Електронни пари: Пътят до Bitcoin и поглед напред

Пейо Попов <peio@peio.org>
OpenFest 06.11.2011

Форми на парите?

- Банкноти и монети
- Банкови сметки
- Електронни пари

Какво са електронни пари?

Чл. 76. (2) ЗПУПС Електронните пари са парична стойност:

1. съхранявана в електронна, включително магнитна форма,

2. вземане към издателя, издава се при получаване на средства

3. с цел извършване на платежни операции и се

4. приема се от физическо или юридическо лице, различно от издателя на електронни пари.

Примери

- PayPal
- MoneyBookers
- WebMoney

Средства подобни на пари

- Алтернативни валути
- Timeshare
- Социални/Общностни
- Регионални валути
- Ваучери и схеми за лоялност
- Facebook Credits

Wirtschaftsring-Genossenschaft

WIR

- Основан: 1932
- Членове: 62 000
- Оборот: CHF 1 650 000 000
- Паричната маса: CHF 839 000 000

Още примери

- Ven
- Der Chiemgauer
- Die Havelblüte
- Der Urstromtaler
- Der Sterntaler

Основни отлики

- Без право на обратно изкупуване
- Не са законно платежно средство
- Не винаги са парична стойност
- Обезпечение

Необходими ли са ни?

- За какво ще ползвате електронни пари?
- Какви са предимствата и каква е цената за тези предимства?
- Колко нови проблема създаваме като разрешаваме този?

Дефиниране на задача

- Кой - Колко - Кога
- Колко пари има общо?
- Как са се отзовали в държателя си?

- Как се създават?
- Как се използват?

Общи рискове

- Подправяне
- Кредитен риск
- Неоторизирано изтегляне
- Подмяна
- Многократно използване
- Липсващо или грешно отразяване
- Denial of Service
- Оттегляне
- Неизпълнение на от продавача
- Набеждаване
- Тайна
- Ресто
- Погиване

Правни и счетоводни

- Пране на пари и финансиране на тероризъм
- Избягване на данъчно облагане
- Надзор над паричната маса
- Защита на потребителя
- Сключване на договори
- Възможност за проверка (одит)
- Кредитни/Дебитни известия (reverse и refund)
- Разрешаване на спорове
- Разпределение тежестта на доказване
- Разбираеми от човек

Всичко си има цена

- Привличане на потребители и търговци
- Опериране и управление
- Клиентска поддръжка
- Маркетинг и реклама
- Инфраструктура

Човешките проблеми

- Сетълмент риск
- Идентификация и авторизация
- Постигане на съгласие в група
- Определяне на състояние на система във всеки един момент от времето
- Доверие. Парите като доверие

Онлайн и офлайн системи

Необходима ли е връзка с трета страна, за да се осъществи транзакция?

Примери: PayPal и Blind signature/PayWord системи

Централизирани и децентрализирани

Необходима ли е централна институция, доверена трета страна?

Примери: Liberty Reserve и Ripple/BitCoin

Анонимни и… не толкова

Знае ли се кой е държател на парите?

Примери: eCache и Базелския комитет

Проследими ли са транзакциите?

"Твърди" и "меки"

Дали има защита от сетълмент риск и потребителска защита?

Примери: BitCoin и Card based money (Digicashm Chipknip)

Приносът на Bitcoin

- Децентрализирана
- Анонимна
- Без разходи
- Отворена
- Самомаркетираща

Проблемите на Bitcoin

- Цената на създаване
- Метод за постигане на консенсус
- Скалируемост
- Без реално обезпечение
- Сетълмент риск
- Анонимност
- Гаранции за потребителите
- Множество потребители (Sybil attack)

По-ефективно издаване

- Разпределение (случайно или честно)
- Идентификация
- Доказателство за работа
- Обмен за пари или друго благо

Как да постигнем консенсус?

- Какви предимства имат централизираните системи?
- Децентрализирана (P2P) или разпределена система?
- Приложима ли е WebofTrust (OpenPGP подобна) схема на доверие?
- Социалната индентификация може ли да помогне?
- Trusted peers
- Trusted backbone
- Удостоверяване на време
- Practical byzantine tolerance срещу distributed timestamping?
- Техниките на triple accounting полезни ли са?

По-добра анонимност

- Възможна и неоходима ли е пълната анонимност?
- Какви са нивата на анонимност?
- Може ли да се определя режим на анонимност?
- Приложими техники за анонимизиране

- Офшорна/независима юрисдикция
- Банкова тайна

- Разделение на ролите

Летете легиони