Market Talks
ОБРАЗОВАТЕЛЬНЫЙ ЦЕНТР

БЛОКЧЕЙН · НАЧАЛЬНЫЙ · УРОК 3 ИЗ 13

До биткоина: эксперименты с цифровыми деньгами

Двадцать пять лет попыток, почти удач и провалов, и то, что каждая из них оставила биткоину

8 мин чтения Вопросов в тесте: 6, с ответами

БЛОКЧЕЙН · НАЧАЛЬНЫЙ · УРОК 3 ИЗ 13

До биткоина: эксперименты с цифровыми деньгами

СУТЬ В ОДНОМ ПРЕДЛОЖЕНИИ

Биткоин не появился на пустом месте. Он объединил идеи более ранних проектов цифровых денег и был задуман так, чтобы избежать одной слабости, которая погубила большинство из них.

Мечта старше веб-браузера

В уроках 1 и 2 мы познакомились с двумя проблемами: цифровые деньги можно скопировать, а систему, которой управляет одна сторона, можно заморозить, закрыть или подкупить. Задолго до биткоина криптографы и предприниматели уже пытались решить обе.

Их проекты появлялись с начала 1980-х до середины 2000-х. Некоторые стали настоящим бизнесом с настоящими клиентами. Другие так и остались на бумаге. Ни один не добился полного успеха, но почти каждый добавил что-то, что позже использовал биткоин. Проследить их историю проще всего, чтобы понять, почему биткоин устроен именно так.



Рисунок 1. Биткоину предшествовали более 25 лет экспериментов с цифровыми деньгами. Каждый оставил деталь итоговой конструкции.

DigiCash: приватно, но под управлением одной компании

В 1982 году криптограф Дэвид Чаум описал технику под названием **слепая подпись**. Она позволяет банку подписать цифровую монету и подтвердить её подлинность, не видя, какую именно монету он подписывает. В результате получаются цифровые деньги, которые можно

тратить анонимно, почти как наличные: банк не может связать платёж с человеком, снявшим монету.

В 1989 году Чаум основал DigiCash, чтобы превратить идею в продукт, а в 1995 году Mark Twain Bank из Сент-Луиса начал предлагать клиентам её eCash. Технология работала. Бизнес нет: подключилось слишком мало банков и магазинов, и в 1998 году DigiCash объявила о банкротстве.

Более глубокая слабость была в самом устройстве. Каждую монету по-прежнему выпускал центральный банк или компания, и та же центральная сторона проверяла двойные траты. Когда компания разорилась, вместе с ней исчезли и деньги.

e-gold: реальное обеспечение, одна точка отказа

e-gold, запущенный в 1996 году, выбрал другой путь. Каждая единица была обеспечена физическим золотом в хранилищах, и пользователи могли за секунды переводить друг другу балансы в золоте по всему миру. Проект быстро рос: к 2006 году через него проходило более 2 миллиардов долларов платежей в год.

Но e-gold была одной компанией, а значит, одной мишенью. Отсутствие проверки личности привлекало преступников, и в 2007 году власти США предъявили обвинения компании и её директорам. В 2008 году они признали вину в сговоре с целью отмывания денег и в ведении нелицензированного бизнеса по переводу денег, а в 2009 году переводы были приостановлены. Владельцы счетов годами ждали процедуры возврата своих средств.

Урок 2 подтвердился на практике: единая точка контроля является и единой точкой отказа, будь причиной хакер, банкротство или решение суда.

Hashcash: намеренно сделать дорого

В 1997 году криптограф Адам Бэк предложил **Hashcash** как защиту от спама. Перед отправкой письма компьютер отправителя должен был решить небольшую задачу, потратив немного вычислительной работы. Для одного письма эта цена незаметна. Для спамера, рассылающего миллионы, она быстро растёт.

Хитрость в асимметрии: задачу решать долго, а проверить можно мгновенно. Любой получатель письма может убедиться, что работа выполнена, не повторяя её. Эта идея называется **доказательством работы** (proof of work), и в whitepaper биткоина Hashcash прямо назван источником вдохновения.

АНАЛОГИЯ: ПРОВЕРКА СУДОКУ

Сложное судоку можно решать час, а проверить готовую сетку можно за минуту. Если вам дают заполненную головоломку, вы знаете, что человек потрудился, хотя и не видели, как он это делал. Доказательство работы превращает эту идею в цифровую отметку о затраченных усилиях, которую может проверить любой компьютер.

b-money, Bit Gold и RPOW: чертежи

В 1998 году два предложения на бумаге оказались поразительно близки к биткоину. Инженер Вэй Дай описал **b-money**: каждый участник хранит копию записей о том, кому что принадлежит, а новые деньги создаются решением вычислительных задач. Примерно тогда же юрист и специалист по информатике Ник Сабо предложил **Bit Gold**, где решения доказательства работы сцеплялись друг с другом вместе с метками времени, создавая нечто редкое и дорогое в производстве, своего рода цифровое золото.

Ни один из проектов так и не был запущен. Оба оставили открытым важный вопрос: если записи ведёт множество независимых людей, как им договориться, какая запись верна, без главного?

В 2004 году криптограф Хэл Финни создал **RPOW** (многоразовые доказательства работы), который позволял передавать токены доказательства работы от человека к человеку. Система действительно работала, но для защиты от двойных трат полагалась на доверенный сервер на специальном защищённом оборудовании. В центре по-прежнему стояла одна доверенная сторона. Пять лет спустя именно Финни получит первый биткоин, отправленный одним человеком другому.

Цепочка меток времени

Ещё одна деталь пришла не из мира денег. В 1991 году исследователи Стюарт Хабер и У. Скотт Сторнетта задались вопросом, как доказать, когда был создан цифровой документ и что с тех пор его не меняли.

Их ответ: связать записи в цепочку. Каждая новая запись содержит цифровой отпечаток предыдущей, поэтому изменение любой старой записи разорвёт все последующие звенья. История становится **защищённой от незаметных изменений**: переписать её всё ещё можно попытаться, но все увидят, что вы это сделали. Whitepaper биткоина ссылается на их работу трижды, а идея такого связывания записей стала «цепью» (chain) в слове блокчейн. В уроке 6 мы подробно разберём, как работают эти отпечатки.

РЕАЛЬНЫЙ ПРИМЕР

Чтобы их цепочку нельзя было тихо переписать, компания Хабера и Сторнетты с 1995 года начала публиковать отпечаток своих последних записей в рубрике частных объявлений The New York Times. Любой мог сравнить печатную газету с цепочкой, и никто не смог бы задним числом изменить тысячи напечатанных экземпляров.

Недостающая деталь

К середине 2000-х почти все части уже существовали. Не хватало самой трудной:

Проект	Что он добавил	Чего ещё не хватало
DigiCash (1989)	Приватные цифровые платежи	Зависимость от центрального эмитента
Цепочка меток времени (1991)	Связанные записи, историю которых нельзя тихо изменить	Не создавалась для денег
e-gold (1996)	Глобальные переводы в больших масштабах	Одна компания, которую можно закрыть
Hashcash (1997)	Доказательство работы: дорого создать, дёшево проверить	Не деньги, а лишь отметка
b-money, Bit Gold (1998)	Общие записи и деньги, созданные работой	Нет способа договориться без лидера; так и не запущены
RPOW (2004)	Токены доказательства работы, которые можно передавать	Опора на один доверенный сервер

Каждая попытка либо зависела от главного, либо так и не решила, как незнакомцам договориться об одной истории без него. В 2008 году анонимный автор собрал детали вместе и добавил недостающую. Об этом урок 4.

Почему это важно трейдерам

- **Центральные эмитенты терпят крах знакомым образом.** DigiCash обанкротилась, а e-gold закрыла прокуратура. Тот же сценарий повторился в 2013 году, когда власти США закрыли Liberty Reserve, ещё одну централизованную цифровую валюту. Любой актив, зависящий от одного эмитента, несёт деловые и юридические риски этого эмитента.
- **Сегодняшние стейблкоины напоминают e-gold.** Стейблкоин, обеспеченный долларом, устроен похоже: компания держит резервы и выпускает под них токены. Поэтому стоит разобраться в резервах, лицензиях и правовом положении эмитента, прежде чем полагаться на его токен.
- **У нарратива «цифрового золота» глубокие корни.** Идея Bit Gold о чём-то редком, потому что его дорого создать, до сих пор влияет на то, как многие инвесторы сравнивают биткоин с золотом. Понимая, откуда взялся нарратив, легче судить, какой вес ему придавать, когда он двигает рынок.

Ключевые термины

Слепая подпись	Способ, которым банк или эмитент одобряет цифровую монету, не видя, какую именно, чтобы платежи оставались приватными.
Доказательство работы	Подтверждение того, что компьютер потратил реальные усилия на решение задачи. Создаётся медленно, проверяется мгновенно.
Обеспеченный активом	Деньги или токены, стоимость которых подкреплена реальным активом, например золотом или долларами, у эмитента.
Метка времени	Доказательство того, когда была создана цифровая запись и что с тех пор она не менялась.
Защита от незаметных изменений	Такое устройство, при котором любое изменение прошлых записей видно всем, даже если физически его не предотвратить.
Цифровая редкость	Ограниченный запас чего-то цифрового, что нельзя просто скопировать или создать бесплатно.

Главное

1. Эксперименты с цифровыми деньгами начались в начале 1980-х, более чем за 25 лет до биткоина.
2. DigiCash принесла приватность, а e-gold глобальный масштаб, но обе зависели от одной компании и рухнули вместе с ней.
3. Hashcash ввёл доказательство работы: усилие, которое долго создавать, но мгновенно проверять.
4. b-money, Bit Gold и RPOW наметили общие записи и деньги на основе работы, но ни один не решил, как незнакомцам договориться без доверенной стороны.
5. Связанные метки времени показали, как сделать историю защищённой от незаметных изменений. Биткоин объединил эти детали и добавил недостающую.

Проверьте себя

Обведите один ответ на каждый вопрос. Ответы с пояснениями находятся на следующей странице. Пройти этот тест можно и онлайн на markettalks.info, сразу узнав свой результат.

1. Какое ключевое нововведение лежало в основе DigiCash?

- A Золото в хранилищах
- B Слепые подписи, делавшие цифровые платежи приватными
- C Доказательство работы против спама
- D Реестр, копию которого хранит каждый пользователь

2. Почему прекратил существование e-gold?

- A Судебное преследование единственной компании, которая им управляла
- B Его золотые резервы украли
- C Ошибка позволяла пользователям копировать монеты
- D Его пользователи перешли на биткоин

3. Для чего изначально создавался Hashcash?

A Сделать онлайн-платежи приватными
B Хранить балансы, обеспеченные золотом
C Сделать рассылку спама дорогой
D Ставить метки времени на юридические документы

4. Какое свойство делает доказательство работы полезным?

A Его любой может создать мгновенно
B Его может проверить только центральный сервер
C Его легко скопировать
D Его долго создавать, но мгновенно проверять

5. Что дала работа Хабера и Сторнетты 1991 года?

A Цифровые деньги, обеспеченные золотом
B Связывание записей в цепочку, при котором изменение истории становится заметным
C Анонимную электронную почту
D Первую криптовалютную биржу

6. Какой детали ещё не хватало до 2008 года?

A Более быстрого интернета
B Способа сделать платежи приватными
C Способа для незнакомцев договориться об одной общей истории без главного
D Компьютеров, достаточно мощных для доказательства работы

Ответы

1 B

Слепые подписи, делавшие цифровые платежи приватными

Слепые подписи Дэвида Чаума позволяли банку одобрить монету, не видя, какую именно, поэтому платежи оставались приватными, почти как наличные.

2 A

Судебное преследование единственной компании, которая им управляла

e-gold управляла одна компания. После обвинений прокуратуры она и её директора признали вину в 2008 году, а в 2009 году переводы были приостановлены. Одна компания означала одну точку отказа.

3 C

Сделать рассылку спама дорогой

Адам Бэк предложил Hashcash для борьбы со спамом. Каждое письмо требовало немного вычислительной работы: пустяк для одного сообщения и очень дорого для миллионов.

4 D

Его долго создавать, но мгновенно проверять

Как и решённое судоку, доказательство работы требует усилий для создания, но проверяется за мгновение. Поэтому любой может убедиться, что работа выполнена, не повторяя её.

5 B

Связывание записей в цепочку, при котором изменение истории становится заметным

Каждая запись содержит отпечаток предыдущей, поэтому изменение старой записи разрывает все последующие звенья. Эта идея стала «цепью» в слове блокчейн.

6 C

Способа для незнакомцев договориться об одной общей истории без главного

Прежние системы либо опирались на доверенную сторону, либо так и не решили, как множеству независимых участников договориться об одной записи. Биткоин добавил эту недостающую деталь, о чём расскажет урок 4.

ИСТОЧНИКИ

- Министерство юстиции США, признание вины по делу e-gold (июль 2008): https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html
- Википедия, DigiCash: https://en.wikipedia.org/wiki/DigiCash
- Википедия, e-gold: https://en.wikipedia.org/wiki/E-gold
- Satoshi Nakamoto Institute, Хэл Финни: RPOW: https://nakamotoinstitute.org/finney/rpow/
- Cointelegraph, соавтор блокчейна о том, почему он не Сатоси Накамото: https://cointelegraph.com/news/co-inventor-of-blockchain-on-why-he-is-not-satoshi-nakamoto

Market Talks

ПРОДОЛЖАЙТЕ ОБУЧЕНИЕ

Далее: урок 4
2008 год и рождение биткоина

Этот урок входит в бесплатный курс «Блокчейн» Образовательного центра MARKET TALKS: уроки начального, среднего и продвинутого уровней, в каждом из которых есть тест и PDF для скачивания.

Образовательный центр
Уроки от базовых принципов до продвинутых тем

Анализ рынков
Технический и фундаментальный анализ ключевых рынков

Отчёты
Биткоин, золото, серебро, SPX и другое

markettalks.info

Telegram @MARKET_TALKS

Только в образовательных целях. Ничто в этом документе не является финансовой рекомендацией. © 2026 MARKET TALKS. Вы можете свободно делиться этим PDF без изменений.