Глава 1

10 января 2009 года

В этот субботний день у Хэла Финни был праздник — день рождения его сына. Погода в Санта-Барбаре была прекрасной, и в гости приехала сестра жены из Франции, но Хэл надолго застрял за компьютером. Этого дня он ждал много месяцев, а в каком-то смысле и почти всю жизнь.

Хэл редко делился со своей женой Фрэн подробностями работы. Как врач она мало что понимала в его компьютерных делах. Вот и на этот раз он даже не пытался что-то объяснить. Да и что бы он сказал? “Дорогая, я собираюсь поучаствовать в создании нового вида денег?”

А ведь именно такими были его намерения, когда после утренней пробежки он расположился за компьютером в своем скромном домашнем офисе — уголке гостиной со старым столом, на котором громоздились четыре разномастных монитора, подключенных к жужжащим компьютерным блокам. Во всех местах, не занятых компьютерным оборудованием, возвышались стопки бумаг, книги и старые руководства по программированию. Сидя за столом, Хэл мог видеть примыкающее к гостиной патио, даже в середине января щедро залитое калифорнийским солнцем. Слева от него на ковре лежал Арки, преданный пес, названный в честь звезды в созвездии Волопаса — Арктур. Здесь Хэл чувствовал себя дома и именно здесь он написал большинство своих программ.

Он запустил свой громоздкий IBM ThinkCentre, устроился поудобнее и щелкнул на ссылке, которую получил по электронной почте днем ранее. Еще несколько секунд, и на экране появилась главная страница сайта `www.bitcoin.org`.

Хэл узнал о Биткойне пару месяцев назад из сообщения, отправленного в одну из многочисленных почтовых рассылок, на которые он был подписан. Хэл много лет знал большинство участников этой специализированной группы для программистов, но то письмо было отправлено незнакомцем. Некто по имени Сатоши Накамото описывал "электронную наличность" со звучным названием "Биткойн". Хэл давно экспериментировал с цифровыми деньгами — достаточно для того, чтобы скептически отнестись к очередной подобной идее, — но все же что-то в этом письме привлекло его внимание. Сатоши описывал цифровые наличные, для работы которых не требовалось ни банка, ни какого-либо другого посредника. Предлагаемая им система могла функционировать за счет работы компьютеров рядовых пользователей. Хэла особенно заинтересовало заявление Сатоши о том, что пользователи могут владеть биткойнами и отправлять их друг другу, не предоставляя своих персональных данных никаким центральным организациям. Хэл и сам большую часть профессиональной жизни посвятил разработке программ, помогавших людям защититься от всевидящего и всепроникающего ока "Большого брата".

Девятистраничный документ Сатоши, написанный в строгом академическом стиле, вызвал у Хэла неподдельный прилив энтузиазма. "Когда был запущен сайт Wikipedia, я думал, что из этого ничего не выйдет, но проект оказался очень успешным, и во многом по тем же причинам", — написал он в группу. Однако остальные участники переписки отнеслись к предложению скептически.

Хэл посоветовал Сатоши запрограммировать описанную им систему, чтобы проверить ее потенциал в действии. Через несколько месяцев, как раз в этот январский день, он скачал код Сатоши с веб-сайта Биткойна. Запустив обычный EXE-файл, Хэл установил биткойн-программу, и она автоматически открыла окно на рабочем столе его компьютера.

При первом же запуске программа сгенерировала для Хэла список биткойн-адресов и закрытый ключ — своеобразный

пароль для доступа к каждому адресу. Кроме того, программа имела еще пару-тройку функций. Самая интересная, “Отправить монеты”, была Хэлу недоступна, потому что у него еще не было никаких монет, которые можно было бы кому-то отправить. Увы, прежде чем Хэл смог поэкспериментировать с программой, она завершилась из-за какого-то сбоя.

Это не остановило Хэла. Просмотрев файлы журналов, он написал Сатоши письмо, в котором объяснил, что именно произошло, когда его компьютер попытался связаться с другими узлами сети. Как выяснилось, кроме компьютера Хэла к сети были подключены лишь два компьютера Сатоши с одним и тем же IP-адресом, принадлежащим калифорнийскому интернет-провайдеру.

Вскоре Сатоши прислал ответ, в котором не скрывал своего разочарования. Он написал, что тщательно тестировал весь код и давно не сталкивался с какими-либо проблемами. Причиной сбоя могло стать лишь то, что он сжал программу, чтобы ускорить ее передачу по сети. “Видимо, я зря это сделал”, — написал Сатоши и предложил продолжить эксперимент.

Сатоши отправил Хэлу одну из прежних версий программы и поблагодарил его за помощь. Эта программа тоже завершилась сбоем, но Хэл не привык отступать. Наконец ему удалось запустить код на компьютере с другой операционной системой. Когда все заработало, он выбрал в меню наиболее интригующую команду, “Генерировать монеты”. Как только он это сделал, вентилятор процессора в его компьютере заметно ускорился и зашумел.

Довольный собой, Хэл решил сделать перерыв и присоединиться к семейному празднику. В инструкциях, которые Сатоши выслал вместе с программой, говорилось, что на генерирование монет могут потребоваться “дни или месяцы, в зависимости от производительности компьютера и конкуренции среди участников сети”. Хэл уведомил Сатоши, что все работает и что он пока не будет выключать компьютер с запущенным на нем биткойн-узлом.

К тому времени Хэл прочитал достаточно, чтобы понять, что делает его компьютер. Как только биткойн-программа запустилась, она зарегистрировалась в специальном канале чата, чтобы найти другие компьютеры, на которых выполнялось такое же ПО, — в то время там были только компьютеры Сатоши. Все подключенные к биткойн-сети компьютеры пытались получить новые биткойны, которые создавались пакетами по 50 монет. Каждый новый пакет биткойнов отправлялся тому пользователю, который выиграл последний раунд своеобразного конкурса на решение специальной вычислительной задачи. Когда один из компьютеров побеждал в очередном раунде конкурса и получал новые монеты, все остальные узлы сети обновляли свою копию данных о количестве биткойнов, принадлежащих владельцу соответствующего адреса. После этого узлы сети автоматически приступали к решению очередной задачи в попытке выиграть следующий пакет из 50 монет.

Вернувшись вечером к компьютеру, Хэл увидел, что тот в его отсутствие заработал 50 биткойнов, которые были зачислены на один из его биткойн-адресов и зарегистрированы в общедоступном журнале, служащем для отслеживания всех когда-либо созданных биткойнов. Этот блок стал 78-м по счету, и хотя на тот момент заработанные Хэлом биткойны не стоили ровным счетом ничего, это ничуть его не смутило. В поздравительном письме к Сатоши, копию которого Хэл отправил в группу подписчиков, он позволил себе немного помечтать.

> “Представьте, что Биткойн станет главной платежной системой в мире, — дал он волю фантазии. — Тогда его общая стоимость сравняется со стоимостью всего богатства в мире”.

По его подсчетам в этом случае каждый биткойн должен был бы стоить около 10 миллионов долларов.

“Даже если шансы Биткойна достичь такого уровня призрачны, неужели они меньше, чем 1 против 100 миллионов? — написал он, прежде чем покинуть группу. — Есть над чем подумать”.

ХЭЛ ФИННИ давно интересовался тем, как технологии формируют облик будущего.

Один из четверых детей инженера-нефтяника, Хэл в юности прочитал много классических научно-фантастических романов, позже перешел на книги по высшей математике и в итоге поступил на учебу в Калифорнийский технологический институт. Сложные задачи никогда не пугали его, а скорее раззадоривали. Достаточно сказать, что уже в первый год учебы в институте он записался на курс по теории гравитационного поля, предназначенный для аспирантов.

Но он не был и типичным компьютерным гиком. Высокий и атлетично сложенный, Хэл любил покататься на лыжах в калифорнийских горах и не имел никаких проблем с социальной адаптацией, бывших частым явлением среди студентов Калтеха. Активный творческий дух распространялся и на интеллектуальные увлечения Хэла. Читая романы Ларри Нивена, в которых обсуждалась возможность замораживания людей с целью их последующей реанимации, Хэл не просто оценивал реалистичность таких технологий. Он нашел фонд продления жизни Alcor, который занимался подобными исследованиями, и подписался на его журнал. Позднее он заплатит за сохранение своего тела и тел членов его семьи в криохранилищах Alcor неподалеку от Лос-Анджелеса.

Изобретение Интернета Хэл воспринял как величайшее благо: сеть позволила ему свободно общаться с теми немногими людьми, которые увлекались подобными радикальными идеями. Еще до появления первого веб-браузера Хэл вступил в интернет-сообщества “шифропанков” и “экстропианцев”, участники которых страстно обсуждали возможные способы влияния на будущее с помощью технологий.

Мало что волновало участников этих групп больше, чем вопрос, как технологии изменят баланс власти между корпорациями и государствами с одной стороны и отдельными людьми — с другой. Безусловно, информационные технологии предоставили людям беспрецедентные возможности

продвижения своих взглядов и поиска единомышленников. Но в то же время постепенное проникновение цифровых технологий в нашу жизнь позволило государствам и крупным компаниям усилить контроль над наиболее ценным и опасным товаром информационной эпохи — самой информацией.

Конечно, правительства всех стран пытались следить за своими гражданами и в докомпьютерную эпоху, но собрать много информации о большинстве людей было просто невозможно. Однако уже в 1990-е годы — задолго до того как выяснилось, что АНБ прослушивает телефонные разговоры обычных граждан, а политика конфиденциальности Facebook стала предметом национальных дебатов — шифропанки ясно увидели, что компьютеризация всех сфер жизни значительно упрощает для властей сбор сведений о людях и манипулирование ими. Больше всего шифропанков беспокоил вопрос, как люди могут защитить свою личную информацию и конфиденциальность. Достаточно сказать, что "Манифест шифропанка", который в 1993 году опубликовал Эрик Хьюз, математик из Беркли, начинается словами "В электронную эпоху конфиденциальность стала для открытого общества необходимостью".

Эти воззрения во многом произрастали из либертарианских взглядов, которые приобрели популярность в Калифорнии в 1970- и 1980-е годы. Подозрительное отношение к государству было естественным для программистов, которые на работе самостоятельно создавали новый мир, не полагаясь на чью-либо помощь. Хэл проникся этими идеями еще в Калтехе, отчасти благодаря романам Айн Рэнд. Однако проблема конфиденциальности в эпоху Интернета вызывала немалый интерес и вне либертарианских кругов, в том числе среди защитников прав человека и активистов других протестных движений.

Конечно, никто из шифропанков не призывал к отказу от технологий — напротив, именно в технологиях, а особенно в науке о шифровании (криптографии) они видели решение проблемы. Шифрование исторически было привилегией лишь самых влиятельных организаций. Частные лица могли

попытаться кодировать свои данные тем или иным способом, но спецслужбы и военные прекрасно научились взламывать такие шифры. Однако в 1970- и 1980-е годы математики из Стэнфорда и MIT сделали ряд открытий, которые впервые в истории позволили обычным людям шифровать сообщения так, что их невозможно было взломать даже с помощью самых мощных суперкомпьютеров. Новая технология получила название "криптография с открытым ключом".

Чтобы зашифровать данные с ее помощью, пользователь должен сгенерировать открытый ключ — уникальное случайное сочетание букв и чисел, служащее чем-то вроде адреса, который можно свободно сообщать кому угодно — и соответствующий закрытый ключ, который нужно сохранить в секрете. Эти два ключа связаны математическим отношением, которое гарантирует, что только обладатель закрытого ключа — Алиса, как ее традиционно зовут криптографы — может расшифровывать сообщения, отправленные ее открытому ключу. Уникальное отношение между открытым и закрытым ключами определяется с помощью сложных математических уравнений, которые исключают возможность вычислить закрытый ключ по открытому даже на самом мощном суперкомпьютере. Подобные криптографические хитрости позже будут положены в основу Биткойна.

Хэл узнал о потенциале криптографии с открытым ключом в 1991 году благодаря Дэвиду Чому — талантливому криптографу, который экспериментировал с технологиями защиты конфиденциальности.

"Все показалось мне совершенно очевидным, — рассказывал Хэл другим шифропанкам о своем первом впечатлении от работы Чома. — Мы думаем, как решить проблемы утраты конфиденциальности, всеобъемлющей компьютеризации, централизации баз данных, но ищем решения не там, где следует. Чом предлагает двигаться в другом направлении, чтобы отнять власть у правительств и корпораций, наделив ею простых людей".

Как обычно, обнаружив новую захватывающую идею, Хэл не ограничился чтением о ней, а начал в свободное время

помогать проекту PGP (Pretty Good Privacy). Участники проекта разрабатывали ПО, позволявшее отправлять и получать сообщения, зашифрованные с помощью криптографии с открытым ключом. Основатель PGP Фил Циммерман был категорическим противником ядерного оружия и хотел, чтобы диссиденты могли общаться без контроля со стороны государства. В скором времени Циммерман принял Хэла на работу в PGP.

Идеалистические проекты наподобие PGP обычно получают совсем малую известность, но и ее оказалось достаточно, чтобы федеральная прокуратура инициировала уголовное расследование относительно деятельности Циммермана и PGP. Дело в том, что ранее правительство США засекретило надежные технологии шифрования, что сделало их экспорт нелегальным. Хотя иск в итоге был отозван, Хэлу пришлось годами скрывать свое участие в работе над PGP, из-за чего его вклад в проект так и не получил должного признания.

БОРЬБА ЭКСТРОПИАНЦЕВ и шифропанков с традиционными формами власти принимала разные формы, но все же с самого начала в центре их внимания были деньги. Для рыночной экономики деньги — это такой же базовый элемент, как вода или огонь для человечества. Представить экономику без денег практически невозможно. Все существовавшие валюты, действительные только в пределах конкретного государства и контролируемые некомпетентными банкирами, казались программистам-шифропанкам безнадежно устаревшими и ограниченными, особенно в сравнении с возможными альтернативами. Далеко ходить за примерами не требовалось: во многих научно-фантастических романах, на которых выросли Хэл и его соратники, описывались те или иные универсальные деньги, например в “Звездных войнах” это были галактические кредиты.

Даже если вынести за скобки эти причудливые амбиции, шифропанки видели в финансовой системе одну из опаснейших

угроз для конфиденциальности. Мало что характеризует человека точнее, чем его финансовые операции. Получив доступ к выпискам по кредитной карте, можно узнать, чем увлекается ее владелец, какие магазины и рестораны посещает, что для него важно и что ему безразлично… Неслучайно финансовые записи — один из главных способов отслеживания беглых преступников. В "Манифесте шифропанка" Эрик Хьюз описывает проблему гораздо подробнее: "Если механизмы транзакции таковы, что моя личность раскрывается, значит, конфиденциальности у меня нет. У меня нет возможности раскрывать себя избирательно, я вынужден делать это всегда… Для сохранения конфиденциальности в открытом обществе требуются системы анонимных транзакций".

Анонимные платежи возможны испокон веков благодаря наличным деньгам, но мы не смогли взять с собой наличные в цифровой мир. Как только деньги переводились в цифровую форму, они попадали под контроль банков или других организаций, которые получали возможность с легкостью отслеживать транзакции. Чего хотели Хэл, Чом и шифропанки, — так это создать наличные для цифровой эпохи, которые были бы безопасными и защищенными от подделки, но при этом не вынуждали людей жертвовать конфиденциальностью. В тот же год, когда Хьюз опубликовал свой манифест, Хэл отправил в группу единомышленников сообщение с описанием цифровых наличных, позволяющих не хранить никакие записи о том, где и на что кто-то их потратил. Предполагалось, что банк будет лишь знать, сколько денег его клиент снял за конкретный месяц. Хэл даже придумал для цифровых наличных звучное название: "CRASH", или "CRypto cASH".

К тому времени, когда проблемой финансовой конфиденциальности заинтересовались шифропанки, Чом уже изобрел DigiCash — интернет-деньги, которые можно было тратить без обнародования каких-либо личных сведений. Для сохранения личности в секрете в DigiCash использовались так называемые слепые подписи, также основанные на криптографии с открытым

ключом. Когда один из американских банков решил поэкспериментировать с DigiCash, Хэл тут же открыл в нем счет.

К сожалению, работы Чома обозначили не совсем правильный путь к решению проблемы. В DigiCash каждую цифровую подпись должна была проверять центральная организация, принадлежавшая Чому, а это означало, что она требовала доверия со стороны потенциальных клиентов. Когда компания Чома обанкротилась в 1998 году, с ней пришел конец и всему проекту DigiCash. Этот печальный опыт показал, что никакая центральная организация не должна контролировать цифровые наличные. На первый взгляд, проблема казалась неразрешимой: если бы никакая организация не контролировала цифровые деньги, ничто не мешало бы людям тратить их дважды, ведь скопировать данные в цифровом мире проще простого. Некоторые из шифропанков сочли задачу неразрешимой и оставили проект, но Хэл не привык отступать.

Как ни странно, человек, приложивший столько усилий ради создания нового вида денег, вовсе не стремился к богатству: PGP и другие программы, которые писал Хэл, распространялись в основном бесплатно. Его недоверие к государству также не было обусловлено желанием уклониться от уплаты налогов; напротив, в 1990-е годы Хэл каждый год выплачивал налоги с полного дохода, не пользуясь какими-либо вычетами или льготами, чтобы как можно меньше возиться с бумагами. Много лет он прожил в скромном домике на окраине Санта-Барбары. Казалось, его совершенно не заботит то, что он вынужден работать в углу своей гостиной или что обивка на его кресле прохудилась. Хэл был движим, прежде всего, интеллектуальным любопытством, которое буквально сочилось из каждого написанного им письма, и осознанием права каждого человека на достойную жизнь.

“Главная цель того, чем мы занимаемся, — это отправить Большого брата на свалку истории, — писал Хэл своим единомышленникам. — Не стоит недооценивать эту задачу. Возможно, когда-нибудь мы оглянемся и увидим, что это было самое важное из всего, что мы сделали”.