Overview of Cryptofinance Oct. '14

“You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete.”

- Buckminster Fuller

Overview of FOSS Cryptofinance

- Free open source software

- “Crypto2.0” or 2nd generation bitcoin tech.

- Financial cryptography techniques

- Bleeding edge, high risk/reward, demanding computer security

Financial Cryptography Basics

- Possession of Public-Private key pairs that control digital assets confers legal ownership
- Legal contracts, titles, records as electronic files when hashed, digitally signed, time-stamped, i.e. “e-notarised”
- Machine executable contract clauses, programmable transactability, “smart” contracts
- Distributed ledger and time-stamp server of bitcoin blockchain provides immutable data consensus

Smart Contract Concept

- Nick Szabo – 1997
- http://szabo.best.vwh.net/smart_contracts_idea.html
- Contracts in property; usually valuable and controlled by digital means
- Dynamic monitoring and enforcement of contract clauses
- Can be linked to “real-world” event triggers
- Hash embedded in blockchain provides robust timestamp
- EG: http://etherscripter.com/0-5-1/

Why Bitcoin overlays?

- Blockchain space is expensive
- Confirmation time is “slow”
- Bitcoin TX scripting functionality is limited
- Network strength is robust, global, distributed-consensus, secured data and historical record
- Embedded hashes leverages security of the blockchain for protocols with broader functionality and faster, cheaper

Bitcoin Scripting - Op_Codes

https://en.bitcoin.it/wiki/Script

- Forth-like scripting (assembler code)
- Core transactional stack engine in bitcoin

  EG: storing data in blockchain

  scriptPubKey: OP_RETURN {zero or more ops}
- Contract examples: https://en.bitcoin.it/wiki/Contracts

- EG: http://webbtc.com/script

Coloured Coins Concept

- Coins get a colour 'tag' in the bitcoin blockchain
- Colour follows the coin in a traceable history
- Protocols interpret metadata attached to coin
- https://en.bitcoin.it/wiki/Colored_Coins
- Chromawallet - http://chromawallet.com/
- CoinPrism - https://www.coinprism.com/

Counterparty

- Issue digital crypto-assets 'on' the bitcoin blockchain
- Trade digital assets on decentralised exchange
- Recent development backing by Overstock.com
- http://counterparty.io/
- https://bitcointalk.org/index.php?topic=395761.0
- http://en.wikipedia.org/wiki/Counterparty_(technology)
- http://www.blockscan.com/

Mastercoin

Metadata **A**rchival by **S**tandard **T**ransaction **E**mbedding **R**ecords

- A protocol that embeds data in blockchain
- Allows issuance of user-defined currencies
- Uses multi-sig and OP_RETURN

http://en.wikipedia.org/wiki/Mastercoin

http://www.mastercoin.org/

CoinSpark

- OP_RETURN used extensively for embedding metadata in bitcoin blockchain
- Create asset contracts
- Transact assets across bitcoin network
- Like coloured coins without tagging coins directly

http://coinspark.org/

Ripple and Stellar

- Payment systems platforms
- Data-type is an IOU crypto-token USD, EUR, NZD, etc
- Gateways manage transaction consensus
- Users send different currencies and network balances
- http://ripple.com/
- https://www.stellar.org

BitShares and Ethereum

Alternate blockchain technologies with greater scripting

Easier integration of smart contracting, asset issuance, etc

Have their own built-in cryptocurrencies (BTSX, Ether)

http://bitshares.org/

https://www.ethereum.org/

http://en.wikipedia.org/wiki/Ethereum

Open Transactions - openTXS

- Ricardian contracts used extensively as basic data type
- Truledger, triple signed receipts, Chaumian blinded cash
- Last signed receipt IS the account
- Issue asset contracts
- Account transfers, vouchers, checks, cash, smart contracts
- Untrusted notary servers, clients with unlimited (pseudo)Nyms
- http://opentransactions.org
- Currently refactoring library structure, libopentxs

Ricardian Contracts

- Formalised by Ian Grigg
- http://iang.org/papers/ricardian_contract.html

- Contract includes: Data, Public Key, Signature
- Self-signed with the private key
- Hash of Ricardian contract provides immutable data

Moneychanger and opentxs-cli

- Reference Open Transactions client implementations
- QT/C++
- Connect to multiple notary servers
- Manage multiple Nyms, accounts, assets
- Proof of concept
- $opentxs client on command line

Crypto2.0 Applications

- Financial markets, insurance, asset title
- Replacing any centralised “notarising” layers
- Global supply chain financing, escrow, B2B
- International asset transfers
- ECommerce ... shopping, advertising, rewards, vouchers
- Decentralised, P2P finance, crowdfunding
- Personal control of assets
- Wild Unexpected Innovations and Disruption!!