Ну и остается последний раздел – это «Новостная лента». Там будут показаны последние новости. А именно: кто зарегистрировался новый, кто выложил новую картину, какие-то посты об искусстве от администратора. В дальнейшем этот раздел можно расширить. Например, можно сделать чтобы сами пользователи смогли выкладывать не только картины, но и посты писать. Или пойти дальше и сделать не рандомную ленту, а по подпискам.

Проект Pickofpic может и не уникальный, но точно станет востребованным. Особенно примечательна его масштабируемость. Он может разрастись до полноценной социальной сети, то есть до весьма перспективной площадки с будущим.

УДК 004.056+003.26

Студ. К.М. Процукович
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМИЧЕСКИХ СВОЙСТВ КРИПТОВАЛЮТНЫХ ТЕХНОЛОГИЙ

Ниже будет проведен сравнительный анализ наиболее широко распространенных криптовалютных платформ, и, в частности, мы исследуем Bitcoin, Ethereum и Ripple. Проанализируем консенсусные и стимулирующие механизмы, используемые различными протоколами. Затронем некоторые аспекты безопасности [1-4].

Криптографическая валюта *Bitcoin* [3] впервые популяризировала концепцию Blockchain. Вплоть до того, как Bitcoin и его распределенная глобальная бухгалтерская книга были изобретены, цифровые активы полностью управлялись централизованными органами, отслеживающими все транзакции.

Ethereum – одна из технологий Blockchain второго поколения, целью которой является создание новой модели для построения децентрализованных приложений.

Ripple является типом консенсус-ориентированной распределенной базы данных. Эта система не является технологией Blockchain, поскольку транзакции не добавляются в виде блоков, которые связаны друг с другом хеш-цепью. Однако, подобно моделям согласования блоков, сеть Ripple обновляет регистр посредством согласованного процесса между узлами [1-2].

Технология Blockchain позволяет организациям осуществлять транзакции напрямую, без необходимости отправлять предложенные транзакции централизованной третьей стороне, действующей в каче-

стве доверенного посредника. Каждый узел хранит отдельную копию цепочки блоков, состояние которой обновляется по мере добавления новых блоков. Однако узлы могут иметь совершенно непоследовательное представление данных, записанных в цепочке блоков, из-за расходящегося порядка, в котором транзакции перечислены в репликах. Поэтому участникам необходимо координировать действия друг с другом, чтобы определить законный регистр и гарантировать согласованность системы на всех узлах.

В таблице 1 приведены для сравнения данные о механизмах подтверждения рассмотренных технологий.

Proof-of-Work (PoW – дословно: доказательство работы) — алгоритм защиты главной особенностью заключается в асимметрии затрат времени решения — они значительны на нахождение решения и весьма малы для проверки.

Схема Bitcoin PoW заложила теоретическую основу для современных консенсусных моделей, и все еще появляются новые, обеспечивающие инновационные функции и свойств.

Таблица 1 – Сравнительный анализ механизмов подтверждения

	Bitcoin	Ethereum	Ripple
Метод верификации	PoW	PoW (Ethash)	Консенсус
Вовлеченные узлы	Все	Все	Валидаторы
Алгоритм хеширования	SHA-256	Keccak-256	SHA-512Half
Время на подтверждение блока	10 минут	14 секунд	5-10 секунд
Скорость транзакции	Низкая	Низкая	Высокая
Награда майнерам	?	?	X
Комиссия за перевод	?	?	?

Хотя доказательство, используемое в Ethereum, аналогично протоколу Bitcoin PoW, в Ethash он использует другой криптографический примитив для своей функции хеширования, называемый Keccak-256, вместо того чтобы полагаться на алгоритм двойного хеширования SHA-256.

Однако есть модели, которые используют другой подход для демонстрации согласованности транзакций. Среди них Ripple, которая выбрала схему голосования, называемою консенсусом. Цель состоит в том, чтобы все узлы могли договориться о том, какие транзакции следует включить в последнее закрытие реестра.

Поскольку в Ripple отсутствует процесс решения криптографической загадки с подтверждением работы, консенсус быстр, и регистры проверяются за считанные секунды. Поскольку новая транзакция закрывается примерно каждые 5 секунд. Это значительно отличается от времени блокировки Bitcoin. Действительно, новый блок генериру-

ется примерно каждые 10 минут. Сеть Ethereum, для сравнения, производит блок в среднем каждые 14 секунд.

Важной функцией в поддержании неизменности системы Blockchain является стимулирование. Поскольку процесс консенсуса требует сотрудничества между участниками с неприсоединившимися интересами. Bitcoin включает в себя механизмы стимулирования, которые приходят в форме вознаграждений за майнинг и комиссионных за транзакции. Первый узел, который успешно решает PoW и получает возможность добавить свой блок в цепочку блоков, может получить *вознаграждение* за *блок*.

Подход, принятый Ripple, полностью отличается от только что описанных моделей, поскольку он не обеспечивает прямого денежного вознаграждения за поддержку узлов. Причина такого отсутствия механизма стимулирования заключается в том, что в Ripple не используется процесс майнинга.

По замыслу, как только транзакция добавлена в цепочку блоков и подтверждена, она никогда не может быть отменена. Однако, несмотря на то, что целостность данных является одним из ключевых моментов Blockchain, они не являются неуязвимыми для кибератак, потому что законные изменения в глобальной записи могут быть сделаны в принципе любым.

Таблица 2 – Сравнительный анализ аспектов безопасности

	Bitcoin	Ethereum	Ripple
Проблема двойной траты	?	?	?
51% атаки	X	X	?
Атака «отказ в обслуживании»	?	?	?

Проблема двойной траты относится к случаю повторная продажи одних и тех же активов. Bitcoin решает эту проблему путем хронологического упорядочения блоков транзакций в непрерывную цепочку проверок работы, которая видна всем пользователям. Точно так же Ethereum использует свой алгоритм на основе PoW, чтобы предотвратить риск того, что пользователь может одновременно потратить одну и ту же единицу валюты в нескольких транзакциях.

Ripple предлагает альтернативное решение проблемы двойных расходов через процесс консенсуса. Так как процесс требует согласования порядка транзакций, если две транзакции представляют собой двойные затраты, атака решается простым согласованием того, какая из двух транзакций будет первой (другая считается недействительной и, следовательно, не применяется).

В нынешних условиях дизайн Blockchain по своей природе уязвим для атаки на 51%. Если злоумышленник контролирует более 50% мощ-

ности майнинга, он может создать независимую ветвь. Таким образом, если эта атака успешна, злоумышленник может манипулировать реестром в свою пользу. Эмпирические данные показывают, что эта атака неосуществима для любого отдельного пользователя, поскольку для ее перерасчета все доказательства для всех предыдущих блоков в цепочке потребуют огромных вычислительных ресурсов. Однако, хотя сам Bitcoin является чисто децентрализованным, снижение стимула для майнинга приводит к централизации функции майнинга. Утверждают, что эта тенденция к централизации увеличивает риск атаки на 51%. Ethereum обладает теми же слабостями, что и Bitcoin, в отношении атаки на 51%.

Ripple, как известно, не полагается на распределенную вычислительную мощность для защиты целостности сети. Он заменяет голосование за вычислительную мощность понятия майнеров о механизмах консенсуса на основе PoW на голосование валидатор. Основное предположение заключается в том, что большинство узлов Ripple не будут вступать в сговор с целью манипулирования результатом голосования. На самом деле, если 80% проверяющих серверов вступают в сговор, можно подтвердить мошенническую транзакцию. Однако в случае, если большинство валидаторов становятся вредоносными, они могут переписать всю историю транзакций системы.

Наконец, поскольку технология Blockchain основана на общедоступном реестре информации, поддерживаемой сетью компьютеров по всему миру, злоумышленники могут транслировать большое количество спама в транзакциях, пытаясь нарушить нормальную работу сети. Наиболее заметным последствием такой атаки является создание избыточной нагрузки на сеть [5], что вызывает трудности в обработка законных транзакций.

Чтобы смягчить атаки типа «отказ в обслуживании», Ripple вводит плату за транзакцию. Это создает сильный сдерживающий фактор против спама в журнале, потому что любые атаки, направленные на потерю пропускной способности сети, становятся очень дорогими для злонамеренных агентов

Мы рассмотрели консенсусные и стимулирующие механизмы, а также некоторые аспекты безопасности трех платформ: Bitcoin, Ethereum и Ripple. Bitcoin является первой полноценной крипловалютой, в некоторых аспектах он отстает от аналогов, в связи с тем, что конкуренты предлагают решение тех проблем, с которыми Bitcoin справиться не в состоянии, будь то атака 51% или скорость транзакций, но

даже так он всё же остается самой капитализированной и популярной криптовалютой в мире.

ЛИТЕРАТУРА

1. Ethereum Wiki, Ethash. [Электронный ресурс]. – Режим доступа: https://github.com/ethereum/wiki/wiki/Ethash. – Дата доступа: 15.04.2019.

2. Schwartz, D., Youngs, N. and Britto, A. 2014. The Ripple Protocol 2.Consensus Algorithm. White Paper. [Электронный ресурс]. – Режим доступа: https://ripple.com/files/ripple_consensus_whitepaper.pdf. – Дата доступа: 15.04.2019.

3. Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. [Электронный ресурс]. – Режим доступа: https://bitcoin.org/bitcoin.pdf. – Дата доступа: 15.04.2019.

4. The free encyclopedia Wikipedia. [Электронный ресурс]. – Режим доступа https://en.wikipedia.org/wiki/Bitcoin. — Дата доступа: 15.04.2019.

5. Урбанович, П. П. Компьютерные сети: учебное пособие для студентов высших учебных заведений по техническим специальностям / П. П. Урбанович, Д. М. Романенко, Е. В. Кабак. - Минск: БГТУ, 2011. – 399 с.

УДК 004.056+003.26

Студенты К. В. Клицунова, Е. И. Дубовик
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

СТЕГАНОГРАФИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Некоторые основные понятия из предметной области [1,2], которые будут использованы в докладе.

Стеганография — это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

Стеганографическая система – объединение методов и средств, используемых для создания скрытого канала для передачи информации.

Контейнер – любая информация, используемая для сокрытия тайного сообщения.

Стеганографический канал – канал передачи стегоконтейнера.

Ключ – секретная информация для сокрытия стегоконтейнера и излечения информации из него.