Blockchain - Technical Overview

Yaron Welner, Phd
Smart Ledger Labs

The 5th , China Yunnan - Israel Innovation Cooperation Forum

Blockchain and Me

- PhD computer science
- Academic publications on game theory and blockchain protocols
- CTO of company that processed > $0.5B over blockchain
- Smart contracts security auditing and consultation

Agenda

1. Blockchain - auditable database
2. Digital currency
3. Beyond currency
4. Public blockchain vs private blockchain vs traditional database

Blockchain

Ordered ledger

Hold records of events sorted by order of appearance

- Money transfers
- Product supply chain

Fully auditable

Precise (mathematical) predefined rules dictates when new record can be added

- Cryptographic signatures
- Current state

Multi-party

Can be operated by multiple, possibly adversarial, parties who jointly decide on the order of events

- Multiple companies
- Multiple states
- Fully distributed

Digital Currency

Bitcoin

- Not backed by any entity
- Highly speculative and volatile
- Not recognized as a currency by any country
- Give rise to regulatory issues worldwide

Facebook (Libra)

- Backed by financial assets
- Stable, but might be considered as a security/investment
- Aim to facilitate international payments
- Regulatory status is unclear

CBDC

- Backed by central bank
- Liability of the central bank just as physical currency is
- More efficient banking system and money wires.
- Mitigates regulation breaches

Beyond Currency

Ordered database

1. Insurance records
2. Medical records
3. Supply chain
4. General purpose smart contracts
5. ...

Blockchain in Insurance

- Health insurance
  - Secure sharing of medical data among healthcare providers and insurers
- Fraud prevention
  - Common types of insurance fraud can be eliminated by moving insurance claims onto a blockchain-based ledger that is shared among insurance companies and cannot be modified.
- Claims management
  - Automatic execution of claims

Medical records

- Patient controls his records and can share it with
    - Hospitals and health providers
        - Different country
        - Different health system
    - Medical researches
        - Big data
    - Insurance companies

Supply Chain

- Blockchain database is:
  - Immutable
  - Temper proof
  - Transparent
- Collaborative effort across multiple companies or countries

Smart Contracts

- A program that is self-executed on the blockchain
- An agreement between parties written as a programming language code
  - Future swap contracts
  - Auctions
  - Roles in an organization

Should I Use a Blockchain?

Should I Use Blockchain?

	Public blockchain	Private (consortium) blockchain	Standard database
Example	Bitcoin, Ethereum	IBM hyper-ledger, R3’s corda	Standard cloud service
Participants	Anyone, anonymous	Organizations and approved parties	Organizations and approved parties
Speed	Very slow	Much faster	Fastest
Security	● Secured by BFT consensus ● Consumes intensive amount of resources	● Participants pre-approved ● Less resource intensive	● Secured by the cloud service provider
Privacy	None	Possible	Possible
Auditable and temper proof	Yes	Yes	Yes (*) (*) data might become unavailable

Thank You

yaron@welner.net