ОСОБЕННОСТИ И ПЕРСПЕКТИВЫ РЕАЛИЗАЦИИ БАНКОВСКИХ СИСТЕМ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ НА ТЕХНОЛОГИИ БЛОКЧЕЙН

М.Ю. Федосенко, *Национальный исследовательский университет ИТМО, fedosenkomaksim98@gmail.com.*

УДК 004.056

Аннотация. Цель данной работы – установить возможность реализации систем противодействия мошенничеству на децентрализованных системах. В работе рассматриваются особенности разработки банковских систем выявления мошенничества на технологии блокчейн. На основе сравнительного анализа результатов использования технологии блокчейн в промышленных системах крупными отечественными компаниями установлены перспективы и особенности использования данной технологии в системах дистанционного банковского обслуживания. В результате выбрана оптимальная для реализации системы блокчейн-платформа и установлен состав информации для блоков транзакций.

Ключевые слова: блокчейн; *Waves Enterprise;* системы дистанционного банковского обслуживания; антифрод; транзакции.

FEATURES AND PROSPECTS FOR IMPLEMENTATION OF ANTI-FRAUD BANKING SYSTEMS USING BLOCKCHAIN TECHNOLOGY

M. Fedosenko, *engineer at the Faculty of Security Information Technology ITMO University, postgraduate.*

Annotation. The purpose of this work is to establish the possibility of implementing anti-fraud systems on decentralized systems. The paper discusses the features of developing banking fraud detection systems using blockchain technology. Based on the results of a comparative analysis of the results of using blockchain technology in industrial systems by large domestic companies, the prospects and features of using this technology in remote banking systems have been established. As a result, the most optimal platform for implementing the blockchain system was selected and the composition of information for transaction blocks was established.

Keywords: blockchain; Waves Enterprise; remote banking systems; antifraud; transactions.

Введение

Направлением научного поиска, описанного в данной работе, является определение возможностей и особенностей реализации систем противодействия мошенничеству на децентрализованных системах с целью улучшения процесса работы систем выявления мошенничества. Задачами исследования является установление конкретной платформы, с учетом ее возможностей и соответствия законодательству РФ, а также определение конкретной информации транзакций о помещении в блок, хешировании и обработке в рамках децентрализованной системы.

Распределенные реестры блокчейн

Технология распределенных реестров блокчейн появилась в 2009 г. в качестве основной составляющей криптовалюты *Bitcoin* [1]. Однако, в настоящее время распределенные реестры активно используются в производственной сфере,

а также изучаются и улучшаются в научной. Распределенные реестры используются в следующих отраслях и компаниях, представленных в табл. 1 [2]:

Таблица 1.

Отрасли	Компании
• Криптовалюта • Банковское дело • Удостоверение личности • Документооборот • Кибербезопасность	• ПАО «ГМК «Норильский никель» • ПАО «Газпром» • ПАО «Сбербанк» • АО «Авиакомпания «Сибирь» • ПАО «Сбербанк» • АО «Дом РФ» • ПАО «Банк ВТБ» • ООО «Банк России» • АО «Альфа банк» • *X*5 *Retail Group* • Госкорпорация «Роскосмос»

Особое внимание стоит уделить разработкам в финансовой сфере – блокчейн-лаборатории ПАО «Сбербанк» и АО «Альфа банк». Основные результаты для АО «Альфа банк» представлены ниже [2]:

1. Полностью внедрена технология распределенных реестров для работы с самозанятыми лицами.
2. Документооборот и отчетность для ФНС реализован на *Waves Enterprise* [3].
3. В 2019 г. запущен сервис *Distributed Treasure and Cash Management* (*DTCM*) совместно с *X*5 *Retail group*.
4. Реализована возможность прямого взаимодействия при покупке билета с *S*7 *Airlines* через блокчейн [4].

Характеристика результатов внедрения блокчейн в производственные процессы ПАО «Сбербанк» представлена ниже [2]:

1. Создана собственная лаборатория по разработке и тестированию распределенных систем [5].
2. Прорабатывается перевод всех банковских операций на блокчейн [6].
3. Тестирован «Мастерчейн» на этапе ее разработки [7].
4. Ведутся переговоры с Центральным банком (ЦБ) о получении криптовалютой «Сберкоин» правового статуса [8].
5. Разрабатывается собственный блокчейн-стартап «*Crypterium*».

На данный момент проведено исследование актуальности разработок в данной области, опирающееся на информацию об имеющемся прогрессе внедрения распределенных решений в крупных отечественных компаниях. На основании полученных данных был произведен сравнительный анализ приватных блокчейн-платформ, использовавшихся упомянутыми компаниями для реализации их распределенных разработок – *Waves Enterprise*, Мастерчейн, *Hyperledger* [3, 9, 10]. Были выявлены достоинства и недостатки, соответствие требованиям в области информационной безопасности в рамках законодательства РФ, возможности их использования для реализации платежных сервисов.

В результате проведенного анализа, представленного в работе [2], наиболее подходящей под особенности банковских транзакций и удовлетворяющей требованиям законодательства РФ в области криптографии [11] оказалась *Waves Enterprise*. Данная платформа, за счет своих особенностей, оказалась соответствующей всем требованиям для реализации системы противодействия

мошенничеству и хранения данных. Архитектурная схема ее составляющих представлена на рис. 1.

Данная платформа была протестирована такими финансовыми организациями, как ПАО «Сбербанк» и АО «Альфа банк».

Что касается случаев конкретных использований распределенных платформ данными компаниями, то у ПАО «Сбербанк» большинство имеющихся сервисов реализовано на платформе *Hyperledger* [10], которая является иностранной разработкой и не соответствует требованиям безопасности для работы с критически важной информацией в рамках законодательства РФ. Помимо прочего, в 2016 г. Сбербанком было протестировано использование платформы «Мастерчейн», которую разработала Ассоциация «ФинТех» [12] для возможности работы с юридически важной информацией в соответствии с нормами законодательства РФ. В результате было принято решение отказаться от нее в силу низкого быстродействия. Поскольку системы противодействия мошенничеству должны обрабатывать информацию в режиме реального времени, то необходимо поискать более производительное решение.

У АО «Альфа банк» первоначальная тестовая реализация сервисов осуществлялась на *Hyperledger Fabric*, однако необходимость обработки юридически важной платежной информации самозанятых лиц вынудила впоследствии отказаться от ее использования. Поэтому, в настоящее время распределенные сервисы данной компании реализованы на отечественной платформе *Waves Enterprise*, которая обладает следующими преимуществами [2]:

1. Сертификат № 3796/2020 в рамках программы технологического партнерства «*Ready for Astra Linux*» [13].
2. Наличие смарт-контрактов.
3. Референтное хранение данных.

Таким образом, выбор данными финансовыми организациями платформы *Waves Enterprise* для реализации на ней технических сервисов осуществлен экспериментальным путем и обусловлен прежде всего ее быстродействием, удобством использования под конкретные наборы финансовых данных, соответствием требованиям законодательства РФ.

Определение состава блока распределенной системы на основе характеристик наборов данных банковских транзакций

Что касается задачи исследования, а именно реализации системы противодействия финансовому мошенничеству на распределенной системе блокчейн, то имеются следующие ключевые подходы:

1. Блоки представляют собой транзакции, которые осуществляются в криптовалюте.
2. Блоки представляют собой какую-либо информацию (например, платежную), необходимую для выявления и предотвращения мошенничества.

Что касается криптовалют, то на данный момент они не имеют правового статуса в Российской Федерации. ПАО «Сбербанк» активно ведет переговоры с Центральным банком РФ о достижении правового статуса собственной криптовалюты «Сберкоин», однако сроки и успешность окончания переговоров на данный момент предсказать сложно [8]. Также, имеется противоречивое суждение о действительной необходимости предотвращения мошенничества при осуществлении платежей в криптовалюте, поскольку в блокчейн подтверждение легитимности записи подтверждают все остальные блоки системы за счет подсчета

хеш-значений и наличия смарт-контрактов. Однако, имеется перечень действующих атак на данные системы в рамках информационной безопасности, например, атака 51% [14]. Несмотря на сложность ее реализации, киберпреступники ведут поиски новых уязвимостей системы. К тому же, транзакции, осуществленные при помощи применения социальной инженерии и в процессе легализации (отмывания) доходов являются вполне себе легитимными для системы, что приведет к ошибкам второго рода [15].

Что касается хранения информации, то тут стоит рассматривать именно транзакции, поскольку хранение и последующая обработка хэш-значений пользовательского поведения не даст результатов, в силу особенностей алгоритма получения хэша. Однако, в данном случае стоит определить – в каком количестве хранение транзакций позволит производить обработку в режиме реального времени в рамках промышленных систем.

На данный момент разработан концепт реализации системы противодействия мошенничеству на распределенных реестрах. Установлено, что в хешированные блоки информации целесообразнее помещать сами транзакции, нежели модели пользовательского поведения и модели искусственного интеллекта. Архитектурная схема распределенного блока с указанием этапов, требующих исследование, представлена на рис. 2 [1].

На схеме цифрами отражены основные проблемы, поиск технического решения которых является задачами данного исследования. В контексте данной работы необходимо проработать следующие вопросы, исследование которых позволит выяснить потенциальную возможность реализации систем противодействия мошенничеству на распределенных реестрах:

1. Какие правила взаимосвязи блоков использовать и на какой платформе реализовать систему?
2. Что именно стоит поместить в блоки информации и в каком количестве?
3. Какую именно информацию хэшировать и каким алгоритмом?
4. Какие протоколы использовать для взаимосвязи блоков?

В результате исследовательской работы, заключающейся в анализе литературы и документаций, а также изучении особенностей приватных блокчейн-платформ (в частности, *Waves Enterprise*), были получены следующие результаты, являющиеся ответами на поставленные в задачах исследования вопросы:

1. Система должна удовлетворять требованиям российского законодательства в области хранения и обработки данных, а также обеспечивать достаточную производительность для работы с высокой нагрузкой в режиме реального времени.
2. Помещать на первоначальном этапе стоит информацию о платежах в хэшированном виде в количестве, позволяющем работать конкретному блоку без перебоев и готовностью выдержать масштабирование системы в целом.
3. Хэшировать необходимо непосредственно совокупность всех реквизитов платежа, а также метки их легитимности при помощи ГОСТ алгоритмов.
4. Использовать протокол, который поддерживает конкретная платформа при соответствии его требованиям безопасности.

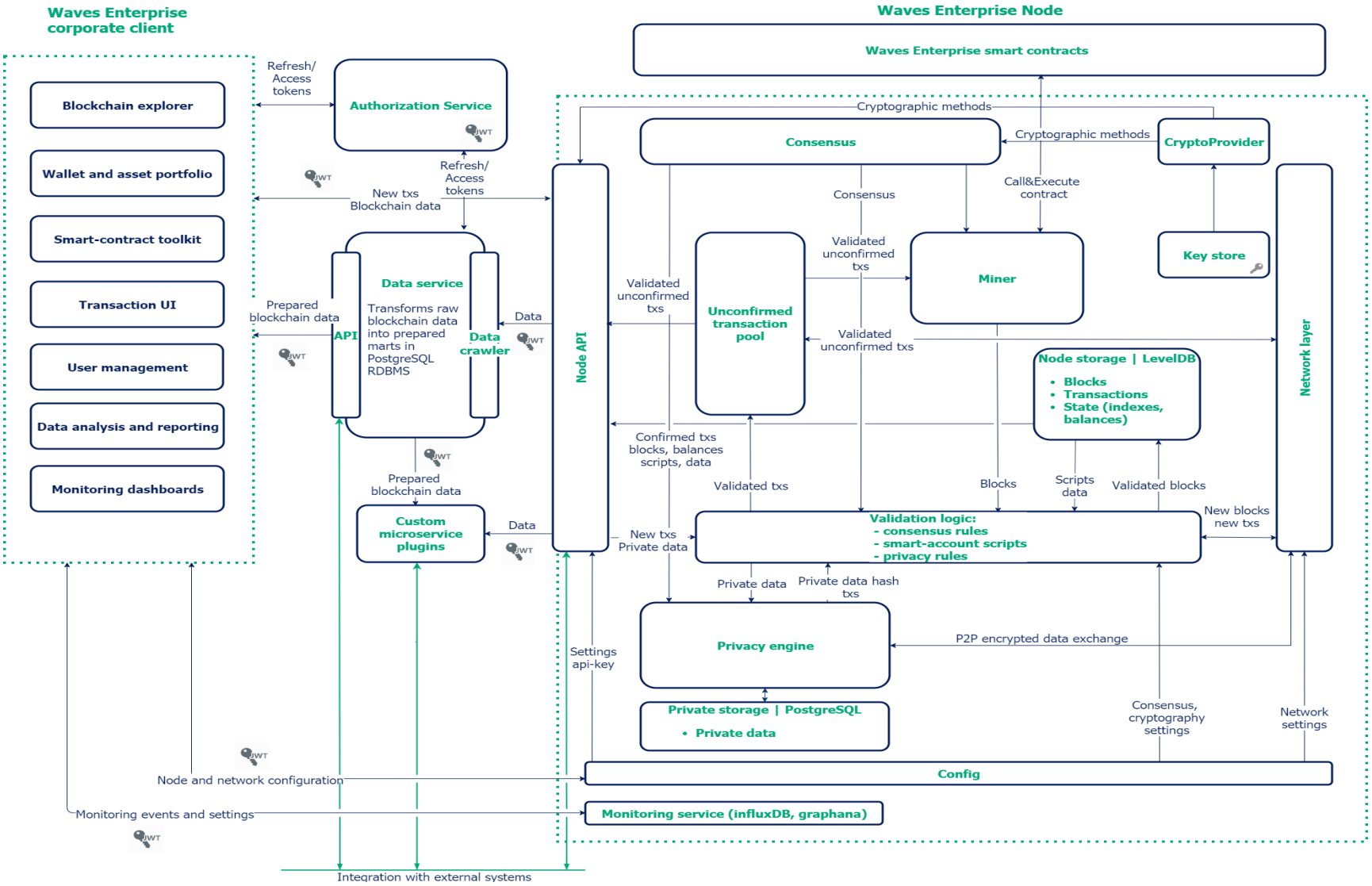
Waves Enterprise corporate client
Blockchain explorer
Wallet and asset portfolio
Smart-contract toolkit
Transaction UI
User management
Data analysis and reporting
Monitoring dashboards
Refresh/ Access tokens
Authorization Service
JWT
Refresh/ Access tokens
New txs Blockchain data
Prepared blockchain data
API
Data service
Transforms raw blockchain data into prepared marts in PostgreSQL RDBMS
Data crawler
Data
Prepared blockchain data
Custom microservice plugins
Data
Node and network configuration
Monitoring events and settings
Integration with external systems
Waves Enterprise Node
Waves Enterprise smart contracts
Cryptographic methods
Consensus
Cryptographic methods
CryptoProvider
Consensus
Call&Execute contract
Key store
Node API
Validated unconfirmed txs
Unconfirmed transaction pool
Validated unconfirmed txs
Miner
Validated unconfirmed txs
Network layer
Node storage | LevelDB
Blocks
Transactions
State (indexes, balances)
Confirmed txs blocks, balances scripts, data
Validated txs
Blocks
Scripts data
Validated blocks
New blocks new txs
New txs Private data
Validation logic:
- consensus rules
- smart-account scripts
- privacy rules
Private data
Private data hash txs
Settings api-key
Privacy engine
P2P encrypted data exchange
Private storage | PostgreSQL
Private data
Consensus, cryptography settings
Network settings
Config
Monitoring service (influxDB, graphana)

Рисунок 1

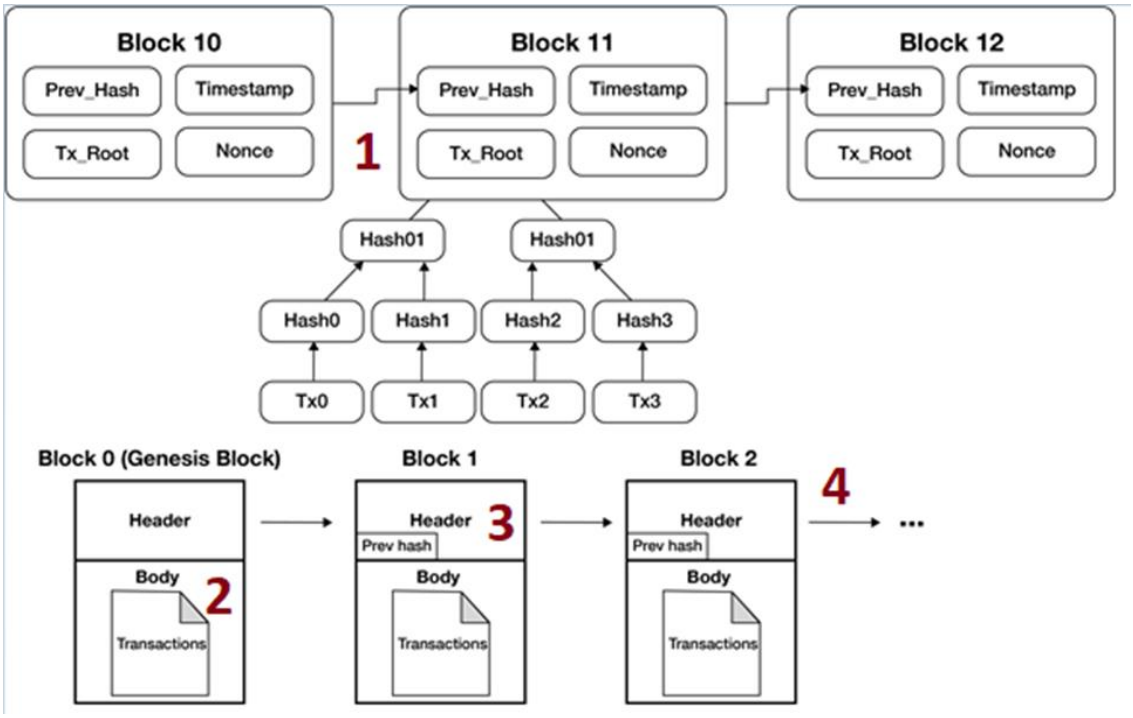

Рисунок 2

Заключение

Таким образом, в качестве дальнейшего направления научно-исследовательской деятельности была актуализирована задача практической реализации системы противодействия мошенничеству на распределенных реестрах. В данной работе был произведен аналитический обзор используемых отечественными компаниями приватных блокчейн-платформ в производственных процессах. Выбрана наиболее перспективная платформа по защите данных и возможности работать с юридически важной информацией – *Waves Enterprise*. Выдвинуты гипотезы состава блока транзакций на основе обрабатываемых данных в банковской системе противодействия мошенничеству. Основная идея заключается в хранении и хэшировании пользовательских транзакций, состоящих из совокупности реквизитов платежа и характеристик участников процесса.

Реализация хранения наборов данных транзакций на блокчейн позволит защитить их от подмены, атак, направленных на реализацию помех в работы систем искусственного интеллекта, *DOS/DDOS* атак на централизованный сервер хранения и обработки данных. В дальнейшем, данная реализация позволит работать и выявлять мошенников с платежами в криптовалюте, в том числе, осуществляемые в «Сберкоинах» после признания ЦБ РФ официального статуса криптовалют [16].

Литература

1. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. – 9 p.
2. Беззатеев С.В., Федоров И.Р., Федосенко М.Ю. Перспективы внедрения технологии блокчейн в производственные процессы отечественных компаний // Проблемы информационной безопасности. Компьютерные системы, 2022. – № 3. – С. 96-120.
3. Waves Enterprise - grade hybrid blockchain platform. URL: https://wavesenterprise.com/ (дата обращения – январь 2024 г.).

4. Блокчейн для агентов S7 Airlines. – АО «Альфа банк». URL: https://alfacorp.digital/dlt (дата обращения – январь 2024 г.).
5. Лаборатория блокчейн СберБанка. Уникальная инновационная лаборатория, которая изменит мир. – ПАО Сбербанк. – URL: https://www.sberbank.ru/ru/person/promo/blockchain (дата обращения – январь 2024 г.).
6. Блокчейн добрался до сбербанка. – Дмитрий Шустов (EX4.ru). – URL: https://ex4.ru/blokchejn/blokchejn-dobralsya-do-sberbanka (дата обращения – январь 2024 г.).
7. Цифровой актив в блокчейне. Исследуйте доступные возможности децентрализованных приложений – ПАО Сбербанк. URL: https://sbercoin.one/ (дата обращения – январь 2024 г.).
8. Криптовалюта от СберБанка: дата выхода в России и особенности монеты. – Ищенко Виталий (Crypto.ru). – URL: https://crypto.ru/kriptovalyuta-ot-sberbanka/ (дата обращения – январь 2024 г.).
9. «Мастерчейн» – первый юридически чистый блокчейн - Ассоциация ФинТех. URL: http://masterchain.rbc.ru/ (дата обращения – январь 2024 г.).
10. Hyperledger Foundation. Building enterprise blockchain ecosystems through global, open-source collaboration. URL: https://www.hyperledger.org/ (дата обращения – январь 2024).
11. Ахрамеева К.А., Федосенко М.Ю. Защита информации методами криптографии в современной России // Студенческий научно-образовательный журнал «StudNet», 2020. – Т. 3. – № 9.
12. Возможности использования blockchain для разработки финансовых сервисов Мастерчейн как первая сертифицированная платформа - ФинТех Ассоциация. URL: https://www.osp.ru/netcat_files/userfiles/Blokcheyn_2018/Konkin_blockchain_2018.pdf (дата обращения – январь 2024).
13. Astra Linux. Waves Enterprise ПО - 1.3.1. - ООО «РусБИТех-Астра». URL: https://astralinux.ru/ready-for-software/waves-enterprise-po/waves-enterprise-po-1.3.1 (дата обращения – январь 2024).
14. Атака 51% – Binance Academy. URL: https://academy.binance.com/ru/glossary/51-percent-attack (дата обращения – январь 2024).
15. Менщиков А.А., Федосенко М.Ю. Возможности применения методов социальной инженерии в организации телефонного мошенничества // Экономика и качество систем связи, 2021. – № 4 (22). – С. 36-47.
16. Федосенко М.Ю. Разработка модели поведения злоумышленника, осуществляющего действия по легализации доходов, применительно к автоматизированным банковским системам дистанционного обслуживания // Экономика и качество систем связи, 2022. – № 4 (26). – С. 53-61.