УДК 519.683

ВЫДЕЛЕНИЕ КЛЮЧЕВЫХ КОМПОНЕНТ ТЕХНОЛОГИИ БЛОКЧЕЙН НА ОСНОВЕ АНАЛИЗА РЯДА РЕАЛИЗАЦИЙ[1]

П. А. Сазонова

Технология блокчейн была впервые реализована в 2008 году, и за последние 12 лет в индустрии появилось более 2000 различных ее реализаций. Исследователи в мире рассматривают данную технологию либо в прикладном аспекте, либо улучшая ее отдельные компоненты. Такой фрагментарный подход приводит индустрию к проблеме отсутствия общей картины, что приводит к невозможности определения реальной ценности новой разработки и, как следствие, замедлению развития технологии. Целью данной работы является выделение ключевых компонент внутреннего устройства технологии блокчейн и предложение ее универсальной модели. На основе технического анализа наиболее популярных блокчейнов были выделены компоненты, присутствующие у всех блокчейнов и определена их роль при решении тех задач, для которых данный блокчейн разрабатывался. Результаты данной работы могут быть использованы архитекторами новых блокчейн-сетей для достижения целей их разработки.

Ключевые слова: *блокчейн, распределенный реестр, Ethereum, Bitcoin, EOS, NEO, Dash.*

Введение

Технология блокчейн получила широкое распространение за счет свойств открытости, неизменяемости и невозможности удаления хранимых данных, децентрализованности и возможности принятия решений в недоверенной среде между равноправными участниками сети без участия доверенной стороны. Тем самым найдя применение в самых разных предметных областях, особенно в логистике, банковском деле и процессах документооборота.

Определение 1. Блокчейн - это разновидность децентрализованных систем, которая занимается сбором, хранением и управлением данными, в которой:

— возможно достижение консенсуса в недоверенной среде;
— транзакции хранятся в структуре данных, называемой блоки и каждый последующий блок хранит значение хэш-функции от содержимого предыдущего;
— копии блокчейна хранятся одновременно у всех его пользователей и автоматически обновляются.

В данной работе под блокчейном понимается система, которая в качестве технологии хранения данных использует цепочку блоков, устройство которой обеспечивает неизменяемость и целостность хранимых в блоках данных. В отличие от централизованных систем, где возможно достижение консенсуса за счет центрального узла, технология блокчейн позволяет достигать консенсус в среде без центра. Более того, в блокчейн-системе консенсус может быть достигнут тогда, когда узлы сети не являются авторизованными, а значит, повышается вероятность появления в сети узлов злоумышленников, либо византийских узлов [1]. В децентрализованных сетях с неавторизованными (недоверенными) узлами возможно возникновение атаки Сибиллы [2],

[1]Работа выполнена при поддержке Математического Центра в Академгородке, соглашение с Министерством науки и высшего образования Российской Федерации номер 075-15-2019-1613 и лаборатории криптографии JetBrains Research.

когда узел, производящий вычисления, подключается только к узлам, контролируемым злоумышленником, что влечет за собой некорректное поведение и достижение консенсуса в принятии решения, выгодном злоумышленнику. Технология блокчейн позволяет принимать верные решения в децентрализованной сети с недоверенными узлами при условии, что 51% узлов не являются злоумышленниками.

Первая практическая реализация технологии блокчейн была осуществлена в 2008 году, она была описана в статье С. Накомото о первой цифровой денежной системе Bitcoin [3]. Bitcoin - это протокол для обмена цифровыми деньгами в децентрализованной недоверенной среде, позволяющий совершать транзакции без участия третьих лиц.

Но до опубликования данной статьи был проведен ряд исследований, оказавших значительное влияние на появление и практическую реализацию технологии блокчейн. Еще в 1982 году Д. Чаум предложил алгоритм слепой подписи и ввел понятие цифровых денег [4]. С. Хабер и С. Шторнетта в 1991 году представили теоретическое описание системы для удостоверения неизменяемости документов, построенную на временных метках [5]. Механизм доказательства выполнения работы (PoW) был предложен А. Бэком в проекте Hashcash для предотвращения спам-рассылок [6]. Идея умных контрактов была предложена Н. Сабо в 1996 году [7]. Н. Сабо также также предложил протокол для цифровых денег Бит-золото в 1998 году, который был опубликован в 2005 г [8]; он основывался на вычислении цепочки битов и использовал механизм консенсуса PoW. Но система не была реализована на практике и была подвержена атакам Сивиллы.

Однако, первая реализация технологии блокчейн была создана только в рамках проекта криптовалюты Bitcoin. Впоследствии стали появляться другие криптовалютные системы, схожие по строению с Bitcoin - добавлялись механизмы сокрытия данных, как например в Zcash [9], механизмы ускорения транзакций, как например в Litecoin [10], были созданы валюты для различных назначений, например, предоставляющие комплекс альтернативных серверов DNS - Namecoin [11]. Первым реализованным блокчейном, на базе которого функционировали смарт-контракты, стал Ethereum, созданный в 2013 г. В. Бутериным [12].

Задача построения модели блокчейна

Анализ статей на тему блокчейн-технологий показал, что практически нет работ, рассматривающих технологию блокчейн целиком, вне зависимости от конкретных реализаций, охватывая все компоненты данной технологии, основное внимание уделяя ее техническому устройству. В данном направлении можно выделить работу [13], обзор компонент технологии блокчейн от разработчиков Дорожной карты развития технологий распределенного реестра в РФ [14], исследование Ассамблеи сектора стандартизации электросвязи (ITU) Женевы [15] и комиссии ISO/TC 307 [16], но результаты работы большинства исследователей пока не представлены в открытом доступе либо имеют явные недостатки. Это подтверждает предположение о том, что знания о технологии фрагментарны и исследователям не видна общая картина. Это замедляет развитие данной технологии и затрудняет анализ новых блочейнов в вопросе определения реальных инноваций, в отличие от результата применения маркетинговых инструментов.

В рамках данной работы задача построения модели заключалась в том, чтобы предложить такую модель, которая бы отвечала следующим критериям: она позволяла бы сделать универсальное описание текущих систем, ответить на вопросы о строении си-

стемы и поставить новые вопросы перед исследователями и инженерами индустрии. Для построения модели использовался экспериментально-аналитичекий подход: на основе существующих программных реализаций технологии блокчейн проводился анализ составных частей технологии, полученные компоненты были обобщены, для них сформулирована система понятий и затем было показано, что каждая конкретная реализация технологии соответствует предложенной модели.

Для построения модели технологии, были проанализированы пять популярных блокчейнов, которые являются самостоятельными реализациями платформ для разработки децентрализованных приложений и криптовалют. Среди них: Bitcoin [17], Ethereum [18], NEO [19], DASH [20], EOS [21]. Выбор данных технологий обусловлен их востребованностью в качестве платформ для разработки децентрализованных приложений, высоким уровнем готовности технологии к прикладному применению, развитым сообществом для их поддержки и наличием удовлетворительной для их изучения документации. Характеристики выбранных блокчейнов представлены в таблице.

Таблица 1

Характеристики исследуемых блокчейнов

	Скорость исполнения транзакций	*Размер блока*	*Скорость создания одного блока*	*Скорость обработки транзакции, тр./сек.*
Bitcoin	78 мин.	1 Мб	10 Мин.	3
Ethereum	6 мин.	1 Мб	15 сек.	20 (PoW), 400 (PoA)
EOS	1,5 сек.	Около 1 Мб	1 сек.	50000
NEO	15 сек.	Около 1 Мб	15 сек.	1000-10000
DASH	15 мин.	2 Мб	1 сек.	28-56

Для решения данной проблемы в рамках иследования был разработан единый каркас строения технологии блокчейн, который не зависит от конкретных реализаций. Определены составные части данной технологии и разработаны их определения с целью исключения разногласий трактовок. Разработанная модель представлена в следующем разделе.

Разработанная модель технологии блокчейн

Для пяти выбранных блокчейнов была проанализирована техническая документация, технические концепции, «желтые бумаги», выделены общие компоненты, которые однозначно определяют технологию блокчейн с точки зрения архитектуры. Эти компоненты представлены на рисунке и описаны в тексте далее.

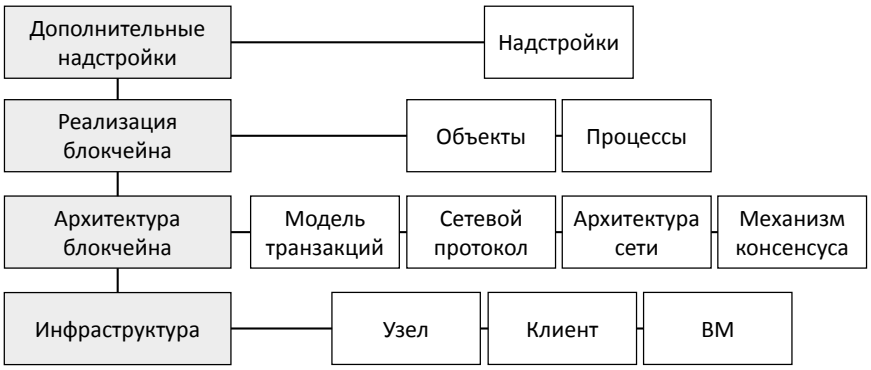

Рис. 1. Модель строения технологии блокчейн.

На **первом**, базовом, уровне модели расположены инфраструктурные компоненты, обеспечивающие функционирование системы. Это *узел (нода)* – единичный компьютер, осуществляющий действия в сети, *клиент* – программное обеспечение, реализующее протокол взаимодействия с блокчейном, и *виртуальная машина* – программная система, эмулирующая работу распределенной децентрализованной блокчейн-платформы и исполняющая децентрализованные приложения и смарт-контракты.

На **втором** уровне размещены компоненты, которые обеспечивают работоспособность блокчейн-сети. В зависимости от того, как построен данный уровень, устанавливаются особенности реализации.

Архитектура сети – комбинация узлов сети, а также набор правил, в соответствии с которыми производится передача сообщений по сети. Блокчейн-сети могут быть однослойные либо двуслойные, публичные либо приватные, могут иметь разделение узлов по ролям.

Механизм консенсуса – протокол, позволяющий прийти к соглашению между равноправными участниками децентрализованной сети. Существует множество реализаций, но наиболее популярными консенсусами являются PoW, PoS, dPos, aBFT, dBFT.

Модель транзакций – набор алгоритмов и особенностей проектирования блокчейна, определяющие способ проведения транзакций и фиксации состояния распределенной системы. В настоящее время существует две модели – UTXO либо модель учетных записей.

Сетевой протокол – правила, по которым осуществляется передача данных в сети.

На **третьем** уровне расположены объекты и процессы, устройство которых зависит от реализации предыдущего уровня. Для начала перечислим **объекты**, наличие которых однозначно определяют технологию блокчейн.

Блок – это структура данных, используемая для хранения данных в блокчейне. Блок хранит транзакции, состояние сети, смарт-контракты, разрешения на доступ к данным и другие сведения.

Цепочка блоков – структура данных, построенная за счет последовательного объединения блоков в цепочку. За счет хранения значения хэш-функции от предыдущего блока, все блоки строго последовательны, нумеруются сквозной нумерацией, дочерний блок всегда ссылается только на один родительский блок.

Транзакция – минимальная логически осмысленная операция перевода или обмена активов, которая имеет смысл и может быть совершена только полностью. Транзакция может осуществлять передачу сообщения, действия, создавать контракт и другое.

Адрес (аккаунт, учетная запись) – это средство идентификации действующего объекта в сети. Адреса однозначно определяют отправителя и получателя ценностей, переводимых в сети блокчейн, с адресом ассоциированы все действия пользователя в сети. В зависимости от блокчейна, адрес может быть как строкой так и структурой данных, может быть ассоциирован с пользователем или с смарт-контактом.

Смарт-контракт – это набор формализованных правил, реализованных в виде программного кода, выполнение которых влечет за собой некоторые события в реальном мире или цифровых системах. Смарт-контракты не являются обязательным компонентом блокчейн-сети, однако, как показала практика, контракты стали основным функциональным элементом. В зависимости от строения блокчейна, смарт-контракты могут быть реализованы либо на Тьюринг-полных языках, либо не Тьюринг-полных.

Перечисленные выше объекты являются частью процессов. Основные **процессы**, протекающие в блокчейн-сети, представлены ниже.

Жизненный цикл транзакции: процесс подписания транзакции; широковещательная рассылка по сети; проверка транзакции; завершение транзакции. *Включение транзакции в блок*: процесс набора транзакций для блока; валидация транзакции; процесс подписания блока; отправка блока в сеть; фиксация блока в общей цепочке. *Поддержание работы сети*: механизм консенсуса; регуляция сложности сети; выбор цепочки, которая продолжит блок из нескольких разветвлений; оплата вычислительных ресурсов.

Четвертый уровень определяет дополнительные надстройки для блокчейн-сетей, которые не влияют на внутреннюю архитектуру технологии, но значительно расширяют ее функционал. Например, механизмы, обеспечивающие повышенную скорость и конфиденциальность транзакций, механизмы для офф-чейн транзакций, модули, защищающие от атак, совершаемых с помощью квантовых компьютеров и другие.

Выводы

Проведя анализ блокчейнов, выявив закономерности и построив модель технологии блокчейн, можно предложить *методологию рассмотрения каждой новой разрабатываемой технологии.* Для анализа нового блокчейна в первую очередь следует обратить внимание на модель хранения транзакций. В настоящее время представлены две модели - UTXO и модель учетных записей. От модели зависит: строение блоков блокчейна, строение адресов (аккаунтов), наличие смарт-контрактов и принципы их построения, подходы к фиксации состояния системы. Далее следует обратить внимание на количество слоев в сети системы, выявить назначение каждого из слоев, рассмотреть механизмы консенсуса, используемые в каждом слое. Эта информация даст понимание процесса валидации транзакций, и на ее основе можно предположить максимальную скорость подтверждения транзакции и пропускную способность сети. На основе этого можно сделать выводы о необходимой инфраструктуре, которая потребуется для обеспечения сети. Скорость проведения транзакций определяется механизмом консенсуса, на котором функционирует блокчейн, количеством узлов, задействованных в процессе валидации транзакций и принципами работы с блоками-сиротами.«Степень децентрализованности» блокчейна обратно пропорциональна скорости проведения транзакций. Возможность проектирования смарт-контрактов определяется моделью учета транзакций.

Используя результаты данного исследования и предложенной методологии, можно *обосновать подходы к реализации конкретных технологий блокчейн.* Можно предположить, что в подавляющем большинстве блокчейнов за основу взяты модели по-

строения Bitcoin и Ethereum, и впоследствии они были дополнены рядом улучшений на разных уровнях. По данным, полученных из открытых источников, складывается впечатление, что в блокчейне NEO создана конфигурация из сетей по моделям UTXO и модели учетных записей с целью сгладить недостатки сети Bitcoin, взятую за основу для данного блокчейна. Такое предположение сделано также и потому, что дублирование активов в данных сетях выглядит искусственным. Есть предположение, что блокчейны EOS и NEO скорее не являются блокчейнами, так как по определению блокчейн функционирует в недоверенной среде, а у данных сетей основными валидаторами транзакций являются авторизованные узлы, что наводит на мысль о централизации данных сетей. Блокчейн Dash обеспечивает конфиденциальность данных и скорость транзакций за счет механизмов, функционирующих на четвертом уровне модели блокчейна, хранящего транзакции.

Заключение

В результате данной работы была разработана модель технологии блокчейн. Данная модель позволяет сделать универсальное описание текущих систем, ответить на вопросы о строении системы и поставить новые вопросы перед исследователями. В работе было доказано, что предложенная модель не зависит от конкретных реализаций пяти выбранных блокчейнов. В дальнейшем планируется исследовать большее количество блокчейнов с целью подтверждения корректности модели и ее уточнения.

ЛИТЕРАТУРА

1. *L. Lamport, M. Pease, R. Shosta* The Byzantine Generals Problem. //ACM Transactions on Programming Languages and Systems 4, т. 3, p. 382—401, 1982.
2. *Douceur, J. R.* The sybil attack. //International workshop on peer-to-peer systems. Springer, Berlin, Heidelberg, 2002. – С. 251-260.
3. *Satoshi, Nakamoto* Bitcoin: A Peer-to-Peer Electronic Cash System. //The Cryptography Mailing List, 2008. URL: `https://bitcoin.org/bitcoin.pdf`.
4. *Chaum, D.* “Blind Signatures for Untraceable Payments”. //Advances in Cryptology Proceedings of Crypto 82, Plenum. 1982. pp. 199-203, 1982.
5. *Haber, S., Stornetta, W.S.* How to time-stamp a digital document. //J. Cryptology 3. 1991. pp. 99–111.
6. *Back, A.* Mail “Hash cash postage implementation”. //The Cypherpunks Mailing List. URL: https://cypherpunks.venona.com/date/1997/03/msg00774.html.
7. *Szabo, N.* Smart Contracts: Building Blocks for Digital Markets. //A partial rewrite of the article which appeared in Extropy No 16. 1996. URL: `http://www.alamut.com/subj/economics/nick_szabo/smartContracts.html`.
8. *Szabo, N.* Bit gold. //Unenumerated: N. Szabo’s blog. 2005. URL: `https://web.archive.org/web/20060329122942/http://unenumerated.blogspot.com/2005/12/bit-gold.html`.
9. Zcash is a privacy-protecting, digital currency. //URL: `https://z.cash/`.
10. Litecoin - decentralised money, free from censorship and open to all. //URL: `https://litecoin.com/en/`.
11. Namecoin - a trust anchor for the Internet. //URL: `https://www.namecoin.org/`.
12. Ethereum - глобальная платформа с открытым исходным кодом для децентрализованных приложений. //URL: `https://ethereum.org/ru/`.
13. *Paik, H. Y. et al.* Analysis of Data Management in Blockchain-Based Systems: From Architecture to Governance. //IEEE Access. – 2019. – Т. 7. – С. 186091-186107. URL: `https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8938787`.

14. *Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.* Дорожная карта развития «сквозной» цифровой технологии «Системы распределенного реестра». //URL: https://digital.gov.ru/ru/documents/6670/.
15. *ITU's Telecommunication Standardization Sector (ITU-T).* ITU-T Focus Group on Application of Distributed Ledger Technology. //URL: https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx#.
16. *Technical cometees ISO/TC 307.* Blockchain and distributed ledger technologies. //URL: https://www.iso.org/committee/6266604.html.
17. Bitcoin developers documentation //URL: https://developer.bitcoin.org/.
18. *Wood, G.* Ethereum: a secure decentralized generalized transaction ledger //URL: https://ethereum.github.io/yellowpaper/paper.pdf.
19. A Technical Specification for Neo Blockchain. //URL: https://github.com/neoresearch/yellowpaper.
20. *Duffield, E., Diaz, D.* Dash: A Payments-Focused Cryptocurrency. //URL: https://github.com/dashpay/dash/wiki/Whitepaper.
21. EOSIO Developer Portal. //URL: https://developers.eos.io/.

Sazonova P. A. **KEY COMPONENTS OF BLOCKCHAIN TECHNOLOGY BASED ON AN ANALYSIS OF IMPLEMENTATIONS.** Blockchain technology was first implemented in 2008, and 12 years later more than 2000 different implementations of it have appeared. Commonly, approach for development blockchain technologies is fragmented, so the industry have the problem of the lack of a common picture, a common understanding of technology by researchers. The aim of this work is to highlight the key components of the internal structure of blockchain technology and to propose a universal model of blockchain technology. This work approach is based on a technical analysis of the most popular blockchains. The characteristics presented in all blockchains were identified and the differences in their implementation in each individual case were determined. The results of this work can be used by architects of new blockchain networks to achieve the goals of their development.

Keywords: *blockchain, Ethereum, Bitcoin, EOS, NEO, Dash.*

САЗОНОВА Полина Андреевна — аспирантка Новосибирского государственного университета, лаборатория JetBrains Research, м.н.с. Института математики им. С.Л.Соболева, г. Новосибирск. E-mail: **psazonova@gmail.com**