Zold: Новая Криптовалюта

Green Paper

Yegor Bugayenko
yegor256@gmail.com
www.zold.io

0.9.1

12 августа 2018 г.

За последние несколько лет цифровые валюты успешно продемонстрировали свою способность стать альтернативным финансовым инструментом на различных рынках. Большая часть доступных в данный момент технологий построена на принципах архитектуры Blockchain, туда можно отнести такие распространенные валюты как Bitcoin и Ethereum. Несмотря на свою популярность, Blockchain — хорошее решение не для всех ситуаций. Один из примеров — быстрые и дешевые микротранзакции. Zold — экспериментальная альтернатива, которая делает возможными распределенные транзакции между анонимными пользователями, которые удешевляют и ускоряют микроплатежи. Zold заимствует принцип «доказательства выполнения работы» у Bitcoin и предлагает новую архитектуру для обслуживания цифровых кошельков, о чем подробнее в White Paper.

Рынок

С момента выпуска в 2009 году, Bitcoin из «либертарианской сказки» и «модного движения в Силиконовой Долине» превратился в «катализатор изменения финансовой системы в пользу большей эффективности для физических лиц и фирм», пишет Andreessen. Несмотря на заявление Cheah и др. о том, что «фундаментальное значение Bitcoin равняется нулю», Van Alstyne утверждает: «Вопрос не в том, имеет ли ценность Bitcoin; а он имеет. Важно то, может ли продуктивность такой криптовалюты как Bitcoin соединиться с надежностью честного Центрального банка».

Основным компонентом Bitcoin является технология Blockchain, которая «гарантирует устранение проблемы двойного расходования при помощи криптосистемы с открытым ключом» и «деньги переводятся посредством электронной подписи в хэше», объясняет Pilkington. Вскоре после того, как создали Bitcoin, были представлены подобные криптовалюты, также основанные на принципах Blockchain, такие, как Ethereum от Buterin.

Несмотря на то, что Blockchain — разумное решение проблемы двойного расходования, существует множество других решений из разряда «доказательство X». К примеру, Everaere и др. опубликовали краткий анализ существующих подходов и объявили о создании своего варианта решения данной проблемы; Boyen и др. описали «действительно распределённую книгу учёта на основе плоского графика кросс-проверочных операций»; недавно IOTA, «криптовалюта на основе сплетений», была запущена Popov; Hedera по их собственным словам признана «первой в мире принятой в массах публичной книгой учёта».

Проблемы

Zold является децентрализованной цифровой валютой, которая поддерживает свои книги учёта посредством непредсказуемого количества анонимных и ненадежных серверных нодов, стараясь гарантировать последовательность данных. Архитектура Zold не основывается на принципах Blockchain. Разработка Zold была мотивирована желанием обойти два очевидных недостатка, присутствующих в большинстве существующих криптовалют:

Первая проблема состоит в том, что обработка транзакции довольно медлительна. Скорость обработки Bitcoin в настоящий момент — семь транзакций в секунду (tps), в то время как PayPal в среднем справляется со 115 tps, а сеть VISA достигает предела в 47000 tps. Karame и др. утверждает, что «Bitcoin нуждается в десятках минут для подтверждения транзакции и, ввиду этого, не подходит для быстрых платежей». Это неизбежно, поскольку «скорость обработки напрямую зависит от механизма безопасности, обеспечивающего правильность работы» отмечает Kiayias и др. По словам Fekkes и др., Ethereum способен обрабатывать «в два раза больше транзакций, чем Bitcoin», но в итоге это всё равно довольно медленно.

Вторая проблема, как было замечено Popov, состоит в том, что «не так-то просто избавиться от налогов в инфраструктуре Blockchain, поскольку они служат стимулом для создателей блоков». Möser и др. говорит, что «пользователям Bitcoin предлагают платить налоги майнерам до 10 центов (в долларах США) за каждую транзакцию вне зависимости от размера платежа», что особенно ощутимо в случае, когда сумма транзакции составляет менее одного доллара. Более того, по словам Kaskaloglu, «увеличение в сумме налогов на транзакции Bitcoin неизбежно».

Таким образом, скорость операций является низкой, а стоимость обработки — высокой. Zold была создана в качестве попытки решения этих двух проблем.

Функции

Во-первых, в отличие от всех других криптовалют, в Zold нет центральной распределённой книги учёта. У каждого кошелька есть своя книга учёта. Все операции в каждой из них подтверждаются RSA-подписями владельцев кошельков. Это делает возможными высокую производительность и масштабируемость базы данных.

Во-вторых, будучи схожей с иными цифровыми валютами, включая Bitcoin, Ethereum, Monero, Plancoin, Dero и другими, криптовалюта Zold использует CPU мощности, затрачиваемые каждым из серверов на выполнение определённых «бессмысленных» вычислений, для нахождения консенсуса между конфликтующими тразакциями, что также известно как принцип «доказательства проделанной работы», изначально представленный Back в 1997. Это гарантирует последовательность данных и устраняет возможность появления проблемы двойного расходования.

В-третьих, Zold — это цифровой премайн-актив, подобный Ripple, Cardano, Stellar, NEO и некоторым другим криптовалютам. Zold алгоритмически ограничивает свой общий запас монет объёмом в 2,15 млрд ZLD. Для сравнения, общий запас других криптовалют составляет: 21 млн у Bitcoin, 100 млрд у Ripple, 84 млн у Litecoin, и 19 млн у Dash. Bohr и др. объясняют, что криптовалюты лимитируют свои запасы с целью «защититься от инфляции»; то же самое делает и Zold, чтобы обезопасить свою ценность на рынке.

В-четвертых, скорость выполняемых Zold операций буквально безгранична, так как все платежи производятся локально на устройствах пользователей, а затем направляются в сеть для соединения и хранения.

В-пятых, стоимость обработки транзакций у Zold значительно ниже, чем может предложить большинство других платёжных систем. Чтобы обработать 1000 транзакций, пользователь должен заплатить около $500 при работе с Bitcoin, $300 с Ethereum, $45 с Litecoin, $12 с Ripple и $9 с Bitcoin Cash. В работе с Zold такое же количество операций обходится всего в $4, что делает её одной из самых финансово выгодных криптовалют.

Стратегия

Zold — это размещённое на GitHub программное обеспечение с открытым исходным кодом, равно как и многие другие криптовалюты. Первая экспериментальная версия была создана и запущена Егором Бугаенко, основателем и CEO компании Zerocracy, Inc., 27 мая 2018 года. Распределённая сеть нодов, которые управляют программным обеспечением Zold, поддерживается анонимными добровольцами. Разработка последующих версий и обслуживание имеющихся зависит от того, насколько активно поддерживают проект участники GitHub, частично финансируемые компанией Zerocracy.

Как недавно отметил председатель SEC Jay Clayton, «криптовалюты вроде Bitcoin — не ценные бумаги». Подобно Bitcoin и Ethereum, Zold — это криптовалюта, а не ценная бумага. Она раздается Zerocracy в качестве цифрового подарка тем, кто активно сотрудничает с экосистемой Zerocracy, участвует в разработке программного обеспечения Zold и занимается поддержкой нодов.

Кроме программирования, добровольцы могут внести свой денежный актив, например, доллары США, в любой из проектов, разрабатываемых и руководимых Zerocracy. Взамен, в качестве вознаграждения, они получают цифровые монеты ZLD. Далее, ZLD можно поменять на другие криптовалюты и бумажные деньги посредством обмена на биржах.

Предполагается, что рыночная стоимость ZLD будет расти благодаря техническим преимуществам и популярности платформы Zerocracy среди программистов и программных компаний.