Анонимность и защита цифровых денег.

Эссе подготовил студент 012 гр. Цыбин В.С.

Вступление

«Уже в 1999 году жители Земли купили товаров в online на сумму 15 миллиардов долларов. В секторе «бизнес-бизнес» (B2B) эта цифра достигла 109 миллиардов долларов.
Только на рождественские подарки в конце 1999 года американцы потратили 5 миллиардов долларов.
На конец 2001 года в Европе число покупок в Интернет достигло 36 миллионов. Эти покупки сделало 30% европейской Интернет-аудитории (9% жителей Европы). Уже в 2002 году общая сумма всех Интернет-покупок жителями Европы превысила сумму в 80 миллиардов евро. По прогнозам Jupiter Research к 2007 году количество Интернет-пользователей в Европе вырастет до 220 миллионов человек. Опять же по прогнозам Forrester Research, к 2006 году объем Интернет-покупок составит 1,400 миллиардов фунтов стерлингов, причем 64% из всей электронной коммерции будут составлять объемы продаж Великобритании, Германии и Франции.
Германия занимает третье место в мире после США и Южной Кореи по количеству совершенных покупок онлайн. Только за несколько месяцев 2002 года 26% из 26.7 миллионов пользователей Интернет в Германии сделали различные Интернет-покупки. Самые популярные купленные товары – книги (33%), CD (24%), одежда (21%), электроника и бытовая техника (19%), бронирование и покупка билетов (14%). Только за первые три месяца 2002 года в США было совершено Интернет-покупок на сумму около 10 миллиардов долларов, что на 10% больше последних трех месяцев 2001 года...»[1]

Почему Digital Money?

Анонимность.

Электронные системы оплаты разнообразны: цифровые чеки, дебетные карты, кредитные карточки, и карты запасенных ценностей. Обычные особенности безопасности таких систем - секретность (защита от подслушивания), подлинность (обеспечивает идентификацию пользователя и целостность сообщения), и неотказ (предотвращение отрицания выполнившейся сделки).

Тип электронной системы оплаты, описанной далее - электронные наличные деньги. Как подразумевает название, электронные наличные деньги - попытка построить электронную систему оплаты, похожую на нашу бумажную наличную систему. Бумажные наличные деньги имеют следующие особенности: они портативные (легко переносить), узнаваемые, следовательно с готовностью принимаемые, передаваемые (без вовлечения финансовой сети), неотслеживаемые (нет никакой записи того, где деньги потрачены), анонимные (нет никакой записи, кто потратил деньги) и имеют способность делать обмен. Проектировщики электронных наличных денег сосредотачивались на сохранении особенностей **неотслеживаемости** и **анонимности**. Таким образом, электронные наличные деньги созданы, чтобы быть электронной системой оплаты, которая обеспечивает, в дополнение к вышеупомянутым особенностям безопасности, свойства анонимности пользователя и неотслеживаемости оплаты.

Транзакции по кредитным карточкам стоят денег, и немалых. Цена транзакции колеблется от 1.5% до 4% в зависимости от типа бизнеса и других условий. Так же обычно цена одной транзакции для продавца не может быть ниже 25 центов. Таким образом, экономически выгодными (для плательщика, с точки зрения минимума процентов за транзакцию) являются транзакции, начиная где-то с 20 долларов.

А что делать с транзакциями на мелкие суммы? Вот, например, взять shareware. Многие пожадничают заплатить за программу 100 долларов. Но большинство пользователей могут

заплатить 5 долларов - если это будет легко сделать. Или другой пример: вам не хочется покупать 6-месячную подписку на электронный журнал, но вы бы с удовольствием попробовали почитать несколько статей по 25 центов за статью, или по доллару за номер.

К недостаткам электронных денег стоит отнести возможные мошенничества с повторным использованием одной и той же купюры. Электронная банкнота - некая последовательность бит, которая может быть многократно размножена в отличии от бумажной банкноты.

Кроме того повреждение физического носителя электронных денег(смарт-карты или жёсткого диска) ведёт к потере электронных средств в отличие от кредитных карт, на которых хранится только информация о состоянии вашего счёта.

Таким образом электронные наличные деньги имеют ряд преимуществ перед электронными чеками и кредитными карточками:

- анонимность и неотслеживаемость
- осуществление микроплатежей

И недостатки:

- если нет соответствующей защиты, электронная банкнота может быть потрачена многократно
- возможность физической порчи электронных денег (как и для бумажных денег)

Электронный сценарий оплаты включает трёх участников :

- Плательщик или потребитель, которого мы назовем Алисой.
- Получатель платежа, торговец. Мы назовем получателя платежа Бобом.
- Финансовая сеть, в которой Алиса и Боб имеют счета. (Например, Банк.)

Электронная монета или банкнота представляет из себя *последовательность бит*, включающая серийный номер, номинал, информацию, предназначенную для раскрытия личности плательщика *только* при совершении мошенничества (что подразумевается под этой информацией см. ниже). Всё это подписывается Банком. Банк может использовать различные подписи для разных номиналов банкнот.

Последовательность событий в электронной наличной оплате следующая:

- Изъятие (Алиса перемещает часть своих средств со счета в Банке на свой физический носитель.)
- Оплата (Алиса передает деньги со своей карты Бобу.)
- Депозит (Боб перемещает полученные деньги на свой счет в Банке.)

Эти процедуры могут быть осуществлены двумя способами:

- Диалоговая оплата (on-line payment) означает, что Боб вызывает Банк и проверяет законность оплаты конкретной банкнотой Алисы *перед* принятием денег и поставкой товаров. (Это похоже на многие из сегодняшних сделок с помощью кредитной карточки.)
- Автономная оплата (off-line payment) означает, что Боб подвергает электронную монету Алисы проверке и депозиту когда-нибудь *после* совершения сделки . (Этот метод похож на оплату чеком.)

Как в любой системе оплаты, существует опасность преступного злоупотребления с намерением

обмануть финансовую систему или использовать механизм оплаты, чтобы облегчить некоторое другое преступление

Есть два злоупотребления электронной наличной системой, аналогичной подделыванию физических наличных денег:

- Символическая подделка, или создание монеты без соответствующего изъятия средств из Банка.
- Многократное расходование, или использование той же самой банкноты снова. (Электронная монета состоит из цифровой информации, которая может быть легко скопирована.)

Ниже рассмотрены алгоритмы, позволяющие контролировать законность платежей и обеспечивающие электронные наличные свойствами, которые были перечислены.

Упрощенная электронная наличная система без особенностей анонимности выглядит так:

ПРОТОКОЛ 1: Диалоговая электронная оплата.

Изъятие:

Алиса посылает запрос изъятия в Банк.

Банк готовит электронную монету и в цифровой форме подписывает её.

Банк посылает монету Алисе и дебетует ее счет.

Оплата / депозит:

Алиса дает Бобу монету.

Боб входит в контакт с банком и посылает монету.

Банк проверяет свою цифровую подпись.

Банк проверяет не была ли монета потрачена ранее.

Банк консультируется с его отчетами изъятия, чтобы подтвердить изъятие Алисой. (необязательно)

Банк вводит монету в базу данных потраченных монет.

Банк кредитует счет Боба и сообщает об этом Бобу.

Боб дает Алисе товары.

Нужно иметь в виду, что термин "Банк" относится к финансовой системе, которая выпускает и погашает монеты. Алиса и Боб могут иметь отдельные банки. Если это так, то процедура "депозита" немного сложнее: банк Боба входит в контакт с банком Алисы, обналичивает монету и помещает деньги на счет Боба.

ПРОТОКОЛ 2: Автономная электронная оплата.

Изъятие:

Алиса посылает запрос изъятия в Банк.

Банк готовит электронную монету и в цифровой форме подписывает её.

Банк посылает монету Алисе и дебетует ее счет.

Оплата:

Алиса дает Бобу монету.

Боб проверяет цифровую подпись Банка. (необязательно)

Боб дает Алисе товары.

Депозит:

Боб посылает монету Банку.

Банк проверяет свою цифровую подпись.

Банк проверяет не была ли монета потрачена ранее.

Банк консультируется с его отчетами изъятия, чтобы подтвердить изъятие Алисой. (необязательно)

Банк вводит монету в базу данных потраченных монет.

Банк кредитует счет Боба и сообщает об этом Бобу.

Для подключения свойства анонимности используется так называемая слепая цифровая подпись.

Алгоритм слепой цифровой подписи на основе RSA:

Пусть (v,N) - открытый ключ Банка, s - секретный ключ, с помощью которого осуществляется подпись

Предположим, что Алиса хочет, чтобы Банк произвел слепую подпись сообщения M. Она генерирует случайное число r и посылает

$$r^v \cdot M \pmod N$$

Банк (после соответствующей аутенификации Алисы) подписывает полученное сообщение и отправляет его Алисе:

$$r \cdot M^s \pmod N$$

Алиса полученное число делит на r и получает M, подписанное банком (M,M^s).

В случае с электронными деньгами Банк подписав банкноту снимает соответствующую сумму со счёта Алисы. Банку известно $r^v \cdot M \pmod N$, но неизвестно r и M (серийный номер банкноты) в отдельности. Следовательно, погашая потраченную банкноту, Банк узнает её серийный номер, но не знает кому была выдана банкнота с таким номером. Следовательно, он не может проследить кто потратил деньги у Боба-продавца. Кроме того предусматривается хеширование сообщения M, то есть происходит подписание $r^v \cdot h(M) \pmod N$ Это нужно для того, чтобы по двум банкнотам нельзя было создать третью ($M2^s * M1^s = (M2*M1)^s$, где $(M2*M1) \pmod N$ - серийный номер "новой" банкноты)

Таким образом механизм изъятия средств несколько изменяется:

ПРОТОКОЛ3: Диалоговая электронная оплата.

Изъятие:

Алиса создает электронную монету и "ослепляет" её.

Алиса посылает "ослеплённую" монету и запрос изъятия в Банк.

Банк цифровой форме подписывает монету.

Банк посылает монету Алисе и дебетует ее счет.

Алиса "деослепляет" подписанную монету.

Оплата / депозит:

Алиса дает Бобу монету.

Боб входит в контакт с банком и посылает монету.

Банк проверяет свою цифровую подпись.

Банк проверяет не была ли монета потрачена ранее.

Банк вводит монету в базу данных потраченных монет.

Банк кредитует счет Боба и сообщает об этом Бобу.

Боб дает Алисе товары.

ПРОТОКОЛ 4: Автономная электронная оплата

Изъятие:

Алиса создает электронную монету и "ослепляет" её.

Алиса посылает "ослеплённую" монету и запрос изъятия в Банк.

Банк цифровой форме подписывает монету.

Банк посылает монету Алисе и дебетует ее счет.

Алиса "деослепляет" подписанную монету.

Оплата: как и в ПРОТОКОЛе2

Депозит:

Боб посылает монету Банку.

Банк проверяет свою цифровую подпись.

Банк проверяет не была ли монета потрачена ранее.

Банк вводит монету в базу данных потраченных монет.

Банк кредитует счет Боба и сообщает об этом Бобу.

Если оплата должна быть диалоговой, мы можем использовать Протокол 3 (учитывающий анонимность плательщика). В автономном случае, однако, возникает новая проблема. При повторной трате монеты, Банк отвергнет её, но правонарушитель останется неизвестным, так как протокол реализует свойство анонимности. Таким образом для Банка необходимо быть способным идентифицировать многократного растратчика. Эта особенность, однако, должна сохранить анонимность для законопослушных пользователей.

Решение - требовать, чтобы Алиса имела, в дополнение к её электронной монете, некоторый вид идентификационной информации, которую она должна сообщать получателю платежа. Эта информация разделена таким способом, что любая её часть ничего не говорит относительно Алисы, но любых двух частей достаточно полностью идентифицировать ее.

Эта информация создаётся в течение изъятия. Протокол изъятия включает шаг, в котором Банк проверяет, что информация - там и соответствует Алисе и специфической создаваемой монете. (Чтобы сохранять анонимность плательщика, Банк фактически не будет видеть информацию, только проверять, что она - там.) Алиса несет информацию наряду с монетой, пока она не потратит её. В ходе оплаты Боб посылает Алисе случайное число-вызов (challenge)

В ходе оплаты, Алиса должна показать одну часть этой информации Бобу. (Таким образом только Алиса может потратить монету, так как только она знает информацию.) Для этого используется протокол ответа-вызова. В таком протоколе, Боб посылает Алисе, случайное число-"вызов", и в ответ Алиса возвращает часть идентификационной информации. (Вызов определяет, которую часть она посылает.) В ходе депозита, вызов и ответ посылаются Банку наряду с монетой. Если

всё идёт как надо, то информация никогда не будет указывать на Алису. Однако, если она потратит монету дважды, Банк в конечном счете получит две копии той же самой монеты, каждый с частью идентификационной информации. Из-за хаотичности в протоколе ответа-вызова, эти две части будут различны. Таким образом Банк будет способен идентифицировать ее. Так как только она может распределять идентифицирующую информацию, мы знаем, что ее монета не была скопирована и заново потраченный кем - то еще.

Для осуществления этого протокола используется алгоритмы Шнорра(*The Schnorr Algorithms*) Эти алгоритмы основаны на доказательстве владения секретным ключом с нулевым знанием.

Пусть - q и p большие простые числа, p-1 делится на q. Пусть g -генератор группы целых чисел (1<g<p) такой, что

$$g^q = 1 \pmod{p}.$$

Если s - целое число (mod q), то модульное возведение в степень есть:

$$f : s \rightarrow g^s \pmod{p}.$$

Обратная операция называется дискретный алгоритм и обозначается:

$$\log_g t \leftarrow t.$$

Если p и q должным образом выбраны, то модульное возведение в степень - односторонняя функция. То есть в вычислительном отношении неосуществимо найти дискретный логарифм.

Теперь предположите, что мы имеем линию

$$(**)\ y = mx + b$$

в области целых чисел (mod q). Линия может быть описана, задавая m и b, но мы " скроем" их следующим образом. Пусть

$$c = g^b \pmod{p},$$

$$n = g^m \pmod{p}.$$

Тогда c и n дают нам "тень" линии под f. Знание c и n не дает нам m и b, но это позволяет нам определить, находится ли данная точка (x, y) на линии. Поскольку, если (x, y) удовлетворяет (**), то точка должна также удовлетворять соотношению

$$(***)\ g^y = n^x * c \pmod{p}.$$

Наоборот, любая точка (x, y) удовлетворяющая (***) должна быть на линии. Соотношение (***) может быть проверено кем угодно. Таким образом любой может проверять, находится ли данная точка на линии, но точки на линии могут быть сгенерированы только тем, кто знает секретную информацию.

Шнорровское доказательство владения:

1. Алиса посылает c (и n, если необходимо) Бобу.
2. Боб посылает Алисе число-"вызов" x.
3. Алиса отвечает величиной y такой, что (x, y) находится на линии.
4. Боб проверяет с помощью (***), что (x, y) находится на линии.

Боб теперь знает, что он говорит с кем - то, кто может производить точки на линии. Таким образом эта сторона должна знать наклон линии, которая является секретным числом m.

Важная особенность этого протокола - то, что он может быть выполнен только один раз с одной линией. Поскольку, если известны любые две точки (x0, y0) и (x1, y1) на линии, verifier может вычислять наклон линии, используя формулу:

$$m = y_0 - y_1 / x_0 - x_1 \pmod{q},$$

Заметим, что на основе алгоритмов Шнорра можно осуществлять идентификацию, подпись, слепую подпись.

Вместо приведённой выше схемы дискретного логарифма, можно пользоваться алгоритмами на основе эллиптических кривых, которые при том же уровне безопасности работают быстрее, чем приведённые выше.

ПРОТОКОЛ5: Автономная электронная оплата

Изъятие:

Алиса создает электронную монету, включая "идентифицирующую" информацию.

Алиса "ослепляет" монету.

Алиса посылает "ослеплённую" монету и запрос изъятия в Банк.

Банк проверяет, что "идентифицирующая" информация присутствует.

Банк в цифровой форме подписывает монету.

Банк посылает монету Алисе и дебетует ее счет.

Алиса "деослепляет" подписанную монету.

Оплата:

Алиса дает Бобу монету.

Боб проверяет цифровую подпись Банка.

Боб посылает Алисе вызов.

Алиса посылает Бобу ответ (показывающий одну часть выделяющей информации).

Боб проверяет ответ.

Боб дает Алисе товары.

Депозит:

Боб посылает монету, вызов и ответ Банку.

Банк проверяет свою цифровую подпись.

Банк проверяет не была ли монета потрачена ранее.

Банк вводит монету вызов и ответ в базу данных потраченных монет.

Банк кредитует счет Боба и сообщает об этом Бобу.

Переносимость

Переносимость - особенность бумажных наличных денег, которые позволяют пользователю тратить монеты, которые он только что получил в оплате без необходимости входить в контакт с Банком. Оплату следует рассматривать как передачу, если получатель платежа может использовать полученную монету в последующей оплате. Система оплаты передаваема, если это позволяет по крайней мере одну передачу монеты. Переносимость была бы удобной особенностью автономной наличной системы, потому что это требует меньшего количества взаимодействия с Банком.

Схемы, представленные выше не передаваемы, потому что получатель платежа не может использовать полученную монету в другой оплате - его единственный выбор внести деньги на

депозит или обменять их на новые монеты в Банке. Любая передаваемая электронная наличная система имеет особенность в том, что монета должна " расти в размере " (то есть, накапливать большее количество бит) каждый раз как потрачена, потому что монета должна содержать информацию относительно каждого потратившего человека так, чтобы Банк мог идентифицировать многократных плательщиков. Этот рост делает невозможным неограниченное число передач. Максимальное число передач, позволенных в любой данной системе будет ограничено допустимым размером монеты.

Есть другие опасности с любой передаваемой электронной наличной системой, даже если число передач ограничено, и мы удаляем свойство анонимности. Пока монета не депонирована, единственная информация, доступная Банку - идентичность индивидуума, который первоначально изъял монету. Любые другие сделки, затрагивающие это изъятие могут быть восстановлены только с сотрудничеством каждого последовательного плательщика этой монетой.

Кроме того, каждая передача задерживает обнаружение заново потраченных или подделанных монет. Многократное расходование не будет замечено, пока две копии той же самой монеты в конечном счете не депонированы. К тому времени, может быть, слишком поздно ловить преступника, и много пользователей, возможно, принимали монеты-подделки. Поэтому обнаружение многократного расходования после факта не может быть удовлетворительным решением для передаваемой электронной наличной системы. Передаваемая система может положиться на физическую безопасность, чтобы предотвратить многократное расходование.

(Такая система может быть реализована, например, на смарт-картах)

Делимость

Допустим Алиса хочет купить товар у Боба на сумму 3.99$ (или 2.46 руб., или 7.89 у.е.) Скорее всего у неё не найдётся монеты, в точности соответствующей сумме. Боб отдаст сдачу своими электронными монетами. Если платёжная система непередаваемая, то Алиса не сможет воспользоваться полученной сдачей без того, чтобы связаться с Банком, произвести депозит и получить новые (не потраченные) монеты. Кроме того Бобу придётся держать у себя множество монет с различным номиналом, чтобы быть готовым выдать сдачу. Ясно, что такая система крайне неудобна. Выход – делимые монеты: монеты, которые могут быть «разделены» на части, суммарная стоимость которых равна стоимости исходной монеты.

Существует несколько схем, позволяющих создать делимые монеты. Эти схемы основаны на двоичных деревьях. Каждому узлу соответствует некая ценность, корню соответствует $w (или w руб., или w у.е.), где $w=2^l$, его предки имеют ценность $w/2, их предки $w/4 и так далее. Листья дерева имеют наименьшую ценность 1.

Чтобы потратить всю монету используется корневой узел. Если же плательщик желает потратить часть суммы, отмечаются узлы сумма ценностей которых равна желаемой при этом должны выполняться следующие правила:

- Как только узел использован никакие его предки и потомки не могут быть использоваться
- Любой узел должен использоваться не более одного раза.

Эти правила гарантируют, что в итоге(после использования всех возможных узлов) будет потрачена сумма, равная исходной ценности монеты.

Отслеживаемость мошенника, нарушающего эти правила может быть сделана на основе алгоритмов Шнорра как это было описано выше. Каждому узлу присваивается секретное число b_j. Пусть m – число, идентифицирующее плательщика. ($y=mx+b_j$)

При оплате очередным узлом (пусть номер его равен n) раскрываются b_j предков этого узла. Далее посылается «вызов» x1, приходит ответ y1. При следующей оплате, если Алиса использует предок узла n узел s, то по раскрытому уже b_s , вызову x и ответу y вычисляется m. Если она использует потомка n узел k, то раскрывается b_n и m вычисляется по ранее сделанному вызову и ответу $m=(y1-b_n)/x1$.

Заметим, что данная схема во многом решает проблему непередаваемости, хотя имеет существенные недостатки. Она требует больше операционного времени и дополнительное хранение.

Хотя эта делимая схема и не отслеживаема, платежи, сделанные одной и той же монетой «связаны друг с другом». Два платежа одной и той же монетой осуществлены одним и тем же человеком. Это не показывает идентичность плательщика, если оба платежа законны (следуют правилам использования узлов, см. выше), но раскрытие идентичности плательщика для одной закупки показало бы идентичность плательщика для всех других закупок, сделанных той же самой монетой.

Цифровые деньги на практике

В заключение стоит рассказать вкратце о существующих организациях, использующих цифровые деньги.

Служба CyberCoin (компания CyberCash)

CyberCoin представляет собой систему микро платежей (от 25 центов до 10 долларов) через Internet.

Перед тем, как осуществлять платеж с помощью CyberCoin, пользователь должен открыть счет "CyberCash Account" и перевести на него некоторое количество денег со своего счета в банке. Управление CyberCoin осуществляется при помощи специального программного обеспечения CyberCash Wallet, которое поставляется бесплатно. Продавец принимает платежи CyberCoin при помощи ПО CashRegister. Фактически происходит перевод денежных средств со счета покупателя на счет магазина по межбанковским сетям.

CyberCoin рекомендуется применять для оплаты электронных товаров и услуг (плата за доступ на Web-сайты, графические данные и т.д.)

Цена транзакций: от 8 центов за 25-центовую транзакцию до примерно 3-5% суммы транзакции для больших сумм. (В зависимости от суммы.)

DigiCash

DigiCash (http://www.digicash.com/) - основанная в 1990 году голландская компания, занимающаяся разработкой платежных систем. Ее основным проектом является eCash (www.ecash.net), система использующая электронные деньги для оплаты товаров и услуг через Internet и при помощи e-mail.

Проект eCash

eCash - электронная валюта, при помощи которой пользователь может осуществлять платежи по Сети в режиме реального времени.

Чтобы стать клиентом системы необходимо открыть счет в одном из финансовых агентов, производящих операции с eCash. Доступ к счету защищен паролем, известным только владельцу.

После этого ему посылается необходимое программное обеспечение и документация, объясняющая, каким образом он может пополнить свой счет.

Электронные деньги eCash хранятся на информационном накопителе клиента и управляются при помощи специального ПО, адаптированного для MS Windows, Unix и Macintosh.

Схема платежа eCash

После того, как пользователь начисляет электронную наличность на счет, он может осуществлять покупки в Web-магазинах. Платеж состоит из нескольких фаз:

1. После формирования заказа покупатель нажимает на витрине магазина кнопку оплаты при помощи DigiCash.
2. Программное обеспечение пользователя переводит продавцу электронные деньги необходимые для оплаты.
3. Программное обеспечение продавца принимает платеж и зачисляет его на счет. Далее он производит поставку купленного товара. Электронные деньги могут быть переведены в наличные в любом банке системы.

Любой посетитель сайта eCash может попробовать провести тестовую покупку в демонстрационном магазине.

В системе eCash применяется технология расчетов "Person-to-Person" (переводы между пользователями, без привлечения третьих сторон). Для этого применяется специальное программное обеспечение, которое можно получить либо у финансового агента eCash либо на сайте компании.

Безопасность

- Пользователь получает пароль и идентификатор для доступа к счету.
- Система использует технологию цифровой подписи и шифрование с открытым ключом.
- Для загрузки электронных денег на компьютер пользователь должен вести пароль, позволяющий ему использовать счет.
- При совершении транзакций клиент, не указывает ни каких данных о себе, что гарантирует высокую степень анонимности.

Mondex

Mondex (http://www.mondex.com/) была разработана несколькими банками (National Westminster Bank, Midland Bank, Royal Bank of Canada, Canadian Imperial Bank of Commerce и др.). Сейчас она является одной из крупнейших платежных систем, применяющих пластиковые карт как средство хранения и перевода денежных средств. Она оперирует на европейском и на азиатском рынках.

В системе используются смарт-карты (smart card). На встроенном в карту чипе исполняющем роль "электронного кошелька" (electronic purse) хранится электронная наличность (electronic cash) пользователь Mondex, которая применяется в системе как денежный эквивалент.

В рамках платежной системы Mondex имеется только один орган (Mondex Originator), обладающий правом выпуска электронных денег. Он снабжает ими коммерческие банки системы.

При переводах денежных средств не используются межбанковские информационные сети, что позволяет значительно снизить стоимость транзакций.

Чтобы стать пользователем Mondex, необходимо приобрести смарт-карту у одного из финансовых агентов системы и перевести на нее некоторую сумму электронных денег с банковского счета. Продавец может принимать платежи от владельцев карт Mondex при помощи POS(Point Of Sale)-терминала.

Особенности

- Пользователь может использовать телефонные линии для управления своим "электронным кошельком" (например, чтобы перевести некоторую сумму со счета на карту).
- Mondex позволяет хранить электронные деньги сразу в пяти валютах на одной смарт-карте. Для этого, наличность распределяется по разным "электронным кошелькам".
- Пользователь может осуществлять покупки с малой стоимостью через сеть Internet с помощью функции формирования и передачи сообщений на персональный компьютер Продавца. Эту функцию рекомендуется использовать для оплаты доступа к Web-сайтам и к информационным хранилищам, для оплаты получения данных и т.д.
- Клиенты Mondex могут производить денежные переводы между своими картами без привлечения каких-либо посторонних лиц. Для этого применяется считыватель карт Mondex Wallet, выполняющий функции POS-терминала. Для того чтобы осуществить перевод "Person-to-Person" пользователи вставляют карты в Wallet, вводится необходимая сумма и нажимается кнопка "Transfer".

Безопасность

- Для защиты транзакций в системе Mondex применяется передача данных по протоколу SSL.
- При покупке смарт-карты, пользователь получает PIN-код, используемый для доступа к средствам, хранящимся на ней.
- Карта сохраняет информацию о десяти последних проведенных транзакциях.
- Электронная наличность на карте может быть заблокирована кодом, назначенным пользователем.
- После того, как владелец карты получает электронную наличность никто, кроме него не сможет отследить куда он ее отправит, что гарантирует ему высокую степень конфиденциальности.

NetCash

Платежная система NetCash (www.isi.edu/gost/info/netcash/) разработана в 1993 году "Институтом Информатики" (Information Science Institute) "Университета Северной Калифорнии" (University of Southern California).

Net Cash использует специальные купоны (NetCash Coupon) для оплаты товаров и услуг в системе через Internet или при помощи электронной почты. Чтобы получить купоны NetCash

пользователь должен купить их в банке системы (NetBank), переслав чек или расплатившись наличными.

Система рекомендована для микроплатежей.

Схема платежа

- После того, как пользователь получает купон, он может производить покупки, пользуюсь услугами NetCash. Для этого он посылает купон продавцу при помощи электронной почты (с указанием товара, который он хочет приобрести).
- Приняв купон, продавец пересылает его в NetBank.
- NetBank либо связывается в финансовым агентом продавца и перечисляет на его счет сумму, необходимую для оплаты товара, либо отправляет продавцу новый купон (с новым серийным номером).
- После того, как продавец получает новый купон или уведомление о переводе он осуществляет доставку купленного товара.

Анонимность

NetBank может проследить все транзакции пользователя, записывая номера купонов (но в соответствии с соглашением он этого не делает).

Безопасность

В системе не применяются практически никакие меры обеспечения безопасности хранения и пересылки информации.

PayCash

PayCash - проект банка "Таврический" (http://www.tavrich.ru/) и группы компании Алкор-Холдинг. Система PayCash является средством проведения платежей электронными деньгами в сети Интернет. Электронные деньги представляют собой "денежные обязательства", хранящиеся на информационном накопителе пользователя и позволяющие владельцу оплачивать услуги и товары и производить денежные переводы в Сети.

PayCash позволяет множеству различных банков одновременно оперировать в одной электронной платежной системе, взаимодействуя на основе универсальных денежных единиц, принимаемых в оборот любым из этих банков. Кроме банков в системе существуют рядовые пользователи. Пользователями могут выступать юридические и физические лица или программные продукты, представляющие их (например, Web-магазины). Все пользователи полностью равноправны с точки зрения банка.

Программное обеспечение

Все пользователи взаимодействуют друг с другом на основе специального программного обеспечения - "кошелька". "Кошелек" обеспечивает хранение и накопление электронной наличности, а также пересылку электронных денег между пользователями системы.

После того, как пользователь получит с сайта платежной системы PayCash (http://www.paycash.ru/) архив с программой "кошелек" и установит его на свой компьютер, он должен будет открыть один или несколько счетов в банке (банках). Далее, при помощи кошелька

он создает одну или несколько "платежных книжек" (с них осуществляются платежи в системе PayCash) и переводит на нее электронные деньги со счета, то есть получает банковские денежные обязательства, выпущенные в электронной форме.

Получение электронных денег в системе PayCash

Пользователь может пополнить свой кошелек несколькими способами:

- переводом через любое отделение Сберегательного Банка России;
- заплатив наличными в офисе компании Алкор Телеком;
- почтовым переводом;
- телеграфным переводом;
- в Санкт-Петербурге пользователь также может вызвать на дом или в офис дилера-консультанта для внесения денег в систему.

Все реквизиты переводов и примеры заполнения квитанций можно увидеть на сайте PayCash (http://www.paycash.ru/).

Схема платежа в системе PayCash

Процедура платежа с помощью системы PayCash происходит по следующей схеме:

1. Кошелек продавца посылает кошельку покупателя требование уплатить определенную сумму. Требование должно содержать текст договора, подписанный электронной цифровой подписью продавца.
2. Если покупатель согласен с условиями договора и у него достаточно денег, его кошелек пересылает кошельку продавца электронную наличность и договор, подписанный электронной цифровой подписью покупателя.
3. После получения электронных денег от продавца, банк проводит их авторизацию. Если процесс авторизации проходит успешно, то банк зачисляет нужную сумму на счет продавца в системе PayCash. Сообщение об этом передается кошельку продавца вместе с электронным чеком для покупателя.
4. Получив от банка данные об авторизации, кошелек продавца передает ему уведомление о зачислении денег на его счет. Далее, чек из банка передается покупателю.

На этом платеж считается завершенным.

Дополнительные технические характеристики системы PayCash

- Система поддерживает одновременное использование до 255 валют.
- Сумма платежа может быть выражена практически любым числом с точностью до 0,001 копейки.
- Применение особенностей построения системы PayCash позволяет пользователю кошелька получить денежные обязательства анонимно.
- Одна операция, при использовании банком компьютера с процессором Pentium-200, может занять от 0,1 до 0,5 секунд.

- Для цифровых подписей используется алгоритм RSA с ключами в 1024 бит.

WebMoney

WebMoney Transfer представляет собой систему мгновенных расчетов электронными деньгами (WebMoney) через Интернет, которая позволяет производить платежи и переводы денежных средств в режиме реального времени. По своей сути WebMoney - это "цифровые титульные знаки", хранящиеся на информационном накопителе, и дающие владельцу право оплачивать услуги и товары и производить денежные переводы в Сети. Проект принадлежит "ВМ Центру", некоммерческой организации, учрежденной на основе добровольных взносов.

"Эмиссию" WebMoney осуществляет International Metal Trading Bank (IMTB) (www.imtb.com). Этот банк связан корреспондентскими соглашениями с Международным промышленным банком, Сберегательным банком РФ и др.

Программное обеспечение

Общение пользователей системы (как владельцев магазинов, так и покупателей) друг с другом производится с помощью WebMoney Keeper. WebMoney Keeper - программа, предназначенная для широкого применения пользователями системы WebMoney Transfer и позволяющая хранить, накапливать, принимать и переводить электронные деньги.

Основные функции WebMoney Keeper

- Пользователь может принять (или отказаться принять) электронные деньги, переведенные другим пользователем системы.
- Пользователь может перевести свои электронные деньги другому пользователю системы (частным лицам, компаниям, магазинам).
- Пользователь может перевести электронные деньги на банковский счет, с последующим переводом в любую валюту.
- Пользователь может перевести любую валюту в электронные деньги.

Плата за использование

За большинство операций в системе WebMoney Transfer взимается определенная плата. Оплате не подлежит получение и дальнейшее использование программы WebMoney Keeper и операции с кошельками одного идентификатора (одного пользователя). Остальные услуги оплачиваются по следующему тарифу:

- За совершение каждой транзакции с кошелька пользователя взимается тариф в размере 0.8% от суммы платежа, но не менее 0.01 единицы WebMoney;
- За все операции, связанные с движением электронных денег в систему или из системы, взимается плата в соответствии с действующими тарифами по данным операциям агентов системы.

Список использованной литературы:

[1] Портал Электронной Коммерции eCentru - e-commerce, http://www.e-centru.md/EC/Main.aspx

[2] Вадим Маслов, *CyberCash: КиберПространство - общее, а КиберДенежки – врозь,.* Zhurnal.ru 1996, http://www.zhurnal.ru/2/maslov.htm

[3] Информационно-консалтинговый центр по электронному бизнесу e-commerce.ru, http://www.e-commerce.ru/

[4] Laurie Law, Susan Sabett, Jerry Solinas, *HOW TO MAKE A MINT: THE CRYPTOGRAPHY OF ANONYMOUS ELECTRONIC CASH*, 1996, http://jya.com/nsamint.htm

[5] Иванащенко Б. М., Харченко А. С., *ОБЕСПЕЧЕНИЕ НЕОТСЛЕЖИВАЕМОСТИ КЛИЕНТА В СИСТЕМАХ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ,* Вычислительные сети, теория и практика 2003, http://network-journal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=3&pa=13&ar=5

[6] Лебедев А.Н., *Электронные деньги: МИФ ИЛИ РЕАЛЬНОСТЬ,* ЛАН Крипто Инт. 2003 http://www.lancrypto.com/index.php?div=publication3_ru

[7] http://baza.444l.ru/inc/paycash.html

[8] Никита Сенченко, Электронные деньги: делай раз, делай два..., Спецвыпуск Xakep, номер #034, http://www.xakep.ru/magazine/xs/034/072/1.htm