Главным преимуществом данного проекта является его высокая аппаратная и программная вариативность. Аппаратная вариативность предоставляет возможность выбирать тот набор датчиков, который необходим для конкретного пользователя или существующей системы. Причем, для внедрения нового датчика в устройство его нужно лишь физически подключить к существующему интерфейсу, а программная составляющая автоматически его интегрирует в информационную систему. Программная вариативность подразумевает возможность выбора того стека технологий, который наиболее эффективно позволит решить поставленные задачи.

Литература

1. Raspberry Pi Series Datasheet Version 3.3 [Electronic resourse] // Espressif Systems. – URL: https://wiki.merionet.ru/servernye-resheniya/36/arduino-vs-raspberry-pi-chto-vybrat/ – Date of access: 21.03.2022.

2. Non-volatile storage library [Electronic resourse] // Espressif Systems (Shanghai). – URL: https://habr.com/ru/post/167459/. – Date of access: 21.03.2022.

3. Arduino core for the Raspberry Pi [Electronic resourse] // GitHub. – URL: https://github.com/raspberrypi. – Date of access: 21.03.2022.

Н. В. Лукашевич
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **Г. Ю. Тюменков**, канд. физ.-мат. наук, доцент

ТЕХНОЛОГИЯ БЛОКЧЕЙН

Криптовалюта – это разновидность валюты в цифровой (виртуальной) среде. Системы таких валют являются децентрализованными (нет центрального органа администрирования). Существуют разные способы создания блоков в блокчейне, но мы рассмотрим майнинг и форжинг (минтинг).

Майнинг в дословном переводе добыча полезных ископаемых – это процесс создания блоков в блокчейне используя вычислительные мощности компьютерного оборудования.

Форжинг в переводе ковка или же минтинг в переводе чеканка монет – это также процесс создания блоков в блокчейне, но на основе подтверждения доли владения.

Блокчейн от английского block – блок, chain – цепь, дословно цепочка блоков, содержащих информацию. Блок содержит информацию о транзакциях. Транзакция считается завершенной и подтвержденной, когда она проходит все проверки в сети и записывается вместе с другими транзакциями в блок. Все блоки связанны между собой, так как каждый новый блок содержит информацию о предыдущем и их содержимое может быть проверено. И соответственно в блокчейне содержится информация обо всех транзакциях, когда-либо совершенных в сети. Например, сегодня блокчейн биткоина весит более 380 Гигабайт. Для добавления блока в цепочку, он должен пройти проверку, называемую консенсусом.

Есть разные механизмы проверки, но мы рассмотрим PoW – Proof of Work (Доказательство выполнения работы) и PoS – Proof of Stake (Доказательство доли владения).

PoW использует оборудование майнера, решая сложные математические задачи. Поиск решения блока – сложный процесс, для которого нужны значительные вычислительные мощности. Когда решение найдено, оно отправляется на другие компьютеры сети для проверки, тем самым закрепляя блок в сети. Особенностью является то, что математическая задача является сложной для майнера, но легкой для сети. Фактически решение ищется методом перебора и для успешного решения требуется множество попыток. Майнер, который первым найдет верное решение, получает награду в виде криптовалюты. Из недостатков защиты такого метода можно отметить «атака 51%» – когда майнер имеет больше половины вычислительных мощностей сети, у него появляется возможность подтверждать свои блоки и игнорировать чужие, но получить половину мощности сети будет очень дорогостоящим занятием. Это позволяет получать ему всю эмитирующую валюту и возможность блокировать транзакции, что будет приводить к исчезновению со счетов криптовалют в новых блоках. Также проблемой является то, что для больших вычислительных мощностей требуется большое количество электроэнергии.

Долгое время PoW был единственным механизмом консенсуса. Из-за его проблем таких как «атака51%», высокий расход электроэнергии и «гонка вооружений» – когда майнеры постоянно увеличивают вычислительную мощность и старое оборудование перестает получать новые блоки, нужно было придумать новые способы кон-

сенсуса. Одним из таких стал PoS. При таком механизме взамен вычислительных мощностей имеет значение количество криптовалюты, находящейся у валидаторов (узлов системы блокчейна, которые поддерживают его работоспособность) на счету. Чтобы стать валидатором нужно заморозить часть монет (сделать ставку), тем самым приняв участие в стекинге, и в этом случае компьютер станет узлом. Криптовалютный алгоритм выбирает случайным образом одного валидатора из всех для создания нового блока. Механизм PoS может учитывать некоторые факторы для выбора, например: сумму активов (долю владения от всего количества криптовалюты), время, когда было получено последнее вознаграждение, срок участия валидатора. Например, участник, который владеет 1% от всего количества криптовалюты, в среднем будет генерировать 1% новых блоков. Если узел выбран для проверки следующего блока, он проверит, все ли транзакции в нем действительны. Если все в порядке, узел подписывает блок и добавляет в блокчейн. В качестве вознаграждения узел получает комиссии, связанные с каждой транзакцией в данном блоке. Далее блок может проверяться некоторым количеством валидаторов для выявления мошеннических транзакций. Для защиты от мошенничества используется ставка, которую нужно внести, чтобы стать валидатором. Например: валидаторы потеряют часть своей ставки, если одобрят мошеннические транзакции. Если узел перестает быть валидатором его ставка и все комиссии за транзакции, которые он получил, будут разблокированы через определенный период времени.

По сравнение с PoW PoS тратит гораздо меньше электроэнергии так как в PoW майнят все пользователи, а в PoS выбирается один валидатор. Так же PoS имеет большую степень децентрализации, так как в PoW майнеры объединяют свои мощности в пулах для увеличения шанса на добычу нового блока и получения вознаграждения, и эти пулы централизуют процесс майнинга, они могут контролировать большую часть всех мощностей майнинга, что может привести к «атаке 51%». И для PoS не нужно дорогостоящее оборудование, что побуждает людей создавать узлы и делать систему более децентрализованной и более безопасной. Но PoS также может быть подвержен «атаке 51%», хотя для этого нужно заиметь более половины всей криптовалюты. И также нужно делать исследования и разрабатывать алгоритмы выбора валидатора, для того чтобы понимать все риски и смягчать их.