Electronic money: The road to Bitcoin and a glimpse ahead

Peio Popov <peio@peio.org>
28 C3 29.12.2011

Pierre De Fermat

The last useful lawyer:

Introduction

- What do I do?
- Why I find the topic important?
- What do I aim to achieve?
    - Define a problem
    - Propose solutions
    - Ask for help
- Disclaimers and more disclaimers

Definition of Electronic money

Electronic money is defined as monetary value which is:

- stored on an electronic device;
- issued on receipt of funds; and
- accepted as a means of payment by persons other than the issuer.

Alternatives to electronic money

Working examples

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

Definition of the problem

Money is hard

and hard from various perspectives:

- Human
- Technical
- Legal/Political
- Business

Each perspective imposes it's requirements to the geneal problem of electronic money.

Human perspective

- Identification and authorization
- Achieving consensus and easy dispute resolution in a group
- Determination of the state of the system at any given moment
- **Trust**

System risks

Secure issuing and usage of electronic money

- Counterfeiting
- Double Spending
- Repudiation
- Secrecy and anonymity
- Purchase Order Modification (MITM)
- Denial of Service / Points of failure
- Failure to deliver, fraud risk
- Framing

Legal and accounting problems

- Entity requirements
- Settlement risk
- Counterfeiting accusations
- Money laundering and finance of terrorism
- Tax evasion prevention
- Consumer protection requirements
- Ways to negotiate and conclude a contract
- Auditability
- Reverse and chargeback transactions
- How the burden of proof is distributed

Why the legal part is important

- Money is a matter of trust, stability and predictability
- Opposition is expensive as you are funding the opponent.
- Solving the wrong problem?
- Regulation is immature and can be made better.

Feedback on the legality

- US - FBI on Liberty Reserve
- Deutche bank on Regiogeld
- Swiss national bank on WIR
- UK Financial Services Authority
- French Court
- Electronic Frontier Foundation

Costs

- Registration
- Operation
- Support
- Marketing
- Customer and merchant negotiation

The contribution of Bitcoin

Six impossible things before Bitcoin

- Source of inspiration
- Decentralised
- Anonymous (relatively)
- No operational costs
- Open platform
- Marketing model included

Better issuing

- ID based
- Exchange for FIAT money or back by any other valuable stock (gold, land, silver);
- IOU credit/debit principle from the community currencies;
- Some fair (random) distribution as an alternative to:
- Proof of Work (as Bitcoin does)

Consensus in a more effective manner

- Can and should we consider any centralized authority?
- Is decentralised (trusted) backbone a ok compromise?
- Can a Trusted peers (OpenPGP alike) scheme of trust be applied?
- What social identification (friend of a friend) can contribute (Ripple project)?
- Can we rely on timestamping services?
- Is practical byzantine tolerance more effective than distributed timestamping?
- How triple accounting techniques may help?

Better anonymity

- Is complete anonymity possible?
- What are the achievable levels of anonymity?
- Can the user set a "mode" of a transaction, sacrificing some protection?
- Can you "escrow" your ID?
- Use dedicated layer (Tor)
- "Laundry" services (E-cache like)
- To what extend the existing bank secrecy will suffice?
- Role and knowledge separation (RBAC)
- Jurisdictional independence as a possible solution / significant contributor.

Reccomended reading

1. **Micro Payment Transfer Protocol** (http://www.w3.org/TR/WD-mptp)

2. **Ben Laurie on Bitcoin** (www.links.org/?p=1164)

3. **US FBI on Liberty Dollar** (http://www.fbi.gov/charlotte/press-releases/2011/defendant-convicted-of-minting-his-own-currency

4. **UK FSA Statement on Bitcoin** (https://bitcointalk.org/index.php?topic=49862.0)

5.**EFF on Bitcoin** (https://www.eff.org/deeplinks/2011/06/eff-and-bitcoin)

6.**Triple Entry Accounting** http://iang.org/papers/triple_entry.html)

Tell me how wrong I am