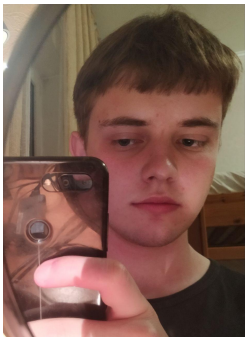
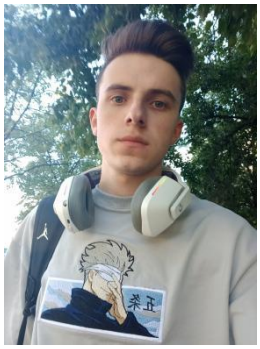
УДК 336.711:004.056.55

БЛОКЧЕЙН И ЭФФЕКТИВНОСТЬ ЦИФРОВЫХ ПЛАТЕЖНЫХ СИСТЕМ





Е. А. Гриз
Инженер-программист ОИТ ЦИИР
evgeniy.hryz@gmail.com

С.Н. Нестеренков
Кандидат технических наук, доцент, декан факультета компьютерных систем и сетей
s.nesterenkov@bsuir.by

Д.В. Кишкевич
Инженер-программист ОИТ ЦИИР
dkishkevich6@gmail.com

Е.А. Гриз
Окончил Белорусский государственный университет информатики и радиоэлектроники в 2022 году по специальности «Вычислительный машины системы и сети». Инженер-программист в отделе информационных технологий ЦИИР БГУИР.

С.Н. Нестеренков
Кандидат технических наук, доцент, декан факультета компьютерных систем и сетей Белорусского государственного университета информатики и радиоэлектроники, доцента кафедры программного обеспечения информационных технологий. Автор публикаций на тему машинного обучения, алгоритмов принятия решений, искусственных нейронных сетей и автоматизации.

Д.В. Кишкевич
Окончил Белорусский государственный университет информатики и радиоэлектроники в 2022 году по специальности «Вычислительный машины системы и сети». Инженер-программист в отделе информационных технологий ЦИИР БГУИР.

Аннотация. Блокчейн технология, впервые представленная в криптовалютах, ныне становится катализатором существенных изменений в мире финансовых транзакций. Данная статья стремится определить недостатки, характерные для традиционных платежных систем, и рассмотреть технологию блокчейн и ее реализацию в криптовалютах, как потенциальное решение этих недостатков. Статья показывает как преимущества блокчейн-систем, так и новые проблемы, возникающие при использовании этой технологии в платежных системах.

Ключевые слова: Блокчейн, криптовалюты, *Bitcoin*, платежные системы.

Введение. С распространением использования интернета для совершения покупок и интернет-банкинга цифровые платежные системы стали все более популярными. При осуществлении покупок в интернете всегда вовлечены цифровые транзакции. Наиболее распространенным случаем транзакции является банковская операция по оплате банковской платёжной картой в торгово-сервисном предприятии. Обмен какого-либо товара на цифровой платеж с помощью банковской карты состоит из следующих этапов:

1 Инициатор транзакции (потребитель) использует платежную карту для оплаты

товара/услуги. Платежную карту выпускает банк-эмиттер.

2 Платежная карта считывается подходящим терминалом, терминал обслуживается банком-эквайером, с которым владелец торговой точки заключил соглашение. Данные карты отправляются в банк-эквайер с целью аутентификации. Далее, информация передается от банка-эквайера в платежную систему, обслуживающую соответствующую карту. В платежной системе проводится проверка наличия платежных данных карты в стоп-листе, и в зависимости от результата транзакция либо отклоняется, либо одобряется. В случае одобрения, она направляется в банк-эмитент, выпустивший карту и обслуживающий связанный с ней банковский счет клиента.

3 Затем уже в банке-эмитенте проводится процесс авторизации для подтверждения того, что карту использует тот человек, которому она принадлежит. Происходят проверки остатка средств на банковском счете клиента или платежного лимита. Если все проверки пройдены успешно, операциия одобряется эмитентом, и ответ отправляется в торговую точку.

4 Эмитент переводит эквайеру сумму запрашиваемых средств по транзакции и комиссию платежной системы за ее обработку. В это время с клиентского счета списывается оплаченная клиентом сумма (для дебетовых карт) или уменьшается доступный кредитный лимит (для кредитных карт).

5 Транзакция считается завершенной, когда в торговую точку приходит ответ с результатом (одобрение или отказ).

Зачастую транзакции требуют отправку персональных данных для авторизации и валидации перечисляемых средств, а также для того, чтобы зарегистрировать транзакцию.

Каждая транзакция между участниками записывается организацией в реестре (*ledger*), ведущей учет транзакций. В каждой записи о транзакции содержатся конфиденциальные данные. В эти данные может входить: идентификация товара, участвующего в обмене, реквизиты для авторизации, сумма перечисляемых средств. По данным транзакции легко можно установить личности участников, или определить организацию-участник. Это свойство доступно для всех участников транзакции.

Помимо этого, у каждого участника может быть свой реестр транзакций. В таком случае будет записано несколько версий транзакции в разных местах.

Процессинг платежных карт требует вычислительные, сетевые ресурсы, память, а также техническую поддержку и менеджмент. Все это означает расходы, которые в конечном итоге передаются для оплаты потребителю.

В этих условиях возникает необходимость в едином учете транзакций, способному зашифровывать передаваемые данные, свести к минимуму обмен конфиденциальной информацией, а также избавиться от необходимости сторонней валидации. Все эти проблемы может решить блокчейн-технология.

Основная цель этой статьи – общее описание блокчейн-технологии, ее использование в системах обработки платежей. Показаны преимущества платежных систем, основанных на блокчейн-технологии над традиционными платежными системами.

Блокчейн технология. Блокчейн – это распределенная технология учета транзакций. Технология основана на хранении данных в виде последовательности блоков, такая структура данных называется цепочкой блоков. При этом каждый следующий блок создается на основе предыдущего с использованием криптографического хеша.

Блокчейн-технология устраняет необходимость в сторонней валидации и верификации участников и данных.

Структура данных блокчейн. Блокчейн представляет собой связанный список блоков, представляющий всю историю транзакций системы. Все транзакции записываются группами в блоках, в заголовке блока есть момент времени создания транзакции, хеш-указатель на предыдущий блок и другая информация. Хеш-указатель

рассчитывается на основе заголовка предыдущего блока. Таким образом, изменение данных в блоке приведет к изменению хеша этого блока, а, следовательно, изменению всех последующих блоков в списке. То есть изменение транзакции не останется незамеченным в цепочке.

Протокол консенсуса. Консенсус – это процесс, согласно которому распределенная система соглашается об определенном решении. Существует несколько способов определения участников консенсуса:

1 *Proof of Authority* (*PoA*) – участники консенсуса определяются заранее.

2 *Proof of Stake* (*PoS*) – участники консенсуса определяются динамически, основываясь на том, у кого есть больше всего цифровой валюты.

У криптовалюты *Bitcoin* [1] набор участников заранее неизвестен, поэтому здесь используется другой механизм определения участников консенсуса. Он основан на концепте *Proof Of Work* (*PoW*) – криптографическое доказательство, которое подтверждает, что определенная сторона затратила некоторые вычислительные усилия.

Открытые и закрытые блокчейн-системы. В открытых (*permissionles*) блокчейн-системах любой желающий может обрабатывать и отправлять транзакции, а также участвовать в консенсусе. Одним из реализаций открытого блокчейна является криптовалюта *Bitcoin*, любой может присоединиться к сети и участвовать в процессе консенсуса. Для участия в закрытых блокчейн системах (*permissioned*) необходимо приглашение, администраторы сети могут определять кто может читать записи транзакций, кто может отправлять их, и кто может участвовать в процессе консенсуса.

Открытые блокчейн-системы обычно поддерживают огромные реестры транзакций, что сказывается на объеме ресурсов нужных для их обработки. В закрытых системах только определенные узлы сети могут участвовать в процессе консенсуса, поэтому такие системы более безопасны.

Процесс обработки транзакций в блокчейн-системе *Bitcoin*. В *Bitcoin* процесс консенсуса заключается в определении того узла, который предложит следующий блок для добавления в блокчейн. При этом чтобы добавление прошло успешно, все остальные узлы должны признать этот блок валидным.

Если каждый участник сети сможет предлагать изменения в блокчейн, то это приведет к слишком большому числу конфликтующих предложений для добавления. Для этого процесса должен быть выбран только один участник, выбор происходит путем вычисления хеш-значения от блока транзакции меньше определенного порогового значения. Первый участник, который подберет хеш, удовлетворяющий условию, получит право на предложение нового блока. Такие участники называются майнерами.

Величина числа, с которым сравнивается очередной хеш постоянно корректируется. Это сделано для того, чтобы скорость обработки транзакций не зависела от общей вычислительной мощности сети *Bitcoin*.

Майнеры получают за свою работу вознаграждение в виде комиссии, которая списывается со счета инициатора транзакции. При этом инициаторы транзакций могут сами назначать размер комиссии. Поэтому высокая комиссия для майнеров в транзакции повышает шансы на то, что транзакция будет добавлена в следующий блок.

Рассмотрим взаимодействие участников децентрализованной сети в процессе обработки транзакций в криптовалюте *Bitcoin*.

1 Пользователь отправляет информацию о транзакции на сервер децентрализованной сети.

2 Сервера получают транзакции и перенаправляют их дальше. Транзакции распространяются по сети и достигают майнеров, которые в свою очередь формируют из этих транзакций блоки. Блок включает в себя заголовок и список транзакций. Заголовок блока содержит свой уникальный хеш, хеш предыдущего блока, а также хеши транзакций.

Для хеширования транзакций используется дерево Меркла [2]. Деревом Меркла называется структура данных, используемая для эффективного хранения хеш-значений транзакций. Это дерево представляет собой полное двоичное дерево, в листьях которого содержатся хеш-значения отдельных транзакций, в остальных вершинах содержатся хеши от сложения значений в дочерних вершинах.

3. Сервер отправляет блок остальным участникам сети, которые валидируют блок. Если остальные участники не нашли ошибок в блоке, то блок добавляется каждым участником в блокчейн.

Возможна ситуация, когда два разных майнера одновременно добавят разные блоки в блокчейн, такое называется ветвлением (*fork*). Для решения этой проблемы в *Bitcoin* есть два механизма:

1 Корректирование сложности подбора хеша для нового блока. Если блоки создаются слишком быстро или слишком медленно, то сложность подбора хеша будет увеличена или уменьшена.

2 Единый для всех участников порядок действий в случае появления разветвления в цепочке. По правилам *Bitcoin* цепочка с наибольшим количеством проделанной работы (самая длинная цепь) считается правильной, а другая ветвь должна быть исключена из блокчейн [3]. Учитывая это, если транзакция попала в новый блок, это не означает, что блок окончательно помещен в цепочку. Позднее цепочка может быть реорганизована из-за того, что ранее произошло разветвление.

Аутентификация пользователей в *Bitcoin*. В криптовалюте *Bitcoin* нет традиционных имени пользователя и пароля для входа в аккаунт, с которым связан счет. Вместо этого каждый пользователь генерирует пару из закрытого и открытого ключей. Закрытый ключ используется для цифровой подписи транзакций, которые создаются пользователем. Для идентификации аккаунта используется открытый ключ, он также нужен остальным участникам сети для того, чтобы они могли отправлять средства на этот аккаунт.

Преимущества использования блокчейн-технологии в платежных системах.

1 Прозрачность и доступность данных. В блокчейн-системах все транзакции доступны всем участникам системы, помимо этого записи в блокчейн неизменяемые. Неизменяемая цепочка транзакций в блокчейне обеспечивает точный учет финансовых операций и упрощает процессы аудита. Прозрачность блокчейн-систем позволяет быстро и надежно проводить аудит, что является важным элементом финансовой отчетности.

2 Децентрализация. Одним из главных преимуществ блокчейна является децентрализация. Вместо централизованных структур, блокчейн распределяет данные о транзакциях по всей сети узлов, что делает систему устойчивой к отказам. Отсутствие единой точки отказа обеспечивает более высокий уровень доступности и надежности, что критично для систем обработки платежей. Децентрализация позволяет избавиться от промежуточных финансовых организаций, участвующих в централизованных системах обработки платежей. Это приводит к уменьшению затрат на обработку транзакций.

3 Безопасность и устойчивость. Благодаря применению криптографии, блокчейн обеспечивает высокий уровень безопасности. Каждая транзакция защищена и неизменна, что существенно снижает риски несанкционированного доступа и атак.

4 Смарт-контракты и автоматизация. Смарт-контракты, программируемые условия соглашений, предоставляют автоматизированный механизм выполнения обязательств при определенных условиях. В системах обработки платежей это означает более эффективную обработку транзакций, исключение необходимости в промежуточных структурах и снижение риска человеческих ошибок.

Проблемы при использовании блокчейн-технологии в платежных системах:

1 Нестабильность. Рынки криптовалют подвержены резким колебаниям цен,

которые могут происходить в короткие сроки. Эта нестабильность создает неопределенность и риски как для инвесторов, так и для пользователей криптовалютных платежных систем. В попытке решения этой проблемы некоторые криптовалюты привязывают цену одного токена к реальной валюте (*stablecoin*) [4].

2 Скорость обработки транзакций. Пропускная способность криптовалюты рассчитывается как число обрабатываемых транзакций в минуту. Окончательность (*finality*) – это время, которое требуется для того, чтобы транзакция была окончательно записана в блокчейн. Из-за того, что *Bitcoin* позволяет разветвления, окончательность у этой криптовалюты никогда не достигается. Должно пройти около одного часа, прежде чем вероятность того, что транзакция будет отменена, становится достаточно низкой.

3 Размер блокчейн. Одной из проблем многих криптовалют – это то, что размер всей истории транзакций быстро разрастается до больших размеров. Пользователи, которые просто хотят попробовать использовать криптовалюту, вынуждены сначала скачивать большой объем транзакций для взаимодействия с сетью.

4 Конфиденциальность. *Bitcoin* позволяет просмотреть всю историю транзакций аккаунта, если известен его открытый ключ. То есть единственное свойство анонимности, которое *Bitcoin* предоставляет – это то, что аккаунт привязан только к открытому ключу. До тех пор, пока никто не установил соответствие публичного ключа с реальным человеком, этот человек остается анонимным.

5 Энергоэффективность. Алгоритм консесуса *Bitcoin* требует больших затрат электроэнергии. В связи с этим, многие современные криптовалюты избегают консенсуса на основе *PoW*. На момент написания статьи (январь 2024) потребление электричества криптовалютой *Bitcoin* составило 0,73% от общего потребляемого электричества в мире [5].

Заключение. В статье было описано проведения транзакции с использованием банковской карты и показаны недостатки этого процесса. Была рассмотрена технология блокчейн как потенциальное решение проблем традиционных централизованных платежных систем. Блокчейн, в частности криптовалюты, решают некоторые проблемы централизованных платежных систем.

Работа блокчейна была рассмотрена на примере криптовалюты *Bitcoin*. Основное отличие *Bitcoin* от централизованных платежных систем – это ее децентрализованная аркитектура и возможность участия в сети для любого человека. Однако криптовалюты создают и ряд новых проблем: нестабильность курса, конфиденциальность, энергоэффективность.

Список литературы

[1] Bitcoin: A Peer-to-Peer Electronic Cash System // Bitcoin URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 29.01.2024).

[2] Wong D. Real-world cryptography. - 1-е изд. - Shelter Island, NY: Manning Publications Co., 2021. - 370 с.

[3] Vojislav B.M., Jelena M., Xiaolin C. On Forks and Fork Characteristics in a Bitcoin-Like Distribution Network // 2019 IEEE International Conference on Blockchain (Blockchain). - Atlanta, GA, USA: IEEE, 2019.

[4] Makiko M., Kensuke I., Shohei O., Hideyuki T What is Stablecoin?: A Survey on Price Stabilization Mechanisms for Decentralized Payment Systems // 2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI). - Toyama, Japan: IEEE, 2020.

[5] Cambridge Bitcoin Electricity Consumption Index // The Cambridge Centre for Alternative Finance URL: https://ccaf.io/cbnsi/cbeci (дата обращения: 29.01.2024).

Авторский вклад

Гриз Евгений Анатольевич – анализ недостатков традиционной платежной системы с участием финансовых организаций для обработки транзакций, исследование принципов работы современных криптовалют, подробное изучение механизма работы криптовалюты Bitcoin.

Кишкевич Дмитрий Витальевич – анализ преимуществ, возникающих при использовании технологии блокчейн в платежных системах, а также исследование возникающих при этом проблем.

Нестеренков Сергей Николаевич – формирование темы исследования, постановка задачи, подбор списка источников.

BLOCKCHAIN AND THE EFFICIENCY OF DIGITAL PAYMENT SYSTEMS

Y.A. Hryz
Software engineer of Information technologies department

S.N. Nesterenkov
PhD, Associate Professor, Dean of the Faculty of Computer Systems and Networks

D.V. Kishkevich
Software engineer of Information technologies department

Annotation. Blockchain technology, first introduced in cryptocurrencies, is now becoming a catalyst for significant changes in the world of financial transactions. This article seeks to identify the shortcomings inherent in traditional payment systems and examine blockchain technology and its implementation in cryptocurrencies as a potential solution to these shortcomings. The article shows both the advantages of blockchain systems and new problems that arise when using this technology in payment systems.

Keywords: blockchain, cryptocurrencies, Bitcoin, payment systems