The Forgotten Art of Anonymous Digital Cash

Jonathan “Smuggler” Logan

Before the Chains

- Blockchain currencies were not the first digital non-government money
- The past is widely forgotten
- I’m here from the past – or from alternative reality

Speaking of Money

- VTS
- Value
- Transfer
- Storage
- Many moneys of one currency (later...)

System Risks of Digital Money

- Third party theft, technical / operational risks
- Lock-in, monoculture
- Theft by issuer: Account manipulation and overissue
- Fungibility

Killer Risks

- Government
- “Privacy” risks
- Market

System design is about risks and...

… Function

- Store of Value vs Settlement / Transfer
- Many moneys of one currency: Depository, giro, debt…
- Movement between functions
- Blockchain is storage over transfer

DBCs: Transfer Over Storage

- WHAT??????
- Digital Bearer Certificates
- Authority certifies properties
- Properties: Owner, expiry, amount, currency
- Like a cheque

DBC Functions

- Private: Issue. Create new DBC
- Private: Spend. Destroy DBC (record spent)
- Public: Reissue. Spend + Issue
- Public Extras: Split, combine

It’s Easy

- Properties encoded as string
- Signed by digital signature algorithm
- Problem I: Double spend
- Problem II: Privacy
- Problem III: Single issuer fraud

Double Spend

- Record spent DBCs in database, bloom filter, other probabilistic datastructure
- Prune storage on signing key rotation
- Cheap, high throughput, trivial
- Alternatives: probabilistic reveal, reveal identity on double spend

Privacy

- Blind unlinkable signatures
- Signer does not know content of signed message
- Signer cannot link signed message to signing event
- Problem: Signer does not know which properties he certifies
- Solution: Encode properties in signing key
- Alternative: Probabilistic unblinding

Single Issuer Fraud

- Meet SCRIT, a Berlin Cryptoanarchist TAZ project
- Another example of completely over-engineering the solution for a trivial problem (pay for toilet)
- Solves the single issuer fraud problem by distributed, unsynchronized issuers

SCRIT: Spendbook

- Transaction: (In-DBCs, blind Out-DBCs), Owner-Signatures, Mint-Signature(s), Blinding parameters
- E[n] = H(E[n-1]), H(Tx[n])
- H(In-DBC) → E[n]
- H(Blinding parameter) → E[n]
- Result: Idempotent interface, 280 bytes per DBC

SCRIT: Signing

- Simple rules:
  - Reissue iff:
    - DBC unknown or Tx – Hash matched records
    - Signed by self or signed by quorum
- Quorum: 8 out of 10
- Issuers only contribute a signature
- Issuers do not have to synchronize
- Money creation: Possible only by quorum

SCRIT: Properties

- No issuers can defraud under quorum
- Issuers do not have to be synchronized
- Issuers are self organized by CodeChain
- **FAST**: 2k Tx/s (quad core i7), linear scalability
- **CHEAP**: 280 bytes storage per DBC, shardable
- **EFFICIENT**: Each issuer adds 33 bytes to DBC
- **ANONYMOUS**: Unlinkable, untraceable. Anonset is all Tx of signing key
- **HALF OFFLINE**: Only one party (or none) needs to be online

SCRIT: Future

- Access control language: Atomic swaps, DBC swaps, deterministic owner generations
- Super cheap hardware wallets: USB stick on steroids
- Distributed automated renewal with deterministic access control
- Distributed “smart” secret contracts
- Craaazy…

Crazy: Cypherpunk Dream Come True

- Trusted computing hardware
- Remote anonymous attestation
- Encrypted RAM
- Verifiable software

Remote anonymous attestation

- Demonstrate that a remote system is of a certain type and in a certain state
- Demonstration is anonymous
- Currently relies on manufacturer trust
- Assurance that a remote system is trustworthy

Encrypted RAM

- All memory is encrypted by a processor generated ephemeral key
- Prevents bus sniffing
- Local secrets are secure against physical attackers

Verifiable software

- Mathematic proof of implementation behavior
- Matches model to implementation

Crazy

- Verify that a remote host runs exactly one specific program
- Verify that local secrets of a remote host are protected
- Allows distribution of any software over anonymous remote hosts

Crazy

- The future of distributed secure systems might be much more powerful, innovative, and unpredictable than envisioned today
- Imagine: Trustworthy cloud backed by DBC micropayments. Anonymous, untracable, fast, cheap, simple, mobile.

Thank you

- Twitshit: @TheRealSmuggler
- Personal: https://opaque.link https://anarplex.net
- Sponsored by: https://select.cryptohippie.com
- Send me coins :)
- Shoutouts: Tatjana Adamov, Frank Braun, Frank Rieger, Paul Rosenberg