УДК 004:338(045)
DOI 10.22213/2410-9304-2018-1-11-14

Р. А. Андреев, аспирант
П. А. Андреева, аспирант
Л. Н. Кротов, доктор физико-математических наук, профессор
Е. Л. Кротова, кандидат физико-математических наук, доцент
Пермский национальный исследовательский политехнический университет

ОБЗОР ТЕХНОЛОГИИ БЛОКЧЕЙН: ВИДЫ БЛОКЧЕЙНА И ИХ ПРИМЕНЕНИЕ

В современном IT-пространстве блокчейн находится в числе наиболее быстро развивающихся технологий. В первую очередь это связано с ростом рынка криптовалют, которые созданы на базе технологии блокчейн. Но это не единственное возможное применение данной технологии. Блокчейн является многопользовательской надежной книгой учета транзакций, которую каждый может проверить, но ни один отдельный пользователь не может контролировать.

Цель работы – анализ различных типов блокчейн технологии по различным параметрам (скорость работы, безопасность, условия доступа и другие).

В данной статье представлен обзор различных типов блокчейна и возможные варианты применения этой технологии. Подробно рассмотрены различные виды данной технологии: публичные, федеративные, частные и гибридные блокчейны. Частные блокчейны имеют важное значение для решения проблем, связанных с эффективностью, безопасностью и мошенничеством в рамках традиционных финансовых учреждений. В то же время публичные блокчейны обладают потенциалом для замены большинства функций традиционных финансовых учреждений программным обеспечением, главным образом переопределяя способ работы финансовой системы. Федеративные блокчейны являются более быстрыми и обеспечивают большую конфиденциальность транзакций. Гибридный блокчейн объединяет возможности масштабируемости распределенной базы данных с неизменяемыми элементами блокчейна. Раскрыты условия и правила работы с тем или иным типом блокчейна. Приведены примеры использования блокчейн-технологии для работы с криптовалютами. Представлены результаты сравнения публичных и частных блокчейнов по доступу, скорости, безопасности и идентификации.

Результаты обзора показали, что технология блокчейн все еще находится на ранних стадиях развития и имеет ряд проблем, требующих решения.

Ключевые слова: блокчейн, криптовалюта, биткоин, смарт-контракт, технология распределенного реестра.

Блокчейн – технология, лежащая в основе системы Биткоин, является многопользовательской надежной книгой учета транзакций, которую каждый может проверить, но ни один отдельный пользователь не может контролировать. Это распределенная база данных, поддерживающая постоянно растущий список записей данных транзакций, криптографически защищенных от изменений и фальсификации. Криптографические наборы правил протокола блокчейн (консенсусный слой) регулируют набор правил поведения и механизм стимулирования всех участников в сети.

Официальное описание системы Биткоин было опубликовано Сатоши Накамото в 2008 году [1], первый блок биткоина был добыт в 2009 году. Поскольку протокол биткоина является открытым исходным кодом, любой может использовать протокол, модифицировать (изменить код) и запустить собственную версию P2P-денег. Так появились так называемые альткоины, которые должны были быть лучше, быстрее или быть более защищенными, чем биткоин. Вскоре не только код был изменен для создания лучшей криптовалюты, но и саму идею блокчейна попытались изменить вне вариантов использования P2P-денег.

Была высказана идея о том, что блокчейн может фактически использоваться для любого рода сделок или соглашений, например P2P-страхования, P2P-торговли и т. д. Colored Coins и Mastercoin попытались решить эту проблему на основе биткоин-блокчейн-протокола. Проект Ethereum [2]

решил создать свой собственный блокчейн с различными свойствами, предлагая радикально новый способ создания онлайновых рынков и программируемых сделок с использованием смарт-контрактов. Смарт-контракт – это электронный алгоритм, описывающий набор условий, выполнение которых влечет за собой появление некоторых событий в реальном мире или цифровых системах. Для реализации смарт-контрактов требуется децентрализованная среда, полностью исключающая человеческий фактор, а для возможности использования в смарт-контракте передачи стоимости требуется криптовалюта.

Банки, в свою очередь, стали применять идею блокчейна в качестве технологии распределенного реестра (DLT) и создали контролируемый блокчейн (федеративный или частный), где подтверждающая сторона является членом консорциума или отдельным юридическим лицом той же организации. Термин «блокчейн» в контексте DLT является весьма противоречивым. Именно поэтому термин «технология распределенного реестра» превратился в более общий.

Частные блокчейны имеют важное значение для решения проблем, связанных с эффективностью, безопасностью и мошенничеством в рамках традиционных финансовых учреждений. Частные блокчейны не устроят революцию в финансовой системе. В то же время публичные блокчейны обладают потенциалом для замены большинства функций традиционных финансовых учреждений программным обеспечением, главным образом переопределяя способ работы финансовой системы.

Современное состояние публичных блокчейн-протоколов, основанных на доказательстве выполнения работы (POW), являются неконтролируемым открытым программным обеспечением, поэтому каждый может принимать участие в работе протоколов и исследовать их. Любой пользователь может загрузить код и начать работу с открытым узлом на своем локальном устройстве, проверяя транзакции в сети, тем самым участвуя в процессе определения того, какие блоки будут добавлены в цепочку, и их текущего состояния. Любой человек в мире может отправлять транзакции через сеть и ожидать, что они будут включены в блокчейн, если они подтверждены. Любой пользователь может прочитать транзакцию в открытом обозревателе блоков. Примеры: Bitcoin, Ethereum, Monero, Dash, Litecoin, Dodgecoin, Emercoin [3]. Эффекты: потенциальные возможности для выведения из строя текущих бизнес-моделей через дезинтермедиацию (отлив денежных ресурсов из кредитно-финансовых институтов, избавление от посредников); отсутствие затрат на инфраструктуру. Отсутствие необходимости в обслуживании серверов радикально снижает затраты на создание и запуск децентрализованных приложений (dApps).

Федеративные блокчейны действуют под руководством группы. В отличие от публичных блокчейнов они не позволяют какому-либо лицу, имеющему подключение к Интернету, участвовать в процессе проверки сделок. Федеративные блокчейны являются более быстрыми (более высокая масштабируемость) и обеспечивают большую конфиденциальность транзакций. Блокчейн-консорциумы в основном используются в банковском секторе. Процесс согласования контролируется заранее выбранным набором узлов. Например, можно представить консорциум по 15 финансовым учреждениям, каждый из которых использует узел и 10 из которых должны подписывать каждый блок, чтобы этот блок был действителен. Право на чтение блокчейна может быть публичным или ограничено участниками. Примеры: R3 (банки), EWF (электроэнергия), B3i (страхование), Corda. Эффекты: сокращает операционные издержки и избыточность данных и заменяет устаревшие системы, упрощая обработку документов и избавляясь от механизмов обеспечения соответствия с частичным ручным режимом; в этом смысле он может рассматриваться как эквивалентный SAP в 1990 году – сокращение затрат, но не разрушительное!

Технология блокчейн все еще находится на ранних стадиях развития. Неясно, каким образом эта технология будет применяться. Многие утверждают, что частные или федеративные блокчейны может постичь судьба интрасетей 1990-х годов, когда частные

компании строили свои собственные частные или глобальные сети вместо использования общедоступного Интернета, но эти сети в той или иной степени устарели, особенно с появлением SaaS в Web2 [4].

Разрешения на запись хранятся в централизованном порядке в одной организации. Разрешения на чтение могут быть открыты или ограничены в произвольном масштабе. Приложения включают в себя управление базами данных, аудит и другие внутренние операции одной компании, и поэтому во многих случаях публичное считывание может оказаться ненужным, хотя в других случаях желательно иметь возможность публичного аудита. Частный блокчейн – это способ использования преимуществ блокчейн-технологии путем организации групп и назначения участников, которые могут контролировать внутренние операции. Это ставит нас под угрозу нарушения безопасности, как в централизованной системе, в отличие от публичных блокчейнов, обеспечиваемых теоретико-игровыми механизмами стимулирования. Тем не менее частный блокчейн имеет свой вариант использования, особенно когда речь идет о масштабируемости и соблюдении государствами правил конфиденциальности данных и других нормативных вопросов. Такой тип блокчейна имеет определенные преимущества в плане безопасности, а также недостатки, как указано выше, в сравнении с публичными блокчейнами. Примеры: MONAX, Multichan. Сравнение публичного и частного блокчейна приведено в таблице.

Сравнение публичного и частного блокчейна

Показатель	Публичный	Частный
Доступ	Открытая запись/чтение	Контролируемая запись/ чтение
Скорость	Медленнее	Быстрее
Безопасность	POW, POS (Proof of Stake, с защитой по методу «подтверждение доли»)	Предварительно утвержденные участники
Идентификация	Анонимно/псвевдоанонимно	Определенные участники
Активы	Собственные ресурсы	Любые ресурсы

На основании проведенного анализа можно сделать вывод, что технология блокчейн еще имеет ряд проблем, требующих решения. Состояние современного публичного блокчейна в настоящее время имеет проблему масштабируемости, что означает, что сеть может обрабатывать только несколько транзакций в секунду, что делает их неосуществимыми для крупномасштабных приложений с большими объемами транзакций. Биткоин и Ethereum могут обрабатывать менее дюжины сделок в секунду, но только одна виза потребует 100 тысяч операций в секунду в пиковое время. BigchainDB [5], как гибридный блокчейн, объединяет возможности масштабируемости распределенной базы данных с неизменяемыми элементами блокчейна для решения этой проблемы на стороне базы данных. Возникают разногласия в том, можно ли технологию BigchainDB называть блокчейном. Однако она является важной в технологическом стеке распределенных вычислений и устраняет большую проблему масштабируемости. В настоящее время перестраивается структура данных для Web3, происходит переход от централизованных вычислений к децентрализованной/распределенной вычислительной технике и децентрализованной сети.

Библиографические ссылки

1. Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008 [Electronic resource]. URL: https://bitcoin.org/bitcoin.pdf (accessed: 23.09.2017).

2. *Buterin V.* Understanding Serenity, Part 2: Casper, 28 December 2015. [Electronic resource]. URL: https://blog.ethereum.org/2015/12/28/ understanding-serenity-part-2-casper (accessed: 23.09.2017).

3. List of cryptocurrencies [Electronic resource]. URL: https://en.wikipedia.org/wiki/ List_of_cryptocurrencies (accessed: 23.09.2017).

4. What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software [Electronic resource]. URL: http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html (accessed: 23.09.2017).

5. BigchainDB. The scalable blockchain database [Electronic resource]. URL: https://www.bigchaindb.com (accessed: 23.09.2017).

References

1. Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008 [Electronic resource]. URL: https://bitcoin.org/bitcoin.pdf (accessed: 23.09.2017).

2. *Buterin V.* Understanding Serenity, Part 2: Casper, 28 December 2015. [Electronic resource]. URL: https://blog.ethereum.org/2015/12/28/understanding-serenity-part-2-casper (accessed: 23.09.2017).

3. List of cryptocurrencies [Electronic resource]. URL: https://en.wikipedia.org/wiki/List_of_cryptocurrencies (accessed: 23.09.2017).

4. What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software [Electronic resource]. URL: http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html (accessed: 23.09.2017).

5. BigchainDB. The scalable blockchain database [Electronic resource]. URL: https://www.bigchaindb.com (accessed: 23.09.2017).

* * *

R. A. Andreev, Post-graduate, Perm National Research Polytechnic University

P. A. Andreeva, Post-graduate, Perm National Research Polytechnic University

L. N. Krotov, DSc **(**Physics and Mathematics), Professor, Perm National Research Polytechnic University

E. L. Krotova, PhD **(**Physics and Mathematics), Associate Professor, Perm National Research Polytechnic University

Review of Blockchain Technology: Types of Blockchain and Their Application

In today's IT space, blockchain is among the fastest growing technologies. First, it is connected with the growth of the crypto currency markets, which are based on blockchain technology. However, this is not the only possible appliance of this technology. Blockchain is a multi-user, reliable transaction ledger that everyone can verify, but no single person can control.

The purpose is to analyze different types of blockchain technology according to various parameters (speed, security, access conditions and others).

This paper provides an overview of the different types of blockchain and possible appliances for this technology. Different types of blockchain technology are considered in detail: public, federated, private and hybrid blockchain. Private blockchain is important for dealing with problems related to efficiency, security and fraud in traditional financial institutions. At the same time, public blockchain has the potential to replace most of the functions of traditional financial institutions with software, mainly by redefining the way the financial system works. Federated blockchain is faster and provide greater transaction confidentiality. The hybrid blockchain combines the scalability capabilities of a distributed database with immutable blockchain elements. Conditions and rules of work with one or another type of blockchain are revealed. Examples of using blockchain-technology for cryptocurrencies are given. The results of comparison of public and private blockchains on access, speed, security and identification are presented.

The survey showed that blockchain technology is still in its early stages of development and has a number of problems to be solved.

Keywords: blockchain, cryptocurrency, bitcoin, smart contract, distributed ledger technology.

Получено: 26.02.18