LONG HASH & CRYPTIC LABS

LongHash Crypto Festival Berlin

How can we prevent physical form of digital assets from being lost ?

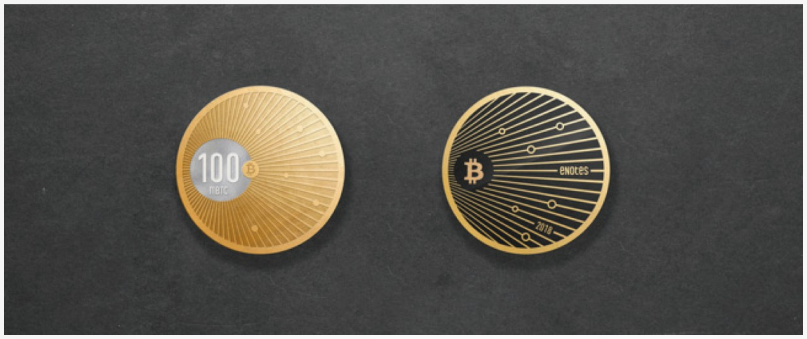
Aslan Mehrabi
Vlad Karl

28.Oct.2018

Machine Xchange Coin

Problem Definition

- **Physical form of digital asset**



* eNotes WHITEPAPER A Physical Form of Cryptocurrency

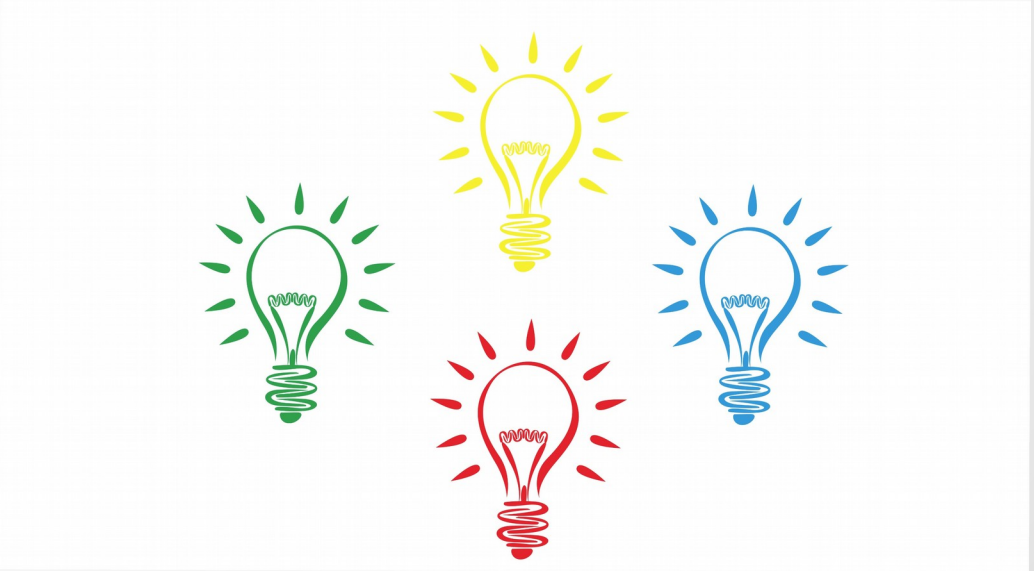
- **Security is the most important consideration**

Think big, think fast, think ahead.

Dhirubhai Ambani

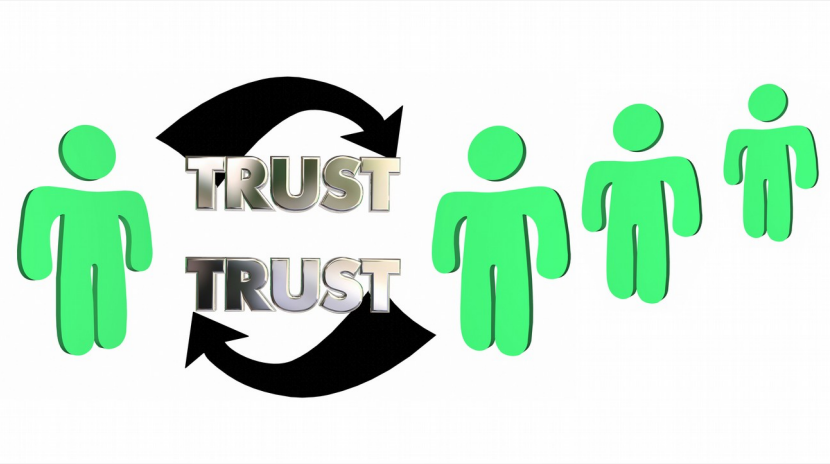
Securing the Physical Digital Asset

- **Problem**: Lost of physical digital asset
  - How to secure the transactions
  - How to restore the account



- **We need:**
  - Trustable Parties / Signatures
- **Solutions**:
  - Based on the smart contracts
  - Independent of smart contract

Truastable Parties

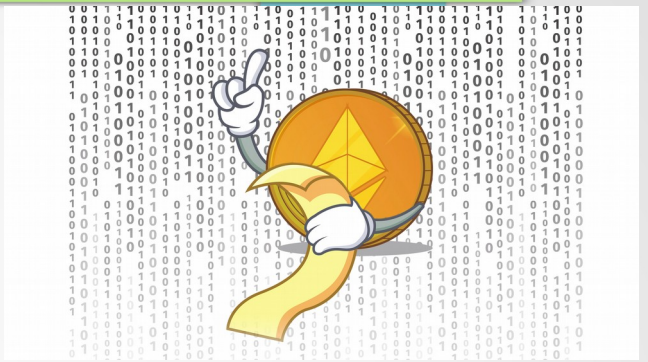


- **Defined trusted parties**
  - Address of relatives, friends, etc
  - Address from which this coin was bought
  - Trustable devices (my laptop, mobile phone, etc)
  - Another physical asset (backup) of the account

Personal Signatures

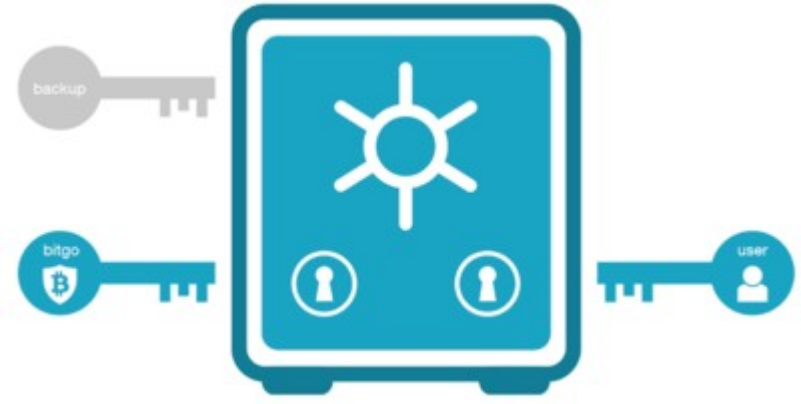
- **Personal Signatures**
  - Finger print
  - Face detection
  - DNA
  - Retina
  - Type style detection
  - Movement style
  - Set of questions
  - Games

Solutions Based on Smart Contracts



- **Conditions on the security of transactions**:
  - Getting confirmation from a trustable party for a transaction
  - Define thresholds for transactions to be confirmed, e.g.
    - total amount of the transaction:
      - Between 0.1 and 1 => Put 30 min delay on the transaction
      - More that 1 => A second signature from my brother / second coin is needed

Solutions Based on Smart Contracts



- **Lose of physical digital asset**
  - Conditions to restore the account :
    - N trustable parties are defined and signature of M of them can restore my account
    - N personal signatures are defined and confirmation of M of them can restore my account

Solutions independent of Smart Contracts

- Avoid stealing the money in case of lose of physical asset

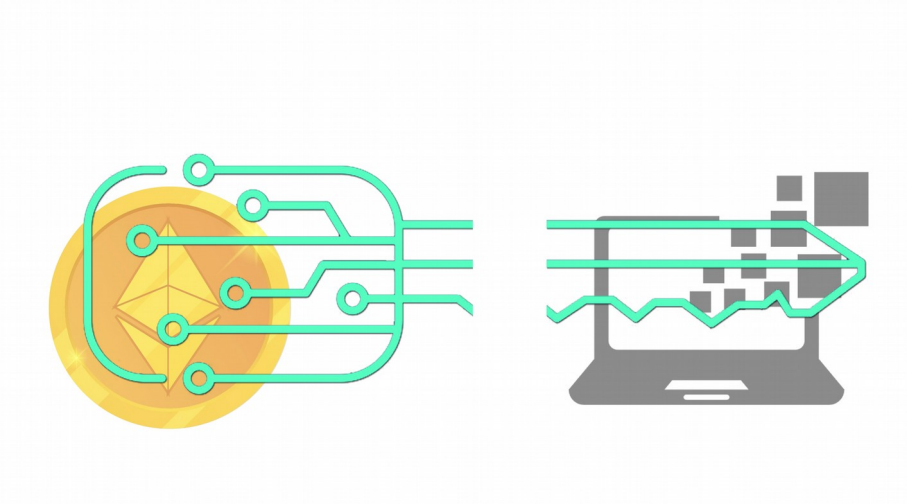
- **RSA Algorithm** (Rivest–Shamir–Adleman)
  - Idea behind public / private key
  - The private key can be separated into two parts, both of them are needed to generate the main private key
  - One of the separated parts can be stored on the physical asset and the other one on our trusted device

Solutions independent of Smart Contract

How to get access to our account if the Physical digital asset is lost?

Reed–Solomon Algorithm

- The private key can be divided to N parts
- Restoring needs getting access to M of the parts



Conclusion

- **Problem**: How to secure the transactions / restore the account in case of Lost of physical digital asset
- **Defined trusted parties**
  - Address of friends, trustable devices, backup physical digital asset, etc.
- **Personal Signatures**
  - Finger print, Face detection,Retina,Type style detection, etc.
- **Solutions Based on Smart Contracts**
  - Conditions on the transactions:
    - Getting confirmation from a trustable party
    - Define a lower threshold for the confirmation
  - Conditions to restore the account in in case of lose of physical coin:
    - N trustable parties / signatures are defined and signature of M of them can restore my account

Solutions independent of Smart Contracts

- RSA Algorithm (dividing the private key)
- Reed–Solomon Algorithm (restoring the private key)


Thank you