BLOCKCHAIN

A Socio-Technical System

Mariusz Nowostawski NTNU, Gjovik, Norway
Associate Professor
Testimon Research Group

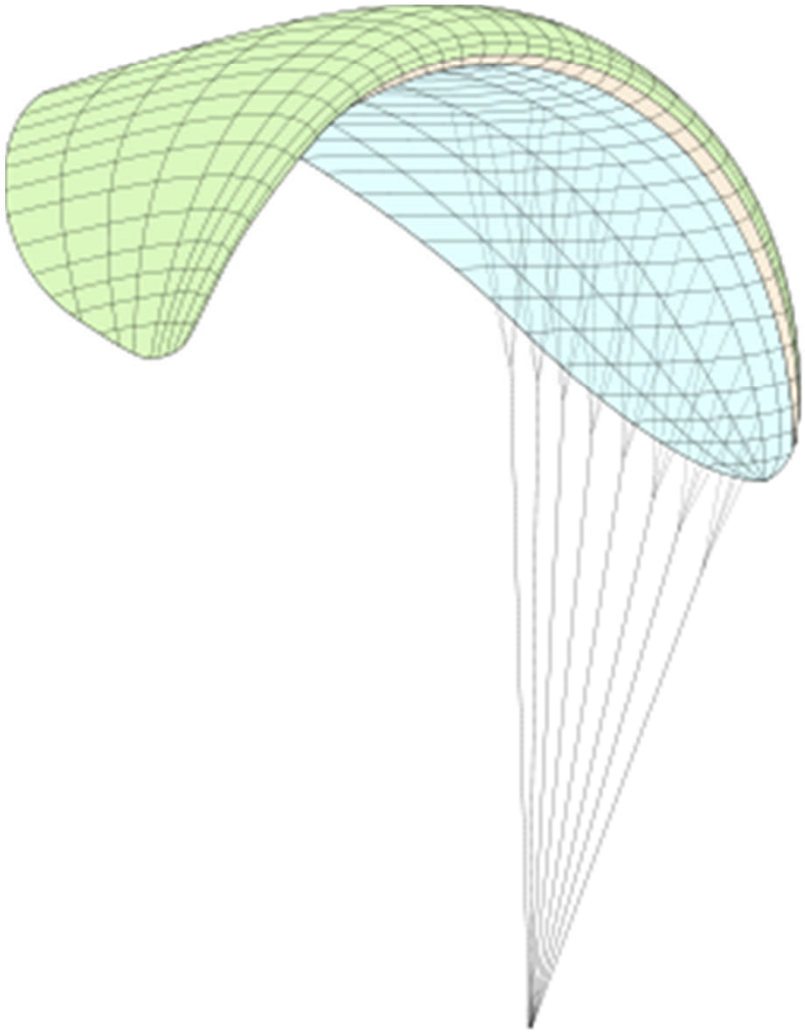
About me

- Academic
  - NTNU, Norwegian University of Science and Technology

- Mobile/Web Computing/Development
- Games, Game Design, Serious Games
- Peer to peer autonomous systems

- Running
- Rock Climbing
- Paragliding

Passion



Wikipedia

Bitcoin

What do you see?

Distributed money

- Limited supply (or fixed supply)
- Socially agreed value
- Users must keep a history of who owns what
- The history, the ledger, must be agreed upon, consistent.

- Distributed money is not centrally managed
- There is no government or entity able to “print/mint” it
- … and therefore deflation/inflation is market-based, and cannot be manipulated by any entity: banks, government.
- The concept appeals to many in the context of financial markets crisis and instability.

The Bitcoin community is having an "I told you so" moment.

The value of the virtual currency has been on the rise this past month amid the growing panic about Greek's financial future. Across the country, banks are shuttered and capital controls are in place until the referendum on Sunday. By Saturday, a rush emptied as many as 500 ATMs, Bloomberg reported.

It's in this context that using Bitcoin may seem appealing. The virtual currency is touted by its fans as the future of finance because it isn't subject to any governmental control or central authority.

For many, including well-known Internet entrepreneur and businessman Kim Dotcom, the crisis in Greece serves as a huge argument in favor of Bitcoin.

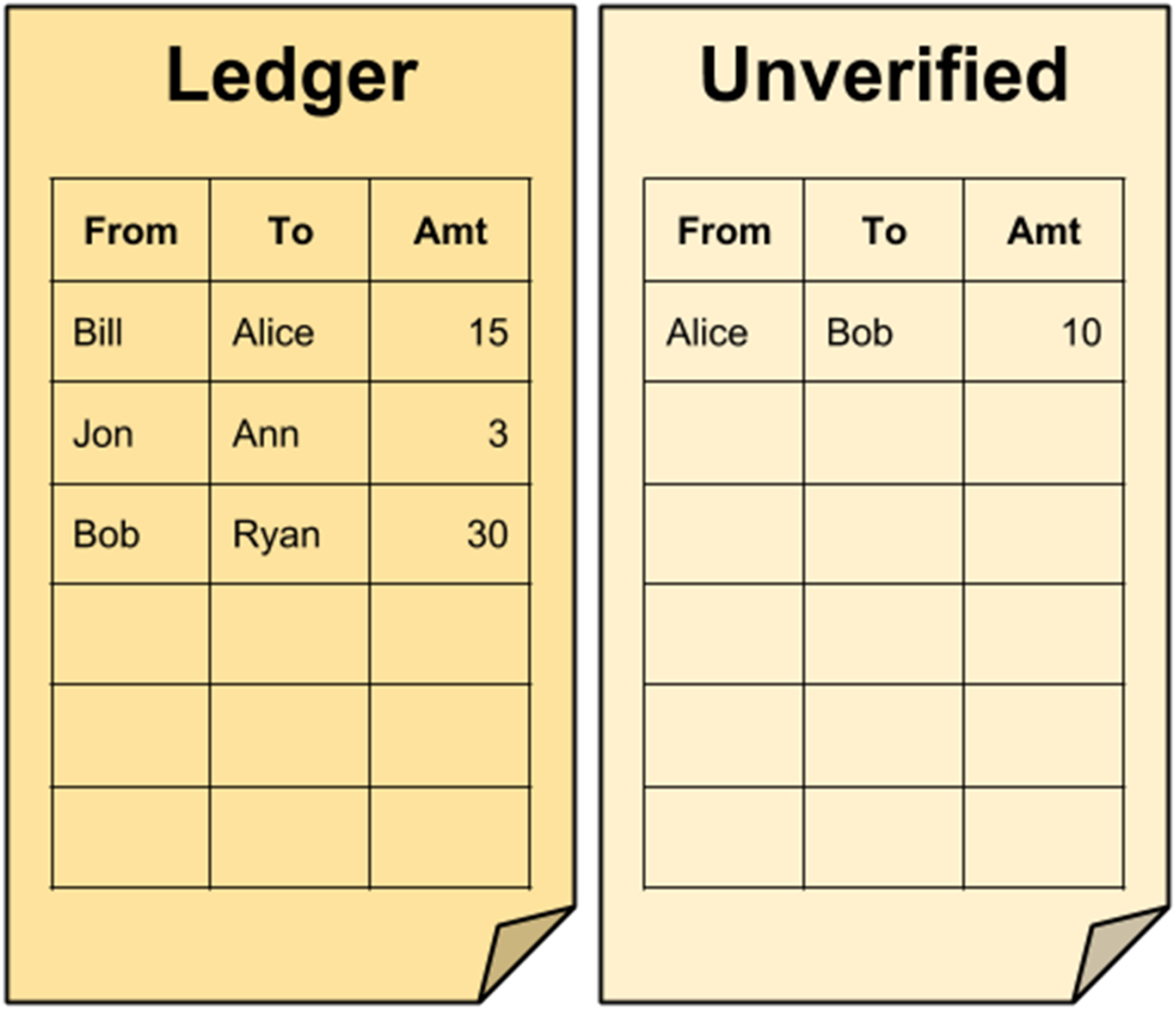
Public Private cryptography system

- Public and Private key pair

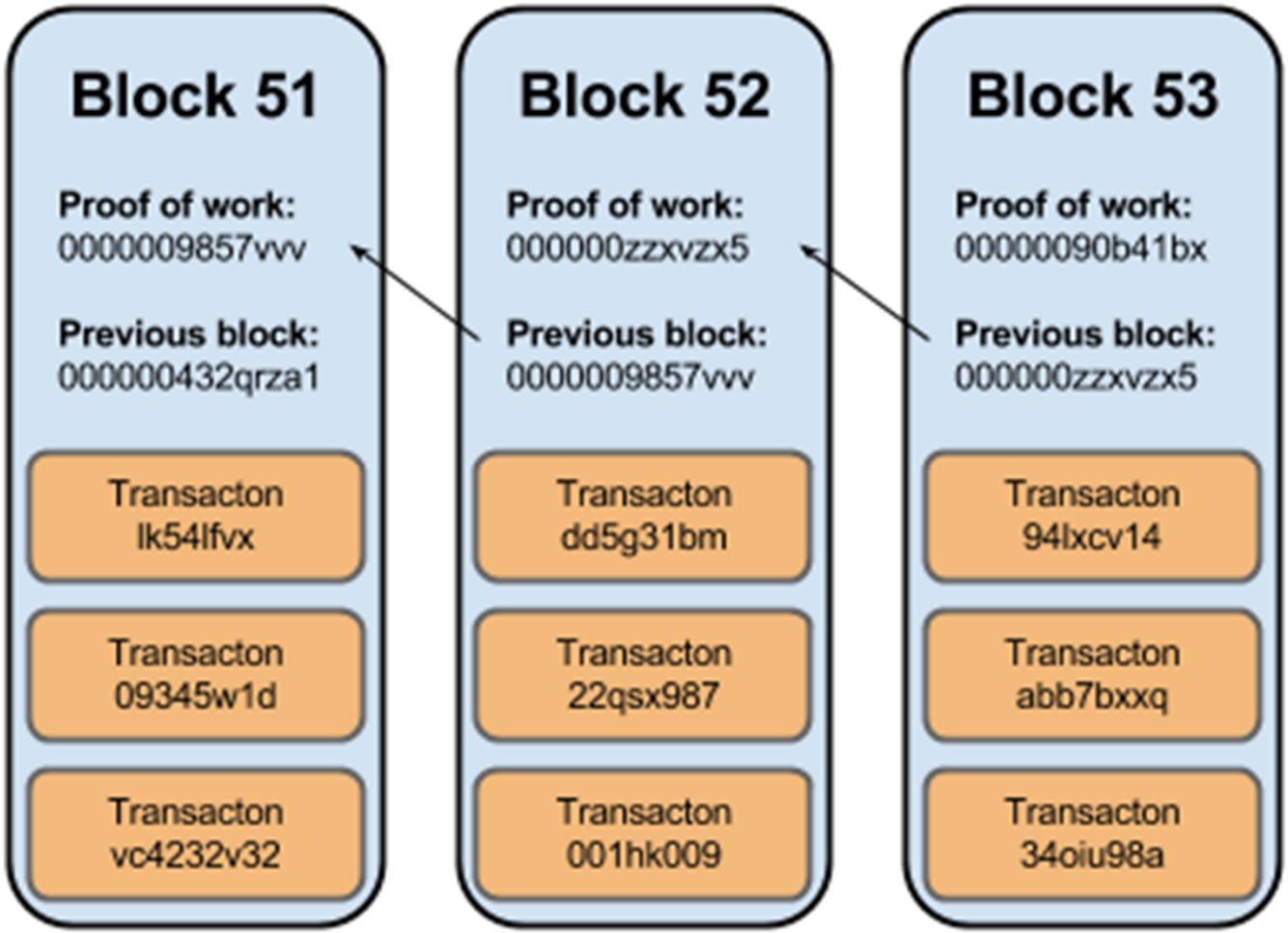
- Private key used to hash a message
- → Public key used to verify the message
- → proof of authenticity

- Public key used to encrypt a message
- →Private key used to decrypt the message
- → prove of ownership (of a private key)

- Private key == Anonymous/Pseudonymous Identity



http://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/



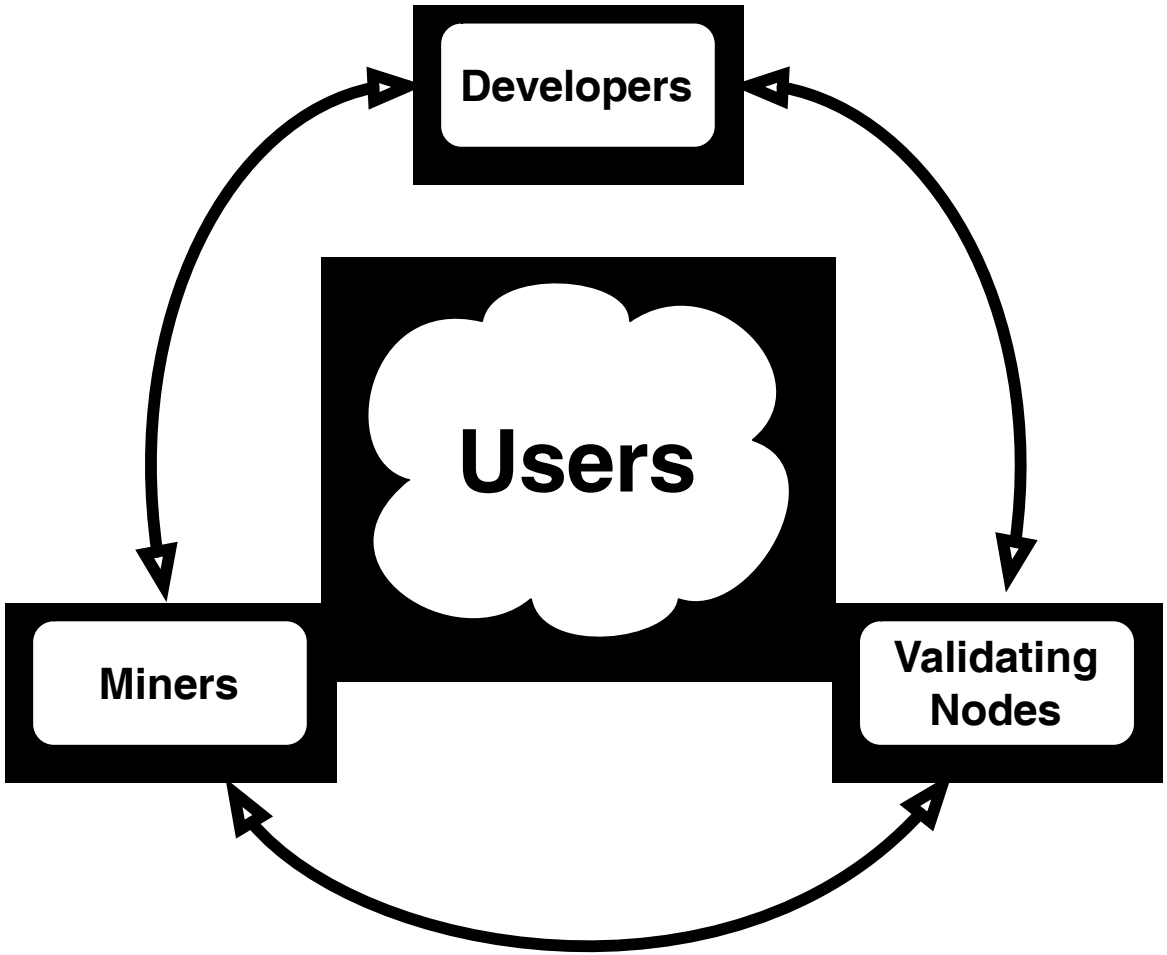
http://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/

Blockchain mechanics

- Blocks contain transactions
- Blocks are organized into a linked-list (a chain)

- Reward for mining blocks (reward plus transactions fees)
- Proof of work
- Value of the network tokens linked to real-world value

Bitcoin blockchain stakeholders



Blockchain – summary

- Blockchain is a solution to the data consistency problem in distributed peer-to-peer systems
- It uses cryptography, and clever incentive social engineering tricks to achieve consensus, and consistent global state.
- The global state is stored in the network. It is distributed.
- The transactions are non-revocable.
- There is an internal “clock”.
- All the participants are stakeholders.
- It is all electronic/digital.

Blockchain examples

- Financial tokens
  - Bitcoin (Litecoin, Dashcoin, and many others)
- Asset tokens
  - ColourCoins
  - Digital Assets
- Proof of ownership
  - Stocks ownership
  - Land ownership

Some financial examples

Bank example

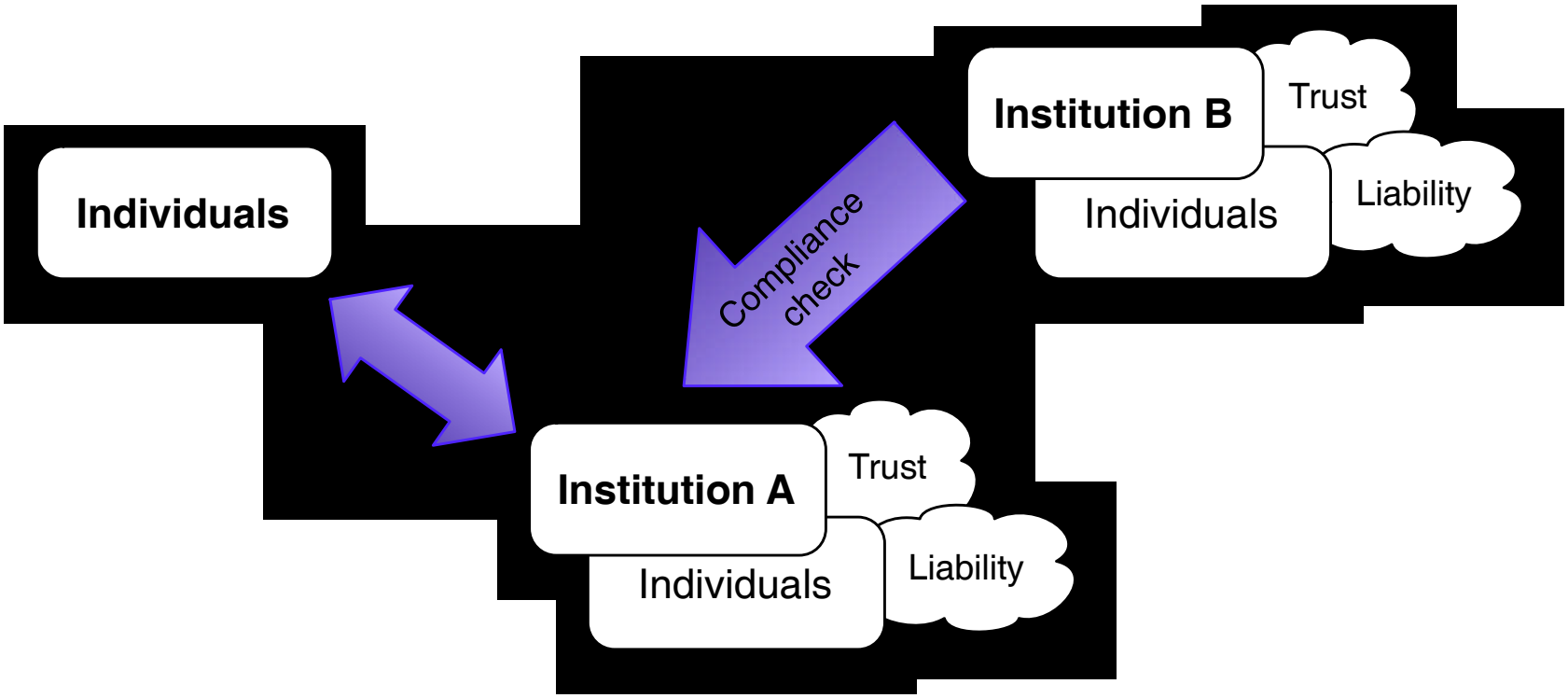
- Deposit money and
- Pass the liability to the bank
- Requires trust in the bank
- Withdraw the money

Escrow service

- Two parties do not trust each other
- Trusted Third Party
- Enables transactions between semi-trusted parties

Trusted Third Party

Institutions



Institutions

Spoken language

- Disambiguates communication
- Enables complex interactions

Written language

- Disambiguates communication
- Enables complex interactions
- Enables asynchronous interactions (time domain)
- Enables persistent storage of state (data domain)

Institutions

Human institutions rely on 3 fundamental elements

- **Communication** (social interactions)
  - ability to communicate and synchronize
- **Persistence** (stability of structures)
  - ability to store communication or data
- **Ability to compute** (procedural prescriptions)
  - ability to execute a finite sequence of steps, an algorithm
  - Prescriptions of desirable behaviour (codified or socially constructed)

Global computer: web, early days

- Peer to peer network
- Client-server architecture
- Some nodes store the state (servers)

- Take down the server – data disappears
- Take down the server – communication is impossible

Global computer: peer-to-peer

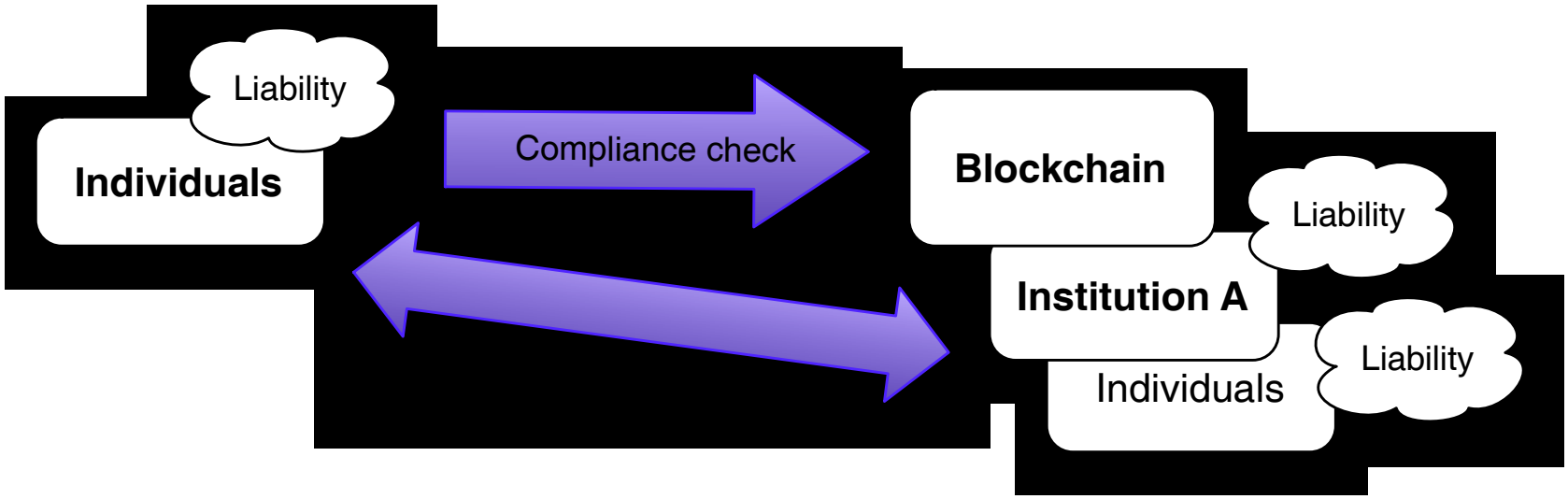
- Peer to peer systems solve the “single point of failure” problem
- Examples: Napster, Torrent, Tor

- Resilient
- State stored inside the network – take down individual node, the state persists

Global computer: blockchain-based

- All the features of P2P system
- Ability to compute
- Ability to provide distributed trust system

Blockchain Institution



Trusted Third Party – without human!

What is possible?

- Online casino, verifiably trusted, without “the house”
- Insurance scheme, verifiably trusted, without the insurer

Blockchain computing?

- Bitcoin: limited crypto operations only
- NXT smart transactions: limited operations

- Turing complete computing?

Ethereum

- **Blockchain computing**

- Global distributed computer
- Capable of Turing complete execution
- Smart contracts (arbitrary code execution)

Turing complete?

- In theory: infinite tape
- In practice: infinite looping

- Can we predict if a program will stop? What if someone writes an infinite loop? A perfect attack…

- Computing and storage costs internal currency.
- Executing contracts consumes “gas”, that needs to be covered by the entity executing the contract.

Examples

- Wallet
  - Track how much money you have
  - Track who paid you
  - Track who you paid
- Bank
  - Track accounts and money transfers between accounts
  - Track deposits and withdrawals
  - Limit who can do what

- Clock
  - http://www.ethereum-alarm-clock.com/

Rock – Paper – Scissors

- Rock → Scissors → Paper → Rock

Rock – Paper – Scissors

- Rock → Scissors → Paper → Rock

1. Contract: voting
2. Player A → encoded “vote” hashed([R | S | P]) + fee
3. Player B → encoded “vote” hashed([R | S | P]) + fee
4. Contract: validation
5. Player A and B validate their votes by posting the password to decode the vote
6. Contract: resolution
7. Winner gets reward
8. There are timeouts for step 4 and 6.

Other examples

- Crowd-funding campaigns
- Digital currency issuance and management
- Digital assets issuance and management (see NXT/Ardor)

- DApps → distributed autonomous applications

Open innovation platform?

- Imagine:
  - A group of developers and designers work on a mobile game
  - All the people involved are anonymous
    - (side story → applying for programming job on black market)
  - The tasks are agreed upon, and people bid through auction system
  - The progress is tracked by Git version tracking system
  - The game is released on iTunes, and the revenue is shared through the smart contract based on the contributions to the project

Possible? Almost:

- A bit tricky to get “definition of done” agreed upon. Acceptance tests? Who/what tests the tests?
- iTunes revenue go to a “old-fashioned” bank. Need decentralized payment system (e.g. Bitcoin).

http://dapps.ethercasts.com/

Research areas

- Transaction throughput
  - Limited by the blockchain “clock” and block capacity
  - Promising solutions: Off-chain transactions, Lightning Network
- Anonymity and de-anonymisation of transactions
  - Law enforcement, financial compliance
- Social modeling
  - None have predicted that the majority of hashing power will reside in China
- Complex contracts and verification of (non-)intended consequences and side-effects

Oracles

What is an Oracle?
https://en.wikipedia.org/wiki/Oracle_machine

Oracle in computational theory, is a hypothetical computer, a black box, that can compute anything, in a single step. It can compute ANYTHING, even things that normal computer cannot.

Why Oracles in Ethereum

Computing off-chain.

Getting information from the real world.

Linking to real world events, people, identities, objects.

Example Ethereum Oracles

Linking phone number to Ethereum identity.

Linking Social Media account to Ethereum identity.

Example Ethereum Oracles

Linking phone number to Ethereum identity.

→ **KYC - Know Your Customer.**

Linking Social Media account to Ethereum identity.

→ **Reputation.**

Example Ethereum Oracles

http://www.blockchainlabs.org/blockgrant-x-en/

Linking phone number to Ethereum identity.

→ **https://www.proofofphone.com/**

Linking Social Media account to Ethereum identity.

→ **Reputation.**

Questions, please

Mariusz Nowostawski

NTNU, Applied Computer Science Department
Testimon Forensics Group

mariusz.nowostawski@ntnu.no

- Twitter: @praeteritio
- Skype/Google: nowostawski