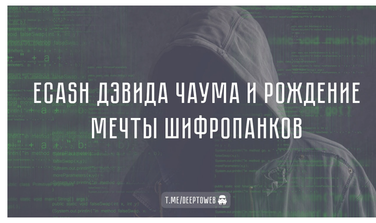
eCash Дэвида Чаума и рождение мечты шифропанков

Темная Сторона Интернета • July 23, 2018



> *«Вы можете оплачивать доступ к базам данных, покупать программное обеспечение или же подписки на новостные ресурсы, играть в компьютерные игры по сети, получать пятидолларовый долг от друга или же заказывать пиццу. Возможности действительно безграничны».*

Это не цитата из видеоролика о биткоине от 2011 года. Более того, речь вообще не о биткоине и даже не об этом тысячелетии. Это слова криптографа и доктора наук Дэвида Чаума из его выступления на первой конференции ЦЕРНа в Женеве в 1994 году. И говорит он о eCash.

Если у движения шифропанков и был крестный отец, то бородатый Чаум с прической «конский хвост» идеально подходит под эту роль. Сказать, что он опередил свое время, будет откровенным преуменьшением. До того, как интернет стал доступен широким массам, до того, как в большинстве домов появились персональные компьютеры, до того, как Эдвард Сноуден, Джейкоб Эпплбаум и Павел Дуров родились на свет, Дэвид Чаум уже размышлял над проблемой приватности в онлайне.

> *«Вы должны объяснить своим читателям, насколько это важно, — сказал он однажды журналистам издания* ***Wired****. — В киберпространстве нет физических ограничений, нет никаких стен. Это совершенно другое, жуткое и странное место, и вопрос идентификации здесь — чистый кошмар. Понимаете? Все, что вы делаете, может видеть другой человек, все может быть записано навсегда. Это резко противоречит основному принципу демократии».*

Чаум начал свою карьеру в университете в Беркли. Будучи профессором компьютерных наук, он был не только сторонником цифровой приватности, но и принимал активное участие в реализации этой концепции. В 1981 Чаум опубликовал работу «Неотслеживаемая электронная почта, обратные адреса и цифровые псевдонимы». Этот документ положил начало исследованиям в области зашифрованных коммуникаций в интернете, которые в конечном итоге приведут к созданию конфиденциальной технологии Tor.

Но приватность регулярных коммуникаций не была приоритетом для Чаума. Вероятно, у него изначально появилась более масштабная идея — приватные цифровые деньги.

> *«Вопрос, должна ли информация храниться в руках отдельных людей или же организаций, появляется каждый раз, когда правительство или бизнес решают автоматизировать ряд транзакций. Будущее общества во многом зависит от подхода, который будет доминировать», — заявил Чаум в интервью научному журналу* ***Scientific American*** *в 1992 году.*

Примечательно, что за десять лет до этого, в 1982 году, Чаум уже решил существующую проблему в исследовании «Слепые подписи и неотслеживаемые платежи». В то время, когда сегодняшние биткоин-ветераны — Питер Велле, Эрик Ворхес и Питер Тодд, — только делали первые вздохи, Чаум уже разработал решение для создания анонимной платежной системы в интернете.

Слепые подписи

В основе концепции цифровых денег по Чауму лежат «слепые подписи».

Чтобы понять, как работают слепые подписи, необходимо разобраться в тонкостях криптографии с открытым ключом в целом и механизме обычных криптографических подписей в частности.

Криптография с открытым ключом использует пары ключей. Каждая пара состоит из открытого ключа, на первый взгляд, представляющего собой случайный набор чисел, математически рассчитанного на основе другого случайного набора чисел — приватного ключа. Сгенерировать открытый ключ крайне легко, если в распоряжении есть приватный. Однако наоборот этот механизм не работает: практически невозможно воссоздать приватный ключ, имея лишь открытый.

Криптография с открытым ключом может использоваться для установления приватной коммуникации между двумя людьми — в академических кругах это почти всегда условные Алиса и Боб — которые обмениваются только открытыми ключами, оставляя приватные в тайне.

Приватные коммуникации — это не единственная возможность, которую предоставляет этот метод. Алиса и Боб также могут криптографически подписывать любые данные. Для этого необходимо математически скомбинировать приватный ключ с данными, которые нужно подписать. Результатом будет так называемая подпись — это, на первый взгляд, случайная последовательность чисел. По аналогии с открытым ключом, подпись также не позволит воссоздать приватный ключ Алисы или Боба.

Примечательно, что Боб или любой другой участник сети может проверить подпись Алисы, используя ее открытый ключ. Это позволит подтвердить, действительно ли Алиса использовала свой приватный ключ для того, чтобы подписать данные. Подпись может означать, что Алиса согласна с содержанием данных.

Слепые подписи переносят эту концепцию на совершенно новый уровень. Теперь Бобу необходимо сгенерировать случайную последовательность чисел (нонс) и математически скомбинировать ее с данными, таким образом получив еще одну последовательность случайных чисел. Подписывая этот своего рода скрэмбл, Алиса не сможет воссоздать изначальные данные, поэтому ей приходится делать это вслепую. Именно так и появилась слепая подпись.

Интересно, что в этом случае слепая подпись привязана не только к ключу Алисы, зашифрованным данным, но и к исходным данным, которыми они были до комбинации с нонсом. Используя открытый ключ Алисы, каждый может проверить, что она подписала зашифрованную версию исходных данных, в том числе и сама Алиса.

---

eCash

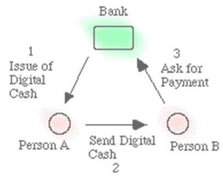
На основе слепых подписей Дэвид Чаум создал цифровую денежную систему. В этой системе Алиса превратилась в банк — условно Банк Алисы. Это обычный банк, такой же как и современные банки, где клиенты хранят свои депозиты, в этом случае в американских долларах.

Предположим, у Банка Алисы есть четыре клиента: Боб, Кэрол, Дэн и Эрин. Предположим также, что Боб хочет купить что-то у Кэрол.

Бобу необходимо запросить вывод средств из Банка Алисы. Чтобы осуществить это, он сам создает так называемые цифровые банкноты в виде уникальных последовательностей чисел — серийных номеров. Затем он комбинирует эти номера с нонсом и отправляет банку.

Задача банка в этом контексте вслепую подписать банкноты и отправить их Бобу обратно. Банк Алисы вычитает по доллару с его банковского счета за каждую отправленную Бобу зашифрованную банкноту.

И поскольку Банк Алисы подписал так называемый скрэмбл, то его подпись также привязана к исходным незашифрованным банкнотам. После этого Боб может отослать Кэрол именно исходные банкноты. Получив их, Кэрол должна направить их в Банк Алисы, где банкноты проходят проверку слепой подписью. Сверив серийные номера, Банк Алисы убеждается, что эти же банкноты не были внесены на другие депозиты, чтобы защититься от угрозы повторного расходования.



Данные faculty.bus.olemiss.edu

После проверки на банковский счет Кэрол поступают доллары. Получив оплату от Боба, Кэрол может отправить ему заказанный товар. Интересно, что сам банк увидит незашифрованные банкноты только после того, как они окажутся на депозите у Кэрол. Таким образом у банка нет возможности проверить, принадлежали ли те банкноты Бобу. Они могли прийти как от Дэна, так и от Эрина.

DigiCash

В 1990 году, почти через 10 лет после публикации своих первых работ и еще до рождения таких разработчиков, как Мэтт Коралло, Виталик Бутерин и Олаолува Осунтокун, Дэвид Чаум основал DigiCash в Амстердаме. Компания специализировалась на цифровых деньгах и платежных системах. Также ее задействовали в правительственной программе по отказу от пунктов дорожных сборов (в итоге были отменены) и смарт-карт (что-то похожее на современные аппаратные кошельки). Флагманским продуктом DigiCash стала цифровая денежная система — eCash, с денежной единицей CyberBucks.

Команда DigiCash

В то время гигантами технологической индустрии были Netscape и Yahoo, и многие думали, что именно микроплатежи станут основной моделью монетизации интернета, а не реклама. Именно поэтому многие предприниматели считали DigiCash восходящей звездой. Разумеется, сам Чаум и его команда верили в жизнеспособность своей технологии.

> *«Платежная система становится все более зрелой. Скоро вы будете платить за каждую мелочь, производя намного больше платежей, чем сегодня. Каждая прочитанная статья, каждый ответ на вопрос — вы будете платить за это», — заявил Чаум в интервью New York Times в 1994 году.*

В том же году в системе eCash состоялись первые платежи, поскольку разработка длилась четыре года. Тогда же начался испытательный срок: банки могли приобрести лицензию на использование технологии у DigiCash.

Стоит отметить, что интерес к технологии был весьма оживленным. К концу 1995 года Mark Twain Bank из Сент-Луиса уже получил лицензию на использование eCash. Более того, к началу 1996 года Deutsche Bank также начал тестировать решение Чаума, а за ним уже и Credit Suisse, Australian Advance Bank, Norway's Norske Bank и Bank Austria.

Интереснее сделок, которые DigiCash заключил, могут быть только сделки, которые компании не удались. Крупнейшие голландские банки ING и ABN Amro предположительно предлагали компании десятки миллионов долларов, а платежная система Visa якобы хотела инвестировать вплоть до $40 млн. Примечательно, что даже Netscape проявлял интерес: eCash мог быть интегрирован в самый популярный веб-браузер своего времени.

По некоторой информации, крупнейшее предложение компании сделала корпорация Microsoft — Билл Гейтс якобы предложил $100 млн за интеграцию eCash в Windows 95. По слухам, в ответ Чаум попросил доход в размере $2 с каждой проданной версии операционной системы. Так сделка и провалилась.

Несмотря на имидж восходящей звезды, DigiCash не удалось заключить финансовую сделку, которая смогла бы существенно помочь компании достичь намеченных целей и полностью раскрыть свой потенциал.

В 1996 году из-за неудачных сделок сотрудники DigiCash потребовали изменений в политике компании. Тогда же и был назначен новый гендиректор — ветеран Visa Майкл Нэш. Стартап также получил дополнительное финансирование, а место в совете директоров досталось основателю Media Lab при Массачусетском технологическом институте Николасу Негропонте (сейчас эта организация обеспечивает финансированием нескольких разработчиков Bitcoin Core). Главный офис DigiCash переехал в Кремниевую долину, а Чаум занял должность технического директора.

Кардинально это ничего не изменило, поскольку широкая общественность все равно не использовала eCash после нескольких лет испытаний. Крупные банки проводили свои эксперименты, но не продвигали технологию на новый уровень развития. К 1998 году Mark Twain Bank зарегистрировал всего 300 мерчантов и 5000 пользователей. И хотя грядущая сделка с Citibank могла изменить ситуацию в пользу eCash, банк вышел из переговоров по не связанным с проектом причинам.

> *«Трудно было привлечь достаточное количество мерчантов, необходимых для расширения пользовательской базы, и наоборот. Интернет быстро развивался и искушенность пользователей стремительно исчезала. Сложно было объяснить им преимущества приватности», — сказал Чаум в интервью Forbes в 1999 году.*

Восхождение мечты шифропанков

Падение DigiCash повлекло за собой и падение eCash. Несмотря на то, что технология не преуспела в бизнес-формате, идеи Чаума вдохновили группу криптографов, хакеров и активистов, связанных между собой электронной почтовой рассылкой. Именно эта группа, в которую входили члены команды DigiCash Ник Сабо и Зуко Уилкокс О'херн [ZCash], станет известна как шифропанки.

Вероятно, представители этой группы придерживались даже более радикальных взглядов, чем сам Чаум. В течение 1990-х годов и в начале 2000-х они внесли несколько предложений в контексте электронных денежных систем. И только в 2008 году, через 10 лет после падения DigiCash, некто Сатоши Накамото представил протокол биткоина в еще одной рассылке, которая стала преемником группы шифропанков.

Биткоин и eCash имеют мало общего. Ключевым моментом было то, что централизованный контроль над eCash находился в руках DigiCash и технология не смогла предложить полностью независимую валюту. Даже в том случае, если бы каждая транзакция в мире проводилась с помощью eCash, необходимость в банках оставалась бы для открытия счетов и подтверждения транзакций. Это означает, что, несмотря на приватность, eCash был не сильно устойчив к цензуре. И если WikiLeaks удалось получать финансирование в биткоинах в ходе банковской блокады, то с eCash это было бы невозможным, поскольку у банков были бы полномочия по блокировке счетов организации.

Тем не менее работа Чаума над цифровой валютой, которая началась еще в начале 1980-х, остается актуальной. Протокол биткоина не предполагает использования слепых подписей, но уровни масштабирования и приватности могут быть построены поверх блокчейна. Модератор форума Bitcointalk и сабреддита r/bitcoin Theymos некогда призывал к имплементации сайдчейна по модели eCash для решения проблемы масштабирования биткоина.

Разработчик Адам Фискор задействовал слепые подписи для разработки микшерных технологий для биткоина, что ранее предложил Грегори Максвелл из Bitcoin Core. Стоит подчеркнуть, что Lightning Network также может интегрировать слепые подписи для усовершенствования безопасности.

Что же до Чаума, то он вернулся в Беркли, где написал множество трудов на тему электронных выборов и репутационных систем. Возможно, лет через 20 совершенно новое поколение разработчиков, предпринимателей и активистов возьмет эти работы за основу для технологии, которая изменит мир.