§ 2. ЭЛЕКТРОННЫЕ ДЕНЬГИ

- Как вы видите будущее цифровых денег?

- Я думаю, что в конце концов они заменят деньги бумажные и станут основной формой денег. Цифровая наличность, разработанная мной, на самом деле лучше бумажных денег физического мира, поскольку она решает проблему анонимности и, в то же время, уменьшает возможность мошенничества. Более того, у этой формы денег есть то преимущество, что они доступны не только в физическом, но и в виртуальном мире. Что и дает мне уверенность в том, что когда-нибудь цифровая наличность заменит бумажную.

[*Телефонное интервью с David Chaum, создателем первой схемы электронных денег DigiCash, 1999*]

ЦИФРОВЫЕ ДЕНЬГИ - платежные средства, представленные и обращаемые в электронном виде, оборот которых гарантирует анонимность. По аналогии с наличными купюрами Ц.д. как электронные документы содержат номинальную стоимость, указание на эмитента, индивидуальные признаки (серия, номер, и т.д.) и элементы защиты от подделки (заверение их цифровой подписью эмитента).

Электронные деньги (ЭД)— это денежные обязательства эмитента (организация, выпустившая ценные бумаги) в электронном виде, которые находятся на электронном носителе в распоряжении пользователя. Такие денежные обязательства:

- фиксируются и хранятся на электронном носителе;
- выпускаются эмитентом при получении от иных лиц денежных средств в объёме не меньшем, чем эмитированная денежная стоимость;
- принимаются, как средство платежа другими.

Нельзя отождествлять электронные деньги с безналичными. Электронные деньги, являясь неперсонифицированным платежным продуктом, могут иметь отдельное обращение, отличное от банковского обращения денег, однако могут обращаться и в государственных или банковских системах. Очевидно, в будущем центробанки будут производить эмиссию электронных денег, так же как сейчас печатают банкноты. Обращение электронных денег происходит при помощи компьютерных сетей, Интернета, платёжных карт, электронных кошельков и устройств, работающих с платежными картами (банкоматы, POS-терминалы, платежные киоски и т. д.).

Критерии, которым в идеале должны удовлетворять электронные деньги:

- ***анонимность покупателя*** (оплата электронными деньгами не должна позволять проследить, кто именно купил данный товар);
- ***независимость от места хранения*** (безопасность ЭД не должна зависеть от места их физического хранения на носителях информации);

- ***защита от мошенничества*** (нельзя использовать точную копию электронной монеты второй раз);
- ***автономность*** (желательно, чтобы при осуществлении платежа не возникала необходимость в сторонних проверках третьим лицом);
- ***делимость*** (если сумма в ЭД больше цены товара, то ЭД должны быть разделены на мелкие части, чтобы покупатель получил сдачу после покупки).

Третье из этих требований отражает существенное отличие автономной системы электронных денег от централизованных платежных систем. Централизованная система не позволяет клиентам потратить одну и ту же банкноту дважды, т.к. банковская верификация платежа пресекает эти попытки. Автономная же система лишь идентифицирует нарушителя в какой-то момент после повторного использования монеты. Разумеется, банк попытается снять соответствующую сумму со счета нарушителя, но при этом может обнаружить, что последнему нечем расплатиться. Такова плата за эффективность. Но в ответ на возражения, разработчики автономных систем обычно просто отмечают, что подобный риск не является чем-то новым; он принят во многих ныне действующих платежных системах.

Прикладные криптографические протоколы, обеспечивающие функционирование электронных денег, их передачу между абонентами и гарантию эквивалентности операций с обычными деньгами, называются ***протоколами электронных платежей с помощью электронных денег***.

Центральные понятия протоколов электронных платежей – «подпись вслепую» и «цифровой конверт». «Подпись вслепую» позволяет подписывать документы, при условии, что подписывающий не знает содержания самих документов. Например, если банк ставит «слепую подпись» под чеком на предъявителя, то:

1. слепая подпись банка на чеке является правильной и подтверждает, что именно банк заверил этот чек, когда тот потом будет ему предъявлен;
2. банк не может связать заверенный им чек с моментом подписывания.

Базовый вариант платежной системы с ЭД:

Пусть покупатель хочет подписать в банке чек (обозначим его m) с указанной на нем суммой, которую он хочет снять со своего банковского счета. При этом покупатель не хочет, чтобы банк увидел сам чек или пометил его. Тогда покупатель подготавливает большое число чеков на нужную сумму, запечатывает их в конверты вместе с копировальной бумагой и все отправляет в банк. Банк вскрывает все

конверты, кроме одного, и убеждается в корректности чеков. Тогда он подписывает последний конверт, не распечатывая его, и списывает со счета покупателя требуемую сумму. Благодаря копировальной бумаге, подпись банка автоматически оказывается на чеке (т.е. банк подписал чек, не видя его).

Использование криптосистемы RSA для формирования конверта и получения слепой подписи.

Пусть n – модуль шифрования, e – открытая экспонента банка.

1. Покупатель выбирает из интервала $(1;n)$ столько случайных чисел r, сколько конвертов он будет отправлять в банк (чем больше r, тем лучше; числа r называются ***маскирующими***).

2. Каждое число r шифруется на открытом ключе банка и умножается на значение чека m, т.е. $y = m \cdot r^e (\mathrm{mod}\, n)$. Значения y пересылается в банк.

3. Запросив у покупателя числа r (кроме одного), банк вычисляет $m = y \cdot r^{-e} (\mathrm{mod}\, n)$ для всех конвертов, кроме одного, т.е. вскрывает конверты. Без ведома покупателя процедура не осуществима, так как требует знания r. Вычисленные банком значения m должны совпасть с заявленной суммой в чеке.

4. Не вскрытый конверт банк подписывает

$$y^d = m^d (r^e)^d (\mathrm{mod}\, n) \equiv m^d r (\mathrm{mod}\, n)$$

и отсылает покупателю.

5. Покупатель проверяет подпись банка на конверте с помощью проверки равенства $(y^d)^e = y$. Если оно соблюдается, то вскрывает конверт и извлекает из него подписанный чек $m^d = y^d r^{-1} (\mathrm{mod}\, n)$.

6. Подписанный чек покупатель отдает продавцу. Тот проверяет подпись банка $(m^d)^e = m (\mathrm{mod}\, n)$ и пересылает чек в банк.

7. Банк таким же образом проверяет свою собственную подпись на полученном чеке. Если она правильная, то перечисляет деньги на счет продавца.

Однако данный проток никак не решает вопросов мошенничества покупателя или продавца, когда те пытаются вторично использовать чек.

Пример. Подписать «вслепую» чек на 1200 грн.

Р е ш е н и е. $m = 1200$.

1. Генерация ключей банка: $p = 673$, $q = 431$, $n = 290063$, $\varphi(n) = 288960$, $e = 337$, $d = 156913$.

2. Подготовка покупателем цифровых конвертов: произвольно выбирает пять простых чисел из интервала $(1;n)$ $r_1 = 4523$;

$r_2 = 92174;\ r_3 = 78923;\ r_4 = 54096;\ r_5 = 23568$. Далее он формирует по формуле $y = m \cdot r^e \pmod n$ конверты:

$$y_1 = 1200 \cdot 4523^{337} \pmod{290063} \equiv 254539;$$

$$y_2 = 1200 \cdot 92174^{337} \pmod{290063} \equiv 196420;$$

$$y_3 = 1200 \cdot 78923^{337} \pmod{290063} \equiv 202248;$$

$$y_4 = 1200 \cdot 54096^{337} \pmod{290063} \equiv 272877;$$

$$y_5 = 1200 \cdot 23568^{337} \pmod{290063} \equiv 36463.$$

Покупатель отправляет все 5 конвертов в банк.

3. Подпись банком «вслепую» одного чека: банк выбирает наугад конверты y_1, y_2, y_4, y_5, запрашивает для них маскирующие числа и получает числа r_1, r_2, r_4, r_5. Далее банк вскрывает конверты по формуле $m = y \cdot r^{-e} \pmod n$, предварительно вычислив обратные элементы $r^{-1} \pmod n$:

$$m_1 = 254539 \cdot 157056^{337} \pmod{290063} = 1200;$$

$$m_2 = 196420 \cdot 87141^{337} \pmod{290063} = 1200;$$

$$m_4 = 272877 \cdot 81851^{337} \pmod{290063} = 1200;$$

$$m_5 = 36463 \cdot 194963^{337} \pmod{290063} = 1200.$$

Банк убеждается, что все m одинаковые и подписывает «вслепую» последний запечатанный конверт y_3:

$$F = y_3^d \pmod n = 202248^{156913} \pmod{290063} = 69667$$

и отправляет подписанный конверт покупателю.

4. Извлечение покупателем подписанного чека из конверта: покупатель снимает маску с подписанного чека:

$$m^d = F r_3^{-1} \pmod n = 69667 \cdot 157996 \pmod{290063} \equiv 86671.$$

Покупатель проверяет, что подпись – подлинная, используя открытый ключ банка:

$$(m^d)^e = m \pmod n \Rightarrow\ 86671^{337} \pmod{290063} = 1200.$$

Покупатель передает чек на сумму 1200 грв продавцу.

5. Продавец принимает чек: получив чек, он снова проверяет

$$(m^d)^e = m \pmod n \Rightarrow\ 86671^{337} \pmod{290063} = 1200.$$

Так как подпись на чеке – правильная, то продавец соглашается принять чек для оплаты товара.

6. Обналичивание чека. Банк, получив чек от продавца, проверяет, что он – не фальшивый с помощью равенства

$(m^d)^e = m(\mathrm{mod}\, n)$, т. е. $86671^{337}(\mathrm{mod}\, 290063) = 1200$. Банк переводит эту сумму на счет продавца.

Как исправить второй недостаток – возможность двойной платы? Для этого можно использовать online и offline контроль. Online–контроль – это связь продавца с банком в момент оплаты с целью выяснить, является ли действительным предъявляемый чек. Этот метод абсолютно надежен (если, конечно, банк не жульничает), но обладает многими недостатками: необходима постоянная связь продавца с банком, медленная скорость обслуживания. Offline–контроль – "продавец связывается с банком вечером".

Рассмотрим подробнее offline–контроль. Мы хотим, чтобы имя покупателя осталось неизвестным, если он потратил чек, а если он использовал его более одного раза, то мы хотим его узнать. Для этого можно поступить так:

Участники (покупатели) генерируют $x_1 \dots x_k, y_1 \dots y_k$ по правилу: имя участника $ID = x_i \oplus y_i$ для каждого i.

Участники посылают банку хэш-функции от этих значений и включают хэш-значения в текст чека.

К каждой электронной купюре добавляют набор из k значений x_i или y_i по выбору продавца (то есть продавец говорит покупателю: "Дай мне x_1, y_2, y_3, x_4".)

Если деньги тратили 2 раза, то можно с вероятностью $1–2^{-k}$ установить нарушителя: у продавцов окажутся половинки имени (x_i и y_i), и они будут разными с большой вероятностью.

Истинность ID проверяется выборочной проверкой. С вероятностью 2^{-k} магазин может получить убыток при двойной оплате.

Дэвид Чаум (англ. David Chaum) – создатель слепой схемы подписи и электронных денег. В 1990 г. стал доктором наук по информатике в университете Беркли, где позднее преподавал сам. Профессор католического университета Левена (Бельгия). Изобрел две анонимные сети: сети соединения и сети постоянного тока. Внес значительный вклад в продвижение электронных денег частично в роли основателя DigiCash и электронной платежной системы. Создатель системы шифрования электронного голосования.