# Криптовалюты от А до Я

**Автор:**
Александр Герасимович

Криптовалюты от А до Я

Александр Герасимович

«Криптовалюты от А до Я» – это словарь о криптовалютах, в котором собран также криптожаргон и сленговые выражения. Здесь вы найдете информацию не только о том, что такое майнинг, криптовалюта, биткойн, блокчейн, но также познакомитесь с такими понятиями, как криптоанархизм, криптоослепление, сайдчейн и найдете много другой полезной информации. Всего в книге содержится около 850 терминов. Кроме того, в словаре много иллюстраций.

Криптовалюты от А до Я

Александр Герасимович



ISBN 978-5-0050-5682-5

Создано в интеллектуальной издательской системе Ridero

Введение

Приветствую каждого, кто читает этот словарь. Меня зовут Герасимович Александр, я автор книги «Цифровое золото: как заработать в сети», доступной также на английском языке. Начал интересоваться биткойном и криптомиром в начале 2017-го года. Тогда же начал инвестировать в криптовалюты. В начале 2018-го года посетил Blockchain Economy Istanbul Summit, где получил много полезной информации. Там встретил Тома Ли – основателя компании Fundstrat Global Advisors и финансового аналитика, а также Кэла Эванса – Члена правления Британской Блокчейн Ассоциации. Считаю себя криптоэнтузиастом и, в какой-то степени, криптоевангелистом.

«Криптовалюты от А до Я» – это словарь о криптовалютах, в котором собран также криптожаргон и сленговые выражения. Здесь вы найдете информацию не только о том, что такое майнинг, криптовалюта, биткойн, блокчейн, но также познакомитесь с такими понятиями, как криптоанархизм, крипто-ослепление, сайдчейн и найдете много другой полезной информации. Всего в книге содержится около 850 терминов. Кроме того, в словаре много иллюстраций.

Если не нашли необходимой информации в русских терминах – поищите в английских, и наоборот. Больше информации о трейдинге вы сможете найти в моей книге «Цифровое золото: как заработать в сети.»

Сокращения

Русские и русскоязычные термины

А

Адрес возврата – см. Refund address.

Адрес кошелька (адрес криптокошелька, он же публичный ключ или публичный адрес; англ. – wallet address) – это уникальная буквенно-цифровая комбинация, используемая для покупки/обмена криптовалют. Выглядит он примерно вот так: 1Ji16JGi9dzyfa8KyCqteK6TDcNaZ3R2cy. Также может быть представлен в виде сканируемого QR-кода. Его можно приравнять к международному номеру банковского счета (IBAN, International Bank Account Number) в мире фиатных денег. Биткойн-адрес также используется держателями биткойнов для цифровой подписи транзакций.

Адрес тщеславия (от англ. vanity address) – биткойн-адрес, содержащий определенный элемент (например, имя).

1BitcoinEaterAddressDontSendf59kuE

Ай-ди кошелька – см. Идентификатор кошелька.

Алгоритм – процесс или набор правил, которым необходимо следовать при решении проблем или расчетных операциях, хотя люди также выполняют алгоритмические действия (скажем, решают математические задачи или следуют рецепту).

Алгоритм майнинга (от англ. mining algorithm; consensus mechanism) – это алгоритм хеширования, используемый для функции проверки работоспособности

в различных криптовалютах. Это алгоритм интеллектуального анализа, реализованный сетью. У Ethereum это Ethash, у ZCash – Equihash, у Монеро – CryptoNight.

Алгоритм Peercoin (PPCoin, PPC; пиринговая платёжная система, созданная в августе 2012 года разработчиками Скоттом Нэдалом и Санни Кингом) – использование гибридной системы эмиссии – она возможна через выполнение работы (PoW) или через расчёт доли (PoS). [1] Peercoin использует тот же механизм доказательства работы, что и Биткойн – основанный на хеш-функции SHA-256.

АлгоритмProof-of-Activity (иногда встречается название «протокол», или consensus mechanism) («доказательство активности») – алгоритм функционирования блокчейн, совмещающий в себе принципы работы популярных PoW и PoS протоколов. Алгоритм устроен таким образом, что блоки могут формировать как PoW, так и PoS майнеры. Представляет собой гибрид, который решает проблемы самых популярных протоколов. Майнинг не дает возможности PoW майнерам монополизировать сеть, так же как и PoS-минтинг – холдерам. По сути, данный механизм универсален, но не нашел своего практического применения, так как существует только на бумаге. [2] [3]

Алгоритм Proof-of-Authority (PoA) – механизм консенсуса blockchain, который обеспечивает быстрые транзакции с использованием идентификаторов, которые означают, что валидаторы блока не создают стейки монеты, а вместо этого имеют собственную репутацию. Следовательно, блокчейн PoA защищен проверяющими узлами, которые произвольно выбирают заслуживающего доверия. Модель Proof-of-Authority основана на ограниченном количестве валидаторов блока, и именно это делает ее масштабируемой системой. Блоки и транзакции проверяются заранее утвержденными участниками, которые выступают в качестве модераторов системы. [4]

Алгоритм Proof-of-Burn (PoB): вместо сжигания электричества нужно «уничтожать» цифровые монеты. «Сжигание» происходит путем отправки криптовалюты на такой адрес, с которого их гарантированно нельзя потратить.

Например, на адрес, который является хешем случайного числа, – шансы подобрать к нему соответствующий публичный и приватный ключи ничтожно малы. Избавляясь таким образом от своих монет, вы получаете право на пожизненный майнинг, который тоже устроен как лотерея среди всех владельцев сожженных монет. Чем больше вы сожгли – тем больше ваши шансы. [5]

Алгоритм Proof-of-Capacity: чем больше майнер может предоставить дискового пространства для майнинга, тем выше будет его доходность. Пионером среди криптовалют с протоколом Proof-of-Capacity стала монета BURST. Для заработка хотя бы 1 доллара в день, необходимо более 500 терабайт дискового пространства. Добыть биткойн или лайткоин этим методом нельзя.

АлгоритмProof-of-Concept, «доказательство концепции» – это алгоритм, в котором работа направлена на определение того, может ли идея стать реальностью. Доказательство концепции предназначено для определения осуществимости идеи или для проверки того, что идея будет функционировать так, как предполагалось. В основном используется на платформе Эфириум.

Алгоритм Proof-of-Cooperation (PoC) – алгоритм основан на группе аутентифицированных узлов, называемых «совместно проверенные узлы» (от англ. Cooperatively Validated Nodes, CVNs). Эти узлы взаимодействуют друг с другом для создания новых блоков в циклическом режиме. Конкурентоспособной добычи или минтинга нет. Блоки создаются с согласованными интервалами. Создание блоков происходит без затрат энергии или вычислительных ресурсов. [6] Используется в блокчейне FairCoin.

АлгоритмDelayed Proof-of-Work (dPOW), задержанное доказательство работы – это консенсусный механизм, который использует протокол POW (как и Биткойн), однако включает механизм, который «нотариально» заверяет блоки в цепочке. Это обеспечивает полную неизменность системы и дает транзакции дополнительный уровень безопасности.

Алгоритм Proof-of-Developer (PoD) – алгоритм, в котором есть свидетельство о реальном, живом разработчике программного обеспечения, создавшем криптовалюту, чтобы предотвратить сбегание анонимного разработчика с собранными во время ICO средствами. [7]

Алгоритм Proof-of-Elapsed-Time – протокол, который подразумевает, что прав больше у того участника, который дольше находится на связи.

Алгоритм Proof-of-Existence («доказательство существования») – алгоритм, реализуемый через блокчейн, который позволяет пользователям хранить доказательства существования для любого документа, доступного онлайн. Это позволяет людям доказать, что документ существует в определенный момент времени, и продемонстрировать свое право собственности на него.

Алгоритм Proof-of-Importance (PoI) («доказательство важности») – алгоритм, использующийся в криптовалюте NEM. На вероятность получить право сформировать блок влияют три компонента:

1) количество единиц криптовалюты на балансе (значимыми для PoI являются балансы более, чем оговоренное число единиц, например, не менее 10 тыс. для NEM);

2) активность аккаунта (число транзакций);

3) время нахождения аккаунта в сети.

Алгоритм Proof-of-Provenance (PoP), «доказательство происхождения» – это протокол для отслеживания движения физических активов из рук – от поставщика слитков золота до хранилища. PoP решает вопрос о доказательстве существования физического актива, подлинности его владельца и безопасности его хранения в хранилище. Это осуществляется путем проверки транзакций в блокчейне.

Алгоритм Proof-of-Research («доказательство проведенного исследования») – был разработан в проекте GridCoin для того, чтобы направить вычислительные мощности PoW-сетей на решение научных задач на платформе BOINC. В Proof-of-Research одновременно используется Proof-of-Work для вознаграждения участников за выполненные вычисления и Proof-of-Stake для поощрения долговременного участия в проекте. [8]

АлгоритмProof-of-Retrievability (PoR), «доказательство возможности извлечения» – владелец файловой системы (доказывающий, prover) должен доказать клиенту (verifier), что он действительно хранит некий файл F и что он не поврежден, в том смысле, что клиент может полностью восстановить его. Награда майнеру выплачивается за количество скачанных файлов. Похож на алгоритм Proof-of-Storage.

Алгоритм Proof-of-Security – алгоритм, в котором существует способность криптографической программы доказать безопасность системы. Алгоритм основан на устойчивости журнала транзакций. Используется в криптовалюте Кардано (ADA).

Алгоритм Proof-of-Service – концепция впервые применена в криптовалюте DASH. Здесь, чтобы получать награду, необходимо приобрести 1000 монет DASH и запустить мастерноду. Монеты должны находится на счету без движения; как только вы потратите их или даже небольшую их часть, вы перестанете получать награду как мастернода. [9]

Алгоритм Proof-of-Space (PoSpace) – то же, что и Proof-of-Capacity. [10]

Алгоритм Proof-of-Stake (PoS, дословно: «подтверждение доли») – механизм консенсуса во многих криптовалютах, при котором вероятность формирования участником очередного блока в блокчейне пропорциональна доле, которую составляют принадлежащие этому участнику расчётные единицы данной криптовалюты от их общего количества. То есть, чем больше криптовалюты в вашем криптокошельке, тем большее вознаграждение вы получаете. Данный метод является альтернативой методу PoW, при котором вероятность создания очередного блока выше у обладателя более мощного оборудования. [11]
В данном случае расход электроэнергии минимален.

Алгоритм Proof-of-Stake-and-Trust (PoST) – консенсус в экосистеме Waltonchain. PoST похож на Proof-of-Stake тем, что он вознаграждает держателей токенов (и узлов) дивидендами WTC. Waltonchain дополнительно добавляет механизм дальнейшего поощрения узлов с репутацией более высокого качества и более

честных узлов. Криптовалюту Waltonchain нельзя добывать.

Алгоритм Proof-of-Storage – то же, что и Proof-of-Capacity.

Алгоритм Proof-of-Time (PoT) – консенсус в экосистеме ChronoLogic, которая рассматривает время как актив, который не зависит от хешрейта сети и потраченного на поддержание работы сети электричества. В этой сети токены будут производиться по другому принципу – за определенный промежуток времени. [12] Сеть проекта TimeNode состоит из исполнительных off-chain агентов из сообщества ChronoLogic.

Алгоритм Proof-of-Work (PoW) – алгоритм, основанный на необходимости выполнения на стороне клиента некоторой достаточно длительной работы (нахождение решения задачи), результат которой легко и быстро проверяется на стороне сервера. То есть, чем мощнее ваше оборудование для майнинга, тем большее вознаграждение вы получаете. Используется в сети Биткойн и других криптовалют.

Аллигатор Уильямса – см. Williams Alligator.

Альткойн (от англ. altcoin, alternative coin) – это все криптовалюты, появившиеся после биткойна (например, Litecoin, Ethereum, Ripple).

Анархо-капитализм (от англ. anarcho-capitalism) – политическая философия и школа мысли, которая верит в устранение централизованных государств в пользу самостоятельного управления, частной собственности и свободного рынка. Многие из ранних последователей Биткойна были сторонниками анархо-капитализма, полагая, что он вернет власть и контроль массам. [13]

Андресен, Гевин (англ. Gavin Andresen) – главный научный сотрудник Bitcoin Foundation, Bitcoin разработчик.

Анти-отмывочные механизмы (от англ. Anti Money-Laundering, AML) – применяются, чтобы предотвратить превращение незаконно добытых средств в законные. Эти механизмы по природе могут быть правовыми или техническими. Обычно применяются регуляторами по отношению к крипто-биржам [14] (например, в виде KYC).

Аппаратные кошельки – кошельки для хранения криптовалют. Напоминают внешне обычные «флешки.» Очень удобные и, наверное, самые безопасные; есть возможность восстановления в случае утери или кражи. Примеры: KeepKey, Ledger USB Bitcoin Wallet, Trezor.

Арбитраж – разница курса одного и того же актива на разных биржах. Благодаря арбитражу появляется возможность переводить активы с одной биржи на другую, или осуществлять арбитражные внутрибиржевые сделки без трейдинга за счет разницы курсов торговых пар на одной и той же бирже.

Асик (ASIC, от англ. application-specific integrated circuit, «интегральная схема специального назначения») – специальное устройство для майнинга криптовалют. ASIC-процессоры изготавливают специально для майнинга. Такие устройства имеют высокий уровень окупаемости и их легко обслуживать. Минусы – быстрое «устаревание» асика в связи с растущей сложностью сети, а также высокая стоимость.

Атака 51% – если в руках злоумышленника находится больше половины всех вычислительных мощностей в сети, то у него появляется возможность подтверждать только свои блоки, при этом игнорируя чужие, что позволяет ему получать 100% всех производимых биткойнов, а также блокировать любые другие транзакции. Объем инвестиций, необходимый для осуществления атаки на сеть Биткойн (по данным сайта gobitcoin.io) – более 15 млрд долларов на майнинг-оборудование и более 10 млн долларов на оплату электроэнергии ежедневно (на середину октября 2019 года).

Атака взятками – разновидность атаки на сеть, когда злоумышленник пытается «подкупить» других пользователей системы, чтобы создать свой, альтернативный блокчейн и сделать его действительным. Возможна при

завладении более чем 50% от всего объема определенной криптовалюты за несколько часов. В системе Биткойн считается дорогостоящей и трудновыполнимой, так как другим пользователям проще отличить поддельный блокчейн от настоящего.

Атака возрастом монет (атака накоплением возраста монет) – разновидность атаки на сеть, при которой злоумышленник «отпирает» свои средства, «уничтожая» возраст монет, и «переводит» их на другой адрес. Подробнее можно почитать здесь: Proof of Stake vs. Proof of Work / White Paper BitFury Group 21 сентября 2015 (Версия 1.0-ru).

Атака грубой силы – см. Brute Force Attack.

Атака Сибиллы (от англ. Sybil attack) – такой вид атаки, в которой атакующий нарушает работу сети, создавая в ней большое количество неправильно работающих нод.

## Б

Бакт (от англ. Bakkt) – криптовалютная торговая площадка, которая разрабатывалась оператором Нью-Йоркской фондовой биржи ICE с использованием технологии Microsoft. В Bakkt обещали профинансировать специальный гарантийный фонд, который фактически будет исключать риски невыплат по обязательствам в процессе торгов. Одна из задач Bakkt – предоставить доступ институциональным инвесторам на криптовалютный рынок и предоставить им множество инструментов для торговли и управления рисками, присущих рынку фьючерсов. 23 сентября 2019-го платформа подтвердила начало торгов биткойн-фьючерсами на собственном рынке оператора Нью-Йоркской фондовой биржи Intercontinental Exchange (ICE).

Батчинг – процесс объединения нескольких транзакций в одну с целью уменьшения размера комиссии.

Баунти (от англ. bounty) – это возможность получить награду в криптовалюте за определенные рекламно-информационные действия без необходимости вкладывать свои деньги в проект. Это могут быть посты в соцсетях Facebook или Twitter, подписные кампании на форуме Bitcointalk или email-рассылка, переводы информации о проекте на другие языки, поиск багов, дизайн лого, буклетов, разработка мобильных приложений, кошельков или других программных надстроек. Для получения выплат нужно открыть ETH-кошелек (рекомендуется myetherwallet – он совместим с большинством проектов). На баунти-кампанию может быть зарезервировано, к примеру, около 1% всех токенов проекта. Далее этот 1% распределяется среди участников кампании. Для начала вам нужно зарегистрироваться в баунти-кампании, заполнив простую форму. Далее вы можете разместить предложенные реферальные или обычные ссылки на своей страничке в Facebook (реклама ICO на Facebook разрешена лишь в одобренных модераторами сообществах), Twitter, vk, написать об ICO статью, создать ролик для YouTube, отвечать в групповом чате Telegram и т. д. Всё зависит от требований каждого определенного проекта. То есть, по сути, вам нужно будет заниматься рекламой проекта для привлечения в него средств инвесторов. Общие правила для участия следующие: каждый участник может использовать лишь один аккаунт для участия (чаще всего допускаются аккаунты в соцсетях возрастом более 1 месяца), запрещены любые методы спама, запрещено поручать работу кому-то другому, запрещено удалять созданный контент или выходить из групп проектов в соц. сетях до окончания ICO. От вас требуется соблюдать правила кампании и честно выполнять поставленные перед вами задачи, вовремя отправлять отчеты о проделанной работе. Необходимо иметь в виду, что руководители проекта имеют право в любой момент изменить правила баунти-кампании.

Баунтихантер, баунтист – человек, который зарабатывает на баунти-программах.

Белая книга – см. White Paper.

Бенчмарк (от англ. bencmark) – обобщённый индикатор на финансовых рынках, используемый для оценки их состояния в целом или отдельных сегментов рынка.

Бигблокеры (от англ. Big Blockers) – сторонники увеличения лимита размера блоков Биткойна свыше 1 Мб как способа масштабирования сети. Чаще всего бигблокерами называют представителей Bitcoin Unlimted и сторонников Bitcoin Cash.

Биткойн (или биткоин, от англ. Bitcoin; жарг. – биток) – это платежная система, а также одноименная цифровая валюта. Использование слова со строчной буквой «b», обозначенного как «биткойн», обычно ассоциируется с биткойном в качестве валюты. Биткойн с большой буквы «B» обычно ассоциируется с Биткойн-протоколом и платежной сетью. Прописная форма «Биткойн» также часто используется для обозначения экосистемы в целом. [15] Эту криптовалюту, как правило, нельзя подержать в руках. Это портативная, легко делимая и взаимозаменяемая валюта, транзакции с которой необратимы. Для обеспечения функционирования и защиты системы используются криптографические методы. Вся информация о транзакциях между адресами системы доступна в открытом виде. Выпуск новых биткойнов децентрализован, не зависит от какого-либо регулирующего органа; объём эмиссии известен заранее.

Является одним из вариантов комбинированного применения алгоритма PoS.

Интересные факты. Центр по санкциям и незаконному финансированию Фонда защиты демократических государств провел исследования и проанализировал операции в биткойнах, проведенных в период с 2013 по 2016 годы, и заключил, что только 0,61% торговых операций за этот период считались связанными с незаконной деятельностью.

Биткойн «хоронили» 376 раз (по данным 99bitcoins), начиная с курса в 0,23 доллара, а он продолжает вылезать из могилы.

Классическая банковская система

Система Биткойн

Биткойн-адрес – см. Адрес кошелька.

Биткойн-демон (bitcoind) – программа, в которой реализован протокол Bitcoin; управляется через командную строку.

Биткойн-кран (от англ. bitcoin faucet) – это любой ресурс-раздатчик биткойнов своим посетителям, «живущий» за счет рекламы. Они размещают на своем сайте рекламу, за просмотр и за клики от которой получают доход. А пользователи могут зарегистрироваться и вводить капчу в определенном поле, за что получают небольшое вознаграждение в биткойнах. Считается, что реально заработать на них практически невозможно и что это лишь трата времени. Так, за один ввод капчи (вводится с определенным промежутком, чаще через каждый час) вы получаете около 9 Сатоши (10-? биткойна).

Пример биткойн-крана

Биткойн-миксер – инструменты для препятствия отслеживания транзакций, сервисы «смешивания» (mixing services).

Биткойн-пузырь (от англ. Bitcoin Bubble) – мнение о том, что Биткойн – это спекулятивный пузырь, финансовая пирамида. У. Баффет назвал bitcoin «миражом». В марте 2014 года ученый-экономист Роберт Шиллер также высказался о том, что bitcoin очень похож с экономическим пузырем. В апреле 2018-го команда исследователей из Bank of America Merrill Lynch (BAML) заявила,

что Биткойн – это пузырь, при чем пузырь самый огромный за всю историю. BAML сравнили Биткойн с «тюльпаноманией» в Европе, которая оказалась тогда первым в истории биржевым крахом и первым лопнувшим пузырем. [16]

Биткойн-фьючерс – это стандартизированное юридическое соглашение о покупке или продаже биткойна по заранее определенной цене в указанное время в будущем.

Биткойн-ETF (сокращенно от англ. Exchange Traded Fund) – торгуемый на бирже фонд на основе Биткойна. По сути, это ценные бумаги на владение биткойном, это акции фонда, стоимость которых выражается в криптовалюте. Например, у вас есть 100 биткойнов и на них выпустили ценные бумаги, где стоимость каждой составляет 2 биткойна. Таким образом, трейдер, который покупает эти акции напрямую, инвестирует фиат в криптовалюту. Но при этом ему не нужно регистрироваться на криптовалютной бирже, заводить криптокошелёк и помнить ключ от него. Биткойн-ETF позволяет инвестору купить ценную бумагу и при этом не переживать за возможности взлома биржи или кошелька.

Битнейшн (от англ. Bitnation) – это первая в мире децентрализованная добровольная нация без границ (Decentralized Borderless Voluntary Nation, DBVN). Bitnation начала свою работу в июле 2014 года и зарегистрировала первый в мире блокчейн-брак, свидетельство о рождении, удостоверение личности беженца, всемирное гражданство, конституцию DBVN и многое другое. В организации есть Государственный нотариус, зарегистрированы десятки тысяч граждан, есть посольства по всему миру. Bitnation является лауреатом премии ЮНЕСКО Netexplo Award 2017. [17]

Конец ознакомительного фрагмента.

---