Блокчейн Plan
2020

White Paper ver 1.0

Содержание:

1. Предисловие

Все сенсационные и революционные составные части протокола Биткойн и идеи, заложенные в нем, в общем-то, были известны и до 2009 года, но вот слепить все вместе и заставить это работать удалось именно авторам Биткойна и именно в 2009-м. Авторы идеи крипто валюты хотели сделать инновационное платежное средство, которое будет универсальным, независимым от внешнего регулирования, доступным везде и простым в использовании. У авторов Биткойна была задача: при которой одним из ключевых принципов являлось заставить это как-то работать при условии, что центра нет и что никто никому не доверяет, и авторы задачу выполнили, электронные деньги функционируют!

Для того, чтобы пользоваться массовой популярностью, виртуальные деньги должны быть не только удобными, но и защищенными. Согласитесь, никому не интересна валюта, которую легко взломать, или которая может вдруг «умереть», когда станет неинтересна ее создателям. Чтобы этого не случилось, используют децентрализации сети.

a. Децентрализация

Децентрализация криптовалюты – это рассредоточенность ее основных ресурсов (данных) по всему миру, с многократным дублированием для предотвращения их потери. Цепочка данных (блокчейн) не хранится на каком-то основном сервере, а находится одновременно на множестве компьютеров пользователей по всему миру.

b. Proof-of-Work -Доказательства выполнения работы

Майнинг — это процесс, в ходе которого отдельные лица, группы или компании с помощью мощных компьютеров решают сложные математические уравнения для проверки блоков транзакций. Эти математические задачи — часть процесса шифрования, защищающего транзакции от киберпреступников и доступа третьих лиц. Первый, кто успешно решает задачу и подписывает блок транзакций, получает вознаграждение.   Наряду большого количества преимуществ у BTC имеются и недостатки, и вот некоторые из них:

Постоянное усложнение процесса майнинга, при котором объем вознаграждения за каждый новый блок уменьшается. Это требует постоянного увеличения добывающих мощностей, чтобы получать относительно стабильную прибыль. Миллионы компьютеров проверяют одни и те же транзакции по одним и тем же правилам, производят идентичную работу записывают в блокчейн одно и то же, хранят всю историю за все время, одинаковую, одну на всех.

Отсутствие СМАРТ- контрактов. Blockchain биткоина не позволяет устанавливать условия для совершения транзакции в новом блоке, поскольку он содержит только информацию о самой транзакции.

2. Smart-contract

Принцип интеллектуальных контрактов был описан американским криптографом и программистом Ником Сабо еще в 1996 году задолго до появления технологии блокчейн. Согласно концепции Сабо, интеллектуальные контракты — это цифровые протоколы для передачи информации, которые используют математические алгоритмы для автоматического выполнения транзакции после выполнения установленных условий и полного контроля процесса. Это определение, которое опережало свое время более чем на десять лет, остается точным и по сей день. Однако в 1996 году эта концепция не могла быть реализована: в то время необходимые технологии не существовали, в частности, блокчейн. Тем не менее появление технологии послужило толчком для разработки смарт-контрактов.

3. Ethereum

Ethereum – глобальная платформа с открытым исходным кодом для децентрализованных приложений.
Поэтому, когда речь идет о Ethereum, то в первую очередь речь идет о платформе, и только во вторую о криптовалюте.
С помощью Ethereum вы сможете писать доступные всему миру программы для управления цифровыми данными, работающие именно так, как задумано.   Блочная платформа Ethereum позволила использовать смарт-контракты на практике. Сегодня рынок предлагает множество платформ, которые позволяют использовать смарт-контракты, но Ethereum остается одним из самых распространенных.

Революционное решение, “покусившееся на святое” и подвинувшее блокчейн Сатоши Накамото, обеспечило Ethereum небывалую популярность. Из-за легкости обеспечения выполнения смарт-контрактов Ethereum стал основной платформой для проведения ICO, количество которых растёт от года к году.
Впрочем, хотя это все выглядит как небывалая история успеха, известность сыграла с Ethereum плохую шутку. Поскольку сейчас Ethereum — основная площадка для проведения ICO, количество транзакций и операций в сети растет ежедневно, что обнажает основную ее проблему — недостаточность производительности. Нагрузку на Ethereum помимо многочисленных ICO обеспечивают и разрабатываемые децентрализованные приложения (DAPP), и собственная служба доменных имен (ENS). Проблема с пропускной способностью делает дальнейшие перспективы сети довольно туманными — контрактов выполняется все больше и больше, и чтобы они могли работать в полную силу необходимо радикальное увеличение производительности. (Пропускной способности узлов).

a. POW-POS

С переходом на новую версию пропускная способность Ethereum будет повышаться постепенно. Первоначально разработчики повысят масштабируемость данных, после чего займутся улучшением параметра для общих вычислений.

ETH 2.0 (также известный как Serenity) относится к следующему крупному обновлению базового протокола Ethereum. Он объединяет некоторые улучшения базового протокола Ethereum (уровень 1) и переход на Proof-of-Stake.

b. Proof-of-Stake -доказательства владением долей(стэйка)

Proof of Stake представляет класс консенсусных алгоритмов, в которых валидаторы голосуют за следующий блок, и вес голоса зависит от размера его ставки. Это считается улучшением по сравнению с Proof of Work (PoW) из-за меньшего потребления электроэнергии, снижения рисков централизации, защиты от различных типов атак на 51% и многих других.

c. Преимущества

Каковы преимущества Доказательства Стэйка перед Доказательством Работы?

- Не нужно потреблять большое количество электроэнергии для того, чтобы обезопасить блокчейн.
- Из-за отсутствия высоких требований к потреблению электроэнергии не так много нужно выпустить новых монет, чтобы мотивировать участников продолжать участвовать в сети
- Доказательство стэйка открывает двери для более широкого спектра методов, использующих теоретико-игровые механизмы, чтобы более эффективно препятствовать формированию централизованных картелей.
- Снижение рисков централизации.
- Способность использовать экономические штрафы, чтобы сделать различные формы атак на 51%, значительно дороже, чем Proof of Work. Перефразируя Влада Замфира, «ваша ферма ASIC сгорела, если вы участвовали в атаке на 51%».

Существует много видов согласованных алгоритмов и множество способов назначения вознаграждений валидаторам, которые участвуют в согласованном алгоритме, поэтому существует множество «разновидностей» PoS. Однако с алгоритмической точки зрения существует два основных типа: PoS на основе цепочки и BFT-стиль. В PoS в BFT-стиле валидаторам случайным образом назначается право предлагать блоки, но согласование того, какой блок является каноническим, осуществляется посредством многоэтапного процесса, когда каждый валидатор отправляет «голос» за какой-то конкретный блок во время каждого раунда, и на конец процесса все валидаторы постоянно соглашаются, является ли какой-либо данный блок частью цепочки. Обращаем внимание, что блоки все еще могут быть связаны друг с другом; ключевое отличие состоит в том, что консенсус по блоку может прийти в пределах одного блока и не зависит от длины или размера цепочки после него.

4. Развитие как неизбежность

Рассмотрев лидирующие блокчейны предлагаю выделить основополагающие тезисы, которые являются неотъемлемой составляющей развития современной криптовалюты:

- Децентрализация, как процесс распределения власти, финансов или усилии без вмешательства глобального управляющего органа.
- Масштабируемость, как способность блокчейна справляться с наплывом большого числа транзакции в один момент. Proof of Stake
- Смарт-контракт, как средство совершения и (или) исполнения сделки.
- Демократия, как основополагающий принцип честности и открытости заложенный в политику развития блокчейна.
- Безопасность.
- Простота и доступность.

Теперь, когда мы знаем и видим основные векторы развития ведущих криптовалют мира, и те современные решения, к которым они прибегают давайте перейдём к Блокчейну PLAN.

5. Блокчейн PLAN создан на базе Cosmos SDK и Tendermint

a. Cosmos и его возможности

Самой прогрессивной технологией года является Cosmos и экосистема Cosmos Network «Глобальная сеть блокчейнов» в которой разные системы могут напрямую обмениваться своими токенами. В сети это явление называют Blokchain 3.0 И именно на данном модульном фреймворке Cosmos SDK и Tendermint разработан блокчейн PLAN.
Перейдём к более подробному изучению Cosmos SDK, Tendermint и DPOS –майнингу.

b. Tendermint

Византийская отказоустойчивость (BFT) консенсусные протоколы. Термин «византийский» был использован из-за сходства проблемы с той, с которой столкнулись генералы византийской армии, пытавшиеся скоординировать свои действия для нападения на Рим, используя только гонцов, где один из генералов может быть предателем.

Tendermint это алгоритм консенсуса устойчивый к византийским падениям. Византийские падения для тех кто не знает, это какие-то злоумышленные действия. В отличие от Nakamoto консенсуса, где выбирается цепочка с самым большим количеством работы, в Tendermint выбирается цепочка где за блок проголосовало 2/3 участников сети.

Высокий уровень безопасности

Высокая скорость производительности (до 1000 тр./ сек.)

Масштабируемость

Доступность в использовании

Тендерминт BFT – это не зависимый от приложения «механизм консенсуса» который может превратить любое детерминированное приложение в распределенную репликацию блокчейна. Подключение к приложению блокчейна используется Application Blockchain Interface – интерфейс который определяет границу между механизмом создания цепочки блоков и конечным приложением.

c. Delegated Proof-of-Stake (DPoS)

DPoS – Делегированное доказательство доли. Согласованный алгоритм делегированного доказательства доли (DPoS) был разработан Даниэлем Ларимером в 2014 году, и является одной из разновидностей алгоритма POS.

(DPoS) — это алгоритм, с помощью которого распределённые узлы в сети достигают согласия относительно элемента данных, при котором определённому узлу (валидатору) достанется право добавить в цепь новый блок.

В DPoS, держатели доли в системе могут выбирать валидаторов, которые будут голосовать от их имени. Все узлы производят блоки - по одному за раз - по циклическому принципу. Это не позволяет узлу публиковать последовательные блоки, тем самым, не давая ему возможность осуществлять атаки двойной траты. Если валидатор не производит блок в отведенном ему временном интервале, то этот временной интервал пропускается, и следующий валидатор производит следующий блок. Если валидатор постоянно пропускает свои блоки или публикует недействительные транзакции, то он штрафуется и держатели доли голосуют против него и заменяют его другим валидатором.

Основными преимуществами алгоритма DPoS являются:

- держатели доли имеют возможность делегировать свои голоса, при этом не передавая сам баланс.
- держатели балансов имеют возможность получить дополнительный доход от их владения,
- минимизация издержек на поддержку Блокчейн сети, снижается количество «ненужной работы» при выборе следующего голосующего.

6. Blokchain PLAN

Блокчейн PLAN создан на базе Cosmos SDK и Tendermint

Блокчейн PLAN- над созданием и развитием которого работает очень большая команда, где каждый член комьюнити вносит свой вклад для создания современной мощной и безопасной экосистемы, перспективы развития которой просто безграничны. Команда имеет колоссальный опыт по созданию и воплощению в жизнь большого количества программ, идей и проектов, где идеология развития тесно переплетается с такими понятиями, как честность и открытость. Согласно этой идеологии, партнёр, не просто может, а должен и обязан зарабатывать. И только с таким подходом можно говорить о долгосрочной перспективе работы и развития.

Для реализации всех своих программ и проектов нужен надёжный, современный и качественный инструмент, развитие которого будет идти в ногу со временем, использовать все технологии и инноваций современного мира блокчейна. Именно поэтому Блокчейн PLAN создан на базе Cosmos SDK и Tendermint.

a. Преимущества

Децентрализация, как процесс распределения власти, финансов или усилии без вмешательства глобального управляющего органа.

Масштабируемость, способность блокчейна справляться с наплывом большого числа транзакции в один момент, более 1000 т/сек

Смарт-контракты, как средство совершения и (или) исполнения сделки, по средством Cosmos Network и Cosmos Hub.

Демократия, как основополагающий принцип честности и открытости заложенный в политику развития блокчейна, посредством голосования.

Высокий уровень безопасности.

Простота и доступность в использовании.

Открытый код на GitHub

b. Майнинг

Экономическая модель блокчейна PLAN такова, что каждый пользователь монеты имеет право получать награду
в виде дополнительных монет.

Вариант -1. Валидатор – это нода (узел) которая участвует в поддержании сети и создании блоков. При честной работе такой узел получает часть награды от комиссий которые были собраны с тех транзакций, которые вошли в состав блока.

Вариант -2. Делегатор – это участник сети, делегирующий свои монеты валидатору (но не передающий право на их владение) тем самым голосует и добавляет свои монеты в стек валидатора, деля с ним награду за создание блока.

Вариант -3. Pos mining -Самая интересная часть награды участника сети блокчейн PLAN.

Монеты в личном кошельке		Монеты в кошельках последователей		Дней с последней транзакции	
Количество монет в кошельке	Рост количества монет в день, %	Количество монет последователей	Повышающий коэффициент	дней	Дополнительный коэффициент
1+	0,08	0+	1.0	0+	1.0
100+	0,11	10 000+	1.9	30+	1.6
1 000+	0,12	100 000+	2.2	90+	1.8
10 000+	0,14	1 000 000+	2.4	180+	2
100 000+	0,16	10 000 000+	2.6	270+	2.2

7. Дополнительные материалы

https://docs.ethhub.io/
https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md#appendix
https://github.com/tendermint/tendermint
https://cosmos.network/intro
https://cosmos.network/sdk
https://hub.cosmos.network/master/hub-overview/overview.html
https://www.homeonrails.com/
https://docs.tendermint.com/master/spec/consensus/consensus.html
https://medium.com/cosmos-russia/
https://blog.cosmos.network/tendermint-explained-bringing-bft-based-pos-to-the-public-blockchain-domain-f22e274a0fdb
https://smart-contracts.ru/cosmos.html

Данную версию Белой Книги считать версией White Paper ver 1.0 Которая будет дополняться и дорабатываться, по мере обновления Блокчейна Plan, но исключается искажение подмена или подлог основных понятий и основополагающих принципов заложенных в Блокчейн Plan.