УДК 681.0.245

ПРОБЛЕМЫ ДОВЕРИЯ В ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ БЛОКЧЕЙН

Ищукова Е.А., Красовский А.В.

Южный федеральный университет Институт компьютерных технологий и информационной безопасности, Таганрог, e-mail: an.krasowsckij@gmail.com

В последние годы набирает оборот использование технологии блокчейн. При этом речь уже идет не только о криптовалюте, как было в самом начале, а о совершенно разных сферах бизнеса. Показательно то, что компетенция «Разработка решений с использованием блокчейн технологий» входит в одну из компетенций будущего FutureSkills в рамках соревнований WorldSkills. Несмотря на широкую известность, в применении блокчейн технологий существуют достаточно большие пробелы. Доверие к P2P алгоритмам, основанным на технологии блокочейн, порождает значимые проблемы для будущего освоения и использования данной децентрализованной технологии. Предполагается, что недостаточное исследование сущности доверия в области блокчейн является одной из ключевых проблем, а сама технология позволит качественно и положительно изменить будущее. В данной работе на основании анализа различных реализаций криптовалют (Bitcoin, Ethereum, Monero, ZeroCash, Litecoin) и децентрализованных проектов (IPFS, Plasma, Filecoin) даётся новое определение категории технологического доверия в блокчейне, проводится разделение на социальный, технический и игровой аспект. В результате определяется доверие и описываются его основные свойства и параметры. Работа направлена на выполнение задачи популяризации блокчейн технологии, что невозможно без определения сущности доверия или актуализации данного вопроса.

Ключевые слова: определение, доверие, блокчейн, проблема принятия, криптография, оценка доверия

CONFIDENCE IN THE USE OF BLOCKCHAIN TECHNOLOGY

Ishchukova E.A., Krasovsckiy A.V.

Southern Federal University Institute of Computer Technologies and Information Security, Taganrog, e-mail: an.krasowsckij@gmail.com

In recent years, the use of blockade technology has been gaining momentum. At the same time, we are talking not only about the crypto currency, as it was at the very beginning, but about completely different spheres of business. It is significant that the competence «Development of solutions with the use of block technologies», is part of the competence of future FutureSkills within the framework of WorldSkills competitions. Despite the wide popularity, there are quite large gaps in the use of block technologies. Confidence in P2P algorithms based on blockbuster technology generates significant problems for the future development and use of this decentralized technology. It is believed that an inadequate study of the essence of confidence in the field of blockade is one of the key problems, and the technology itself will allow a qualitative and positive change in the future. In this paper, based on the analysis of various implementations of crypto-currencies (Bitcoin, Ethereum, Monero, ZeroCash, Litecoin) and decentralized projects (IPFS, Plasma, Filecoin), a new definition of the category of technological trust in the detachment is given, and the social, technical and game aspect is divided. As a result, trust is defined, and its main properties and parameters are described. The work is aimed at fulfilling the task of popularizing the blockchain technology, which is impossible without determining the essence of trust or updating this problem.

Keywords: definition, trust, block, the problem of acceptance, cryptography, trust assessment

Наука и научные дисциплины регулярно положительно и качественно изменяют устройство социума человечества [1–3]. Изменения не всегда происходят революционным путём, но все глобальные положительные изменения возможны лишь при глубоком и детальном понимании средства изменения. Сегодня таким средством является блокчейн технология. И хотя существуют «пророки» блокчейна, которые провозглашают его инструментом для решения всех накопившихся проблем человека/государства, данная разработка сопровождается «громким шумом» сообщества без понимания его сущности. Высокий рост популярности блокчейна во многом вызывается его монетарной стороной. Соответственно плодятся примеры неверного и неудачного использования блокчейна, что ведёт к снижению доверия среди заинтересованных людей [4–6]. Недоверие принимает различные формы, но оно препятствует распространению технологии и его принятие человеком – не специалистами в данной области.

Соответственно проблема развития и принятия технологии блокчейна может быть в общем визуализирована (рис. 1) с помощью кривой Гартнера [7–9].

На рис. 1 показано (зелёным цветом выделен участок с размещением текущего состояния), что при нормальном развитии технологии произойдёт уменьшение доверия к блокчейну. Кроме того, упадут и ожидания, что негативно повлияет на темпы роста блокчейна, на его развитие и принятие массами. Пропасть ещё не достигнута. Следовательно, она должна быть преодолена. Это может произойти в будущем только вместе с детальным пониманием проблемы доверия и, в частности, пониманием сущности технического доверия.

Рис. 1. Кривая изменения доверия к технологии блокчейн (кривая Гартнера)

Оперативной целью работы является определение технического доверия в блокчейне, описания его отличия от иных видов и структурирование (в соответствии с стратегической целью популяризации). Данные действия позволят инициировать и предложить определение аспекта доверия в рамках сущности блокчейн технологии, что позволит (или ускорит) сформулировать популярную точку зрения на проблему доверия в блокчейне. Таким образом, выполнение цели работы направлено на актуализацию проблемы доверия в блокчейне и частичное решение проблемы принятия (популяризации) блокчейн технологий.

Определение категорий доверия блокчейна

Конкретные имплементации блокчейн технологии предполагают сообщества людей. Сама технология основывается на теории игр, криптографии и сетевой составляющей. Таким образом, можно утверждать, что результат работы блокчейна основывается на социальном и техническом аспекте. Это утверждение является ключевым для данной работы. Оно основывается на статье «The Economic of Bitcoin Miningor, Bitcoinin the Presence of Adversaries» за авторством Joshua A. Kroll, Ian C. Davey и Edward W. Felten[10].

В приведённой выше статье описываются три типа консенсуса работы блокчейна:

1) консенсус правил определения валидности (социальный консенсус);

2) консенсус определения валидности с помощью правил (технический консенсус);

3) консенсус определения ценности (игровой консенсус).

Консенсус решает проблему доверия. Каждый консенсус решает проблему определённого типа доверия. Таким образом, блокчейн основывается на трёх типах доверия (рис. 2): социальное доверие, техническое доверие, игровое доверие.

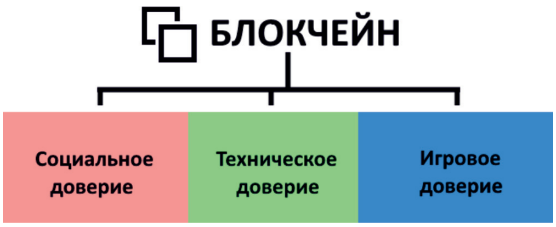

Рис. 2. Категории доверия в блокчейне

Социальное доверие уже было описано с помощью институциональной и иных теорий, социологии, психологии. Игровое доверие описывается с помощью теории игр. Дан-

ная статья написана с целью декларирования определения технического доверия блокчейна, так как он является крайне мало изученным.

Социально-техническая часть технического доверия в блокчейне

Дихотомия блокчейна на социальное и техническое доверие затруднительна, так как именно социальный аспект порождает направленность развития технического. В то же время, после анализа выбранных ранее проектов реализации блокчейна, можно явно выделить свойства социально-технической части технического доверия. Так, это:

1) открытость кода проекта;
2) полнота кода проекта;
3) целостность проекта;
4) актуальность применения методов анализа кода на уязвимости;
5) открытость научных публикаций о криптографических примитивах;
6) количество применимых методов криптоанализа;
7) сложность криптоанализа криптографических примитивов;
8) актуальность применяемых методов криптоанализа;
9) достаточное и полное руководство использования;
10) открытость описания цепочки производства средств майнинга;
11) открытость описания цепочки производства средств хранения блокчейна;
12) полнота документации устройств;
13) открытость теоретического описания алгоритмов проекта;
14) открытость сетевых протоколов;
15) актуальность протоколов проекта.

Описанные выше свойства технического доверия основываются на следующих фактах:

1) технический консенсус предполагает использование вычислительных мощностей;
2) технические мощности в большинстве своём представлены в виде специальных средств (видеокарты, ASIC'ки, ПЛИС и т.д.);
3) разработка технических средств требует создания базы новой технической документации (схемы и руководства);
4) блокчейн использует различные криптографические примитивы (хэш-функции, асимметричная криптография, симметричная криптография);
5) в блокчейнах на основании криптографических примитивов создаются протоколы (Ouroboros,GHOST, Aura, Tendermint, Casper и т.д.);
6) каждая реализация блокчейна предполагает создание приложений;
7) приложения реализуют практическую работу блокчейна и могут содержать уязвимости с незадокументированными свойствами.

В каждом свойстве преобладает техническая часть так как оно не предполагает доверия к человеку. Схематично данные свойства представлены на рис. 3.

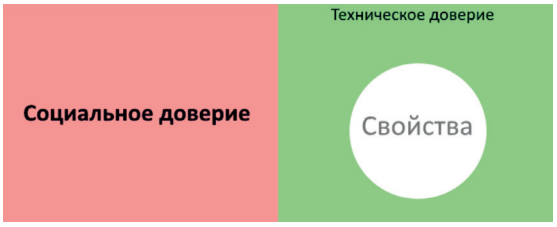

Рис. 3. Схематичное изображение категорий доверия и свойств блокчейна

При обобщении всех свойств можно сделать вывод, что социально-техническая часть технического доверия может быть представлена в нескольких категориях. Данные категории: открытость источников, полнота и достаточность источников, актуальность методов.

Данные категории отображают свойства, но все они явно вытекают из социального доверия человека к группе разработчиков (или определённому представителю разработчиков). Таким образом, получается, что категории связывают социальный аспект доверия и технический. Обозначим их как «конкатенаторы» (рис. 4). Конкатенаторы позволяют более обще представить техническое доверие, где будет в явном виде определена взаимосвязь свойств и социального доверия.

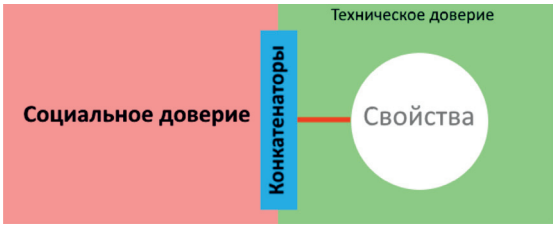

Рис. 4. Схематичное представление конкатенаторов

Параметры технического доверия

Из свойств вытекают конкатенаторы и параметры технического доверия. Все свойства затрагивают несколько сущностей реализаций блокчейн технологии: код проектов с реализацией приложений для взаимодействия в сети с другими участниками блокчейна, криптографические примитивы, протоколы консенсуса, вычислительные устройства для обеспечения работы блокчейна и достижения консенсуса, сеть.

Для каждой из описанных сущностей социальное определение доверия не может быть применимо, так как отсутствует положительное взаимоотношение, взаимодействие с людьми и доброжелательность.

Под доверием относительно сущностей предполагается: отсутствие социального доверия, целостность обрабатываемых данных (вход, внутреннее состояние, выход), чистые процессы выполнения (или ссылочная прозрачность процессов), конфиденциальность обрабатываемых данных, доступность обрабатываемых данным, предсказуемость результатов, однозначность структуры.

На основании доверия к сущностям, выделяемым из социально-технической части технического доверия, можно определить следующие параметры технического доверия:

1) математическая структура криптографических примитивов;
2) вычислительная сложность криптоанализа криптографических примитивов;
3) временная сложность криптоанализа криптографических примитивов;
4) степень энтропии выходных данных криптографических примитивов (в соответствии с Шенноном);
5) размерности криптографических примитивов;
6) парадигма программирования кода;
7) диаграммы и цепочки взаимосвязей сущностей кода;
8) язык программирования;
9) результаты анализа динамического, статического и фазинг-анализа;
10) результаты тестирования приложений;
11) схемы и документации приложений и вычислительных устройств;
12) параметры алгоритма консенсуса;
13) используемые протоколы блокчейна для устранения проблем ветвления и утраты вычислительной мощности из-за ветвления;
14) используемые протоколы общения с внешней средой блокчейна;
15) расширяемость сети;
16) количество блоков в *n* времени;
17) средняя и максимальная скорость транзакций;
18) размерность блока;
19) тип внутренних скриптов;
20) тип сетевых протоколов;
21) уязвимости сетевых протоколов;
22) средства борьбы с атаками.

Параметры явно определяют взаимосвязь определения доверия для сущностей и техническим доверием блокчейна. Таким образом, параметры технического доверия блокчейна вытекают из свойств и основываются на доверии сущностей. Параметры определяют значения для выполнения и реализации блокчейна, что, совместно с вышесказанным, характеризует их как ключевую составляющего технического доверия. Схематичное изображение параметров представлено на рис. 5.

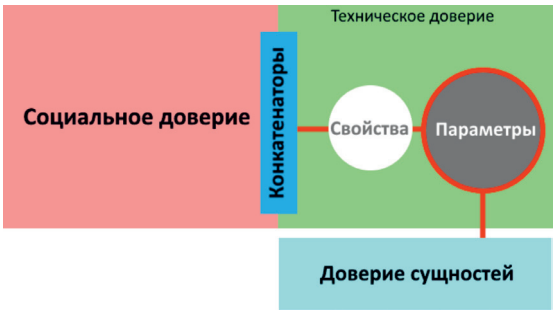

Рис. 5. Схематичное изображение параметров технического доверия

Параметры технического доверия служат для создания стратегий в теории игр, с помощью которой и определяют игровое доверие. Таким образом, параметры связывают игровое доверие и техническое доверие через конкатенатор игрового доверия.

Определение технического доверия

Таким образом, можно заключить, что *техническое доверие блокчейна* – это:

1) вид доверия, которое выражается через социальное и игровое доверие посредством свойств и параметров;
2) вид доверия, связанный с социальным доверием через социальный конкатенатор – обобщённые и сконцентрированные социальные сущности свойств;
3) вид доверия, связанный с игровым доверием через игровой конкатенатор – элементарные правила на основании параметров;
4) вид доверия, которое определяется параметрами используемых практических и теоретических решений, где оно заключается в целостности, доступности и конфиденциальности информации, прозрачности и предсказуемости выполнения;
5) вид доверия, которое основывается на криптографических примитивах, протоколах консенсуса и протоколах устранения утраты стойкости;
6) вид доверия, которое основывается на вычислительных мощностях и степень доверенности которого можно выразить в затрате вычислительных ресурсов.

Более кратко: *техническое доверие блокчейна* – доступное, конфиденциальное и целостное взаимодействие, проявляющееся в параметрах криптографических алгоритмов и методах имплементации, состоящее

из прозрачных и предсказуемых процессов обработки результатов технического консенсуса.

Техническое доверие блокчейна может быть оценено степенью затрачиваемых на его преодоление вычислительных ресурсов, т.е. может быть выражено в категориях временной и вычислительной сложностей, которые необходимо затратить для преодоления доступности, конфиденциальности или целостности (т.е. атакам на криптографические примитивы, протоколы, сетевые узлы, приложений участников).

Проявление технического доверия к блокчейну должно быть основано на сравнении информации об оценке технического доверия к данному блокчейну и информации о текущих распределениях вычислительных мощностей.

Выводы

В данной работе были определены свойства технического доверия блокчейна, параметры технического доверия, логика и вид взаимосвязи технического доверия блокчейна к социальному и игровому аспекту, дано определение технического доверия и способ его оценки.

Соответственно, определение доверия должно разрешить проблему понимания такого явления, как блокчейн технологии и блокчейн имплементации, что предполагает актуализацию осмысления сути проблемы доверия и разрешения проблемы развития технологии блокчейн.

Список литературы

1. Roman Beck, Jacob Stenum Czepluch, Nikolaj Lollike, Simon Malone. Blockchain – the gateway to trustfree cryptographic transactions [Электронный ресурс]. URL: https://pdfs.semanticscholar.org/ee1e/fd77e8b6287438d312b244177bb143f7a072.pdf (дата обращения: 06.09.2018).

2. Qi Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du. MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. IEEE Access The Multidisciplinary Open Access Journal. 2017. vol. 5. P. 14757–14767.

3. John Adler, Ryan Berryhill, Andreas Veneris, Zissis Poulos, Neil Veira, and Anastasia Kastania. ASTRAEA: A Decentralized Blockchain Oracle [Электронный ресурс]. URL: https://arxiv.org/pdf/1808.00528.pdf (дата обращения: 06.09.2018).

4. Danny Harnik, Paula Ta-Shma, Eliad Tsfadia. It Takes Two to #MeToo – Using Enclaves to Build Autonomous Trusted Systems [Электронный ресурс]. URL: https://arxiv.org/pdf/1808.02708.pdf (дата обращения: 06.09.2018).

5. Thomas Locher, Sebastian Obermeier, Yvonne-Anne Pignolet. When Can a Distributed Ledger Replace a Trusted Third Party? [Электронный ресурс]. URL: https://arxiv.org/pdf/1806.10929.pdf (дата обращения: 06.09.2018).

6. Marcus Brandenburger, Rüdiger Kapitza, Christian Cachin, Alessandro Sorniotti. Blockchain and Trusted Computing: Problems, Pitfalls, and a Solution for Hyperledger Fabric [Электронный ресурс]. URL: https://arxiv.org/pdf/1805.08541.pdf (дата обращения: 06.09.2018).

7. Hung Dang, Anh Dinh, Ee-Chien Chang, Beng Chin Ooi. Chain of Trust: Can Trusted Hardware Help Scaling Blockchains? [Электронный ресурс]. URL: https://arxiv.org/pdf/1804.00399.pdf (дата обращения: 06.09.2018).

8. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс]. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 06.09.2018).

9. Buterin V. Ethereum White Paper [Электронный ресурс]. URL: https://github.com/ethereum/wiki/wiki/ White-Paper (дата обращения: 06.09.2018).

10. LITECOIN CASH LTCH WHITE PAPER [Электронный ресурс]. URL: https://litecoin-cash.io/Whitepaper.pdf (дата обращения: 06.09.2018).