Чубаров Дмитрий 013 гр.

«Электронные деньги» – надёжная межбанковская платёжная система.

Введение.

За последние пять лет российский рынок электронных банковских технологий прошел заметный путь от начальной стадии компьютеризации- реализации простейших банковских операций на базе персональных компьютеров, до полноценных автоматизированных банковских систем, отвечающих самым строгим современным требованиям. Количество компаний в мире, занимающихся электронной коммерцией, в 1996 году составило 111 тысяч и возросло к 2000-му до 435 тысяч (данные Volpe Welty & Co.). Розничные продажи через интернет выросли с 500 млн. долларов в 1996 году до 7 млрд. долларов в 2000-м; при этом более половины покупок оплачено с помощью новых средств платежей. Переход в системе оплаты товаров и услуг от бумажных денег к цифровым аналогичен переходу от золотых и серебряных денег к бумажным, имевшему место несколько сотен лет назад. Здесь также должны выполняться условия, присущие всем платёжным системам: обеспечение электронных денег реальной денежной массой и защищённость от подделки либо воспроизведения необеспеченных денежных знаков. На первый взгляд у современных систем безналичных расчетов с помощью карточек по всем параметрам такие преимущества перед расчетами наличными**,** что последние, казалось бы, должны были давно отойти в прошлое:

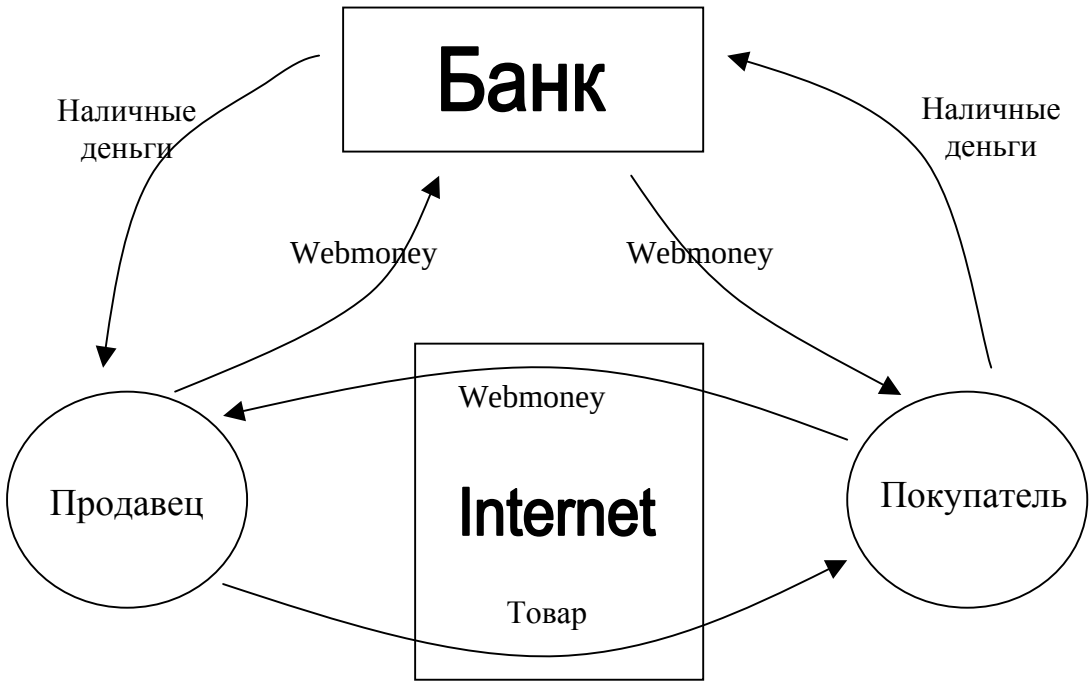
- нет необходимости иметь при себе большой физической массы денег и подвергаться угрозам кражи или ограбления, или нести большие затраты на охрану;
- пластиковые карточки удобны в использовании, хранении и могут быть легко заменены при утрате или порче;
- достаточно широко распространены пункты их обслуживания и банкоматы, обслуживающие карточки большинства международных платежных систем;
- большинство банков обслуживает платежи по карточкам по вполне приемлемым ценам на эти услуги;
- условия предоставления кредитных карточек частным лицам все более либерализуются практически во всех странах мира;
- обладателям привилегированных карточек предоставляется все большее число дополнительных услуг в виде скидок в ценах на проживание в отелях, приобретение авиабилетов, оплату товаров в сети магазинов и т.д.

И всё же пластиковые карты уступают наличности в таком немаловажном аспекте, как анонимность. И это актуально не только для теневого бизнеса, как может показаться на первый взгляд, но и, в первую очередь, для рыночной экономики в условиях жёсткой конкуренции, где информация о ходах противника и возможность скрыть от него свои ходы часто дает решающее преимущество. Далее мы рассмотрим платёжные системы основанные на цифровых технологиях с точки зрения вышеописанных аспектов.

Сначала рассмотрим вид электронных денег, который “недалеко ушёл” от пластиковых дебетных карт. Это не что иное, как Webmoney. Схема работы систем, построенных на этом принципе, достаточно проста. Пользователь устанавливает на свой компьютер виртуальный кошелек, который можно пополнить реальными деньгами через банковский, почтовый переводы, а также за счет перечисления виртуальных же денег от других пользователей.

Электронные деньги призваны устранить главную проблему систем на основе платежных карт – проблему безопасности. Однако, наряду с этим преимуществом, у электронных денег есть несколько существенных недостатков.

- Электронный кошелек – это не более, чем программа, размещенная на жестком диске. В случае порчи носителя, случайного удаления файлов и т.п., восстановление электронного кошелька и находящихся в нем денег сопряжено с большими трудностями либо вообще невозможно.
- Существует вероятность кражи кошелька – не так давно сообщалось о появлении вирусов - троянов, которыми злоумышленники пользовались для воровства электронных денег. Впрочем, соблюдение минимальных мер предосторожности при работе в интернет, может свести вероятность кражи к нулю.
- Возможность неконтролируемой эмиссии. Платежные системы, применяющие электронные деньги, могут незаметно для остальных участников увеличивать объем денежной массы. Этот процесс является неконтролируемым и практически незаметным для клиентов системы. Впрочем, то, что российские платежные системы уже не первый год работают на рынке, позволяет надеяться на их добросовестность и в дальнейшем.
- Неопределенность юридического статуса такого рода систем с точки зрения законодательства РФ.



В такой системе оплаты каждый пользователь клиентской программы имеет свой идентификатор в общей базе данных, и при каких-либо денежных переводах этот идентификатор является фактически подписью клиента. Это не обеспечивает анонимность, зато даёт клиенту возможность потом доказать, что именно он оплатил

некоторую услугу. В общем, это полный аналог пластиковых карт, только здесь продавец и покупатель связаны друг с другом не личным диалогом, а через интернет. Защищённость данного алгоритма определяется стойкостью программы «электронного кошелька» ко взлому. Причём взлом может быть как со стороны третьего лица с целью присвоения себе денег рассматриваемого нами «клиента» так и со стороны «клиента» с целью увеличения количества денег на своём счету.

Теперь перейдём к более прогрессивной с точки зрения интернет – технологий системе расчётов, обладающей большинством положительных качеств наличных денег, как то : надёжность, оперативность и анонимность.

Опишем на понятийном уровне (без использования математических формул) процедуру оборота электронных денег, предложенную Д. Чомом и его компанией DigiCash.

- На своем компьютере вы генерируете "электронные банкноты" (просто строки букв и цифр в привычном виде), включающие номинал, скажем 100 тысяч рублей или 100 долларов, и у каждой из них - индивидуальный серийный номер, который вы и только вы знаете и "запечатываете" часть купюры, содержащую серийный номер в специальный "цифровой конверт"(blinding factor). Пока еще такие купюры не имеют стоимости;
- Присвоить стоимость конкретным купюрам может только банк-эмитент электронных денег. Он проверяет номиналы направленных вами купюр, но не может определить их закрытые серийные номера;
- Затем банк подписывает своей "слепой" цифровой подписью купюры, зная их номиналы, но, не зная серийных номеров, и возвращает их вам уже заверенными.
- Конечно, банк потребует для этого от вас депонировать соответствующие суммы обычных денег или оформить кредитный договор.
- Вы "достаете" их из цифровых конвертов и готовы ими платить. Теперь это есть законные средства платежа, банк готов их принять, от кого бы они не поступили (разумеется, лишь один раз).
- Продавец, получив от вас электронные банкноты, предъявляет их банку, который проверяет их подлинность, дезавуирует их серийные номера и производит зачисление соответствующих сумм на счет продавца или оформляет ему новые электронные банкноты на соответствующую сумму.
- Цикл оборота электронных денег закончен.

В процессе заверения банком электронных купюр (первые три шага операции) для пущей защиты клиента от третьих лиц Чом предложил использовать алгоритмы шифрования с открытыми ключами. Но здесь атака типа “человек посередине” бессильна, ибо даже если он перехватит заверенные банком купюры, он не сможет ими воспользоваться, т.к. без знания секретного ключа клиента расшифрование серийных номеров является вычислительно трудной задачей.
Использование blinding factor и составляет суть приема "слепой подписи", предложенного Чомом в дополнение к обычному методу криптозащиты с открытыми ключами. Благодаря использованию "слепой подписи" банк не в состоянии накапливать информацию о плательщиках, в то же время сохраняя возможность следить за однократным использованием каждой "монеты" данным клиентом и идентифицировать получателя каждого платежа. Чом называет такую логику взаимодействия сторон "односторонней безусловной непрослеживаемостью" платежей. Покупатель не может быть идентифицирован даже при сговоре продавца с банком. В то же время, покупатель при желании может идентифицировать себя сам, и

доказать факт осуществления сделки, апеллируя к банку, если он сохранит копию купюры. Такая логика призвана воспрепятствовать криминальному использованию электронной наличности.

Для вложения наличности клиент просто связывается с банком и отправляет ему полученную "монету", закрыв ее открытым ключом банка. Банк проверяет, не была ли она уже использована, заносит номер в регистр входящих и зачисляет соответствующую сумму на счет клиента.

Сделка между двумя клиентами предполагает лишь передачу "монеты" от покупателя к продавцу, который может либо сразу попытаться внести ее в банк, либо принять ее на свой страх и риск без проверки. Вместе с "монетой" передается некоторая дополнительная информация (в данном примере – серийный номер), которая сама по себе не может помочь идентификации плательщика, но в случае попытки дважды использовать одну и ту же монету позволяет раскрыть его личность.

Появление цифровой наличности также обусловлено необходимостью микроплатежей в Internet. Транзакции по кредитным карточкам стоят дорого. 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 являются транзакции, начиная с 20 долларов.

Теперь на первый план выходят вопросы экономические, политические и моральные. С экономической точки зрения выгоды для банка-эмитента "электронных денег" очевидны:

- во-первых, он получает на депонент реальные безналичные или наличные деньги, которыми обеспечивается эмиссия денег "электронных",
- во-вторых, проценты за обслуживание,
- в-третьих, возможность работать с "остатками" сумм электронных денег, не предъявленных к оплате.

В общем, это дополнительные и в большей части гарантированные финансовые ресурсы: депонированные клиентом средства банк может пустить в оборот полностью и сразу, а с "остатками" работать как с обычными остатками на счетах клиентов. Контроль со стороны Центрального Банка за объемом эмиссии электронных денег конкретным банком-эмитентом или всеми банками-эмитентами также достигается обычными методами банковского контроля и регулирования.

Экономические интересы клиента также понятны, в дополнение ко всем преимуществам расчетов по карточкам он получает возможность проводить их анонимно, не имея при себе больших сумм реальных физических банкнот. Он имеет возможность оперативно оплачивать товары и услуги, не раскрывая перед банком или другими лицами, кому и за что он произвел оплату, но при необходимости точно доказать, даже в суде, что произвел оплату конкретного товара или услуги конкретному продавцу**.**

Остаются экономические (а с ними, как производные, и политические) интересы государства.

- Государство освобождается от необходимости поддерживать и обновлять большую массу наличности, обеспечивать применяемыми сейчас весьма дорогостоящими средствами ее надежную защиту от подделки, надежную охрану при печатании, хранении в ЦБ и распределении по регионам. При

эмиссии электронных денег все эти проблемы решаются гораздо проще и эффективней. Затраты на обслуживание клиентов при этом банки перекладывают на самих клиентов, обеспечивая им дополнительные удобства, о которых мы уже говорили выше (будет за что платить).

- Это практически уменьшит возможность злоупотреблений со стороны исполнителей правоохранительных органов при проведении юридически правомочных действий по наложению ареста на имущество, конфискации, обысках и т.д. (воспользоваться незаконно присвоенными электронными деньгами значительно сложнее, чем обычной наличностью).
- Это стимулирует фискальные органы государства и законодателей к более быстрому введению принятой во всем цивилизованном мире нормальной системы контроля за налогами со стороны расходов налогоплательщика законными методами, а не путем "выбивания" из каждого плательщика кто сколько сможет любыми методами.

А именно это и служит, в конечном счете, любому правительству в достижении его главной цели - такой организации общества, при которой бы динамично развивающаяся экономика гарантировала доход, достаточный не только для выживания как нации, но и для поддержания нормального функционирования не только таких функций государства как армия и охрана порядка, но также науки, искусства культуры, образования, здравоохранения и т.д.

Использованная литература :

1. Описание системы работы webmoney.
   http://www.webmoney.ru/sytechnology.shtml

2. Smart – технологии и электронные платежи в интернет.
   В. Олейник, д. т. н., ас. Академик МАИ
   http://e-commerce.com.ua/secur/sec4.html

3. Электронные деньги : миф или реальность ?
   http://www.lancrypto.com/index.php?div=publication3_ru