

РАСПРЕДЕЛЕННЫЕ РЕЕСТРЫ, КАК ИНСТРУМЕНТЫ РАЗВИТИЯ КРУПНОМАСШТАБНЫХ ФИНАНСОВЫХ СИСТЕМ

Варнавский А.В., Бурякова А.О.

*Финансовый университет при Правительстве Российской Федерации,
Россия, г. Москва, Ленинградский проспект д.49
AVVarnavskiy@fa.ru, AOBuryakova@fa.ru*

Аннотация: Цель настоящего исследования заключается в формировании обобщенной открытой классификации архитектуры блокчейн-платформ. Классификация представляет собой иерархическую структуру, состоящую из шести основных направлений, каждое из которых предполагает наличие ряда характеристик и соответственно множеств. Классификационные признаки с точки зрения разработки решений для крупномасштабных финансовых систем могут рассматриваться как совокупность альтернативных правил функционирования системы.

Ключевые слова: блокчейн-платформы, классификация, крупномасштабные финансовые системы.

Введение

С тех пор как была опубликована статья, описывающая первую блокчейн платформу «Bitcoin: A Peer-to-Peer Electronic Cash System»⁶³, прошло достаточно много времени. Технология блокчейн существенно ушла вперед – появилось множество различных платформенных решений: Hyperledger, Corda, EOS и многие другие. Каждая из блокчейн-платформ обладает собственными технологическими характеристиками и рамками. Совокупность накопленных решений предопределила необходимость формирования обобщенной, глобальной классификации, позволяющей упорядочить процесс разработки решений для оптимизации бизнес-процессов.

Блокчейн представляет собой один из видов технологии распределенных реестров, в котором данные о совершаемых транзакциях структурируются в виде цепочки связанных блоков и защищаются криптографическим способом. Ключевые свойства блокчейна: распределенность, хронологическая запись данных, невозможность подмены данных в прошлом. Вместе с тем, в блокчейн среде становится возможна реализация смарт-контрактов в целях автоматизации операций. Пожалуй, данный перечень будет общим для подавляющего большинства блокчейн-платформ. Однако существует и ряд других характеристик. О них и пойдет речь в настоящей статье.

Более того те или иных технологические особенности целесообразно рассматривать с точки зрения возможности их практической интеграции. Так, блокчейн может служить базой для формирования крупномасштабных финансовых систем. Наиболее ярким примером могут послужить платежные системы – крупнейшие банки, в том числе центральные, а также корпорации уже рассматривают возможность использования блокчейна в качестве транзакционной, технологической основы. Существенное значение здесь будет иметь модель организации взаимодействия элементов системы – правил и связей, которые в свою очередь будут закладываться еще на уровне проектирования архитектуры платформенных решений.

Классификация блокчейн-платформ в современной литературе

Классификации блокчейн-платформ, представленные отечественными и зарубежными авторами, выделяют публичные или приватные, открытые или закрытые блокчейн-платформы⁶⁴⁶⁵⁶⁶⁶⁷. Однако подобная классификация не дает полного представления о присущих каждому из видов характеристиках. Более того, различные авторы рассматривают различные ракурсы «открытости», не принимая во внимание направления исследования своих коллег. В результате мы имеем абсолютно несовпадающие по своим характеристикам «открытые» и «закрытые» блокчейны.

Также выделяют такие классификационные признаки как уровень развития технологии. К примеру, М. Свон в работе «Блокчейн. Схема новой экономики»⁶⁸ выделяет блокчейн 1.0 (расчетный блокчейн биткойна), блокчейн 2.0 (смарт-контракты), блокчейн 3.0 (децентрализованные приложения и организации). Или же блокчейн-платформы части классифицируют по консенсусу: Practical Byzantine Fault Tolerance Algorithm, Proof-of-Work, Proof-of-Stake и другие⁶⁹. В более ранних наших работах мы также обращали внимание на такие классификационные признаки как «доступ к сети», «ограничение действий с информацией», «платности совершения операций» и другие⁷⁰. Однако при более глубоком изучении стало ясно, что обозначенные нами характеристики не будут охватывать все технологические аспекты.

По нашему мнению, достаточно проработанной, можно назвать классификацию авторов Tasca P. и Tessone C. J. В работе «Taxonomy of blockchain technologies. Principles of identification and

⁶³ <https://bitcoin.org/bitcoin.pdf>

⁶⁴ Жданов Иван Николаевич, Федоров Александр Игоревич, Балашов Артем Викторович Введение в блокчейн 2.0 // Научный журнал. 2017. №10 (23). URL: <https://cyberleninka.ru/article/n/vvedenie-v-blokcheyn-2-0> (дата обращения: 30.06.2019).

⁶⁵ Пескова О. Ю., Половко И. Ю., Захарченко А. Д. Применение блокчейн-технологий в системах электронного документооборота: анализ и программная реализация // Латинская Америка. – 2007. – Т. 152. – №. 5. – С. 3.

⁶⁶ Заварзин А. В. Перспективы технологии блокчейн в контексте роста благосостояния общества. – 2018.

⁶⁷ Benos E., Garratt R., Gurrola-Perez P. The economics of distributed ledger technology for securities settlement. Bank of England. – Staff Working Paper Staff Working Paper, 2017. – №. 670.

⁶⁸ Свон М. Блокчейн. Схема новой экономики. – Litres, 2019.

⁶⁹ Puthal D. et al. Everything you wanted to know about the blockchain: Its promise, components, processes, and problems // IEEE Consumer Electronics Magazine. – 2018. – Т. 7. – №. 4. – С. 6-14.

⁷⁰ Варнавский А.В., Бурякова А.О., Себеченко Е.В. Блокчейн на службе государства : монография. — Москва : КНОРУС, 2019. — 218 с.

classification»⁷¹ была представлена таксономия технологии блокчейн, сформированная в виде систематических, иерархических групп. Несмотря на все преимущества классификации Tasca P. и Tessone C. J., в ней все-таки есть некоторые спорные моменты. Стоит ли объединять на одном уровне в рамках одного направления блок и транзакцию? Целесообразно ли относить организационную форму (открытый/закрытый код, отдельный проект/консорциум) и языки сценариев к характеристикам перспектив развития сети? Стоит ли выделять псевдоанонимность как один из субуровней «управления идентификацией»? И многие другие моменты. Свои ответы на поставленные вопросы мы постараемся дать в обосновании выделенных нами классификационных характеристик и множеств.

Общее описание классификации.

Выявление логических связей между сочетанием различных характеристик, помогает обозначить различные альтернативы в работе блокчейн-платформ, что соответственно приводит к разработке наиболее оптимального дизайна, архитектуру под каждую конкретную задачу. В нашем случае речь пойдет о разработке расчетного блокчейн – межбанковской платежной системы. Однако данная классификация может быть использована и для анализа какой-либо иной крупномасштабной системы.

Основу разработанной классификации составляют шесть базовых уровней функционирования блокчейн-платформ. Блокчейн-платформы могут различаться в зависимости от предусмотренной в них возможности создания и функционирования расчетных единиц - токенов. Транзакционная модель описывает, как узлы, подключенные к P2P-сети, сохраняют и обновляют информацию пользователя в распределенном реестре. Задача транзакционной модели состоит в том, чтобы предотвратить появление в сети данных, которым не следует доверять, например занесение в реестр так называемых «двойных расходов». Те или иные правила формирования блока варьируются от платформы к платформе. Однако в качестве характеристических свойств мы выделяем структуру данных в заголовке блока и сам состав блока. В зависимости от того, какая информация хранится в блокчейне, определяется и масштабируемость системы. Блокчейн-платформы можно классифицировать исходя из взаимосвязи языков программирования в конкретной блокчейн-платформе. Защита лицензиями, как признак, выявляет наличие двух вариантов – открытый исходный код и закрытая лицензия. Выбор архитектуры программного обеспечения очень важен для лучшего управления изменениями после их внедрения. Выбор архитектуры программного обеспечения включает в себя конкретные структурные варианты среди возможностей, доступных для разработки ПО. Язык сценариев – полный и неполный по Тьюрингу. Доказательный консенсус или консенсус доказательством - Proof-of-Work, Proof-of-Stake, Proof-of-Authority, Proof-of-Capacity, Proof-of-Burn, Byzantine Fault Tolerance consensus, hybrid consensus и другие. Кроме того, в качестве характеристических свойств выступают виды соглашений о подтвержденности блока. А на уровне блокчейн-сети мы разделим платформы отвечая на вопрос относительно того, как обеспечивается бесперебойная работа самой сети, и как взаимодействуют ноды и узлы, выполняя свои роли. Задержка (latency) - подкомпонент, который описывает правило распространения сообщений в сетях. Тип взаимосвязи между узлами/нодами сети и тип информационного потока между ними формируют конфигурацию сети. Режим диалога (Gossiping) – характеристика того, как информация проходит через серверы. В отношении безопасности мы выделяем два характеристических свойства, которые уже помогают выявить определенны множества платформ: шифрование данных (SHA-2, ZK-SNARKS) и конфиденциальность данных (встроенная конфиденциальность и коденфициальность через надстройки). Экономический уровень на котором платформы различаются в зависимости от мотивации экономических агентов в отношении отдельных аспектов - мы называем уровнем взаимодействия и выделяем на нем три характеристических свойства. В работе рассматривается возможная архитектура блокчейн-платформы межбанковской платежной системы. Соответственно анализируется каждая из возможных альтернатив. К примеру, должна ли это быть сеть только с полными нодами или сеть, сочетающая как полные ноды, так и тонкие клиенты. Соответственно суть сети только с полными нодами будет заключаться в том, что все узлы процесса проверки, относятся к одному виду. Это действительно одноранговая сеть, где все узлы эквивалентны с точки зрения содержащейся информации. Это свойство создает большую избыточность информации, что делает систему более устойчивой к атакам или сбоям в работе, но в тоже время менее гибкой. Или, например, какой режим диалога стоит выбрать – локальный или глобальный. Режим диалога же в свою очередь ответственное за то, что

⁷¹ Tasca P., Tessone C. J. *Taxonomy of blockchain technologies. Principles of identification and classification* //arXiv preprint arXiv:1708.04872. – 2017.

именно информация о закрытом блоке будет распространяться в сети. То есть стоит ли предположить наличие возможность получить информацию о подтвержденных транзакциях сначала только тем банкам, которые ее инициировали. Или информация будет сразу распространяться по сети? Большинство банков все-таки рассматривают платформы с локальным режимом диалога. Например, Quorum, который поддерживает как приватные, так публичные транзакции и имеет много коммерческих сценариев использования.

Выводы

Разработанная классификация представляет собой иерархическую структуру, состоящую из шести основных направлений, каждое из которых предполагает наличие ряда характеристик и соответственно множеств. Предложенный подход включает в себя как технологические, так и экономические (организационные) характеристики. Классификационные признаки с точки зрения разработки решений для крупномасштабных финансовых систем могут рассматриваться как совокупность альтернативных правил функционирования системы. То есть в ходе разработки на каждом из уровней может выбираться какая-либо из предложенных альтернатив, в зависимости от исходных требований к работе всей системы. Подобный подход фактически позволяет стандартизировать процесс формирования архитектуры блокчейн-платформы.

Литература

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. – 2008.
2. Варнавский А.В., Бурякова А.О., Себеченко Е.В. Блокчейн на службе государства. — М.: КНОРУС, 2019. — 218 с.
- Доклад Центра цифровых компетенций ВЭБ и ФИПС. Технологии Блокчейн: Современное состояние и ключевые инсайты. URL: <http://www1.fips.ru/vse-uslugi/patent-analytics/report-blockchain.pdf> (дата обращения 29.06.2019)
3. Жданов И.Н., Федоров А.И., Балашов А.В. Введение в блокчейн 2. 0 // Научный журнал. 2017, №10 (23). – с.39-43.
4. Пескова О.Ю., Половко И. Ю., Захарченко А. Д. Применение блокчейн-технологий в системах электронного документооборота: анализ и программная реализация // Латинская Америка. 2007, №. 5.–с. 3.
5. Заварзин А.В. Перспективы технологии блокчейн в контексте роста благосостояния общества. // Вестни Северо-Кавказског федеральног университета. 2018, № 3 (66) – с.76-84.
6. Benos E., Garratt R., Gurrola-Perez P. The economics of distributed ledger technology for securities settlement. Bank of England. // Staff Working Paper Staff Working Paper. 2017, №. 670 – p.1-33.
7. Свон М. Блокчейн. Схема новой экономики. – Litres, 2019. – 215 с.
- Puthal D. et al. Everything you wanted to know about the blockchain: Its promise, components, processes, and problems // IEEE Consumer Electronics Magazine. 2018, №. 4. – с. 6-14.
8. Tasca P., Tessone C.J. Taxonomy of blockchain technologies. Principles of identification and classification // arXiv preprint arXiv. 1708.04872. – 2017. URL: <https://arxiv.org/pdf/1708.04872.pdf> (access: 29.06.2019)
9. Morrison D.R. PATRICIA - practical algorithm to retrieve information coded in alphanumeric // Journal of the ACM (JACM). 1968, №. 4. – p. 514-534.
10. Wood G. et al. Ethereum: A secure decentralised generalised transaction ledger // Ethereum project yellow paper. 2014. – p.1-32.
11. Ethereum, “<https://ethereum.org/>,” (2015), (Date last accessed: 10-July-2015).
- European Central Bank and Bank of Japan. Stella project. Payment systems: liquidity saving mechanisms in a distributed ledger environment. URL: https://www.boj.or.jp/en/announcements/release_2017/data/re1170906a1.pdf - European Central Bank and (access: 12.01.2018).
12. Project Ubin. URL: <https://github.com/project-ubin> (access: 12.05.2019).
13. Ripple. URL: <http://www.ripple.com> (access: 12.05.2019).