

КРИПТОЭКОНОМИКА. ОСНОВНЫЕ ПОНЯТИЯ

ОСНОВНЫЕ ПОНЯТИЯ



- Само слово «криптоэкономика» может вводить в заблуждение, так как предполагает наличие некой параллельной крипто-версии всей экономики. Но, это не так!
- Криптоэкономика — это не применение макроэкономической и микроэкономической теории для криптовалютных рынков или ICO.
- Это также не разновидность экономики, а скорее область прикладной криптографии, которая учитывает экономические стимулы и экономическую теорию. Криптовалюты, основанные на публичном блокчейне (биткоин, лайткоин, ethereum и пр.) являются продуктами криптоэкономики. Да и сам блокчейн — также лишь один из продуктов этой новой практической науки.
- Криптоэкономика основывается и существует в децентрализованных одноранговых (P2P) системах, которые не дают контроля над какой-либо третьей стороной.
- Криптография, лежащая в основе этих систем, делает безопасной работу одноранговых сетей, а экономика — стимулирует всех участников вносить свой вклад в сеть, чтобы она процветала с течением времени.

БИТКОИН

- **Сатоши Накамото** породил криптоэкономiku, когда он создал Биткойн в 2009 году. Как и Галилей, который известен как отец-основатель физики, Сатоши навсегда будет известен как основатель криптоэкономики.
- **Биткойн—это первый продукт криптоэкономики.** Его инновация заключается в том, что она позволяет многим субъектам, которые не знают и не доверяют друг другу, надежно достигать консенсуса относительно состояния блокчейна (регистра транзакций) биткойнов. Это достигается сочетанием **экономических стимулов и основных криптографических инструментов.**
- Децентрализованные одноранговые (P2P) системы, основанные на криптографии, были известны до появления Биткойна. Но, в этих децентрализованных системах не было экономического стимула, который бы позволил им развиваться и процветать со временем.
- Сатоши добавил экономический стимул к одноранговым системам, когда создал Bitcoin в 2009 году. До появления Биткойна считалось невозможным достичь консенсуса между узлами в одноранговой сети (т. н. **проблема Византийских генералов**) для создания децентрализованной цифровой денежной системы.





КТО ТАКОЙ САТОШИ НАКАМОТО?

Сатоши Накамото (скорее всего псевдоним) является создателем Bitcoin. Мы не знаем, кто скрывается за этим псевдонимом, хотя существует много предположений.

ЧТО НАМ ИЗВЕСТНО:

“Сатоши Накамото” в переводе с японского значит “ясно мыслящий внутри системы”

Сатоши неизвестный гений математики, хорошо разбирающийся в криптографии

Сатоши внес последние изменения в код в середине 2010 и после этого передал бразды правления Гэвину Андерсону, ведущему разработчику Bitcoin

БЕЗОПАСНОСТЬ БИТКОИНА

- Сочетание криптографии и экономических стимулов привело к созданию надежной, процветающей платежной децентрализованной одноранговой сети **Биткоин**, капитализация которой сегодня составляет более **\$70 млрд** и в которой ежедневно совершаются транзакции на сумму более **\$600 млн**.
- **Биткоин основан на экономических стимулах и затратах.** Экономические стимулы используются для привлечения майнеров для поддержки сети. Майнеры вкладывают свои средства и несут затраты на электричество для производства новых блоков транзакций в сети, за что они вознаграждаются некоторым количеством биткоинов, поступающих в сеть в виде эмиссии, а также в виде комиссионных от добавляемых транзакций.
- **Экономические затраты майнеров являются частью модели безопасности биткоина.** Самый очевидный способ атаковать блокчейн Биткоина — получить контроль над большей мощностью (хэшрейтом) сети — так называемая «атака 51%», которая позволила бы злоумышленнику контролировать все последующие транзакции (цензурируя и не пропуская неудобные).
- Но, мощность хеширования стоит денег, в виде оборудования и электроэнергии. **Протокол Биткоина преднамеренно делает майнинг затратным**, а это означает, что получение контроля над большинством вычислительной мощности в сети чрезвычайно дорого для того, чтобы получить прибыль от «атаки 51%». Так, по состоянию на 1 сентября 2017 года стоимость «атаки 51%» на Биткоин составляла бы около **\$2,05 млрд. на аппаратных средствах** и еще более \$3,6 млн. ежедневно на электроэнергию.
- Без этих тщательно откалиброванных экономических стимулов биткойн не работал бы и не развивался. Если бы **майнинг** не был связан с высокими затратами, было бы легко начать «атаку 51%». А если бы не было бы вознаграждения за майнинг, то не было бы и майнеров, которые покупают оборудование и оплачивают электроэнергию, чтобы внести свой вклад в сеть и получить за это вознаграждение.

АКТУАЛЬНОСТЬ ВОПРОСОВ КРИПТОЭКОНОМИКИ

- Без жестких криптографических протоколов, таких как хэширующие функции или криптография с открытым и закрытым ключами, не было бы безопасной расчетной денежной единицы, с помощью которой можно было бы вознаграждать майнеров. Без тщательно откалиброванного набора стимулов для поощрения майнеров эта расчетная единица (биткоин, BTC) не имела бы рыночной стоимости, поскольку не было бы уверенности в том, что система может сохраняться в будущем.
- Таким образом, **криптоэкономика требует мыслить о проблемах информационной безопасности и надежности в экономическом плане.** Она фокусируется на проектировании и создании распределенных децентрализованных систем, работа которых поддерживается экономическими стимулами, которые в свою очередь основываются на криптографии.
- По сути, Криптоэкономика — это междисциплинарный подход, слияние криптографических протоколов и экономических стимулов.

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

- **К основным преимуществам использования Bitcoin можно отнести:**
- Простота в обращении. Операции с Bitcoin осуществляются очень быстро, надежно и в пределах всего мира. Данные платежи происходят без участия каких-либо посредников. Таким образом, стоимость транзакций в Bitcoin сводится к минимуму. При совершении операций с данной валютой предоставлять личную информацию не нужно.
- Возможность заработка. В 2017 году произошло многократное удорожание стоимости Bitcoin. Криптовалюта выросла до 20000 долларов за Bitcoin. После такого значительно роста стоимости Bitcoin, можно утверждать, что в мире появился новый тип активов.
- Увеличение покупательной способности. С каждым годом растет число продавцов, которые готовы принимать Bitcoin. Например, в США сегодня за Bitcoin можно купить даже автомобиль.
- Рост объема инвестиций. Большое количество инвестиционных фондов и банков в мире используют Bitcoin как средство инвестиций.
- Легализация. Из-за большой популярности Bitcoin, национальные банки развитых стран (Германия, Великобритания, США) постепенно приближаются к тому, чтобы признать криптовалюту.
- **Несмотря на большое количество преимуществ криптовалюты, она имеет несколько недостатков:**
- Большая волатильность Bitcoin. Одним из недостатков криптовалюты является большая волатильность. В течение пару дней курс Bitcoin может сильно измениться. Безусловно, при большой волатильности рынка потенциал прибыли возрастает значительно. Но в тоже время, риски могут становиться критическими.
- Риск потери инвестиций. Так как торговля Bitcoin является децентрализованной и без правового регулирования, то инвестор может потерять свои вложения, например при банкротстве Bitcoin-бирж (Mt.Gox, Flexcoin).
- Запрет на использование Bitcoin. Некоторые страны препятствуют обороту криптовалюты, что сказывается на сильном ухудшении перспектив развития данного типа валюты. Например, Китай на законодательном уровне запретил использовать банкам в обращении криптовалюты.