може да се постигнат подобри коефициенти на ефикасност. За таа цел спроведено е дополнително испитување за сценариото каде трансакциите се со големина од 5120000B, при што за тоа сценарио се испитани брзини на генерирање трансакции кои се помали од 128 трансакции во секунда. За ова сценарио се дефинирани четири поставки за конфигурации на валидаторите во мрежата, за кои е извршена дополнителна евалуација на перформансите. Параметрите кои се менуваат се следните:

- За конфигурација А се искористени основните поставки дефинирани во Табела 4.2;
- Конфигурацијата Б е базирана на конфигурацијата А притоа бројот на влезните и излезните соработници е поставен на 65, предавателната и приемната брзина се поставени на 10240000B/s и интервалот за предлагање на трансакции е поставен на 10s;
- Конфигурацијата В е базирана на конфигурацијата Б, но со зголемени параметри за интервалите за пред-гласање и пред-извршување, кои се поставени на 3s;
- Конфигурацијата Г е базирана на конфигурацијата А, но со намалени вредности за бројот на влезни и излезни соработници, кои се поставени на 5.

Во Табела 4.6 се дадени резултатите добиени од емулацијата на четирите конфигурации. Очигледно дека за 16 генерирани трансакции во секунда, мрежата постигнува максимална вредност на протокот на трансакции. Најдобра конфигурација е Г, каде подобрувањето на протокот на трансакции е постигнато како резултат на намалувањето на бројот на влезните и излезните соработници, со што се намалува оптеретувањето на мрежата. Табела 4.7 ги дава коефициентите за ефикасност на четирите конфигурации каде се забележува дека конфигурацијата Г постигнува највисок коефициент на ефикасност за брзина на генерирање на трансакции од 2 трансакции во секунда.

Табела 4.6 и Табела 4.7 покажуваат дека при дизајнирањето и оперирањето на мрежата може да избереме системот да работи во мод на максимален проток на трансакции или максимален коефициент на ефикасност. Притоа треба да имаме во предвид дека високиот коефициент на ефикасност гарантира валидација на трансакции со вообичаено време на чекање за финализирање на трансакцијата и со мал број на невалидирани и отфрлени трансакции, додека при работа во мод на максимален проток, системот може да дојде во ситуација да работи субоптимално.

Дополнителна анализа на резултатите од Табела 4.6 и Табела 4.7 покажува дека 16 трансакции во секунда е брзина на генерирање трансакции која нуди можност за постигнување максимален протокот на трансакции при споредба на четирите конфигурации. Конфигурацијата Г е најдобар избор за да се постигнат поголеми протоци на трансакции, но воедно го става системот да работи со висока ефикасност. Постигнатите резултати на конфигурацијата Г се последица на малата конективност меѓу валидаторите, што за сценарија на големи трансакции во системот позитивно ќе влијае на максимизирање на коефициентот на ефикасност. По однос на конфигурацијата Г, максималната вредност за просечен проток на трансакции постигната при брзина на генерирање на трансакции од 16 трансакции во секунда, нуди помал коефициент на

ефикасност споредено со коефициентот на ефикасност постигнат за 2 трансакции во секунда.

Табела 4.6. Просечен проток на трансакции за различни големини на трансакции и различна брзина на генерирање на трансакции помала од 64 трансакции во секунда

Конфигурација	Брзина на генерирање трансакции (број на трансакции во секунда генерирани во мрежата)						
	1	2	4	8	16	32	64
Конфигурација А	0.1	0.133	0.467	0.833	3.967	2.9	0.533
Конфигурација Б	0.2	0.3	0.767	0.767	3.7	1.233	0.7
Конфигурација В	0.067	0.4	0.3	2.9	5.733	1.967	0.367
Конфигурација Г	0.467	1.6	1.533	4.733	9.233	0.833	0.467

Табела 4.7. Коефициент на ефикасност за различни големини на трансакции и различна брзина на генерирање на трансакции помала од 64 трансакции во секунда

Конфигурација	Брзина на генерирање трансакции (број на трансакции во секунда генерирани во мрежата)						
	1	2	4	8	16	32	64
Конфигурација А	0.1	0.0665	0.11675	0.104125	0.247938	0.090625	0.008328
Конфигурација Б	0.2	0.15	0.19175	0.095875	0.23125	0.038531	0.010938
Конфигурација В	0.067	0.2	0.075	0.3625	0.358313	0.061469	0.005734
Конфигурација Г	0.467	0.8	0.38325	0.591625	0.577063	0.026031	0.007297

4.4. Естимација на покриеност на пациенти

Параметарот *покриеност на пациенти* (P_c) [113] е воведен за да се истражи можноста Tendermint консензус механизмот да се користи како основа за глобален јавен здравствен систем. Овој параметар е приближна проценка за бројот на пациенти кои би можеле да бидат опслужени со имплементираниот систем. За да се пресмета покриеноста на пациентите ќе се употребат вредностите добиени при евалуацијата на перформансите на Tendermint консензус механизмот. Практично максималната вредност на средниот проток на трансакции би претставувала *брзината на генерирање на записи за пациентите во системот* (P_{gr}) во услови на максимална оптовареност. Од друга страна, брзината на генерирање на записи за пациентите во системот може да се претстави како број на записите што секој здравствен работник ќе го внесе за секој пациент при неговата посета во ординација што би можеле да го изразиме со следната релација:

$$P_{gr} = H_p * v \quad (4.1)$$

Тука H_p претставува број на здравствени работници, а v претставува просечен број на пациенти кај здравствениот работник во еден ден.

Големина на панел (P_s) претставува вкупен број на пациенти кои се под здравствена заштита на еден здравствен работник [114]. Доколку го употребиме параметарот големина на панел, дефиницијата за покриеност на пациенти може да се изрази на следниот начин:

$$P_c = H_p * P_s \quad (4.2)$$

Со замена на (4.1) во (4.2) се добива следната релација:

$$P_c = \frac{P_{gr}}{v} * P_s \quad (4.3)$$

Пореалистични резултати за параметарот покриеност на пациенти може да се добијат доколку земеме во предвид реални бројки за големината на панел и за просечниот број на пациенти на ден, за еден здравствен работник. Според [114], просечната големината на панел е 1806 пациенти, а просечниот број на посети кај здравствениот работник е 24 пациенти на ден (или 0.0008333 посети во секунда доколку се смета 8 часовно работно време). Со имплементација на овие параметри во (4.3), крајната релација за покриеност на пациенти е:

$$P_c = \frac{P_{gr}}{0.0008333} * 1086 \quad (4.4)$$

За да се добие претстава за големината на покриеноста на пациентите со систем базиран на Tendermint консензус механизмот, ќе земеме во предвид три различни реализации на таквиот систем. Разликата се состои во конфигурацијата на Tendermint базираниот здравствен систем поврзана со големината на трансакциите што би се користела во таквиот систем, притоа би зеле во предвид документи со големина од:

- 10240B – што претставува извештај за наод од една страна
- 1024000B – што претставува слика
- 5120000B – што претставува слика со голема резолуција или видео.

Приближните вредности за брзината на генерирање на записи за пациентите за овие големини на трансакција, ќе бидат екстрахирани од Табела 4.4 и Табела 4.6. Со замена на сите потребни параметри во релацијата (4.4), се добиваат резултатите прикажани во Табела 4.8.

Табела 4.8. Покриеност на пациенти

Големина на трансакција	Брзината на генерирање на записи за пациентите	Покриеност на пациенти
10240B	≈6000 записи во секунда	≈13 000 000 000 пациенти
1024000B	≈50 записи во секунда	≈100 000 000 пациенти
5120000B	≈9 записи во секунда	≈12 000 000 пациенти

Резултатите од Табела 4.8 го покажуваат потенцијалот за имплементација на Tendermint консензус механизмот во јавен здравствен систем за голема популација со 64 валидатори во мрежата. Доколку во реален здравствен систем преобладаваат документи се текстуалните извештаи или документи со средна големина, тогаш со таквиот систем би било можно да се покрие население со приближно 13 000 000 000 пациенти. Со ова се докажува дека Tendermint консензус механизмот може да се употреби во јавен здравствен систем со 64 валидатори и притоа да се опслужи светската популација на високо ефикасен начин. Но за градење на глобален систем, 64 валидатори во мрежата претставуваат високо централизирано решение со оглед на бројот на земји кои би сакале да партиципираат во таквиот систем. Во принцип секоја земја би сакала да учествува во таквиот систем со најмалку еден валидатор со цел да има целосен увид во управувањето на глобалниот јавен здравствен систем. За таа цел потребно е да се дефинира ново решение кое би овозможило соодветно скалирање на системот според потребите на глобалниот јавен здравствен систем во кој би имале илјадници валидатори кои би учествувале во поддршката на глобалното решение за јавен здравствен систем, со што би се овозможиле универзални здравствени услуги на сите жители во светот.

5. BLOCKCHAIN ТЕХНОЛОГИЈА ЗА ЈАВЕН ЗДРАВСТВЕН СИСТЕМ – BLOHES

Дизајнот на глобален јавен здравствен систем базиран на Blockchain технологија, Blockchain Healthcare System (BloHeS), треба да понуди високо ниво на скалабилност за да може да ја опслужи широка популација и да има високо ниво на децентрализираност на системот. Дополнително Blockchain технологијата врз која би се градел системот потребно е да може да се справи со големиот наплив на здравствени записи што се дел од временски ограничениите сервиси или итните служби (дојави за здравствени проблеми, препраќање на пациенти помеѓу оддели како и комуникација во реално време), но треба да може да се справи и со сите податоци кои доаѓаат од временски нерестриктирани сервиси или сервиси за запишување на податоци (пишување на извештаи и складирање на резултати од извршени испитувања). Ваквиот систем потребно е да имплементира и IoT сервиси за набљудување на здравствените параметри во реално време. Дополнително зголемување на комплексноста на целокупниот систем би довело спојување на здравствениот систем со осигурителни и фармацевтски компании. Доколку се изгради ваков систем, најголем бенефит би имале пациентите. Основен бенефит од имплементацијата на еден ваков систем би била можноста да се управува со личните податоци. *Пациент-центричното* управување со податоците ќе им овозможи на пациентите да управуваат со пристапот кон личните податоци, ќе овозможи реискористување на нивните лични податоци, па дури би овозможило и финансиски бенефит од продавање на нивните лични податоци за спроведување на дополнителни истражувања. За таа цел нов пристап за управување на личните податоци во здравствените системи е од есенцијално значење.

Во склоп на предложената рамковна структура за Blockchain базиран јавен здравствен систем [16], развиено е Blockchain ниво (види Глава 2.4.1) чиј главен фокус е дефинирање на интеракцијата помеѓу пациентот и здравствениот работник преку обезбедување на високо ниво на приватност и можност за управување со пристапот до личните податоци. Покрај пациентот и здравствениот работник, од основно значење е постоењето на IoT уреди кои ќе бидат во служба на зголемување на комодитетот на пациентите и попрецизно набљудување на нивната здравствена состојба, но би имало и други агенти кои би ги претставувале владините институции, фармацевтските и осигурителните компании и агенти со Вештачка интелигенција.

Притоа, IoT уредите би се наоѓале во близина на пациентите, со цел да собираат параметри за виталноста на пациентите. Независно од комуникациската технологија, овие уреди собираат и потоа испраќаат информации до точките за складирање на податоци од пациентите. Поврзувањето на уредите со пациентите може да биде направено од страна на пациентот или здравствениот работник, а за да започне собирањето на податоци, уредот треба да добие дозвола од здравствениот работник.

Владините институции имаат круцијална улога во развојот на системот и управувањето на дел од ентитетите во мрежата. Издавањето на идентификациски број, во форма на адреса на паричник (wallet address), владината институција ќе го прави во затворен систем помеѓу пациентот, здравствениот работник и владината институција. Оваа процедура би подразбирала асоцирање на дигиталниот идентитет на пациентот со адресата на паричникот.

Со дефинирањето на посебни ентитети, за осигурителните компании се овозможува создавање на нова бизнис логика за здравствено осигурување. Целосната здравствена историја на пациентот би дала подобра слика за неговата здравствена

состојба, со што осигурителната компанија ќе може многу подобро да дефинира нови производи. Дополнително фармацевтската индустрија би имала бенефит од дефинирањето на посебен ентитет преку кој би можеле да учествуваат во здравствениот систем. Фармацевтските компании би можеле многу подобро да ја пратат ефикасноста на нивните лекови. Уште повеќе, покрај индивидуалниот, фармацевтските компании би можеле да имаат и групен здравствен статус. Притоа информациите кои се користат би можеле да бидат анонимизирани, за да се заштитат личните податоци. Постоењето на агенти со Вештачка интелигенција во мрежата, може да помогне во зголемена предвидливост на болести како и потенцијални лекови кои би биле развивани од фармацевтските компании. Агент со Вештачка интелигенција поставен во рамките на владиниот агент може да обработува податоци од пациенти и на тој начин да креира извештаи за здравствената состојба на целокупната популација, а згора на тоа би можел и да дава финансиски конструкции и извештаи кои се потребни за владините институции.

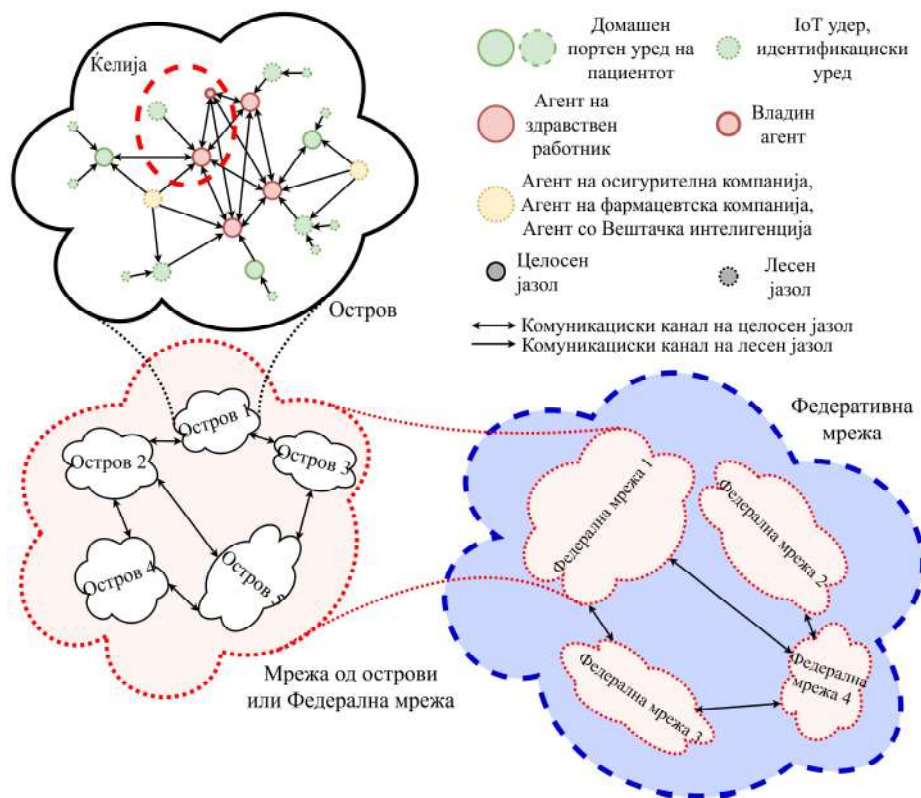
5.1. Архитектура на BloHeS системот

Согласно рамковната дефиниција за Blockchain базиран јавен здравствен систем, потребно е да се дефинираат посебни типови на *агенти* со цел да се направи попрецизно и полесно дефинирање на привилегиите и обврските што би ги имале индивидуалните агенти во системот. Генерално агентите може да бидат од два типа: *целосни* и *лесни* јазли. Целосните јазли (full nodes) се вклучени во управувањето на важни процеси во системот како што се валидирање и складирање на податоци, додека лесните јазли (lightweight nodes) се вклучени само во маргинални процеси генерално поврзани со отчитување на податоци од системот. Така, во рамките на BloHeS системот се дефинираат пет кориснички агенти, како основни градбени единици на мрежата:

- *Агент на здравствен работник* – е целосно функционален јазол во мрежата, кој имплементира оптимална база на податоци и е способен да спроведува валидација на податоците од Blockchain системот, спроведува процедури за генерирање на новчаници, внесува податоци, складира податоци од пациенти и управува со базата на пациенти.
- *Владин агент* – е целосно функционален јазол кој има целосна база на податоци од сите пациенти во мрежата, каде податоците се складираат во екриптирана форма и се достапни само по претходно одобрение од страна на пациентите. Има можност да го надгледува спроведувањето на Blockchain процедурите во целата мрежа.
- *Агент на пациент* – ова е целосен јазол, со опција да учествува во процесот на валидација на податоците доколку таквата можност е дадена од страна на владин агент. Основна улога на агентот на пациентот е да управува со правата за пристап до личните податоци, како и да врши проверка на коректноста на податоците кои се запишуваат во неговата база на податоци. Дополнително овој агент може да управува со домашен портен уред или IoT уред кој е лесен уред и има основна цел да врши собирање на податоци.
- *Помошен агент* – е лесен јазол кој е во доменот на управување на пациентот или на здравствениот работник. Во овој тип на агенти спаѓаат домашен портен уред, IoT уред, идентификациски уред и др. Основна улога на овие агенти е да овозможат собирање и складирање на податоци, но не и валидација на податоци.

- *Јавен агент* – е лесен јазол достапен за осигурителните компании, фармацевтските компании и јазлите со Вештачка интелигенција. Овие јазли имаат привилегија за читање на податоците при претходно одобрување од страна на пациентите.

Дефинираните агенти учествуваат во мрежната организација на BloHeS системот со цел да се подобри *скалабилноста* (скалабилноста на складирањето на податоци, протокот на трансакции, латентноста и адресниот простор) и енергетската ефикасност на Blockchain системот, што се добро познати слабости на јавните Blockchain платформи, како што се Bitcoin и Ethereum. Мрежната организираност на BloHeS системот е прикажана на Слика 5.1.



Слика 5.1. BloHeS мрежна организација

Прво ниво на организација, а воедно и најмала организациона единица во мрежата е *келија* (Cell). Келијата е формирана од агент на пациентот и агент на здравствениот работник. За да се постигне подобра функционалност и робустност на системот, задолжителен учесник од доверба во келијата ќе биде владиниот агент. Опционално, пациентот може да додава и други агенти во келијата како домашни портни уреди од доверба (како референтни точки за складирање на здравствените податоци) и IoT уреди (како подобрувачи на комфорот и собирачи на податоци). Носител на келијата е агентот на пациентот преку постојано одржување и управување на *Личниот Blockchain поток* на пациентот (Personal Blockchain Stream – PBS), воведен во [115]. Личниот Blockchain поток претставува база на здравствени податоци која има Blockchain податочна структура и ги содржи личните податоци на пациентот.

Остров претставува второто ниво на организација во BloHeS мрежата. Островите се временски формации во мрежата кои се создаваат од страна на агенти на здравствените работници, кои се вмрежуваат меѓу себе преку однапред определени протоколи за да го оптимизираат консензус механизмот за зголемена скалабилност на системот. Со користење на само-организациски алгоритам, агентите на здравствените работници може да определат група на соседни агенти на здравствени работници со кои може да постигнат однапред определени нивоа на латентност во комуникацијата и на тој начин да овозможат максимални перформанси на консензус механизмот. Островите се формираат само од агенти на здравствени работници, но во зависност од проценката направена од страна на владините институции во системот, може да бидат вклучени и агенти на пациентите во процесот на верификација на податоците.

Трето ниво на вмрежување во BloHeS архитектурата е мрежата од острови што претставува *Федерална мрежа*. Мрежата од острови или Федералната мрежа е највисоко ниво на автономна организациона единица и истата целосно се вклопува во државните граници, а згора на тоа има можност да биде организирана така што ќе ги следи и правните прописи кои се дадени во државата. Со имплементација на *паметни договори*, може да се дефинира правната регулатива која се применува во државата и истата да биде рефлектирана во работата на BloHeS системот.

Највисоко ниво на организација е *Федеративната мрежа*. Федеративната мрежа е составена од сите Федерални мрежи кои може да воспостават потесни врски и взаемна соработка со други Федерални мрежи следејќи ги договорите помеѓу земјите учеснички. Градењето на Федеративна мрежа би му овозможило на пациентот да има пристап до личните податоци и да добива медицинска нега, надвор од границите на матичната држава.

5.2. BloHeS консензус механизам

Еднониовската архитектура на Tendermint консензус механизмот не овозможува голем раст на бројот на валидатори во мрежата, што за сценарија од голем обем би претставувало проблем. Поради експоненцијалното зголемување на разменети пораки за постигнување на консензус со зголемувањето на бројот на валидатори во мрежата, многу брзо мрежата и самите мрежни интерфејси на валидаторите се загушуваат од големиот број на пораки. За да се овозможи ширење на мрежата, се воведува нова *димензија на скалирање* преку воведувањето на нивовска организација, со што се дефинира новиот BloHeS консензус механизам [116]. BloHeS архитектурата [117] воведува *повеќенивовска хиерархија* која ќе овозможи ширење на системот со подобрени перформанси за мрежи со голем број на валидатори. На Слика 5.2 е даден дијаграмот на BloHeS консензус механизмот.

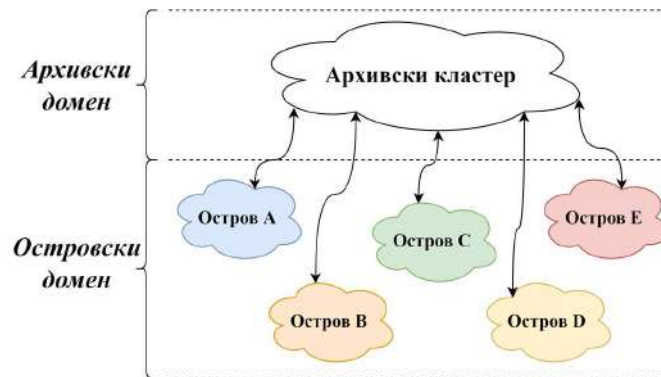
Дизајнот на BloHeS консензус механизмот е базиран на Tendermint консензус механизмот, но за да ја постигне нивовската структура употребува два поврзани и модифицирани Tendermint консензус механизми кои независно ги оркестрираат валидаторите во *Архивскиот* и *Островскиот домен* во BloHeS мрежата. Нивовската организација на BloHeS системот е прикажана на Слика 5.3.

Островскиот домен е ниво од BloHeS мрежата кое е изградено од сите острови во мрежата. Остров претставува кластер на валидатори кои управуваат еден островски консензус механизам. Валидираниот пакет кој произлегува од успешен островски консензус механизам се испраќа за архивирање до Архивскиот домен. Валидаторите во островскиот домен се агентите на здравствените работници.



Слика 5.2. BloHeS консензус механизам

Архивскиот домен е единствен кластер од валидатори во BloHeS мрежата кои управуваат Архивски консензус механизам преку кој се организираат и ги валидираат преходно испратените податочни блокови од страна на островите. Во рамките на Архивскиот кластер задолжително има владин агент, но може да има и валидатори кои се управувани од високодоверливи невладини институции. Постоенето на невладините валидатори би ја зголемила довербата во системот.



Слика 5.3. Нивовска организација на BloHeS системот

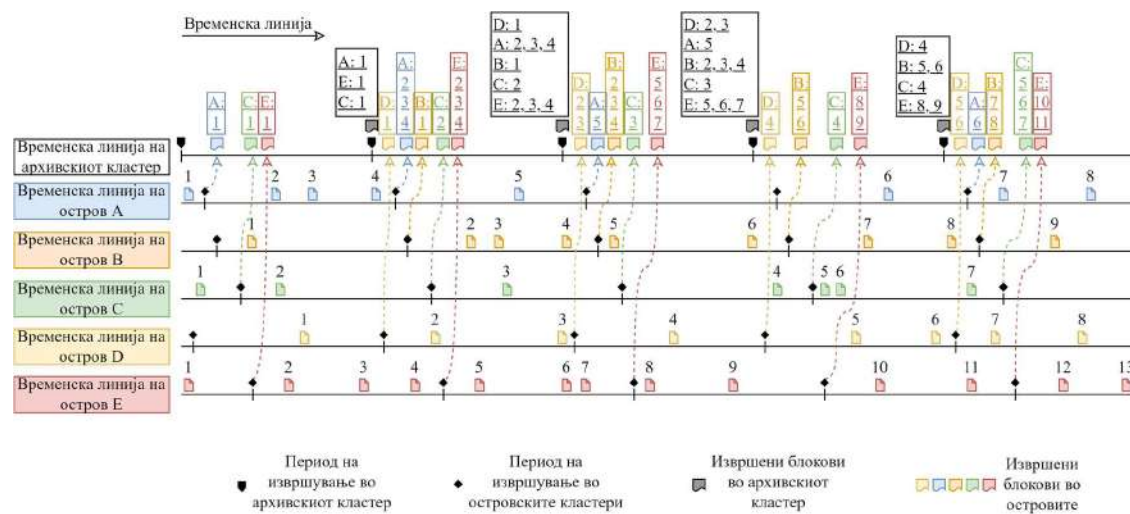
За да се овозможи двонивовското валидирање на трансакциите, покрај mempool меморијата, [103], која е дефинирана кај Tendermint консензус механизмот, BloHeS консензус механизмот воведува дополнителна commitpool меморија. Секој остров управува со посебна commitpool меморија каде валидаторите ги зачувуваат извршените податочни блокови додека истите не бидат потврдени од страна на архивскиот кластер.

Островските консензус механизми се управуваат независно од архивскиот консензус механизам, но истите се поврзани со него со еднонасочни врски. Податочните блокови што островите ќе ги прогласат за извршни, се испраќаат до архивскиот кластер од валидатори, каде привремено се складираат во mempool меморијата на валидаторите од архивскиот кластер по што ќе бидат вклучени како предлог за следниот податочен блок. Архивскиот кластер преку две еднонасочни врски испраќа информации за исходот

од процесот на валидација за претходно примените податочни блокови. Доколку податочниот блок е успешно валидиран се испраќа известување до соодветниот островски предлагач на податочен блок со цел валидаторите во островот да ги тргнат трансакциите од `commitpool` и од `tempool` мемориите. Доколку податочниот блок не е успешно валидиран во архивскиот кластер, се испраќа информација за исходот од процесот на валидирање до островскиот предлагач на пакет по што трансакциите од тој податочен блок се бришат од `commitpool`, но не и од `tempool`, по што би се додаде во нов податочен блок.

Во островскиот консензус механизам е воведена нова фаза во која се врши распространување на информацијата за успешно архивирање и финализирање на трансакциите во островот. Оваа фаза се спроведува доколку островот добие потврден одговор дека податочниот блок поминал успешно низ консензус процесот. За време на оваа фаза, предлагачот во островот ги информира останатите учесници во островот да извршат финализирање на трансакциите од потврдениот податочен блок, по што учесниците го запишуваат финализираниот блок во федералната база на податоци и ги отстрануваат соодветните трансакции од `commitpool` и `tempool`.

На Слика 5.4 е прикажана временската линија од BloHeS консензус механизмот. Како што е прикажано на сликата, сите извршни пакети од независните острови се собираат во `tempool` на архивскиот кластер со цел да се вклучат во следниот податочен блок.

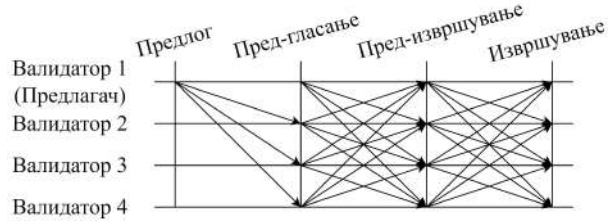


Слика 5.4. Временска линија на BloHeS консензус механизмот

5.2.1. Дијаграм на размена на пораки кај Tendermint и BloHeS консензус механизмите

Сите активни валидатори во Tendermint мрежата учествуваат во процесот на гласање за да се постигне консензус и да се финализира податочниот блок. За успешен процес на валидација кај Tendermint консензус механизмот, бројот на активни валидатори n треба да биде во опсегот $[2*f+1, 3*f+1]$, што остава простор бројот на малициозни јазли да биде во опсегот $[0, f]$, [80]. Тоа значи дека во услови на f малициозни валидатори, потребно е минимум $n=3*f+1$ валидатори во мрежата за да има коректен консензус механизам.

Бројот на разменети пораки помеѓу валидаторите во секоја фаза на процесот на гласање ја дава вредноста на параметарот наречен *број на пораки*. Бројот на разменети пораки е мерка за нивото на комплексност на комуникацијата за постигнување на консензус во системот. Вкупниот број на пораки за финализирање на еден податочен блок во една рунда од консензус механизмот се движи помеѓу M_{min} и M_{max} , соодветно на сценаријата кога има f и 0 малициозни јазли, односно кога имаме $n-f$ и n коректни валидатори. Дијаграмот на размена на пораки кај Tendermint консензус механизмот е даден на Слика 5.5.



Слика 5.5. Дијаграм на размена на пораки кај Tendermint консензус механизмот

Вкупниот број на пораки за финализирање на еден податочен блок кај Tendermint консензус механизмот е збир на бројот на разменети пораки во трите фази од консензус механизмот. За време на фазата за предлагање, бројот на разменети пораки е:

$$M_{propose} = n - 1 = 3f + 1 - 1 = 3f \quad (5.1)$$

каде n е број на валидатори во мрежата, а f е максимален број на малициозни јазли за даден n каде $n = 3f + 1$.

Коректен консензус може да се постигне кога во мрежата има минимум $n-f$ и максимум n коректни валидатори. Соодветно бројот на разменети пораки во фазата на пред-гласање и пред-извршување би се движел во опсег помеѓу соодветните минимални и максимални вредности, зависно од бројот на коректни валидатори во мрежата. Бројот на пораки во пред-гласање и пред-извршување се определуваат како:

$$M_{prevote}^{min} = M_{precommit}^{min} = (n - 1) * (n - f) = 3f * (2f + 1) \quad (5.2)$$

$$M_{prevote}^{max} = M_{precommit}^{max} = (n - 1) * n = 3f * (3f + 1). \quad (5.3)$$

Соодветно формулата за пресметување на вкупниот минимален број на пораки M_{min} и вкупниот максимален број на пораки M_{max} е:

$$M_{min} = M_{propose} + M_{prevote}^{min} + M_{precommit}^{min} \quad (5.4)$$

$$M_{max} = M_{propose} + M_{prevote}^{max} + M_{precommit}^{max}. \quad (5.5)$$

Од анализата на дијаграмот за размена на пораки кај BloHeS консензус механизмот прикажана на Слика 5.6, може да се забележи дека размената на пораки можеме да ја поделиме на размена на пораки внатре во кластерот (интракластерски) и размена на пораки меѓу кластерите (интеркластерски). Од тука вкупниот број на разменети пораки M за финализирање на една рунда на BloHeS консензус механизмот е дадена како:

$$M = M_{intracluster} + M_{intercluster}. \quad (5.6)$$

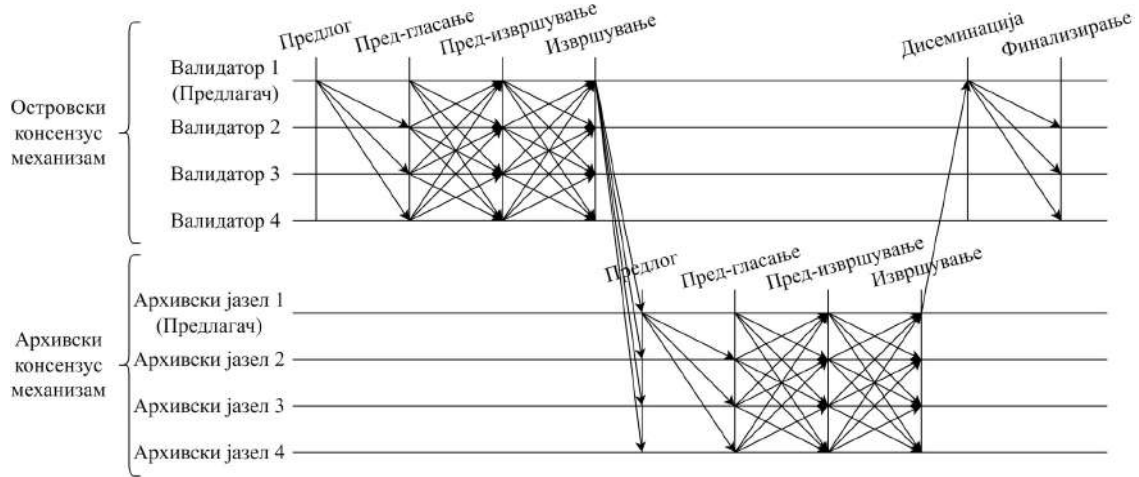
Интракластерскиот број на пораки, $M_{intracluster}$, се пресметува како:

$$M_{intracluster} = n_i * M_{island} + M_{archiving cluster} \quad (5.7)$$

а интеркластерскиот број на пораки, $M_{intercluster}$, се пресметува како:

$$M_{intercluster} = M_{request} + M_{response} = A_V * n_i + n_i \quad (5.8)$$

променливата n_i претставува број на острови во мрежата, а A_V е број на валидатори во архивскиот кластер.



Слика 5.6. Дијаграм на размена на пораки кај BloHeS консензус механизмот

Интеркластерската комуникација во рамките на островот има дополнителна фаза за споделување на повратната информација од архивскиот кластер внатре во самиот остров, па затоа бројот на пораки се пресметува според:

$$M_{island} = M_{propose}^{island} + M_{prevote}^{island} + M_{precommit}^{island} + M_{disseminate}. \quad (5.9)$$

Дијаграмот на размена на пораки за интеркластерската комуникација во архивскиот кластер е ист како кај основниот Tendermint консензус механизам и се пресметува како:

$$M_{archiving cluster} = M_{propose}^{arch} + M_{prevote}^{arch} + M_{precommit}^{arch} \quad (5.10)$$

каде бројот на пораки се пресметува според (5.4) и (5.5) соодветно, за минималниот и максималниот број на пораки во архивскиот кластер.

Бројот на пораки во фазата за предлагање, пред-гласање и пред-извршување се пресметува исто како кај Tendermint консензус механизмот:

$$M_{propose} = n - 1 = 3f + 1 - 1 = 3f \quad (5.11)$$

$$\begin{aligned} M_{prevote}^{min} &= M_{precommit}^{min} = (n - 1) * (n - f) = (3f + 1 - 1) * (3f + 1 - f) \\ &= 3f * (2f + 1) \end{aligned} \quad (5.12)$$

$$M_{prevote}^{max} = M_{precommit}^{max} = (n - 1) * n = (3f + 1 - 1) * (3f + 1) = 3f * (3f + 1) \quad (5.13)$$

додека бројот на пораки во фазата на дисеминација се пресметува според:

$$M_{disseminate} = n - 1 = 3f + 1 - 1 = 3f. \quad (5.14)$$

Бројот на пораки во фазите на пред-гласање и пред-извршување е поврзан со бројот на коректни валидатори во мрежата, заради што е потребно да се определи минимален и максимален број на пораки. Консензус механизмот во архивскиот кластер, како и оној во островските кластери може успешно да се справи во услови на присуство на малициозни валидатори доколку бројот на коректни валидатори остане помеѓу $n-f$ и n , при што соодветно би можеле да се определат минималниот број на пораки M_{min} и максималниот број на пораки M_{max} како:

$$M_{min} = M_{intercluster} + n_i * (M_{propose} + M_{prevote}^{min} + M_{precommit}^{min} + M_{disseminate}) + M_{archiving\ cluster} \quad (5.15)$$

$$M_{max} = M_{intercluster} + n_i * (M_{propose} + M_{prevote}^{max} + M_{precommit}^{max} + M_{disseminate}) + M_{archiving\ cluster} \quad (5.16)$$

каде n_i е број на острови во мрежата.

5.2.2. Капацитет на заштита

Воведен е нов параметар, наречен *капацитет на заштита* P , со цел да се определи квантитативна мерка со која ќе се опише капацитетот на консензус механизмот да постигне коректен консензус во присуство на малициозни валидатори. Капацитетот на заштита е поврзан со бројот на малициозни јазли чиј напад може да биде издржан од страна на консензус механизмот додека сеуште системот испорачува коректни блокови со информации. Се пресметува како збир од максималниот број на малициозни јазли што може да се толерираат, во секој кластер од мрежата:

$$P = \sum_{k=1}^{n_{a+i}} f_k \quad (5.17)$$

каде f_k е максимален број на малициозни јазли што може да се толерираат во еден кластер и $n_{a+i} = n_a + n_i$ е вкупниот број на кластери во мрежата (архивски кластер плус острови).

Tendermint мрежата може да се смета како единечен кластер со што би се имплементирала вредноста $n_{a+i}=1$. По дефиниција Tendermint консензус механизмот може да се справи со f малициозни јазли што се пресметува како:

$$f = \left\lfloor \frac{n-1}{3} \right\rfloor \quad (5.18)$$

каде n е број на валидатори во Tendermint мрежата [80]. Со имплементација на оваа релација во (5.17), капацитетот на заштита на Tendermint консензус механизмот ќе биде:

$$P_T = f = \left\lfloor \frac{n-1}{3} \right\rfloor \quad (5.19)$$

каде P_T е капацитетот на заштита на Tendermint консензус механизмот.

Мрежната организираност на BloHeS системот е повеќекластерска. Кластерите имплементираат интракластерски протокол (архивски или островски консензус механизам) кој е базиран на Tendermint консензус механизмот, па на тој начин може да постигне ист капацитет на заштита на ниво на кластер како и Tendermint мрежа со ист број на валидатори. Различните острови може да имаат различен капацитет на заштита

поради тоа што големината на кластерите не е еднаква. Заштитата од малициозни валидатори на ниво на остров е дадена со (5.18). Валидаторите учествуваат во рамките на островот по автономен избор, што создава неуниформна и случајна распределба на валидаторите низ островите, што го прави тешко пресметувањето на капацитетот на заштита. За да може да се пресмета капацитетот на заштита на BloHeS системот, се претпоставува униформност на распределбата на валидатори, односно:

- Сите острови имаат иста големина;
- Бројот на малициозни јазли во секој остров е ист.

Со имплементација на овие претпоставки, за капацитетот на заштита се добива:

$$P_B = P_A + n_i * P_i \quad (5.20)$$

каде P_B е капацитет на заштита на BloHeS консензус механизмот, P_A е капацитет на заштита на архивскиот кластер, n_i е број на острови во мрежата и P_i е капацитет на заштита на ниво на остров.

5.2.3. Евалуација на перформанси

За да се определи подобрувањето кое се постигнува кај BloHeS консензус механизмот споредено со Tendermint консензус механизмот, се споредуваат потребниот број на разменети пораки за финализирање на еден податочен блок и капацитетот на заштита на овие два консензус механизми со помош на MATLAB [118] софтверскиот пакет.

Перформансите на двата консензус механизми се евалуирани врз мрежи со еднаков број валидатори, бидејќи е потребно да ги земеме предвид структурните разлики на двата консензус механизми. Бројот на валидатори во мрежата се движи меѓу $V = [1, 1000]$.

Tendermint мрежата може да се смета дека е изградена од еден кластер што значи $n_{a+i}=1$, а бројот на валидатори во островот е еднаков на бројот на валидатори во мрежата $n=V$. Бројот на валидатори во Tendermint сценариото формира сет од дискретни вредности за бројот на валидатори што се определува со релацијата:

$$n = 3 * f + 1, \text{ за } f = \left(\frac{n-1}{3}\right) \in N \quad (5.21)$$

каде n е број на валидатори во кластерот, f е максимален број на малициозни валидатори во мрежата за дадено n и N е множеството на природни броеви.

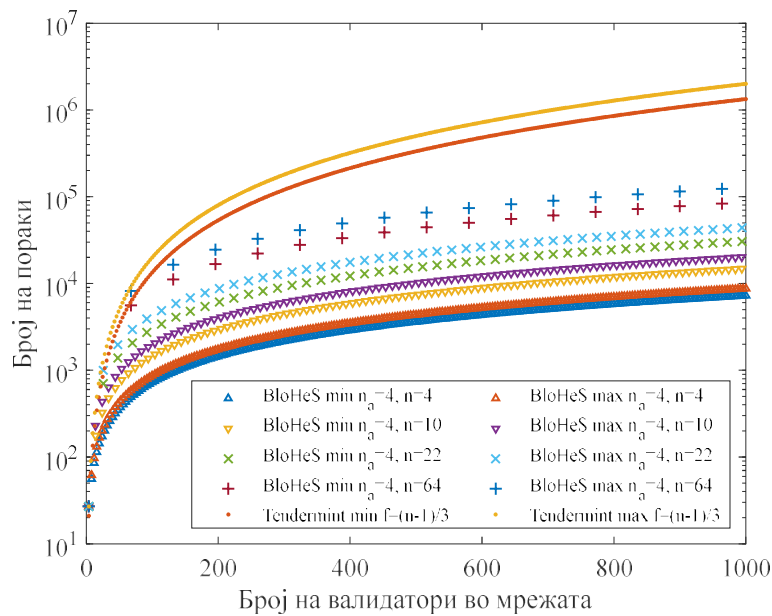
Во симулациското сценарио за BloHeS мрежата, архивскиот кластер се зема дека е еден кластер во кој има 4 валидатори $n_a=1$ и кај него $f=1$ односно $n=3*f+1=4$, притоа претпоставувајќи целосно функционален кластер на валидатори. Распределбата на валидатори во BloHeS мрежата го следи критериумот за униформност (од поглавје 5.2.2). Соодветно, бројот на острови n_i во симулацијата се зголемува со бројот на валидатори во мрежата, притоа формирајќи дискретен број на валидатори во мрежата според:

$$n_i = \frac{V-A_V}{n} = \frac{V-4}{n} \in N \quad (5.22)$$

каде $n=3*f+1$ е број на валидатори во еден остров, V е број на валидатори во мрежата, A_V е број на валидатори во архивскиот кластер и N е множество на природни броеви. Евалуираните сценарија за BloHeS консензус механизмот се определени според

максималниот број на малициозни валидатори што може да се толерираат во островот, при што, за произволно се земени вредностите $f = \{1, 3, 7, 21\}$, и соодветно, за бројот на валидатори во еден остров кој е определен со (5.21), при што се добива $n = \{4, 10, 22, 64\}$.

Резултатот од симулацијата за бројот на пораки, каде се споредуваат Tendermint и BloHeS консензус механизмите е даден на Слика 5.7. Од резултатите се гледа значајно подобрување и особено намалување на бројот на пораки кога се споредуваат мрежите при ист број на валидатори. Бројот на пораки кај Tendermint консензус механизмот покажува поголем раст споредено со растот кај BloHeS консензус механизмот што се истакнува особено за сценаријата со голем број валидатори во мрежата. Најзначајно намалување на бројот на пораки се забележува кај BloHeS консензус механизмот во услови кога $n=4$ валидатори по остров. Намалувањето на бројот на пораки е помалку изразено во сценариото кога бројот на валидатори по остров е $n=64$.



Слика 5.7. Споредба на број на разменети пораки кај Tendermint и BloHeS консензус механизмот

Подобрите перформанси што се постигнуваат кај BloHeS консензус механизмот по однос на бројот на пораки, се резултат на зголемената сегментација на комуникацијата во кластери. Размената на пораки помеѓу островите и архивскиот кластер е неколкукратно помала за разлика од размената на пораките во самите острови.

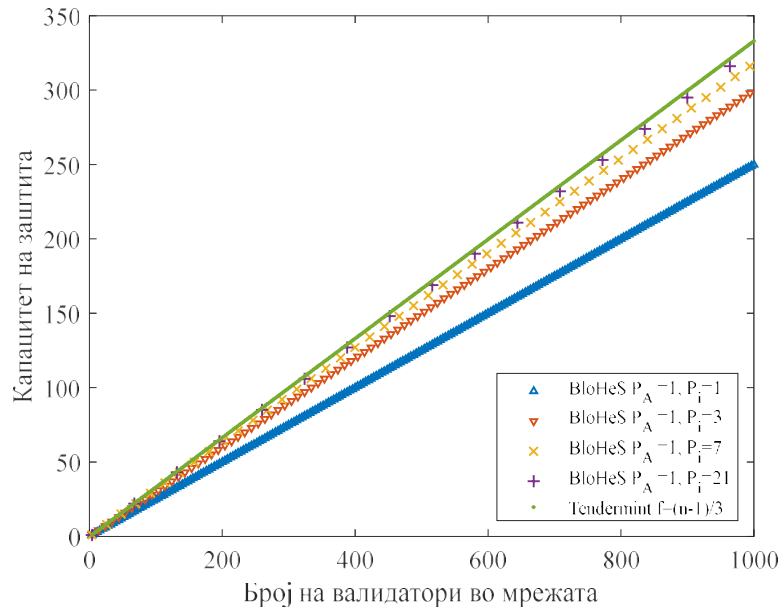
По однос на симулацијата за капацитетот на заштита за Tendermint консензус механизмот дискретното множество на вредности за бројот на валидатори во мрежата се определува со формулата:

$$P_T = f = \frac{n-1}{3} \in N \quad (5.23)$$

каде f е максимален број на малициозни валидатори, n е број на валидатори во мрежата и N е множество на природни броеви.

За симулација на капацитетот на заштита кај BloHeS консензус механизмот се претпоставува дека архивскиот кластер има капацитет на заштита $P_A=1$, островите имаат капацитет на заштита $P_i = \{1, 3, 7, 21\}$, големината на островите соодветно е $n = \{4, 10, 21,$

64}, а дискретното множество на вредности за бројот на острови во мрежата се пресметува со (5.22). На Слика 5.8 се дадени резултатите од постигнатиот *капацитет на заштита* за BloHeS и Tendermint консензус механизмот.

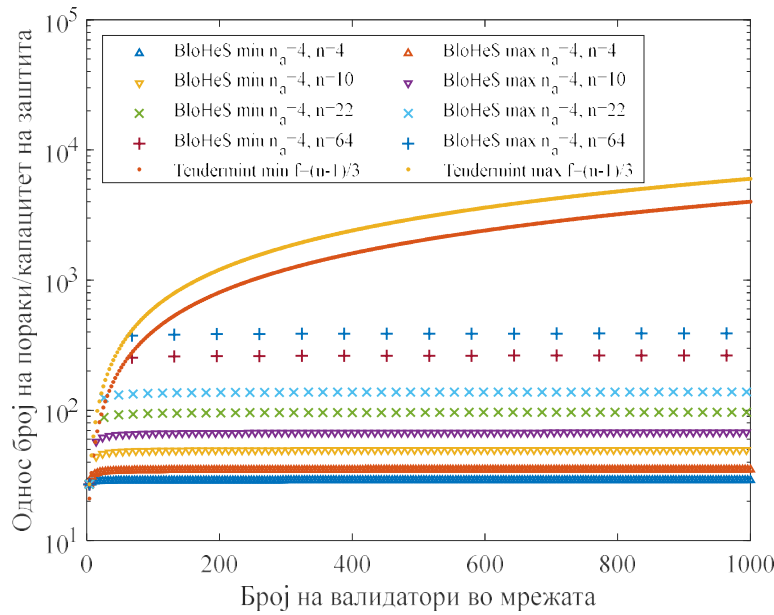


Слика 5.8. Споредба на капацитет на заштита помеѓу Tendermint и BloHeS консензус механизмите

Резултатите покажуваат намален потенцијал за заштита од малициозни валидатори во BloHeS мрежата споредено со Tendermint мрежата. Важно е да се напомене дека капацитетот на заштита значително брзо расте во сценаријата каде бројот на валидатори во рамките на островите се зголемува. Тоа би значело дека валидаторите во BloHeS мрежата треба да се самоорганизираат во поголеми острови со горна граница од 100 валидатори по остров, со цел да се постигне подобар капацитет на заштита, но и намалување на бројот на разменети пораки.

Од Слика 5.8 може да се заклучи дека Tendermint консензус механизмот обезбедува подобра заштита од малициозни валидатори во споредба со BloHeS консензус механизмот, освен за маргинални мали вредности кога капацитетот на заштита кај BloHeS консензус механизмот се доближува асимптотски во услови на големи острови во мрежата. Со цел да се добие претстава дали подобрата заштита која ја нуди Tendermint е доволна за да се занемари значителното намалување на бројот на пораки што BloHeS консензус механизмот го постигнува, се пресметува односот меѓу бројот на пораки и капацитетот за заштита.

На Слика 5.9 се дадени резултати од *односот на бројот на пораки и капацитетот на заштита*, каде е очигледно дека Tendermint консензус механизмот има тенденција на раст на овој однос. Тоа значи дека комплексноста на комуникацијата кај Tendermint консензус механизмот се зголемува побрзо споредено со капацитетот за заштита. Од друга страна константниот однос за бројот на пораки и капацитетот на заштита кај BloHeS консензус механизмот покажува дека нема покачување на комплексноста на комуникацијата споредено со капацитетот на заштита при зголемување на бројот на валидатори во мрежата.



Слика 5.9. Споредба на односот разменети пораки/капацитет на заштита кај Tendermint и BloHeS консензус механизмот

Земајќи ги во предвид резултатите од Слика 5.8 и Слика 5.9, дека за поголеми острови во BloHeS консензус механизмот се постигнува сличен капацитет на заштита како и Tendermint консензус механизмот, односот на бројот на пораки и капацитетот на заштита покажуваат дека BloHeS консензус механизмот постигнува сличен капацитет на заштита со Tendermint консензус механизмот за помалку комплексна процедура на размена на пораки.

5.2.4. Предности и недостатоци на BloHeS консензус механизмот

Главна предност на BloHeS консензус механизмот е намалениот број на пораки потребни за да се постигне консензус. Со додавањето на нова димензија, поточно со воведувањето на повеќенивовска структура на BloHeS консензус механизмот, се намалува бројот на разменети пораки со сите учесници во мрежата за финализирање на трансакциите. Оваа предност се постигнува на сметка на намалениот капацитет на заштита кој асимптотски се доближува на капацитетот на заштита што го постигнува Tendermint консензус механизмот во услови на големи кластери.

Главен недостаток на BloHeS консензус механизмот е зголеменото време кое е потребно за да се финализира еден податочен блок поради потребата да се спроведат два независни циклуси на консензус. Во најдобро сценарио, времето потребно за финализирање на консензусот би било двапати подолго од времето потребно да се финализира податочен блок кај Tendermint консензус механизмот.

Потенцијален проблем би бил кога би постоел малициозен предлагач кој би можел да изврши напад со филтрирање на пораките меѓу островот и архивскиот кластер, но поради промената на предлагачи во секоја рунда, ваквиот напад нема да има далекусежни последици. Во следната рунда на консензус механизмот, проблемот на ваквото филтрирање на пораки би бил надминат.

5.3. Организација на складирањето на податоците во BloHeS системот

Поради размерот на глобалниот здравствен систем, истиот има потреба од паметно решение за складирање на податоците. Моменталниот пристап кој се користи од страна на Blockchain технологиите за складирање на податоците се врши преку целосна синхронизација на содржината на Blockchain базата на податоци во секој кориснички уред во мрежата. Тоа се прави со основна цел да се зацврсти доверливоста на мрежата и да ги заштитат корисниците од лажни трансакции. Ова барање е еден од главните фактори за малата скалабилност на Blockchain технологиите.

Со цел BloHeS системот да има високо ниво на доверливост и доволен степен на редувантност на записите, се предлагаат повеќе начини на складирање на податоците за пациентите. Можните опции се: складирањето на сите податоци поврзани за пациентот да бидат на уреди кои ќе бидат под контрола на пациентот или како енкриптирани податоци да бидат снимени на слободниот простор од дисковите на корисниците кои би сакале да учествуваат во мрежата, за што би добивале одредена награда за отстапување на слободниот простор. Идејата за споделување на слободниот складишен простор и добивање награда за тоа е реализирана од страна на Filecoin [119] што претставува Blockchain базиран простор за складирање на податоци, кој е изграден врз InterPlanetary File System (IPFS) [32]. Дополнителна опција е пациентите да складираат копија од нивните лични податоци на нивен локален компјутер, домашен портен уред или на некој систем во облак. Дополнително како мерка која би овозможила трајност на записите е целокупните податоци кои се генерираат и циркулираат во системот, во енкриптирана форма да се чуваат во складишен простор управуван од владина институција.

Како најпрактично решение, од претходно споменатите можни решенија, е имплементацијата на *домашен портен уред* со чија помош се обезбедува сигурна точка за складирање и управување со податоците. Овие уреди ќе бидат енергетски ефикасни уреди со основна цел да ги чуваат и менаџираат личните податоци. Домашните портни уреди би претставувале складишта за личните податоци, каде пациентите лично би имале брз пристап, а за IoT уредите истите би претставувале собирни точки за генерираните податоци.

5.3.1. Структура на Личен Blockchain поток и организација на базата на податоци за пациентите и заедничката база на податоци

Најважната карактеристика на јавните Blockchain технологии е можноста да ги поврзуваат податочните блокови и да прават Blockchain регистри кои е многу тешко да се променат (промената на регистри не е невозможна, но е многу скап процес). Оваа силна карактеристика на Blockchain технологиите е најголем проблем за нивна имплементација во системи за складирање на лични податоци, поради General Data Protection Regulation (GDPR) регулативата и „правото да се биде заборавен“ (“right to be forgotten”). Секое барање за бришење или промена би повлекло повторно калкулирање на сите хаш вредности од податочниот блок кој треба да се промени до последниот податочен блок кој е генериран. Очигледно Blockchain технологиите кои постојат, не можат да се употребат за градење на решенија кои се во согласност на GDPR прописите, затоа е потребно да се изврши промена на Blockchain технологијата за да се усогласи со GDPR прописите.

Згора на тоа, традиционалните Blockchain технологии одржуваат целосно синхронизиран заеднички регистар кој има фактор на репликација еднаков на бројот на

учесници во мрежата. Ваквиот пристап ја намалува скалабилноста на мрежата по однос на просторот за складирање и го прави системот непрактичен за глобална употреба.

За да се подобри скалабилноста по однос на складишниот простор, BloHeS системот користи целосно редефиниран пристап кон складирањето на податоците и управувањето со пристапот кон податоци преку воведување на Личен Blockchain поток (Personal Blockchain Stream – PBS). Со дефинирањето на посебна база на лични здравствени податоци му се дава можност на пациентот да управува со личните податоци, да ги преместува по барање и потреба на здравствените работници, да ги споделува со компании и други институции. Ова е основната предност за дизајнот на Личниот Blockchain поток како индивидуална Blockchain структура.

Личниот Blockchain поток претставува лична база на податоци која е иницирана од страна на пациентот, но во неа може да запишуваат само здравствени работници со претходно одобрување од страна на пациентот и IoT уреди преку претходно ставање во листата на дозволени уреди за интеракција. Практично PBS претставува лична динамична база на податоци која има Blockchain структура за да ги складира медицинските записи на пациентите. Копија од записите кои се наоѓаат во PBS треба да има и кај здравствениот работник и во владиниот агент, а опционално на локален диск или во складиште во облак. Потребно е во системот да има најмалку три копии од записите, притоа задолжително по една од нив да биде целосно синхронизирана кај пациентот, кај здравствениот работник и кај владиниот агент.

Еден запис во PBS базата на податоци се состои од: *заглавие, содржина на здравствен запис* и *хаш вредност* од финализираниот блок во федералната база на податоци каде е поставена адресата за записот. Заглавието ги содржи основните полиња за хаш вредноста од претходниот блок на кој се надоврзува тековниот блок, адресата на паричникот на пациентот, висината на блокот што претставува и реден број на записот, верзијата на стандардот кој се користи за здравствениот запис и хаш вредност на тековниот блок во чија калкулација не е вклучена хаш вредноста од финализираниот блок во федералната база на податоци. Здравствениот запис се формира врз база на еден од постоечките стандарди за формирање на здравствен запис, а притоа вклучува и адреса на паричникот од здравствениот работник кој го создава записот. Структурата на PBS е дадена на Слика 5.10.

Ваквиот пристап на складирање на податоци има двојна корист. Прв бенефит од ваквата структура на записите е можноста да се употребува GDPR регулативата во рамките на BloHeS системот. Со новиот пристап на организација на складирањето на податоци ќе се овозможи пациентите да се заштитат од откривање на личните податоци на трети лица, а воедно може да се имплементираат механизми за целосна контрола на правата за користење на личните податоци од страна на трети лица. По дефиниција, PBS претставува независна инстанција на податоците за пациентите на сите места каде се складира, па затоа истата може да биде избришана или променета на барање на пациентот. Менувањето или бришењето на личните податоци за пациентот од било кое место каде се складираат, не подразбира интервенција на глобалната Blockchain структура и рекакулација на хаш вредностите за сите податочни блокови од целата мрежа, туку управување со PBS на пациентот како контејнер од податоци кој се наоѓа кај агентите, а за кои пациентот дал дозвола да се користат. На овој начин пациентите би имале подобра контрола на бројот на копии од нивните податоци и на тоа кој поседува копија од тие податоци.



Слика 5.10. Структура на PBS

Втор бенефит од користењето на PBS би бил високиот фактор на скалабилност кој се постигнува заради намалената потреба од репликација на податоците во системот. Поради потребата личните податоци да се складираат во енкриптирана форма, истите нема потреба да бидат складирани во складишниот простор на трети лица кои не се вклучени во процесот на верификација на податоците. На овој начин се исклучуваат трети лица да учествуваат во задолжителното складирање на податоци. Со користењето на PBS, личните податоци би им биле целосно достапни на пациентот и здравствениот работник, а на барање истите би биле целосно отворени и за владините институции. Опционално, пациентите би можеле да складираат копија во енкриптирана форма на други места за кои пациентите би имале доверба дека никој не би се обидел да ги декриптира или злоупотреби на било кој начин.

За да може да се изврши оптимизација на базата на податоци, како и оптимизација на голем дел од процесите во системот и подготвување на системот за имплементација на алгоритми со Вештачка интелигенција, потребно е да се прифати стандардизиран начин за креирање на записи во PBS на пациентот. Моментално постојат повеќе стандарди за структурата на електронските здравствени записи со примарна цел да се постигне интероперабилност помеѓу системите.

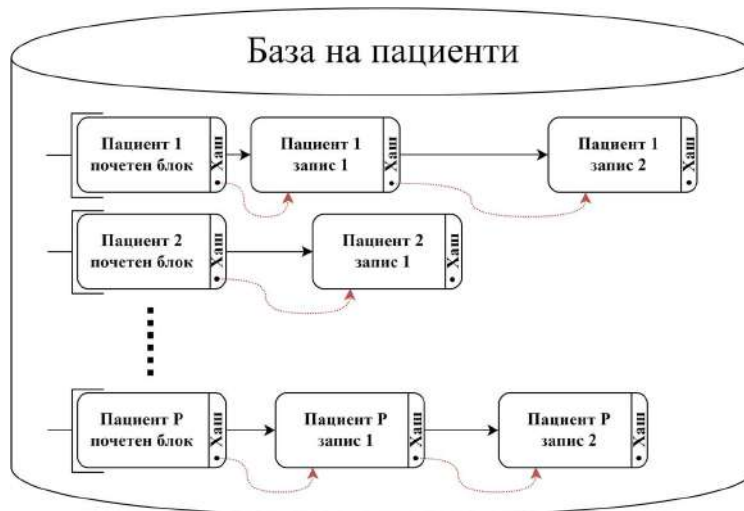
За да постигне висок степен на интероперабилност, BloHeS системот треба да користи стандардизирана форма на електронските записи во Личниот Blockchain поток. За таа цел може да се искористи еден од постоечките стандарди за здравствени електронски записи. Во [120] претставена е споредба на повеќе стандарди и протоколи за електронски здравствени записи (Electronic Healthcare Record – EHR). Генерално со стандардите и протоколите за EHR се дефинира структурата на содржината во записите и сервисите за пристап до записите. BloHeS архитектурата се фокусира главно на дефинирањето на структурата на записите, додека сервисите за пристап ќе бидат управувани преку Blockchain функционалностите. Во [120] се истакнати три стандарди како интернационално прифатени и најкомплетни: EHRcom (Electronic Healthcare Record Communication) [121], HL7 CDA (Health Level 7 Clinical Document Architecture) [122] и DICOM SR (Digital Imaging and Communications in Medicine Structured Reporting) [123] и еден на национално ниво, MML (Medical Markup Language) [124], кој е создаден за Јапонскиот здравствен систем.

За добар стандард кој дефинира структура на содржината важно е да обезбеди голем број на шаблони и архетипови, но и да биде прилагодлив на идните системи преку

имплементирање на опис на содржините и да има семантика разбирлива за машините. Ефективен семантички исказ за здравствените записи може да се генерира со користење на речник на поими и состојби, налик на стандардите SNOMED CT (Systematized Nomenclature of Medicine – Clinical Terms) [125] и GALEN (Generalized Architecture for Languages, Encyclopedias and Nomenclature) [126]. Овие решенија овозможуваат семантичка интероперабилност помеѓу стандардите. Семантичката интероперабилност е важна карактеристика која ја подобрува ефикасноста на алгоритмите за машинско учење, кои пак се способни да предвидат индивидуални здравствени состојби, здравствена состојба на популацијата и епидемии. Оваа карактеристика е предуслов за успешно имплементирање на агентите со Вештачка интелигенција.

Покрај PBS како лична база на податоци за пациентот, се дефинираат и два типа на бази на податоци во BloHeS системот со цел подобро да се рефлектира логиката сегментација на системот меѓу пациентите, здравствените работници и владините институции. Основна поделба на базите на податоци се: *база на пациенти* и *заедничка база на податоци*. Заедничката база на податоци е поделена на *островска база на податоци* и *федерална база на податоци*.

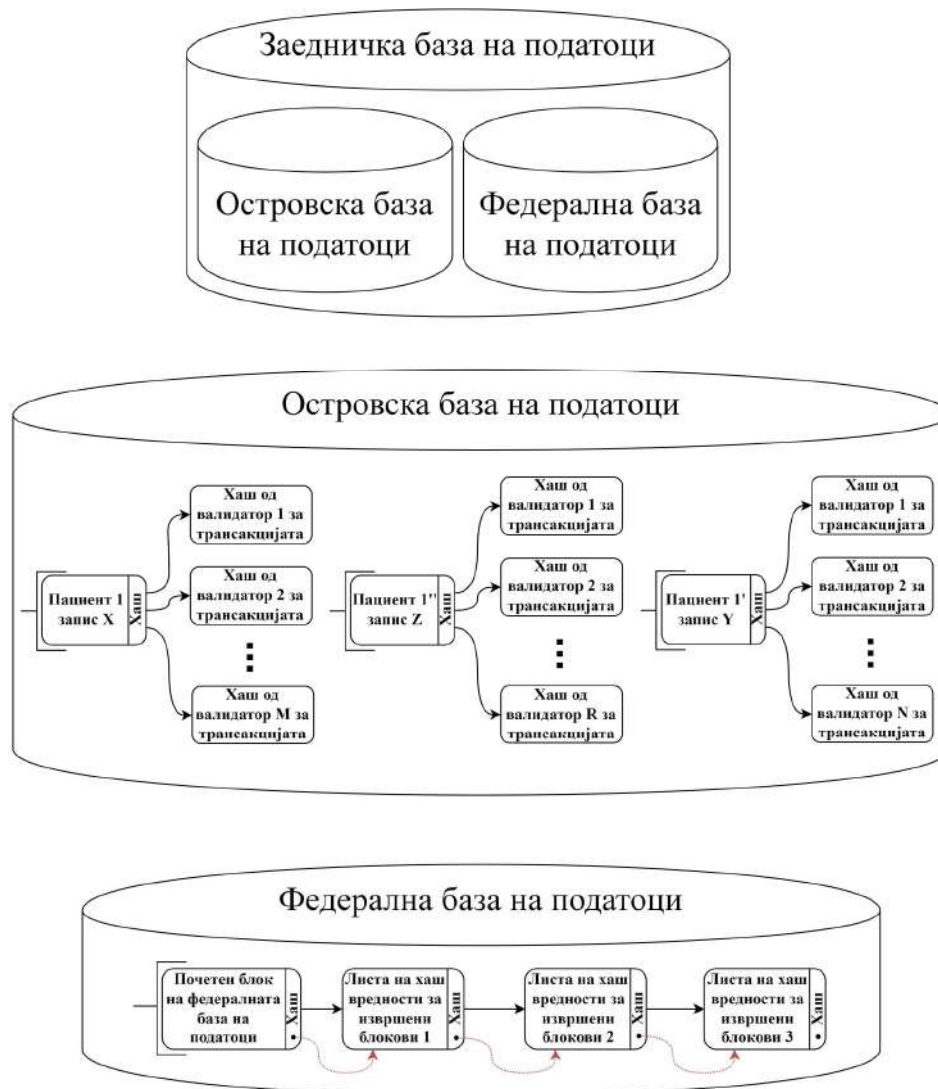
Базата на пациенти (Слика 5.11) има структура за чување на електронски досиеја за пациентите, во која секое досие претставува посебна помала база на податоци која може независно да се прикачи во системот. Овие помали бази на податоци практично се Личните Blockchain Потоци на пациентите кои се под здравствен надзор на здравствениот работник. Записите на Личните Blockchain Потоци во базата на пациенти се само од пациентите кои го избрале здравствениот работник за семеен доктор или пак го посетиле здравствениот работник и му овозможиле пристап до личните здравствени записи. Секој пациент управува со нивниот PBS и дозволува пристап или споделува податоци со здравствениот работник. Во зависност од преференциите на пациентот, PBS записите кои се наоѓаат во базата на пациенти кај здравствениот работник може да бидат во неенкриптирана форма (со давање на постојана дозвола за читање на податоците) или во енкриптирана форма (со давање на привремена дозвола или еднакратна дозвола за читање на податоците).



Слика 5.11. База на пациенти

Островската база на податоци има временска природа и нема Blockchain структура, што е прикажано на Слика 5.12. Островската база на податоци е формирана од

транзакции кои се генерирани во рамките на островот и чекаат да бидат валидирани од другите валидатори во островот. Главна цел на постоењето на оваа временна база на податоци е да се има подобар преглед на процесот на валидирање на транзакциите во островот. Динамичката природа на островската база на податоци е резултат на времената структура на самите острови која се менува во зависност од условите во мрежата, како и во зависност од динамиката на пополнувањето на истата со нови транзакции и валидации за транзакциите што се креирани во рамките на островот.



Слика 5.12. Заядничка база на податоци, островска база на податоци и федерална база на податоци

Федералната база на податоци за разлика од островската база на податоци има Blockchain структура и претставува постојана база на податоци која ги чува финализираните транзакции во системот, поточно ги чува адресите на валидираните транзакции во федералната мрежа. Записите од оваа база на податоци се синхронизираат помеѓу сите здравствени работници во федералната мрежа. Доколку повеќе федерални бази на податоци треба да комуницираат меѓу себе во рамките на една федеративна

мрежа, кон записите се додава идентификатор на државата односно идентификатор на федералната мрежа.

Процедурата за внесување на запис започнува од здравствениот работник кој за да генерира запис потребно е да добие одобрение од пациентот кој тековно се наоѓа во ординацијата. Доколку на здравствениот работник не му е даден постојан пристап до личните податоци, истиот бара дозвола за пристап до Личниот Blockchain поток на пациентот. Записот за пациентот кој се генерира треба да содржи хаш вредност од претходниот запис, временски податоци за посетата, дијагноза, резултати од спроведени испитувања, препишана терапија и хаш вредност од тековниот податочен блок. Создадениот запис се верифицира од страна на агентот на здравствениот работник и се испраќа на верификација до другите агенти на здравствените работници кои учествуваат во островот. Во принцип, процесот на верификација од страна на другите учесници во островот се содржи од проверка на структурата на записот и коректноста на хаш вредностите, но не и коректноста на содржината бидејќи истата е енкриптирана. Откако здравствениот запис ќе биде верифициран, истиот е вклучен во следниот податочен блок кој ќе биде генериран во рамките на островот. Новиот податочен блок ќе биде даден за валидирање во рамките на консензус механизмот кој се спроведува на ниво на остров.

После формирањето на новиот податочен блок и гласањето за коректност на податочниот блок на ниво на остров, извршена е потврда за коректноста на формата на записите во податочниот блок. Потврдениот податочен блок се испраќа до владините агенти за да биде вклучен во следниот податочен блок кој ќе биде запишан во федералната база на податоци. Владиниот агент формира подредена листа од адреси на податочни блокови, за која во рамките на архивскиот консензус механизам ги финализира записите и соодветниот заклучок го испраќа до агентите на здравствените работници за да го вклучат тој блок во федералната база на податоци. Владиниот агент препорачливо е да биде изграден од независни машини кои индивидуално би формирале финални записи, а потоа во процес на донесување консензус би потврдиле дека се е во ред со записите.

Во мрежата опционално може да постојат независни учесници кои ќе извршуваат надзор на работата на владините агенти, со цел да се овозможи повратна спрега за контрола на коректноста на владиниот агент. Било каква ситуација во која ќе се детектира неправилност, би го запреле процесот на валидација во владиниот агент.

5.3.2. *Анализа на скалабилноста на складирањето податоци*

Со новата организација на Blockchain записите се очекува значително подобрување во ефикасноста на складирањето податоци во системот споредено со организацијата на складирање податоци кај класичниот Blockchain пристап.

Стандардниот начин на градење на заедничка дистрибуирана база на податоци која се користи од страна на класичните Blockchain решенија (како што се Bitcoin и Ethereum) е да се одржува целосна содржина од сите трансакции кои се генерираат во системот, кај сите корисници на системот. Во сценарио на јавен здравствен систем тоа би значело дека секој здравствен запис треба да биде прекопиран во базата на податоци кај секој корисник. Очигледно ваквиот пристап не е практичен за мрежи каде има голем број на корисници. Доколку ваквиот пристап на запишување на здравствените податоци би се користел во јавен здравствен систем, тогаш вкупниот складишен простор кој би бил зафатен кај сите учесници во системот, во текот на еден ден се пресметува со:

$$S_t^c = F \times v \times H_p \times (P_a + H_p + G) \quad (5.24)$$

каде S_t^c е вкупен складишен простор што ќе се зафати за еден ден кај класичните Blockchain системи, F е просечна големина на запис, v е просечен број на посети во еден ден кај здравствениот работник, H_p е број на здравствени работници во целиот систем, P_a е број на пациенти во системот, G е број на владини агенти.

Доколку се земат во предвид трите основни типови на агенти, како учесници во системот, естимацијата на искористеното складиште во текот на еден ден, кај секој од нив поединечно се пресметува како:

$$S_p^c = S_{hp}^c = S_g^c = F \times v \times H_p \quad (5.25)$$

каде S_p^c е складиштето кое се искористува во текот на еден ден кај пациентот кај класичните Blockchain системи, S_{hp}^c е складиштето кое се искористува во текот на еден ден кај здравствениот работник кај класичните Blockchain системи, S_g^c е складиштето кое се искористува во текот на еден ден кај владиниот агент кај класичните Blockchain системи. Другите променливи се дефинирани со (5.24).

Предложениот начин на организирање на складирањето на податоците кај BloHeS системот предвидува намалување на бројот на копии во системот, со цел да го намали и вкупниот простор кој се користи за складирање на податоци. Меѓутоа новиот начин потребно е да обезбеди робусност на системот како и достапност и постојаност на записите. Организацијата на базите на податоци кај BloHeS системот овозможува секој пациент да се грижи за своите лични податоци. Тоа би значело дека зголемувањето на податоците во пациентската база на податоци да биде само со лични информации и би зависело само од здравствената состојба на пациентот и неговата честота на посети кај здравствениот работник. Главниот товар на складирањето би го имале агентите на здравствените работници и владините агенти кои би требало да управуваат со поголем број на пациенти.

Според насоките на BloHeS архитектурата, во системот би се чувале најмалку 3 копии од информациите за пациентот. Факторот на репликација од 3 копии е вообичаено прифатен како доволен за да се обезбеди доверливост на системот и достапност на податоците кај традиционалните дистрибуирани складишни системи. Според дефиницијата, вкупниот складишен простор кој би бил зафатен кај сите учесници во системот во текот на еден ден, би се пресметал како:

$$S_t^B = F \times v \times H_p \times r + CDS \times F \times v \times H_p \times (H_p + G) \quad (5.26)$$

каде S_t^B е вкупен складишен простор кој ќе се зафати кај BloHeS системот во текот на еден ден, F е просечна големина на запис, v е просечен број на посети во еден ден кај здравствениот работник, H_p е број на здравствени работници во целиот систем, r е број на копии за пациент, Common Database Storage (CDS) е коефициент со кој се покажува соодносот на големината на записот во заедничката база на податоци и големината на истиот запис во PBS, G е број на владини агенти.

Зафатениот складишен простор во текот на еден ден за секој агент посебно може да се пресмета според (5.27) за агентот на пациентот и според (5.28) за агентот на здравствениот работник:

$$S_p^B = F \times v' / 365 \quad (5.27)$$

$$S_{hp}^B = F \times v + CDS \times F \times v \times H_p \quad (5.28)$$

каде S_p^B е складиштето кое се искористува во текот на еден ден кај пациентот во BloHeS системот, S_{hp}^B е складиштето кое се искористува во текот на еден ден кај здравствениот работник во BloHeS системот, v' е просечен број на посети кај здравствен работник во текот на една година од страна на еден пациент, другите променливи се дефинирани во (5.26).

Очигледно е дека најголемиот товар за складирање на податоци ќе биде врз владиниот агент, што може да се пресмета како:

$$S_g^B = F \times v \times H_p + CDS \times F \times v \times H_p \quad (5.29)$$

каде S_g^B е складиштето кое се искористува во текот на еден ден кај владиниот агент во BloHeS системот, а другите применливи се дефинирани со (5.26).

Коефициентот Common Database Storage (CDS) има минимален ефект на вредностите кои се добиваат за вкупното искористено складиште бидејќи се однесува на зафатнината на записите во заедничката база на податоци. Со оглед на тоа што записите во заедничката база на податоци, поточно оние од федералната база на податоци кои имаат и постојан карактер, се само упатувачки адреси до вистинските места каде се складираат записите, практично би имале големина од 128B или 256B по запис, што споредено со големината на вистинскиот запис во базата на податоци, како на пример, текстуални записи со големина од 1KB или слики и видео записи од неколку мегабајти, може да претпоставиме дека зафатнината на заедничката база на податоци би била не повеќе од 1% од реалната големина на записот. Со ваквата претпоставка CDS факторот би бил 0.01.

За да се споредат перформансите на BloHeS и класичниот Blockchain пристап на запишување на записите, формулите (5.24) – (5.29) се имплементирани во MATLAB при што се анализираат две сценарија каде се претпоставува дека во мрежата има 10^6 и 10^9 пациенти.

Табела 5.1 ги прикажува опсезите на параметрите како што се големина на панел, просечен број на посети од страна на пациентот, број на посети кај здравствениот работник во текот на еден ден и број на работни денови во годината за секој здравствен работник. При пресметката на вкупната и поединечните зафатнини на складишен простор, се користат параметри чии вредности се преземени од [114], [127] и [128], со цел да се пресметаат пореалистични вредности за зафатнината на складишниот простор. За да се добие чувство за влијанието кое го имаат различните начини на организација на складишниот простор, истите се анализираат во сценарија каде популацијата која би учествувала во федералната мрежа би изнесувала 10^6 и 10^9 пациенти. Оптималниот број на здравствени работници за една федерална мрежа се определува според релациите дадени во [129] што претставува однос на бројот на пациенти во федералната мрежа и големината на панелот.

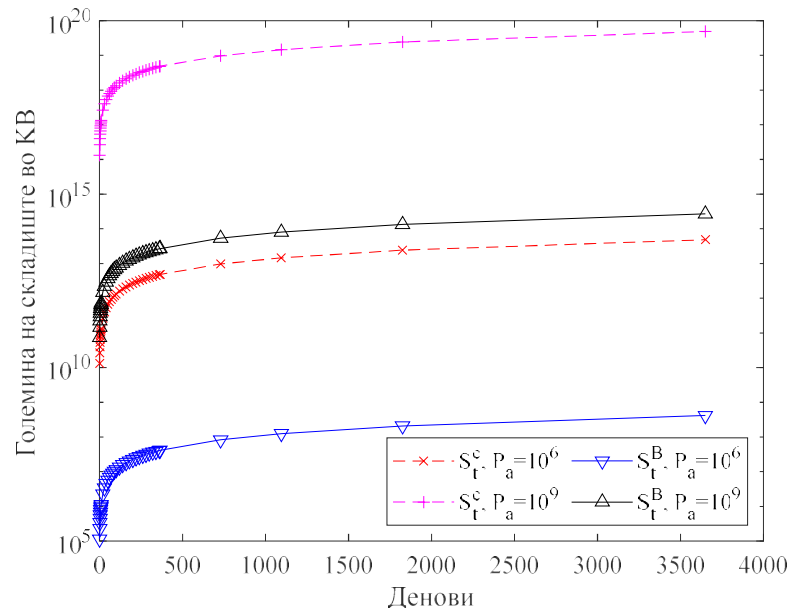
Табела 5.1. Симулациски параметри

	Опсег на параметри	Симулациски вредности
Големина на панел за здравствениот работник (број на пациенти)	1500-2500	1806
Просечен број на посети за пациентите во текот на една година	3	3.19
Број на посети кај здравствениот работник во текот на еден ден	10-30	24
Број на работни денови за здравствениот работник во текот на една година	240	240

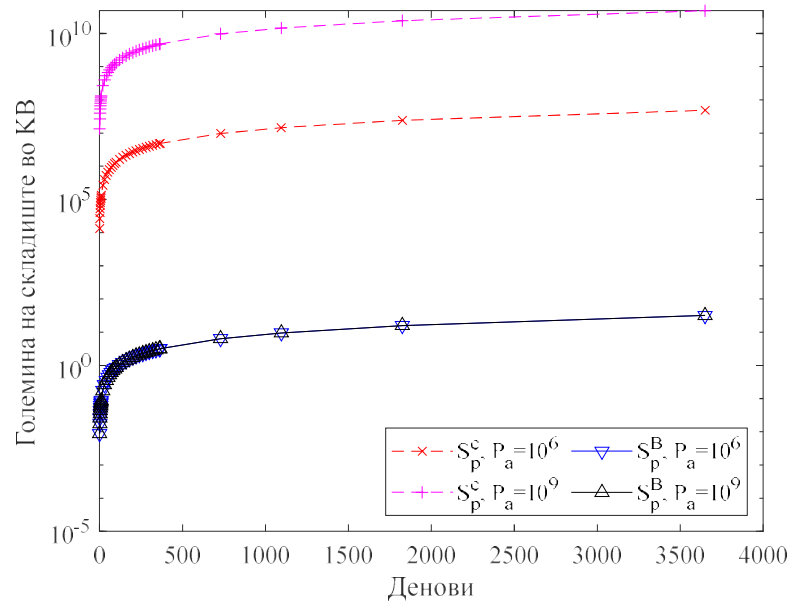
Владините институции ќе бидат претставени со најмалку еден агент кој би ги спроведувал законските норми во системот и би ги финализираше трансакциите. Во случај на повеќе агенти потребно е да се имплементира консензус механизам за координација помеѓу индивидуалните агенти. Основни задачи на владиниот агент се да биде доверливо место за складирање на личните податоци (како и да го поддржи основното барање за управување на 3 реплики во системот) и да дејствува како медијатор во услови на проблеми кои би настанале во системот. Бројот на владини агенти може да се зголеми во системот во зависност од имплементациското сценарио, но тоа значително би ги зголемило трошоците за одржување на таквиот систем. Коефициентот CDS е 0.01 како што е претходно објаснето. По однос на големината на записите, се зема дека записите се со 1KB, што во реален систем тоа би претставувало извештај во кој се внесени дијагнозата и терапијата за пациентот заедно со останатите потребни информации.

На следните слики се гледа споредбата на резултатите добиени за кумулативната зафатнина на складиштето за период од 10 години, за класичните Blockchain системи и за BloHeS системот, при што во системот има 10^6 и 10^9 пациенти. На Слика 5.13 е дадена споредбата на вкупниот складишен простор кој ќе се зафати кај двата типови системи во период од 10 години. Подобрувањето кое го носи BloHeS пристапот на складирање на податоците е очигледно бидејќи разликата на вкупно зафатениот простор за складирање е голема. Исто така може да се забележи дека големината на популацијата има голема улога во степенот на зголемување на зафатнината на складишниот простор што кај класичниот Blockchain пристап би имал големо влијание на долг рок.

На Слика 5.14 е дадена споредбата на кумулативната зафатнина на податочното складиште за период од 10 години во рамките на агентот на пациентот. Очигледно е дека класичниот пристап врши притисок врз складиштето на пациентите со податоци кои се од други пациенти, без притоа да има посети кај здравствениот работник од страна на пациентот. Кај BloHeS пристапот може да се забележи дека потребни се помали складишни простори, но и дека зголемувањето на складиштето не е афектирано од останатите записи во мрежата.

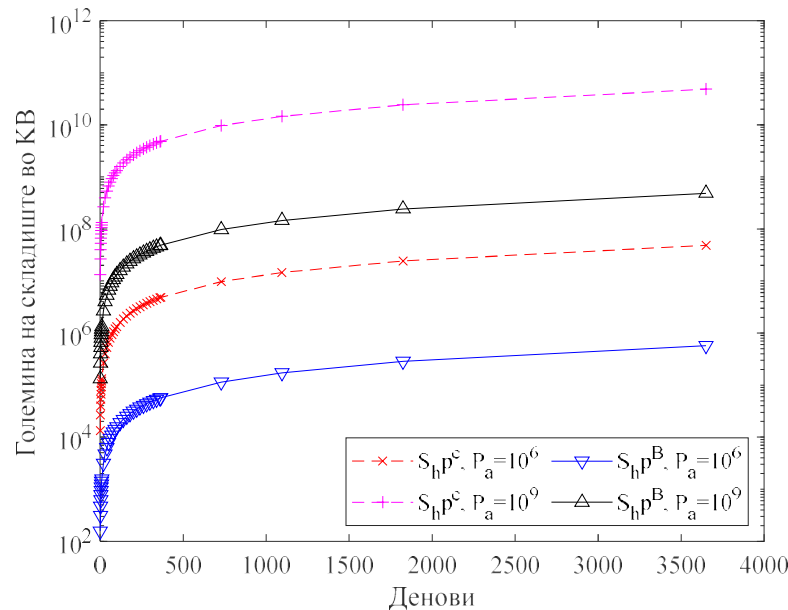


Слика 5.13. Вкупен зафатен складишен простор за цела здравствена мрежа



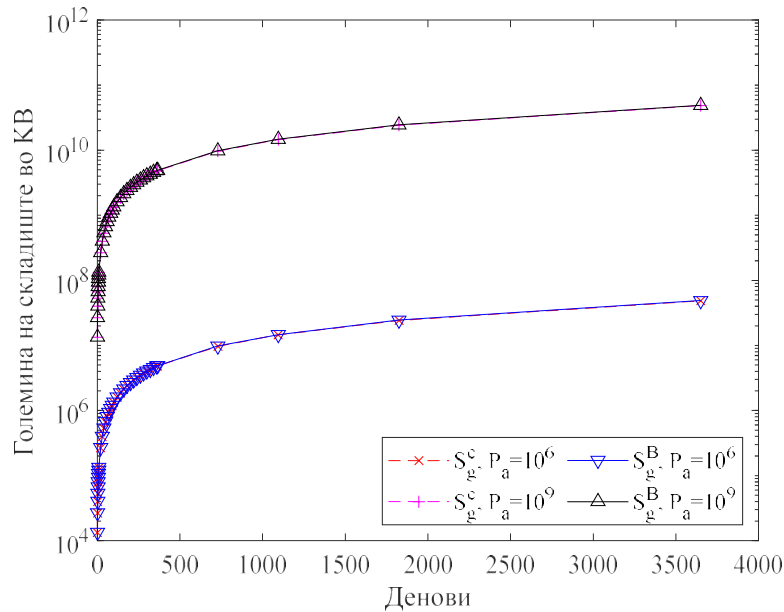
Слика 5.14. Вкупен зафатен складишен простор кај пациентот

На Слика 5.15 е дадена споредбата на кумулативната зафатнина на податочното складиште за период од 10 години во рамките на агентот на здравствениот работник, при што се забележува предноста која ја донесува BloHeS организацијата на податоци споредено со класичната Blockchain организација. Сепак може да се забележи и дека поради потребата агентот на здравствениот работник да ги чува записите од своите пациенти и да ја складира заедничката база на податоци, тоа би било значаен товар на складиштето на агентот од здравствениот работник во ситуација кога има поголема популација во мрежата.



Слика 5.15. Вкупен зафатен складишен простор кај здравствениот работник

Спротивно на прикажаниот успех што се постигнува со имплементација на BloHeS пристапот на складирање податоци, на Слика 5.16 може да се забележи дека истиот не донесува подобрување на заштедата на складишен простор кај владиниот агент. Тоа е очекувано со оглед на начинот на организирање на записите во BloHeS системот.



Слика 5.16. Вкупен зафатен складишен простор кај владиниот агент

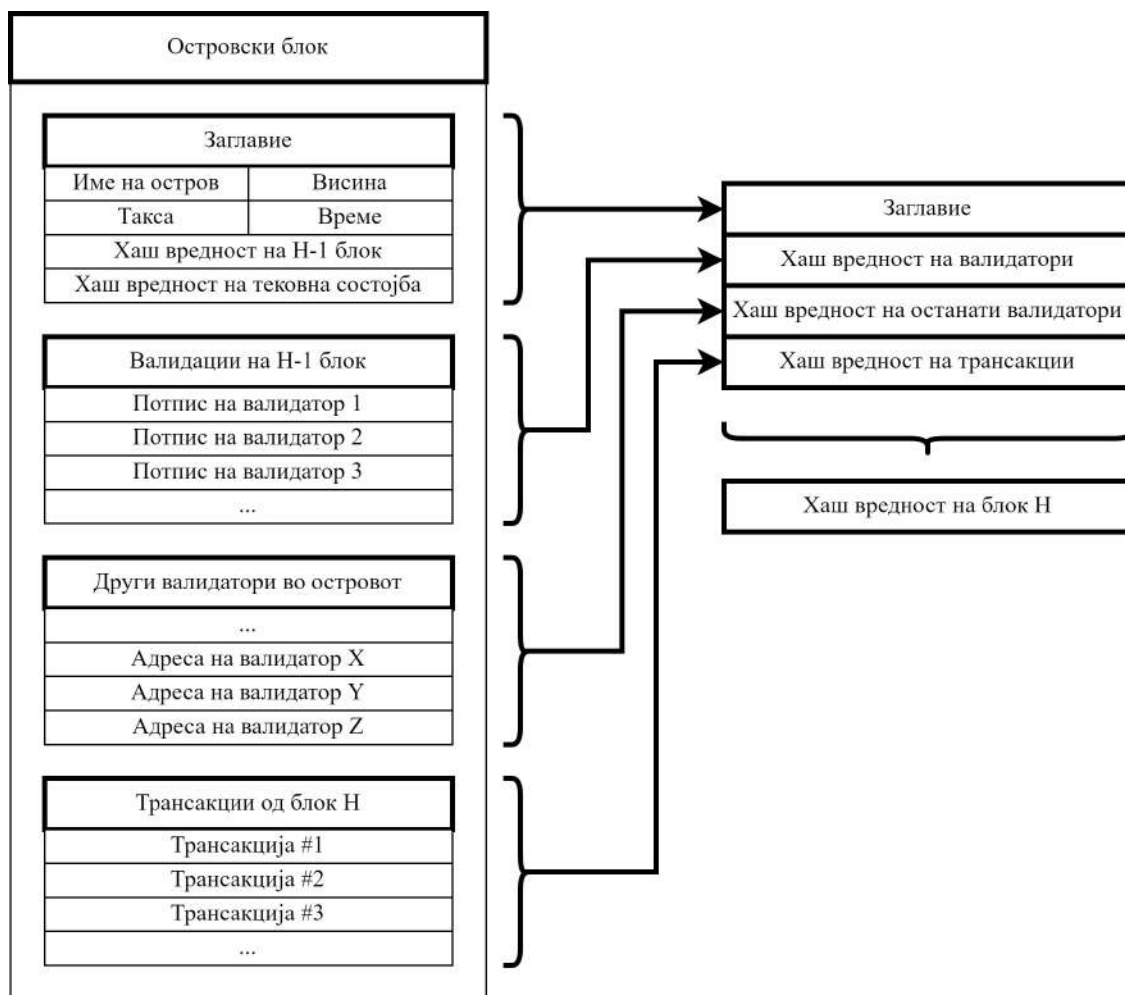
За да се добие подобра претстава за степенот на подобрување на складирање на податоците, во Табела 5.2 се дадени бројните вредности за кумулативниот складишен простор за различна големина на популација (од 10^6 и 10^9 пациенти) кај BloHeS и кај класичниот Blockchain пристап на складирање на податоци. Очигледно е дека со BloHeS начинот на складирање на податоците има значајно намалување на потребниот складишен простор кај пациентите и кај здравствените работници, споредено со класичниот Blockchain пристап. Кај агентите на здравствените работници се намалува потребниот складишен простор, но сеуште истиот е афектиран од големината на популацијата. Од Табела 5.2 се гледа дека BloHeS пристапот на складирање на податоци кај владиниот агент носи незначително зголемување на потребниот складишен простор споредено со класичниот Blockchain пристап на складирање на податоците во системот.

Табела 5.2. Споредба на големината на Blockchain базата на податоци за период од 1 и 10 години за мрежа од 10^6 и 10^9 пациенти во класична и BloHeS архитектура

	Популација 10^6						Популација 10^9					
	Период од 1 година			Период од 10 години			Период од 1 година			Период од 10 години		
	Класична	BloHeS		Класична	BloHeS		Класична	BloHeS		Класична	BloHeS	
Blockchain архитектура												
Вкупно складиште (Килобајти)	$4.85 \cdot 10^{12}$	$4.15 \cdot 10^7$		$4.85 \cdot 10^{13}$	$4.15 \cdot 10^8$		$4.85 \cdot 10^{18}$	$2.69 \cdot 10^{13}$		$4.85 \cdot 10^{19}$	$2.69 \cdot 10^{14}$	
Складиште на пациентот (Килобајти)	$4.85 \cdot 10^6$	3.19		$4.85 \cdot 10^7$	31.9		$4.85 \cdot 10^9$	3.19		$4.85 \cdot 10^{10}$	31.9	
Складиште на здравствениот работник (Килобајти)	$4.85 \cdot 10^6$	$5.73 \cdot 10^4$		$4.85 \cdot 10^7$	$5.73 \cdot 10^5$		$4.85 \cdot 10^9$	$4.85 \cdot 10^7$		$4.85 \cdot 10^{10}$	$4.85 \cdot 10^8$	
Владино складиште (Килобајти)	$4.85 \cdot 10^6$	$4.90 \cdot 10^6$		$4.85 \cdot 10^7$	$4.90 \cdot 10^7$		$4.85 \cdot 10^9$	$4.90 \cdot 10^9$		$4.85 \cdot 10^{10}$	$4.90 \cdot 10^{10}$	

5.4. Податочна блок структура

Блок структурата од трансакциите во рамките на островскиот консензус механизам е изградена врз основната Tendermint блок структура, но направена е надградба на таа блок структура со цел да се адаптира на BloHeS архитектурата. Блок структурата на Tendermint протоколот може да се најде во [7], додека блок структурата на островскиот консензус механизам е дадена на Слика 5.17.



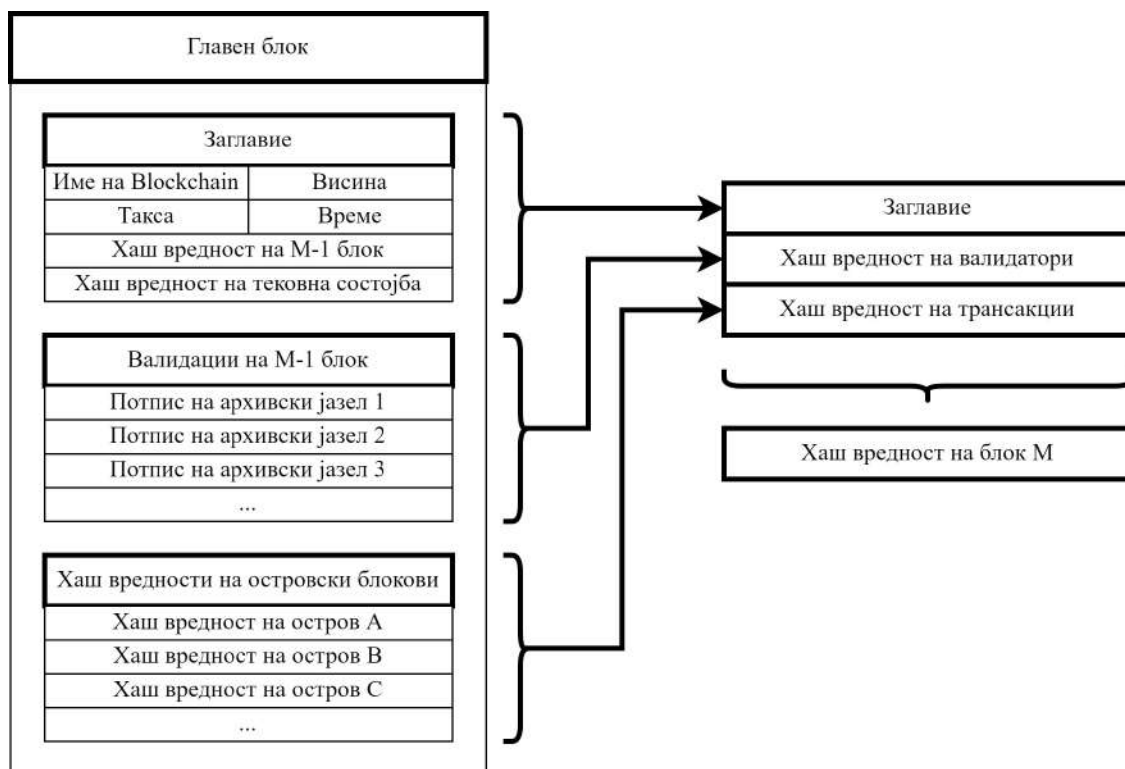
Слика 5.17. Блок структура на островскиот консензус механизам

Секој остров во BloHeS мрежата има уникатен идентификатор кој се генерира како случаен број од страна на првиот предлагач во островот. Островскиот идентификатор практично претставува име на островот или Blockchain идентификатор кој ќе се користи во комуникацијата со архивскиот кластер за да се прави дистинкција на трансакциите во процесот на консолидација на блоковите во финалната трансакција. И тука исто како и кај Tendermint протоколот, се дефинира висина на блокот, со цел да се определи блок секвенцата во процесот на финализирање на трансакциите. Овој параметар за висина на блокот има само интерна употреба во рамките на островот и не е корелирано со висината на главната Blockchain линија. Како и кај Tendermint и тука се користи полето за хаш вредноста на тековната состојба, кое се добива од полињата на тековната состојба за валидаторите во островот, сметките на истите, дополнителните информации за валидаторите и регистрираните имиња за валидаторите. Покрај потписите од страна на валидаторите кои го поддржуваат блокот, во рамките на податочната блок структура, потребно е да се додадат и адресите на останатите валидатори кои се дел од островот но не го потпишале податочниот блок. Со ова поле се овозможува зајакнување на безбедноста на мрежата и избегнување на нападот за двојно гласање како и партиципирање на валидаторите во повеќе острови.

Архивскиот кластер ја контролира главната Blockchain линија, односно главната Blockchain база на податоци што претставува федералната база на податоци каде се складираат финализираните блокови. Записите во федералната база на податоци се сублимација на сите извршни блокови кои се примени од островските предлагачи, подредени по време на генерирање на трансакцијата. Содржината на блок структурата од федералната база на податоци се пополнува со адреси на валидирани трансакции. На тој начин наместо фактичката содржина на трансакцијата, се запишува местото каде истата може да се најде во случај доколку треба да се пронајде одредена информација.

За да се зголеми безбедноста и заштитата на мрежата од малициозни двојни гласања од страна на еден валидатор, архивските валидатори потребно е да ги проверат гласовите кои се испратени во рамките на извршните блокови од страна на островите како и да проверат дали еден валидатор е пријавен како учесник во два острови.

Извршните блокови на архивскиот кластер се додаваат во федералната база на податоци и се испраќаат до сите предлагачи во островите, а потоа тие ги препраќаат до валидаторите во рамките на островите во кои припаѓаат. Во услови кога предлагачот на остров не одговара на примената порака од архивскиот кластер, блокот се испраќа до предлагачот од претходната рунда. На Слика 5.18 е дадена блок структурата на архивскиот консензус механизам.



Слика 5.18. Блок структура на архивскиот консензус механизам

5.5. Протоколи за управување со островите

Еден од главните предмети на изучување во Теоријата на графови и Науката за мрежи [130] е фундаменталниот пристап за градење на кластери и оптимизирање на нивните перформанси. Многу поважно е тоа што теоретските и математички дефиниции што се дадени во рамките на овие две области се користат во пракса за да се решаваат

реални проблеми. Друга истражувачка област каде кластерирањето има важна улога се безжичните сензорски мрежи, односно мобилните ад-хок мрежи, каде значаен предизвик е да се кластерираат подвижни сензори и во исто време да се обезбедат доверливи сервиси [131], [132], [133], [134]. Оптимално кластерирање на сензорите може да се обезбеди преку централизирана анализа на распределбата на сензорите и капацитетот на истите или преку дистрибуирана анализа каде индивидуалните сензори одлучуваат самостојно во кој кластер ќе учествуваат. Процесот на оптимизација на кластерите се спроведува со основна цел да се минимизираат или максимизираат одредени параметри притоа користејќи едноставни процедури или пак комплексни процедури кои може да вклучуваат и Вештачка интелигенција.

Земајќи во предвид дека во некои системи со помош на кластерирањето се постигнуваат подобри резултати, со воведување на механизми за кластерирање во Blockchain околина се очекува да се подобрат перформансите на Blockchain базирани системи. За таа цел во рамките на BloHeS архитектурата дизајнирани се протоколи за *само-организирање на валидаторите* во кластери, односно протоколите за управување со острови во BloHeS системот [135]. За градење на функционална BloHeS мрежа потребно е валидаторите да бидат способни да откријат соработници во мрежата. За таа цел протоколите за управување со острови ја користат процедурата за откривање на соработници (peer discovery) во мрежата која е дефинирана во рамките на Tendermint системите. Истата е надградена за да може да биде во склад со потребите на BloHeS мрежата и да овозможи само-организиран пристап за градење и управување на кластери со проширување на процедурите за управување со книгите за адреси (address books).

Основни процедури за управување со кластери, односно острови, во рамките на протоколите за управување со острови се: *протокол за додавање на нови валидатори во остров*, *делење на остров* и *спојување на остров*. Овие се први протоколи за само-организирање на валидатори во кластерски формации, во рамките на Blockchain технологиите.

5.5.1. Детекција на валидатори

На почетокот на развојот на компјутерските мрежи и зачетокот на Интернетот, комуникацијата помеѓу корисниците била заснована на peer-to-peer (P2P) протоколи. Омасовувањето на Интернетот и новите сервиси имаат потреба од рedefинирање на мрежната архитектура преку нејзино централизирање. За полесно градење на компјутерските мрежи се создава стандардизиран протоколен стек [136] за вмрежување со цел да придонесе кон подобра централизирана мрежна архитектура. Централизираниот начин на градење на мрежите претставува пречка за новите генерации на P2P сервиси особено за коректно функционирање на *процедурите за откривање на соработници* (peer discovery).

Blockchain технологиите и Blockchain базирани апликации, нудат P2P сервиси од новата генерација на мрежни сервиси, но во зачетокот на нивното градење имало проблем со овозможувањето на доверливи сервиси и во спроведувањето на процедурите за откривање соработници во мрежата. Главен проблем за овозможувањето на P2P сервисите се рутерите, поточно firewall [137] и Network Address Translation (NAT) [138] сервисите кои се во склоп на рутерите. За да се надмине проблемот за откривање соработници во мрежата и за да се овозможи P2P сообраќајот да поминува низ firewall и NAT, развиени се протоколи како UPnP [139], PCP [140] и NAT-PMP [141]. Дополнително во рамките на Blockchain технологиите се имплементираат суперјазли и Distributed Hash Table (DHT) [142] табели. Постојењето на суперјазли во мрежата

овозможува новите јазли кои се приклучуваат во мрежата да добијат информација за други јазли кои се веќе присутни во мрежата, а со помош на DHT се овозможува уште побрзо откривање на соработници во мрежата.

Tendermint рамката дефинира протокол за откривање на соработници [143] според кој потребно е да се имплементираат *изворни* (seed) јазли кои се првите јазли на кои треба да се прикачат новите корисници за да може да откријат соработнички јазли во мрежата. Изворните јазлите имаат статичка адреса која е однапред конфигурирана во новиот јазол со цел да може барањата за откривање соработници да бидат коректно испратени низ мрежата. На барањата за соработнички адреси, изворниот јазол одговара со листа на адреси кои се најдобри во мрежата. *Книгата со адреси* во изворниот јазол константно се обновува преку постојано откривање нови адреси и размена на адреси со други соработници од мрежата.

Процесот на откривање на соработници од страна на новите јазли продолжува до моментот додека не се открие доволен број на адреси, по што процесот за откривање на соработници прекинува и новиот јазол може да се интегрира во мрежата. При рестартирање на јазол, истиот може да се обиде да се приклучи веднаш на мрежата преку контактирање на соработничките адреси кои ги има во книгата со адреси и доколку не успее да стапи во контакт со јазлите од книгата со адреси, започнува нова процедура за пребарување на соработнички адреси. Покрај откривањето на соработнички адреси преку контактирање на изворниот јазол, Tendermint рамката дефинира и процедури за рачно додавање на јазли како што се: *постојани соработници* (persistent peers), *приватни соработници* (private peers) и *безусловни соработници* (unconditional peers).

Постојаните соработници се очекува да бидат високодоверливи јазли кои треба да му помогнат на јазолот да биде постојано поврзан на мрежата. Соработничкиот јазол често ги контактира постојаните соработници за да ја следи нивната активност и исправност. Процесот на контактирање на постојаните соработници имплементира експоненцијален back-off алгоритам во случај на достапност на соработничкиот јазол. Приватните соработници не се дел од книгата со адреси и не се споделуваат меѓу корисниците. Безусловните соработници се конектираат дури и во услови кога максималниот број на влезни и излезни соработници биде достигнат.

Книгата со адреси се пополнува со нови соработнички адреси од дојдовните конекции или од појдовните конекции до други соработници при што се разменува листа на познати соработници. Адресите се организираат во *групи* (buckets), од кои еден тип на група е за *проверени* (vetted) или стари соработници, а повеќе други групи се за *непроверени* (unvetted) или нови соработници. Групата практично претставува IP група од адреси со маска на подмрежа (subnet mask) /16 за IPv4 и маска на подмрежа (subnet mask) /32 за IPv6 адресите. Доколку групата е полна, нов соработник се додава кога соработник со најлоши перформанси претходно ќе биде отстранет од листата. Создавањето на IP групи се прави за полесно справување со DoS напади доколку хакер изврши напад на одреден адресен простор. Група за проверени соработници се пополнува со адреси од група за непроверени соработници, откако е направен значаен придонес од страна на непроверениот соработник, преку следење на перформансите на соработничкиот јазол и мерење на довербата. Исто така соработничкиот јазол ја следи достапноста на другите соработнички јазли и ако соработничкиот јазол не е достапен после неколкукратни обиди, истиот се обележува како лош или се отстранува од книгата на адреси.

Во рамките на BloHeS системот, додавањата на нови соработнички јазли во мрежата бараат статична дефиниција на постојани соработнички адреси во конфигурацијата на јазлите кои треба да обезбедат прегледни (look-up) табели со активни учесници. Постојаните соработнички јазли може да бидат дел од постоечки независни јазли, но пред се треба да бидат високодоверливи соработници за новите јазли.

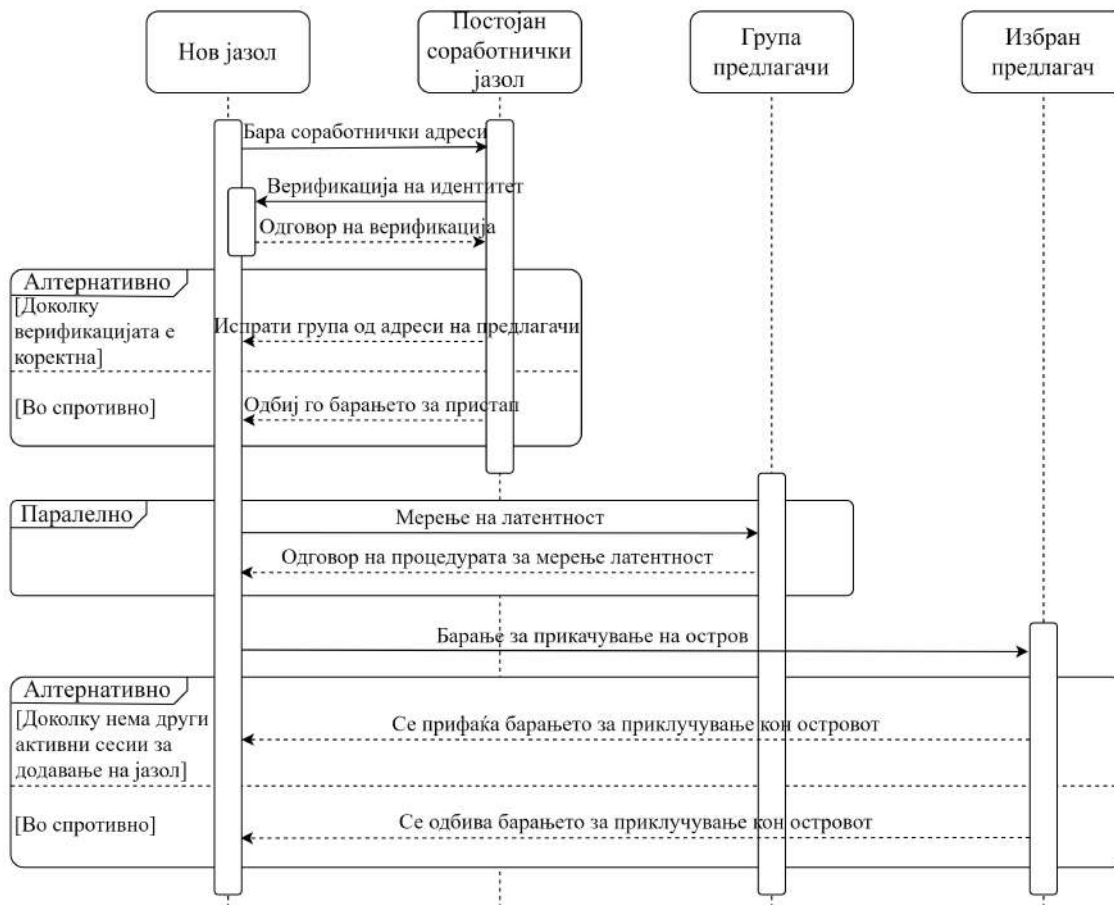
За да се обезбеди целосно автономно работење на валидаторите во BloHeS системот, постојаните соработнички јазли потребно е да управуваат со книгата на адреси во две фази. Едната фаза во која се пополнува книгата на адреси е иницијализациската фаза од развојот на BloHeS системот каде бројот на соработнички јазли е мал и сеуште не е формиран ниту еден остров и не е избран предлагач во островот. Најмалку 4 валидатори потребно е да бидат вклучени во BloHeS мрежата за да може да се формира остров и да се избере предлагач во островот. Во иницијализациската фаза, книгата на адреси во постојаните соработнички јазли ќе има адреси од сите валидатори кои се вклучиле во мрежата, додека во следната фаза постојаните соработнички јазли ја прочистуваат книгата на адреси и започнуваат пополнување на истата со адреси на предлагачи од островите. Распространувањето на адресите на предлагачите е доволно за да се спознаат адресите на сите валидатори бидејќи предлагачите ги знаат адресите од сите валидатори во рамките на нивните острови.

5.5.2. Додавање на нови валидатори во остров

Откако ќе се прикачи нов јазол на мрежата, потребно е истиот да биде додаден во некој од островите за да може да партиципира како валидатор во мрежата. Во таа насока јазолот потребно е да го спроведе протоколот за додавање на јазол, прикажан на Слика 5.19. Процедурата на овој протокол е следна:

1. Новиот јазол бара од постојаниот соработнички јазол листа со адреси од предлагачи во островите.
2. Постојаниот соработнички јазол го верифицира новиот јазол (проверува дали новиот јазол има авторизација да биде вклучен во мрежата). Доколку се изврши успешна авторизација постојаниот соработнички јазол испраќа одреден број на адреси од предлагачи по случаен избор до новиот јазол, а доколку авторизацијата пропадне новиот јазол се одбива да биде вклучен во мрежата. Доколку новиот јазол има пополнета книга со адреси од претходна сесија, овој чекор се прескокнува и новиот јазол се обидува да стапи во контакт со некој од валидаторите чии адреси ги знае. Валидноста на адресите во книгата на адреси е 24 часа, после што се смета дека истите повеќе не се валидни.
3. Новиот јазол иницира тестови за перформансите на врската со сите предлагачи од кои ќе добие адреса. Тестот за перформанси се состои во мерење на латентност до предлагачите. Чека извесен период за да добие одговор од предлагачите. За да се дознае состојбата на врските доволно е да се чека не повеќе од 5 секунди, бидејќи ако се добие одговор после 5 секунди тоа значи дека врската до предлагачот е или преоптоварена или самиот предлагач е пренатрупан со пакети па не може навремено да одговори.
4. Во зависност од тестот за латентност, новиот јазол одбира предлагач и соодветно остров до кој има најмала латентност.

5. Одбраниот предлагач одговара со прифаќање доколку нема други тековни процедури за додавање на нови јазли и тогаш новиот јазол постанува валидатор. Доколку во тек се активни сесии за додавање на нови јазли кон истиот предлагач, новиот јазол ќе биде одбиен по што ќе се обиде да се прикачи на следниот предлагач во листата.

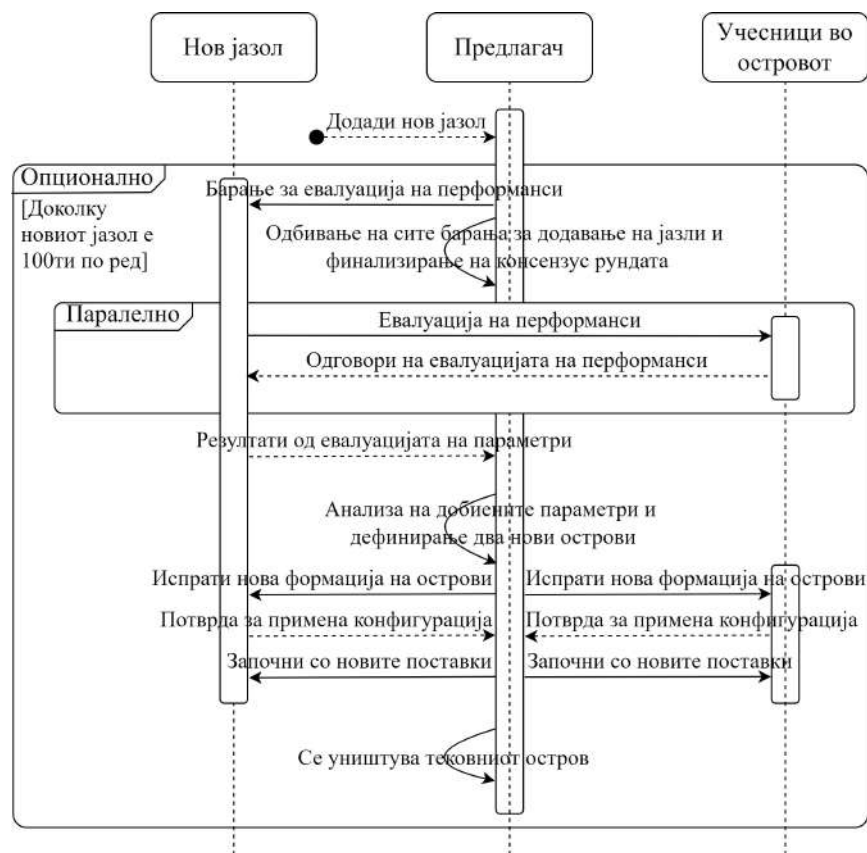


Слика 5.19. Протокол за додавање на јазол

5.5.3. Делење на остров

Втората процедура прикажана на Слика 5.20, делење на остров, се извршува кога новододадениот јазол во островот е 100ти по ред. Од литературата за Tendermint консензус механизмот се препорачува бројот на валидатори во Tendermint мрежата да биде околу 100 за да има оптимални перформанси [14], [81] или да се зголеми до максимални 300 валидатори во мрежата после што перформансите на Tendermint мрежата може да почнат да деградираат. Земајќи ја во предвид корелираноста на BloHeS консензус механизмот и Tendermint консензус механизмот се прифаќа максималната големина на островот да биде еднаква со максималната големина на Tendermint мрежата. Од таму бројот на валидатори по остров би можел да се движи помеѓу 100 и 300, но потребно е да се спроведе дополнителна емпириска анализа за детерминирање на оваа величина. Чекорите на протоколот за делење на остров се следни:

1. Кога новододадениот јазол, односно валидатор во островот е 100ти по ред, предлагачот кој го додал последниот валидатор иницира процедура за делење на островот. Во исто време се финализира консензус рундата и се информираат валидаторите во островот дека се отпочнува процедура за делење на остров. Предлагачот бара од новододадениот валидатор да изврши итна евалуација на перформансите до валидаторите од островот, а од останатите валидатори во островот бара табели со перформанси до останатите членови од островот. Евалуацијата на перформанси помеѓу валидаторите во островот се прави регуларно, па затоа не е потребна итна дополнителна евалуација на перформансите меѓу учесниците во островот.
2. По сублимирање на резултатите добиени од страна на сите валидатори, предлагачот определува две подгрупи од валидатори и ги информира каде припаѓаат истите.
3. Валидаторите ја прифаќаат новата организација и формираат два нови острови.
4. Кога предлагачот ќе добие потврдни пораки од сите валидатори дека ја добиле информацијата за новата конфигурација на островите, праќа сигнал за активирање на новите острови со што стариот остров престанува да постои.
5. Во новите острови се иницира процедура за избор на предлагач и се отпочнува со консензус механизмот во рамките на островот.



Слика 5.20. Протокол за делење на остров

5.5.4. Спојување на остров

Важна карактеристика на консензус механизмот е можноста да се одбрани мрежата од малициозни валидатори. Поради динамиката на мрежата и регуларните излегувања од мрежата, островот може да дојде до ситуација каде бројот на валидатори може да се намали значително. За да се овозможи заштита од малициозни валидатори, најмалиот број на валидатори во мрежата треба да биде четири. Во таа ситуација островскиот консензус механизам ќе може да го заштити островот од еден малициозен валидатор. Земајќи го ова во предвид, валидаторите во мрежата треба да се реорганизираат кога бројот на активни валидатори ќе падне на три. Во тој случај реорганизацијата на островот започнува со протоколот за спојување на остров. Со иницирање на овој протокол се финализира тековната консензус рунда и се уништува островот, по што валидаторите во островот повеќе не се прикачени на островот па потребно е да започнат процедура за додавање на нов јазол. Протоколот за спојување на остров е даден на Слика 5.21, а процедурата е следна:

1. Кога во островот остануваат само три активни валидатори, предлагачот на тековната консензус рунда ја финализира истата, го стомира консензус механизмот и ги информира останатите валидатори во островот да започнат процедура за анализа на перформанси до потенцијални нови острови.
2. Секој партиципант практично започнува процедура за додавање на нов јазол.



Слика 5.21. Протокол за спојување на остров

5.5.5. Предности и недостатоци на протоколите за управување со острови

Протоколите за управување со острови се први од ваков тип кои се употребуваат во Blockchain технологија. Тие се само-организирачки процедури кои во контекст на мрежната организација ќе помогнат да се автоматизира процесот на формирање кластери и во таа насока ќе помогнат кон постигнување конзистентни мрежни перформанси во секој дел на BloHeS мрежата. Основните процедури за формирање на кластер користат едноставни механизми за евалуација на мрежните перформанси

односно евалуација на латентност во мрежата. Евалуацијата на латентноста помеѓу валидаторите ќе му даде на системот можност да спроведе брзи и лесни процедури за мапирање на перформансите на валидаторите во мрежата. За напредно и попрецизно кластерирање, може да бидат евалуирани дополнителни процедури и метрики.

Поради само-организациската природа на протоколите за управување со острови, потенцијално сценарио на неуниформна распределба на валидаторите низ островите може да доведе до деградација на перформансите во некои острови. Корисниците во поголемите острови може да искушат подолги времиња на чекање за финализирање на трансакциите, но сепак истите би биле во прифатливи рамки.

Исто така поради мобилност на валидаторите (независно поради движење на валидаторот или преминување на валидаторот од една на друга мрежа) потенцијално малициозни активности може да бидат искусени од страна на BloHeS мрежата. Овие активности може да предизвикаат повеќекратна регистрација и дерегистрација од системот или да доведат до чести прикачувања кон островите и на тој начин да се остават отворени сесии во повеќе острови.

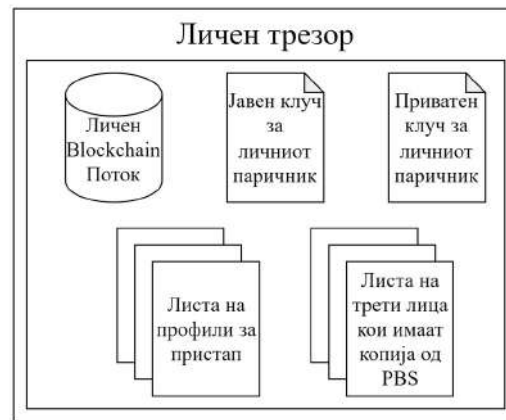
Еден валидатор може да делува малициозно со партиципирање во два различни острови и притоа да оствари двојно гласање во исто време преку двата острови. Ова потенцијално малициозно однесување може да биде детектирано од страна на архивскиот кластер, чија улога е да ги проверува валидираните блокови од сите острови од напади на двојно гласање.

5.6. Личен трезор и паричник

За да може да се управува со личните податоци на безбеден начин, BloHeS системот предвидува користење на *личен трезор* (personal vault). На Слика 5.22 е дадена содржината на личниот трезор. Личниот трезор ќе биде енкриптиран контейнер со податоци, каде корисникот ќе ги чува податоците од Личниот Blockchain поток, паричникот (енкриптиските клучеви), листата на профили за пристап и управување со податоци, како и листата на трети лица кои имаат дозвола за пристап до личните податоци. Личниот трезор во форма на апликација ќе ги чува чувствителните податоци заштитени со лозинка. Управувањето со пристапот до личните податоци од страна на трети лица се прави преку користење на паметен договор кој е поставен во главната Blockchain база на податоци. Паметниот договор за управување со пристапот има универзална форма која може да се користи од страна на сите пациенти. За да се даде пристап на трети лица до одредени податоци, во паметниот договор се внесува адресата на корисникот на кого му се дава пристап, полињата до кои може да се пристапи и со негова помош се врши трансферот на податоци до третите лица.

Јавните Blockchain базирани здравствени системи потребно е да имаат процедура за контрола на пристапот, односно Blockchain технологијата треба да биде со дозвола за пристап со цел да се гарантира уникатноста на дигиталниот идентификатор за пациентот. Сите агенти во системот имаат уникатен идентификатор кој е во форма на адреса на паричник. Создавањето на паричник е на барање на пациентот. Креирањето на паричник се прави само еднаш, кога за прв пат ќе биде вклучен пациентот во системот. Барањето се испраќа до здравствениот работник кој е избран од пациентот како семеен доктор и истото потоа се испраќа до владината институција каде се поврзува со дигиталниот идентитет на пациентот кој што се издава од страна на владина институција. На крај паричникот се создава во уредот на пациентот каде при

процедурата на генерирање на паричник се внесува повратната информација од владината институција.



Слика 5.22. Личен трезор

За да се подобри скалабилноста на системот по однос на адресниот простор, се предвидува здравствените работници да имаат адреса на паричник која ќе биде од посебно множество на адреси што ќе се разликуваат од множеството на адреси за пациентите. Адресата на паричник би се креирала на барање на здравствениот работник и би била поврзана со бројот на лиценца или одобрение за работа што здравствениот работник би ја добил од владините институции.

Другите агенти во мрежата кои не се пациенти или здравствени работници би добиле адреса на паричник од посебни множества на адреси наменети за соодветните агенти.

5.7. Процедура за контрола на пристап до личните податоци

Во трудот [144] авторите предлагаат пациент-центрични процедури за контрола на пристап до личните податоци на пациентите за здравствена апликација која е базирана на Blockchain технологија. Предложени се четири протоколи за размена на податоците: здравствен работник – пациент, пациент – здравствен работник, здравствен работник – здравствен работник и здравствен работник – трети лица. Првите две процедури се пациент-центрични процедури каде барањата за пристап до податоците се испраќаат директно до пациентите. Спротивно на овие две процедури, следните две може да се опишат како псевдо пациент-центрични бидејќи процедурите вклучуваат интеракција помеѓу здравствениот работник и трети лица без директна согласност на пациентот. Овие процедури се базираат на претпоставка за индиректно овластување на здравствениот работник за располагање со податоците на пациентите. Овој пристап е потенцијално штетен и може да предизвика протекување на личните податоци низ агентот на здравствениот работник.

Спротивно на овој пристап, кај BloHeS архитектурата се применува целосно пациент-центрично управување со правата за читање и пишување на податоците за пациентите. За да се поедностави механизмот за контрола на пристап, потребно е да се создадат профили со однапред дефинирани полиња кои се рестриктирани за пристап, а контролата на пристап да се прави преку една процедура: пациент – трети лица. Кај оваа процедура трети лица може да бидат здравствените работници (кои би имале привилегии за читање и пишување), лични уреди (кои би имале привилегии за читање и пишување),

осигурителни и фармацевтски компании (кои би имале привилегии за читање) и др. Практично протоколот е ист за сите барања за пристап и е имплементиран во форма на паметен договор. На овој начин пациентот би имал целосна контрола врз барањата за пристап до личните податоци независно дали истите се пратени директно до пациентот или трети лица преку здравствениот работник имаат одредени побарувања. Процедурата за контрола на пристап е дадена на Слика 5.23.



Слика 5.23. Процедура за контрола на пристап

5.8. Усогласеност со GDPR и HIPAA регулативите

Најсилната точка на Blockchain технологијата е можноста да се поврзат блоковите од податоци и да се направи нивното менување да биде невозможно. Но

моменталната поставеност на GDPR [15] регулативата и „правото да се биде заборавен“ (“right to be forgotten”), претставува пречка за користење на Blockchain технологијата за складирање на лични податоци, заради тоа што моменталните Blockchain технологии не можат да обезбедат решение кое ќе овозможи бришење на личните податоци од базата на податоци на Blockchain системот. Менувањето на било кој сегмент од Blockchain базата на податоци значи целосно рекалкулирање на врските помеѓу податочните блокови на Blockchain базата на податоци.

Спротивно на традиционалните Blockchain технологии, BloHeS системот и начинот на кој се организирани податоците во BloHeS системот овозможуваат целосна контрола врз личните податоци од страна на пациентите. Тоа подразбира дека во BloHeS системот пациентите имаат можност да менуваат или бришат лични податоци кај сите ентитети со кои ги споделиле личните податоци. Во рамките на личниот трезор на пациентот постојат записи во кои пациентот следи со кои трети лица ги има споделено личните податоци, а за истите се додава податочен блок во рамките на Личниот Blockchain поток со потпис од страна на третото лице дека ги поседува информациите. Бришењето на личните податоци од доменот на трети лица се прави преку соодветен паметен договор кој се потпишува од страна на третите лица и податок за истиот се поставува во Личниот Blockchain поток. Поставување на податок во Личниот Blockchain поток за овозможен пристап до информации или бришење на лични податоци кај трети лица, се прави со цел да се заштити пациентот од потенцијални злоупотреби на личните податоци.

Имплементирањето на „правото да се биде заборавен“ е едноставно благодарение на сегментираноста и независноста на Личните Blockchain Потоци во системот. Така, во случај кога пациент бара од трето лице да ги избрише неговите лични податоци, потребно е само да се избришат податоците од Личниот Blockchain поток на пациентот кои се наоѓаат во базата на податоци кај третото лице. На тој начин функционирањето на останатиот дел од BloHeS системот не се афектира воопшто и нема потреба да се интервенира во главната Blockchain база на податоци.

Насоките на Health Insurance Portability and Accountability Act (HIPAA) [145] регулативата за приватност на податоците, бара од системите кои употребуваат лични здравствени податоци да обезбедат висок степен на приватност на личните податоци кои можат да го откријат идентитетот на пациентот. За да се постигне приватност на податоците истите треба да бидат енкриптирани во фазата на поминување на податоците низ мрежата, но и во фазата на нивно складирање во базата на податоци. Тоа значи дека HIPAA препораките се да има целосна крај-до-крај заштита на личните податоци. Во рамките на паметниот договор со кој се испраќаат податоците до барателот на информации се дефинира процедура за воспоставување на енкриптиран тунел помеѓу крајните точки со што се заштитува комуникацискиот канал од прислушувачи и истекувања на податоци надвор од системот. Згора на тоа за да се постигне безбедност на високо ниво во крајните точки од комуникацискиот канал, личниот трезор на пациентот ќе биде чуван во енкриптирана форма.

ЗАКЛУЧОК

Во оваа докторска дисертација е дефиниран јавниот здравствен систем Blockchain Healthcare System (BloHeS) кој е базиран на Blockchain технологија во која се имплементира оптимален консензус механизам. Дефинирањето на системското решение опфаќа дизајн на архитектурата на BloHeS системот, дизајн на соодветен консензус механизам, дизајн на складишен простор прилагоден на системската архитектура и дизајн на помошни процедури за управување со личните податоци.

Потребата за дефинирање на нова Blockchain технологија е резултат на направената опсежна анализа на постоечките Blockchain технологии и нивните општи перформанси. Како најнадежна Blockchain технологија е избрана Cosmos Blockchain технологијата со Tendermint консензус механизмот, која теоретски ветува проток од десетици илјади трансакции во системот. Поради недостаток од резултати за перформансите на Tendermint консензус механизмот изработена е емулирана средина за евалуација на перформансите за максималниот капацитет на Tendermint консензус механизмот во општи услови и во услови на сообраќај со карактеристики на здравствен систем. Евалуацијата на перформансите е изведена преку следење на протокот на трансакции низ системот, притоа анализирајќи повеќе различни параметри за Tendermint консензус механизмот кои би можеле да ги оптимизираат перформансите на истиот. Исто така е извршена анализа на перформансите на Tendermint консензус механизмот за големи трансакции преку кои се емулира сообраќај сличен на тој што циркулира во здравствените системи. Од добиените резултати се согледува слабоста на Tendermint консензус механизмот да обезбеди доволен капацитет за негова имплементација во сценарио на глобален јавен здравствен систем.

Поради големиот број недостатоци на тековните Blockchain технологии и неможноста да одговорат на потребите кои ги поставува глобалниот здравствен систем, во рамките на докторската дисертација е дефиниран дедициран систем со оптимална архитектура и процедури со кои ќе може да се опслужи светската популација. Новиот BloHeS систем е изграден врз нова архитектура, која подразбира повеќенивовска организација на учесниците во мрежата преку дефинирање различни агенти со различни улоги во системот. За да може да функционира новата повеќенивовска архитектура, исто така е дефиниран нов BloHeS консензус механизам со кој за прв пат во рамките на една Blockchain технологија се овозможува финализирање на консензус рундите во кластерска организација на валидаторите во мрежата. Дополнително, кластерирањето на валидаторите во мрежата овозможува имплементација на консензус механизам кој ќе биде независен во секој кластер. За да може мрежата од кластери да функционира во еден систем, истите се поставени на пониско хиерархиско ниво во однос на единачниот архивски кластер кој ќе ги надгледува процесите во системот и ќе ги финализира трансакциите кои ќе бидат генерирани во рамките на кластерите. Овој единачен архивски кластер ќе има архиварска улога, односно ќе ги консолидира записите во мрежата и ќе ја потврдува нивната коректна форма. За да се потврдат подобрите перформанси на BloHeS консензус механизмот во однос на Tendermint консензус механизмот, извршена е анализа на комуникациската комплексност на двата консензус механизми и на капацитетот на заштита. Добиените резултати покажуваат значително намалување на комуникациската комплексност за постигнување на консензус кај BloHeS консензус механизмот споредено со Tendermint консензус механизмот што придонесува кон подобрување на перформансите на целокупниот систем преку зголемување на скалабилноста на истиот. Спротивно на подобрувањето на комуникациската комплексност кај BloHeS консензус механизмот, има намалување на

перформансите во однос на капацитетот на заштита на системот, но истото е незначително особено кога во системот има поголеми кластери при што капацитетот на заштита на BloHeS консензус механизмот асимптотски се доближува до оној на Tendermint консензус механизмот.

Архитектурата и организацијата на корисниците во BloHeS системот дефинира и нов начин на организирање на складирањето на податоци. Кај класичниот начин на складирање на податоци кој е застапен кај Blockchain технологиите, податоците што се генерираат во системот потребно е да бидат реплицирани во сите кориснички јазли во системот, а тоа за глобално решение на јавен здравствен систем значително би ги оптоварило складишните простори на сите корисници. За да се избегне овој проблем, во BloHeS системот складирањето на податоци се врши во одбран сет на јазли кои ќе помогнат во одржување на трајноста на податоците. Дополнително, за да се прилагоди оваа Blockchain технологија на GDPR и HIPAA регулативите, дефиниран е пациент-центричен пристап на складирање на податоците и управување со привилегиите за читање и пишување на истите преку воведување на Личниот Blockchain поток. Со тоа практично BloHeS Blockchain технологијата е првата која овозможува целосна контрола од страна на пациентот за тоа кој поседува копија од неговите лични податоци. Исто така, има и подобрени процедури за обезбедување високо ниво на приватност на податоците преку енкрипција на истите во складишниот простор, но и при циркулирање на истите низ системот. Подобрувањата кои ги нуди новиот начин на складирање на податоците се потврдени со симулацијата на зафатнината на складишниот простор во системи кои користат класичен начин на складирање на податоци и BloHeS начин на складирање на податоци. Притоа се забележува особено намалување на зафатнината на складишен простор кај крајните корисници односно пациентите, додека има незначително зголемување на зафатнината на складишниот простор кај владините јазли. Исто така се забележува одреден степен на намалување на зафатнината на складишен простор и кај јазлите на здравствените работници.

Добиените резултати и дефинираниот систем во рамките на оваа докторска дисертација ја потврдуваат главната хипотеза: Може да се дизајнира јавен здравствен систем базиран на Blockchain технологија кој ќе овозможи глобализирање на здравствените сервиси преку унифициран јавен здравствен систем кој инхерентно би ги наследил високиот степен на доверливост и приватност кои ги овозможува Blockchain технологијата, а воедно би ги надминал проблемите на скалабилност кои се појавуваат кај Blockchain технологиите.

Покрај главната, исто така се потврдуваат и посебните хипотези:

- Постоечките Blockchain технологии не можат да одговорат на волуменот и посебноста на сообраќајот кој би циркулирал во глобалниот јавен здравствен систем.
- Може да се дефинира протокол што ќе овозможи зголемена скалабилност на Blockchain технологијата која ќе се користи за дизајн на глобалниот јавен здравствен систем и притоа ќе го задржи високиот степен на доверливост на Blockchain технологиите.
- Може да се дефинираат протоколи кои ќе овозможат пациент-центричен механизам за управување со пристапот кон приватните податоци.

Имплементирањето на BloHeS систем ќе даде можност да се подобри контролата на личните здравствени податоци преку овозможување пациент-центрично управување со привилегиите за пристап до истите. Со тоа пациентите можат да располагаат со

личните здравствени податоци и истите можат да ги заштитат од неовластено користење и злоупотреба од трети лица. Сето тоа остава простор да се дефинираат и нови бизнис идеи со кои осигурителните компании би можеле да понудат подобри осигурителни планови за пациентите, а фармацевтските компании би можеле да создадат подобри лекови. Употребата на стандардизирана форма на здравствените записи би овозможила користење на системот на глобално ниво притоа лесно надминувајќи ја јазичната бариера кога пациентот би користел услуги надвор од матичната држава. Исто така, би се овозможило и користење на алгоритми за машинско учење со кои би се подобрил процесот на дијагностика кај пациентите и општата популација.

KOPHCTEHA JIITEPATYPA

- [1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008 [Online]. Available: <https://bitcoin.org/bitcoin.pdf>. [Accessed: 03-2022]
- [2] J. Debus, "Consensus methods in blockchain systems," *Frankfurt School of Finance & Management, Blockchain Center, Technical report*, pp. 1–58, 2017.
- [3] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Annual international cryptology conference*, 1992, pp. 139–147.
- [4] M. Jakobsson and A. Juels, "Proofs of Work and Bread Pudding Protocols (Extended Abstract)," *Secure Information Networks*, pp. 258–272, 1999.
- [5] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," 2012 [Online]. Available: <https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf>. [Accessed: 03-2022]
- [6] M. Castro, B. Liskov, and others, "Practical byzantine fault tolerance," in *OSDI*, 1999, vol. 99, no. 1999, pp. 173–186.
- [7] J. Kwon, "Tendermint: Consensus without mining," *Draft v. 0.6*, 2014 [Online]. Available: <https://tendermint.com/static/docs/tendermint.pdf>. [Accessed: 03-2022]
- [8] L. Baird, "The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance," *Swirlds Tech Reports SWIRLDS-TR-2016-01, Tech. Rep.*, 2016 [Online]. Available: <https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf>. [Accessed: 03-2022]
- [9] S. Popov, "The tangle," 2018 [Online]. Available: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf. [Accessed: 03-2022]
- [10] CoinMarketCap, "Total Market Capitalization," 2021. [Online]. Available: <https://coinmarketcap.com/charts/>. [Accessed: 03-2022]
- [11] V. Buterin and others, "Ethereum white paper: A next-generation smart contract and decentralized application platform," 2014 [Online]. Available: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. [Accessed: 03-2022]
- [12] R. Halalai, T. A. Henzinger, and V. Singh, "Quantitative evaluation of bft protocols," in *2011 Eighth International Conference on Quantitative Evaluation of SysTems*, 2011, pp. 255–264.
- [13] W.-K. Fu, Y.-S. Lin, G. Campagna, D.-Y. Tsai, C.-T. Liu, C.-H. Mei, E. Y. Chang, M. S. Lam, and S.-W. Liao, "Soteria: A Provably Compliant User Right Manager Using a Novel Two-Layer Blockchain Technology," *arXiv preprint arXiv:2003.10128*, 2020.
- [14] J. Kwon and E. Buchman, "Cosmos - A Network of Distributed Ledgers," 2018 [Online]. Available: <https://v1.cosmos.network/resources/whitepaper>. [Accessed: 03-2022]
- [15] G. D. P. Regulation, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46," *Official Journal of the European Union (OJ)*, vol. 59, no. 1–88, p. 294, 2016.
- [16] J. Karamachoski and L. Gavrilovska, "Framework for Next Generation of Digital Healthcare Systems," in *International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures (FABULOUS)*, 2019, pp. 12–24.
- [17] U. Der, S. Jähnichen, and J. Stürmeli, "Self-sovereign identity - opportunities and challenges for the digital revolution," *arXiv preprint arXiv:1712.01767*, 2017.
- [18] H. Kohad, S. Kumar, and A. Ambhaikar, "Scalability issues of blockchain technology," *Int. J. Eng. Adv. Technol. IJEAT*, vol. 9, no. 3, 2020.
- [19] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: applying blockchain to securely and scalably share clinical data," *Computational and structural biotechnology journal*, vol. 16, pp. 267–278, 2018.
- [20] A. C. Ekblaw, "MedRec: blockchain for medical data access, permission management and trend analysis," 2017 [Online]. Available: <https://dspace.mit.edu/handle/1721.1/109658>. [Accessed: 03-2022]
- [21] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, p. 218, 2016.

- [22] A. Gropper, “Powering the physician-patient relationship with hie of one blockchain health it,” in *ONC/NIST use of Blockchain for healthcare and research workshop*. Gaithersburg, Maryland, United States: ONC/NIST, 2016.
- [23] C. McFarlane, M. Beer, J. Brown, and N. Prendergast, “Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1.1,” 2017. [Online]. Available: https://www.colleaga.org/sites/default/files/attachments/patientory_whitepaper.pdf. [Accessed: 06-2020]
- [24] “Medicalchain Whitepaper 2.1.” [Online]. Available: <https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf>. [Accessed: 06-2020]
- [25] V. Dhillon, D. Metcalf, and M. Hooper, “The Hyperledger Project,” in *Blockchain Enabled Applications*, Springer, 2017, pp. 139–149.
- [26] “Telehealth.” [Online]. Available: <https://en.wikipedia.org/wiki/Telehealth>. [Accessed: 02-2022]
- [27] H. Shirzadfar and F. Lotfi, “The evolution and transformation of telemedicine,” *International Journal of Biosensors & Bioelectronics*, vol. Volume 3, no. Issue 4, pp. 303–306, 2017.
- [28] P. Chatterjee and R. L. Armentano, “Internet of things for a smart and ubiquitous ehealth system,” in *Computational Intelligence and Communication Networks (CICN), 2015 International Conference on*, 2015, pp. 903–907.
- [29] I. B. Ida, A. Jemai, and A. Loukil, “A survey on security of IoT in the context of eHealth and clouds,” in *Design & Test Symposium (IDT), 2016 11th International*, 2016, pp. 25–30.
- [30] A. F. da Conceição, F. S. C. da Silva, V. Rocha, A. Locoro, and J. M. Barguil, “Eletronic Health Records using Blockchain Technology,” *arXiv preprint arXiv:1804.10078*, 2018.
- [31] Y. Liu, J. Liu, M. A. V. Salles, Z. Zhang, T. Li, B. Hu, F. Henglein, and R. Lu, “Building Blocks of Sharding Blockchain Systems: Concepts, Approaches, and Open Problems,” *arXiv preprint arXiv:2102.13364*, 2021.
- [32] J. Benet, “IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3),” 2014 [Online]. Available: <https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf>. [Accessed: 03-2022]
- [33] S. Haber and W. S. Stornetta, “How to time-stamp a digital document,” in *Conference on the Theory and Application of Cryptography*, 1990, pp. 437–455.
- [34] R. Anderson and others, “The eternity service,” in *Proceedings of PRAGOCRYPT*, 1996, vol. 96, pp. 242–252.
- [35] B. Schneier and J. Kelsey, “Cryptographic support for secure logs on untrusted machines.,” in *USENIX Security Symposium*, 1998, vol. 98, pp. 53–62.
- [36] “What is Bit gold?” [Online]. Available: <https://www.investopedia.com/terms/b/bit-gold.asp#citation-1>. [Accessed: 02-2022]
- [37] “Bit gold.” [Online]. Available: <https://unenumerated.blogspot.com/2005/12/bit-gold.html>. [Accessed: 02-2022]
- [38] J. Karamachoski, L. Gavrilovska, and A. Sefidanoski, “The fusion between Blockchain and IoT for healthcare systems,” in *ETAI conference, Struga, Republic of Macedonia*, 2018, pp. 1–6.
- [39] V. Rakovic, J. Karamachoski, V. Atanasovski, and L. Gavrilovska, “Blockchain paradigm and Internet of Things,” *Wireless Personal Communications*, vol. 106, no. 1, pp. 219–235, 2019.
- [40] G. S. Ramachandran and B. Krishnamachari, “Blockchain for the IoT: Opportunities and Challenges,” *arXiv preprint arXiv:1805.02818*, 2018.
- [41] K. Sadouskaya and others, “Adoption of Blockchain Technologyin Supply Chain and Logistics,” 2017 [Online]. Available: <https://www.theseus.fi/bitstream/handle/10024/126096/Adoption%20of%20Blockchain%20Technology%20in%20Supply%20Chain%20and%20Logistics.pdf?sequence=1>. [Accessed: 03-2022]
- [42] S. Attili, S. Ladwa, U. Sharma, and A. Trenkle, “Blockchain: the chain of trust and its potential to transform healthcare-our point of view,” in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST, 2016.
- [43] S. Kejriwal and S. Mahajan, “Blockchain in commercial real estate: The future is here,” *Deloitte Center for Financial Services*, 2017 [Online]. Available: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-recblockchain-in-commercial-real-estate.pdf>. [Accessed: 03-2022]

- [44] T. Palmisano, V. N. Convertini, L. Sarcinella, L. Gabriele, and M. Bonifazi, “Notarization and Anti-Plagiarism: A New Blockchain Approach,” *Applied Sciences*, vol. 12, no. 1, p. 243, 2022.
- [45] M. Attaran and A. Gunasekaran, “Blockchain for Gaming,” in *Applications of Blockchain Technology in Business*, Springer, 2019, pp. 85–88.
- [46] C. HYPERLEDGER, “An Introduction to Hyperledger,” 2018. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf. [Accessed: 02-2022]
- [47] “Litecoin website.” [Online]. Available: <https://litecoin.org>. [Accessed: Sep-2019]
- [48] “Monero website.” [Online]. Available: <https://www.getmonero.org/>. [Accessed: 02-2022]
- [49] “Dash website.” [Online]. Available: <https://www.dash.org/>. [Accessed: 02-2022]
- [50] S. Goldwasser, S. Micali, and C. Rackoff, “The knowledge complexity of interactive proof systems,” *SIAM Journal on computing*, vol. 18, no. 1, pp. 186–208, 1989.
- [51] “Sovrin website.” [Online]. Available: <https://sovrin.org/>. [Accessed: 02-2022]
- [52] “EOS whitepaper.” [Online]. Available: <https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md>. [Accessed: 02-2022]
- [53] “Ripple website.” [Online]. Available: <https://ripple.com/>. [Accessed: 02-2022]
- [54] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, and others, “Hyperledger fabric: a distributed operating system for permissioned blockchains,” in *Proceedings of the Thirteenth EuroSys Conference*, 2018, p. 30.
- [55] “Holochain website.” [Online]. Available: <https://www.holochain.org/>. [Accessed: 02-2022]
- [56] “LTO network website.” [Online]. Available: <https://www.ltonetwork.com/>. [Accessed: 02-2022]
- [57] “Monet website.” [Online]. Available: <https://monet.network/>. [Accessed: 02-2022]
- [58] “On public and private Blockchains.” [Online]. Available: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>. [Accessed: 02-2022]
- [59] “Private Blockchain vs Consortium Blockchain.” [Online]. Available: <https://101blockchains.com/private-blockchain-vs-consortium-blockchain/>. [Accessed: 02-2022]
- [60] K. Wagner, B. Nemethi, E. Renieris, P. Lang, E. Brunet, and E. Holst, “Self-sovereign Identity: A position paper on blockchain enabled identity and the road ahead,” *Blockchain bundesverband*, 2018.
- [61] “State Machine Replication (SMR) Wikipedia.” [Online]. Available: https://en.wikipedia.org/wiki/State_machine_replication. [Accessed: 02-2022]
- [62] L. Lamport, R. Shostak, and M. Pease, “The Byzantine generals problem,” *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.
- [63] K. Driscoll, B. Hall, H. Sivencrona, and P. Zumsteg, “Byzantine fault tolerance, from theory to reality,” in *International Conference on Computer Safety, Reliability, and Security*, 2003, pp. 235–248.
- [64] R. Sobti and G. Geetha, “Cryptographic hash functions: a review,” *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 2, p. 461, 2012.
- [65] “Merkle tree Wikipedia.” [Online]. Available: https://en.wikipedia.org/wiki/Merkle_tree. [Accessed: 02-2022]
- [66] B. Lashkari and P. Musilek, “A comprehensive review of blockchain consensus mechanisms,” *IEEE Access*, vol. 9, pp. 43620–43652, 2021.
- [67] S. Joshi, “Feasibility of Proof of Authority as a Consensus Protocol Model,” *arXiv preprint arXiv:2109.02480*, 2021.
- [68] M. Bowman, D. Das, A. Mandal, and H. Montgomery, “On elapsed time consensus protocols,” in *International Conference on Cryptology in India*, 2021, pp. 559–583.
- [69] M. Pease, R. Shostak, and L. Lamport, “Reaching agreement in the presence of faults,” *Journal of the ACM (JACM)*, vol. 27, no. 2, pp. 228–234, 1980.
- [70] U. NIST, “Descriptions of SHA-256, SHA-384 and SHA-512,” 2001 [Online]. Available: <https://eips.ethereum.org/assets/eip-2680/sha256-384-512.pdf>. [Accessed: 03-2022]
- [71] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, “The keccak sha-3 submission,” *Submission to NIST (Round 3)*, vol. 6, no. 7, p. 16, 2011.
- [72] T. Fuko, “Intel software guard extensions (sgx) explained,” in *9th International Conference on Computer and Systems Engineering*, 2019.

- [73] K. Olson, M. Bowman, J. Mitchell, S. Amundson, D. Middleton, and C. Montgomery, "Sawtooth: An Introduction," *The Linux Foundation*, Jan, 2018.
- [74] "PoS guidebook." [Online]. Available: https://www.finyear.com/The-Proof-of-Stake-Guidebook-PoS-DPoS-LPoS-BPoS-Kezako_a40716.html. [Accessed: 02-2022]
- [75] VeChain, "VeChain: Development plan and whitepaper," *Whitepaper*, 2018 [Online]. Available: <https://www.vechain.org/whitepaper/>. [Accessed: 03-2022]
- [76] Z. Shi, H. Zhou, Y. Hu, S. Jayachander, C. de Laat, and Z. Zhao, "Operating permissioned blockchain in clouds: A performance study of hyperledger sawtooth," in *2019 18th International Symposium on Parallel and Distributed Computing (ISPDC)*, 2019, pp. 50–57.
- [77] E. Buchman, "Tendermint: Byzantine fault tolerance in the age of blockchains," 2016 [Online]. Available: <https://allquantor.at/blockchainbib/pdf/buchman2016tendermint.pdf>. [Accessed: 03-2022]
- [78] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, "Consortium blockchains: Overview, applications and challenges," *International Journal On Advances in Telecommunications*, vol. 11, no. 1&2, 2018.
- [79] J. Karamachoski and L. Gavrilovska, "Extended Performance Evaluation of the Tendermint Protocol," in *ETAI 2021 Conference Proceedings, Online conference*, 2021, vol. 2, pp. 231–236.
- [80] Y. Amoussou-Guenou, A. Del Pozzo, M. Potop-Butucaru, and S. Tucci-Piergiorgianni, "Dissecting Tendermint," in *International Conference on Networked Systems*, 2019, pp. 166–182.
- [81] S. K. Arora, G. Kumar, and T. Kim, "Blockchain Based Trust Model Using Tendermint in Vehicular Adhoc Networks," *Applied Sciences*, vol. 11, no. 5, p. 1998, 2021.
- [82] M. Fiore and M. Devesas Campos, "The algebra of directed acyclic graphs," in *Computation, Logic, Games, and Quantum Foundations. The Many Facets of Samson Abramsky*, Springer, 2013, pp. 37–51.
- [83] "Hedera website." [Online]. Available: <https://hedera.com/>. [Accessed: 02-2022]
- [84] "IOTA website." [Online]. Available: <https://www.iota.org/>. [Accessed: 02-2022]
- [85] "Bitcoin website." [Online]. Available: <https://bitcoin.org/en/>. [Accessed: 02-2022]
- [86] "Ethereum website." [Online]. Available: <https://ethereum.org/en/>. [Accessed: 02-2022]
- [87] "Cosmos website." [Online]. Available: <https://cosmos.network/>. [Accessed: 02-2022]
- [88] "Hyperledger website." [Online]. Available: <https://www.hyperledger.org/>. [Accessed: 02-2022]
- [89] "Bitcoin Gold website." [Online]. Available: <https://bitcoingold.org/>. [Accessed: 02-2022]
- [90] "Bitcoin Cash website." [Online]. Available: <https://bitcoincash.org/>. [Accessed: 02-2022]
- [91] "Bitcoin SV website." [Online]. Available: <https://bitcoinsv.com/>. [Accessed: 02-2022]
- [92] "Ethereum 2.0: A Complete Guide. Scaling, Part One." [Online]. Available: <https://medium.com/chainsafe-systems/ethereum-2-0-a-complete-guide-3739a74be61a>. [Accessed: Sep-2019]
- [93] "ABCI protocol." [Online]. Available: <https://cosmos-network.gitbooks.io/cosmos-academy/content/cosmos-for-developers/tendermint/abci-protocol.html>. [Accessed: 02-2022]
- [94] "Ethermint website." [Online]. Available: <https://docs.ethermint.zone/>. [Accessed: 02-2022]
- [95] "Cosmos story." [Online]. Available: <https://www.coindesk.com/markets/2019/11/11/how-to-turn-a-17-million-ico-into-104-million-the-cosmos-story/>. [Accessed: 02-2022]
- [96] "IBC protocol." [Online]. Available: <https://tendermint.com/ibc/>. [Accessed: 02-2022]
- [97] H. H. LLC, "Understanding decentralization of Hedera Hashgraph." [Online]. Available: <https://hedera.com/hh-decentralization-of-consensus.pdf>. [Accessed: 03-2022]
- [98] "IBM website." [Online]. Available: <https://www.ibm.com/us-en/>. [Accessed: 02-2022]
- [99] "Intel website." [Online]. Available: <https://www.intel.com/content/www/us/en/homepage.html>. [Accessed: 02-2022]
- [100] "SAP Ariba website." [Online]. Available: <https://www.ariba.com/>. [Accessed: 02-2022]
- [101] L. Ismail, H. Materwala, and M. A. Khan, "Performance evaluation of a patient-centric blockchain-based healthcare records management framework," in *Proceedings of the 2020 2nd International Electronics Communication Conference*, 2020, pp. 39–50.
- [102] S. Alqahtani and M. Demirbas, "Bottlenecks in blockchain consensus protocols," *arXiv preprint arXiv:2103.04234*, 2021.

- [103] L. Miletic, "Formal and simulation analysis of data dissemination algorithms in a blockchain network," *Seniot thesis, University of Belgrade*, 2018.
- [104] "Hyper-V Wikipedia." [Online]. Available: <https://en.wikipedia.org/wiki/Hyper-V>. [Accessed: 02-2022]
- [105] "Tendermint GitHub repository." [Online]. Available: <https://github.com/tendermint/tendermint/releases>. [Accessed: 02-2022]
- [106] "tcconfig GitHub repository." [Online]. Available: <https://github.com/thombashi/tcconfig>. [Accessed: 02-2022]
- [107] "tm-load-test GitHub repository." [Online]. Available: <https://github.com/informalsystems/tm-load-test>. [Accessed: 02-2022]
- [108] "InfluxDB website." [Online]. Available: <https://www.influxdata.com/>. [Accessed: 02-2022]
- [109] "Grafana website." [Online]. Available: <https://grafana.com/>. [Accessed: 02-2022]
- [110] "Prometheus website." [Online]. Available: <https://prometheus.io/>. [Accessed: 02-2022]
- [111] "Ansible website." [Online]. Available: <https://www.ansible.com/>. [Accessed: 02-2022]
- [112] "Linux Bash website." [Online]. Available: <https://www.gnu.org/software/bash/>. [Accessed: 02-2022]
- [113] J. Karamachoski and L. Gavrilovska, "Tendermint Performance with Large Transactions: The Healthcare System Scenario," in *International Balkan Conference on Communications and Networking (BalkanCom)*, Novi Sad, Serbia, 2021, pp. 85–89.
- [114] M. Murray, M. Davies, and B. Boushon, "Panel size: how many patients can one doctor manage?," *Family practice management*, vol. 14, no. 4, p. 44, 2007.
- [115] J. Karamachoski and L. Gavrilovska, "Toward scalable architecture for the next generation Blockchain-based healthcare systems," in *Proceedings of the Conference Balkancom 2019, Skopje, North Macedonia*, 2019, pp. 1–5.
- [116] J. Karamachoski and L. Gavrilovska, "BloHeS Consensus Mechanism – Introduction and Performance Evaluation," in *International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures (FABULOUS)*, 2022.
- [117] J. Karamachoski and L. Gavrilovska, "An optimal storage organization for Blockchain-based Public Healthcare System," *Journal of Electrical Engineering and Information Technologies*, vol. 5, no. 2, pp. 143–152, 2020.
- [118] "MATLAB website." [Online]. Available: <https://www.mathworks.com/products/matlab.html>. [Accessed: 03-2022]
- [119] P. Labs, "Filecoin: A Decentralized Storage Network," 2017 [Online]. Available: <https://filecoin.io/filecoin.pdf>. [Accessed: 33-2022]
- [120] M. Eichelberg, T. Aden, J. Riesmeier, A. Dogac, and G. B. Laleci, "A survey and analysis of electronic healthcare record standards," *Acm Computing Surveys (Csur)*, vol. 37, no. 4, pp. 277–315, 2005.
- [121] "EHRcom (EN13606) website." [Online]. Available: <http://www.en13606.org/>. [Accessed: 02-2022]
- [122] "HL7 website." [Online]. Available: <https://www.hl7.org/>. [Accessed: 02-2022]
- [123] "DICOM website." [Online]. Available: <https://www.dicomstandard.org/>. [Accessed: 02-2022]
- [124] S. Kobayashi, N. Kume, K. Araki, and H. Yoshihara, "The Development of Medical Markup Language Version 4 as a Clinical Document Exchange Format for Nationwide EHR Systems," *Journal of Medical Systems*, vol. 44, no. 4, pp. 1–5, 2020.
- [125] "SNOMED website." [Online]. Available: <https://www.snomed.org/>. [Accessed: 02-2022]
- [126] B. Trombert-Paviot, J. M. Rodrigues, J. E. Rogers, R. Baud, E. Van Der Haring, A.-M. Rassinoux, V. Abrial, L. Clavel, and H. Idir, "GALEN: a third generation terminology tool to support a multipurpose national coding system for surgical procedures," *International journal of medical informatics*, vol. 58, pp. 71–85, 2000.
- [127] J. Altschuler, D. Margolius, T. Bodenheimer, and K. Grumbach, "Estimating a reasonable patient panel size for primary care physicians with team-based task delegation," *The Annals of Family Medicine*, vol. 10, no. 5, pp. 396–400, 2012.
- [128] R. J. Baron, "What's keeping us so busy in primary care? A snapshot from one practice.," *N. Engl. J. Med.*, vol. 362, no. 17, pp. 1632–6, 2010.
- [129] L. Muldoon, S. Dahrouge, G. Russell, W. Hogg, and N. Ward, "How many patients should a family physician have? Factors to consider in answering a deceptively simple question.," *Healthc Policy*, vol. 7, no. 4, pp. 26–34, 2012.

- [130] E. Estrada, "Graph and network theory," *Mathematical Tools for Physicists. 2nd Edition* (editor: M. Grinfeld). John Wiley & Sons, 2013.
- [131] S. Basagni, "Distributed clustering for ad hoc networks," in *Proceedings Fourth International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN'99)*, 1999, pp. 310–315.
- [132] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer communications*, vol. 30, no. 14–15, pp. 2826–2841, 2007.
- [133] S. Diaz, D. Mendez, and R. Kraemer, "A review on self-healing and self-organizing techniques for wireless sensor networks," *Journal of Circuits, Systems and Computers*, vol. 28, no. 05, p. 1930005, 2019.
- [134] M. Aissa and A. Belghith, "Quality of Clustering in mobile Ad Hoc networks," *Procedia Computer Science*, vol. 32, pp. 245–252, 2014.
- [135] J. Karamachoski and L. Gavrilovska, "BloHeS Island Management Protocols," in *International Conference on Information Society and Technology*, 2022.
- [136] "ISO OSI Protocol stack Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/OSI_protocols. [Accessed: 02-2022]
- [137] "Firewall Wikipedia." [Online]. Available: [https://en.wikipedia.org/wiki/Firewall_\(computing\)](https://en.wikipedia.org/wiki/Firewall_(computing)). [Accessed: 02-2022]
- [138] "NAT Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/Network_address_translation. [Accessed: 02-2022]
- [139] "UPnP Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/Universal_Plug_and_Play. [Accessed: 02-2022]
- [140] "PCP Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/Port_Control_Protocol. [Accessed: 02-2022]
- [141] "NAT-PMP Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/NAT_Port_Mapping_Protocol. [Accessed: 02-2022]
- [142] "DHT Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/Distributed_hash_table. [Accessed: 02-2022]
- [143] "Tendermint Peer discovery website." [Online]. Available: <https://docs.tendermint.com/master/spec/p2p/node.html>. [Accessed: 2022]
- [144] K. Ito, K. Tago, and Q. Jin, "i-Blockchain: a Blockchain-empowered individual-centric framework for privacy-preserved use of personal health data," in *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*, 2018, pp. 829–833.
- [145] A. Act, "Health insurance portability and accountability act of 1996," *Public law*, vol. 104, p. 191, 1996.

ЛИСТА НА ИЗРАБОТЕНИ ТРУДОВИ

Журнали:

- [1] J. Karamachoski and L. Gavrilovska, "Design of the functional entities of the BloHeS system," *Journal of Electrical Engineering and Information Technologies*, vol. 7, no. 1, 2022. [Accepted]
- [2] J. Karamachoski and L. Gavrilovska, "An optimal storage organization for Blockchain-based Public Healthcare System," *Journal of Electrical Engineering and Information Technologies*, vol. 5, no. 2, pp. 143–152, 2020.
- [3] V. Rakovic, J. Karamachoski, V. Atanasovski, and L. Gavrilovska, "Blockchain paradigm and Internet of Things," *Wireless Personal Communications*, vol. 106, no. 1, pp. 219–235, 2019. (IF=1.671)

Конференции:

- [4] J. Karamachoski and L. Gavrilovska, "BloHeS Consensus Mechanism – Introduction and Performance Evaluation," in *International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures (FABULOUS)*, Zagreb, Croatia, May 2022
- [5] J. Karamachoski and L. Gavrilovska, "BloHeS Island Management Protocol," in *International Conference on Information Society and Technology*, Kopaonik, Serbia, March 2022
- [6] J. Karamachoski and L. Gavrilovska, "Tendermint Performance with Large Transactions: The Healthcare System Scenario," in *International Balkan Conference on Communications and Networking (BalkanCom)*, Novi Sad, Serbia, September 2021, pp. 85–89.
- [7] J. Karamachoski and L. Gavrilovska, "Extended Performance Evaluation of the Tendermint Protocol," in *ETAI 2021 Conference Proceedings*, Online conference, 2021, vol. 2, pp. 231–236.
- [8] J. Karamachoski, "The end of the Blockchain as we know it," *Computer science and technologies, ACT 2019*, Varna, Bulgaria, vol. 17, no. 1/2019, pp. 52–56, 2019.
- [9] J. Karamachoski and L. Gavrilovska, "Toward scalable architecture for the next generation Blockchain-based healthcare systems," in *Proceedings of the Conference Balkancom 2019*, Skopje, North Macedonia, 2019, pp. 1–5.
- [10] J. Karamachoski and L. Gavrilovska, "Framework for next generation of digital healthcare systems," in *International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures (FABULOUS)*, Sofia, Bulgaria, 2019, pp. 12–24.
- [11] J. Karamachoski, L. Gavrilovska, and A. Sefidanoski, "The fusion between Blockchain and IoT for healthcare systems," in *ETAI conference*, Struga, Republic of Macedonia, 2018, pp. 1–6.

Работилници:

- [12] J. Karamachoski, "Graph theory to help the future Blockchain," *COSTNET ECT Training school*, Munich, Germany, 2019.