On blockchains, things, and information

Pekka Nikander
December 5th 2016
Aalto University and LI co-op

About the speaker

- Lifelong researcher and entrepreneur
  - Ph.D. (1999) from Aalto (then TKK)
  - In 1988 founded Nixu, then a number of others, then in 2016 co-founded Luottamuksen Löyly co-op
- Old-school "full-stack" developer or "hacker"
  - Anything from FPGA to desktop GUI
    - most focus in cryptographic protocols & distributed systems
    - but not really savvy in cloud or HTML5
- Still researcher and entrepreneur
  - Research fellow at Aalto University CS
  - CTO at Luottamuksen Löyly co-op

Why blockchains now?

"Blockchain *distributed consensus model* is the most important invention since the Internet itself", Marc Andreessen

Cf. David Chaum's first papers in 1982 and DigiCash 1990–1998

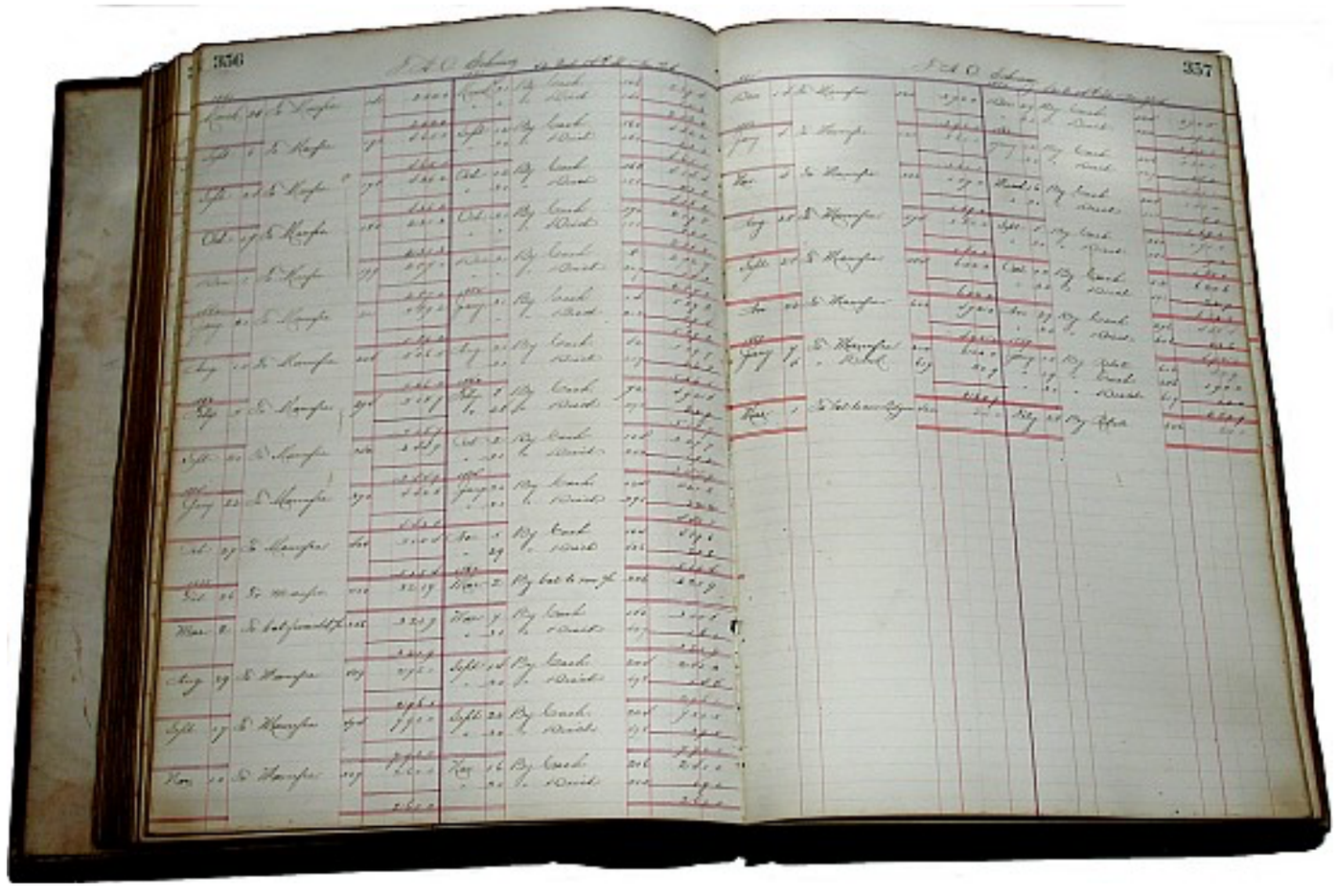
Outline

- Blockchains
  - Open ledger
  - Accumulation of events
  - Design choices
    - A layered model
- Internet of Things
  - Accumulation of data aka Context Model
  - Value bearing transactions
- Information Centric networking
  - Decentralised storage and multicast
- Putting Blockchains, IoT and ICN together

Block chains

- Decentralised open ledger
  - Undeniable transactions
  - Full ordering
  - Accumulation of history
  - Main design choices
    - Identity management — anonymous or not
    - Consistency and consensus models
    - Incentive model(s)

Open ledger



Open ledger

- Open
- Decentralised
- Undeniable
- Consistent
- Event
- Sequence

O’DUCES

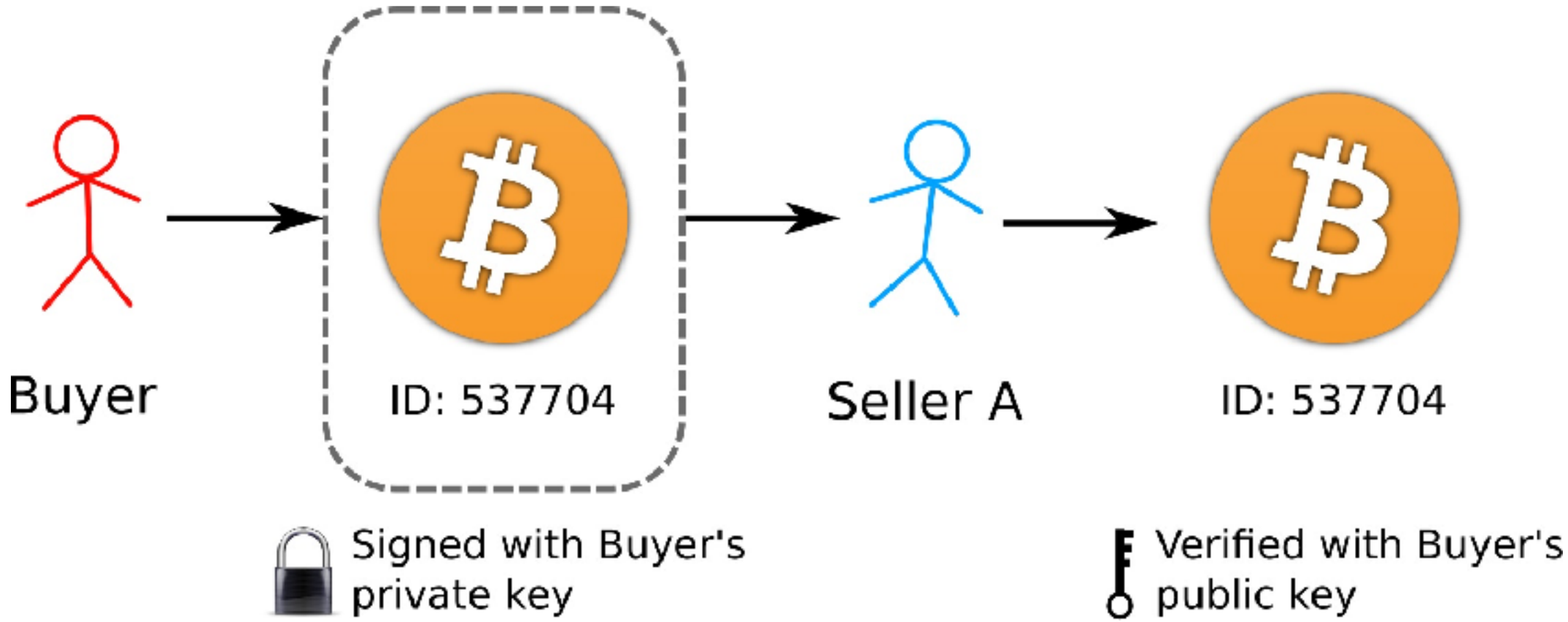
Open ledger

If it is in the ledger
I can believe in it

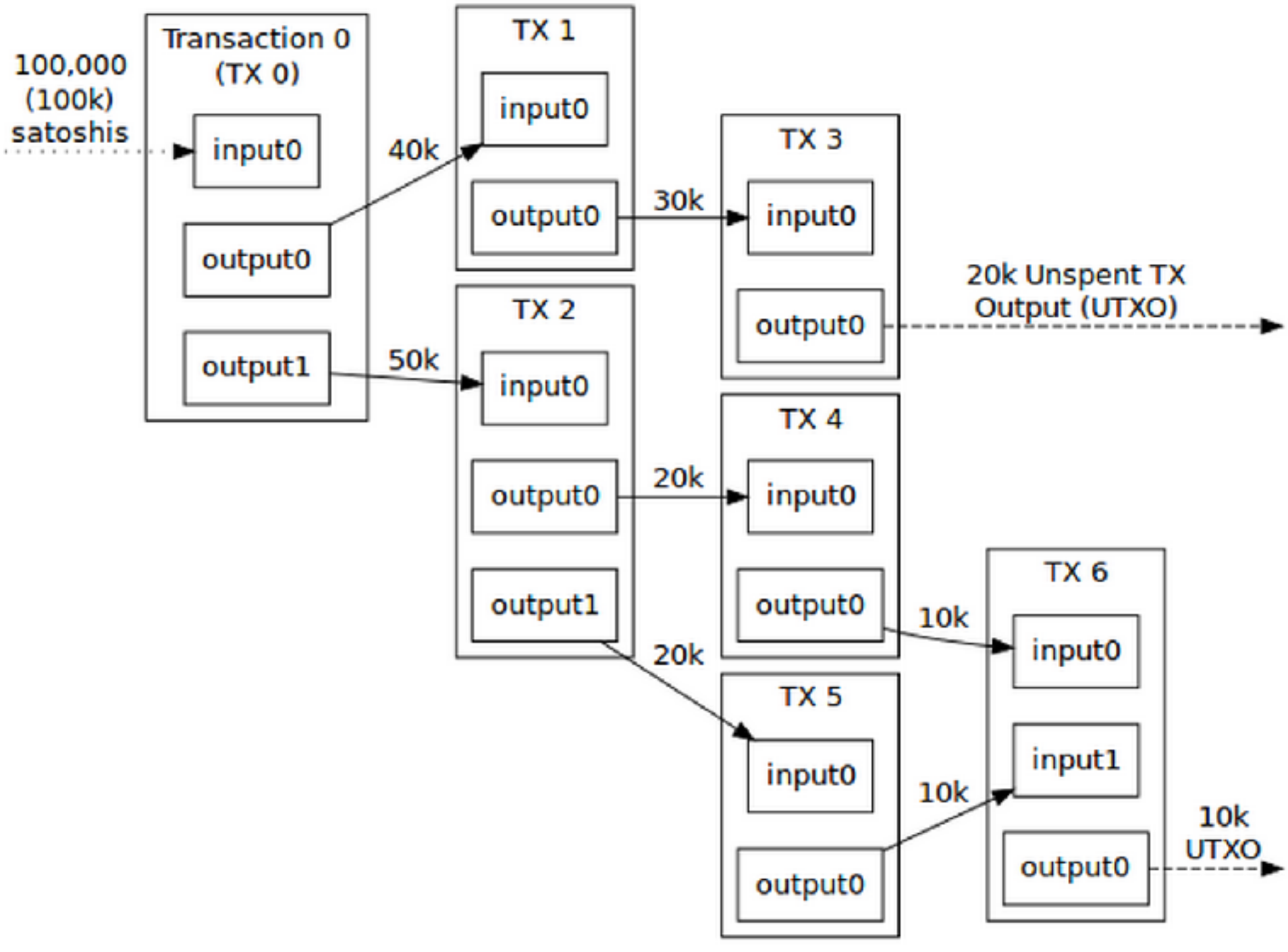
Доверяй, но проверяй
Trust, but verify

Undeniable ordered transactions

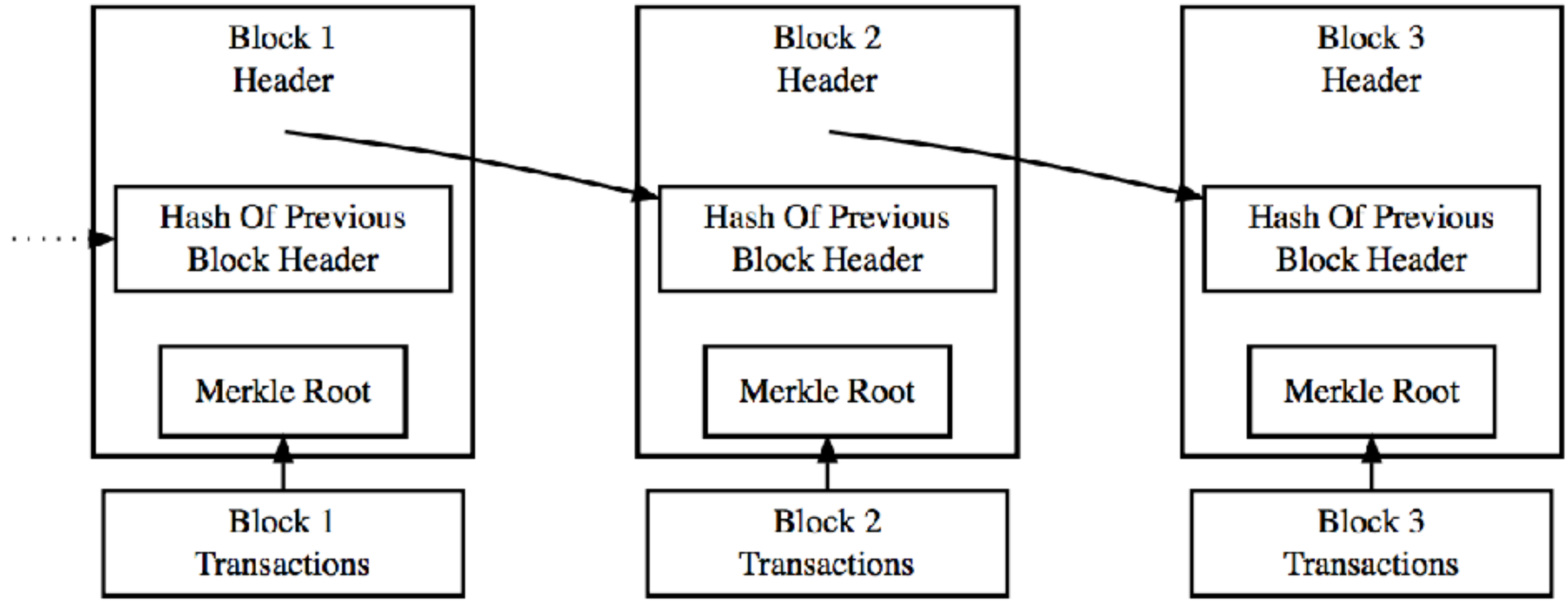
Undeniable …


Buyer
ID: 537704
Seller A
ID: 537704
Signed with Buyer's private key
Verified with Buyer's public key

… transactions …



… ordered with blocks



Simplified Bitcoin Block Chain

[Merkle tree allows one to check that a transaction is in the block in O(log(N))]

Accumulation of events

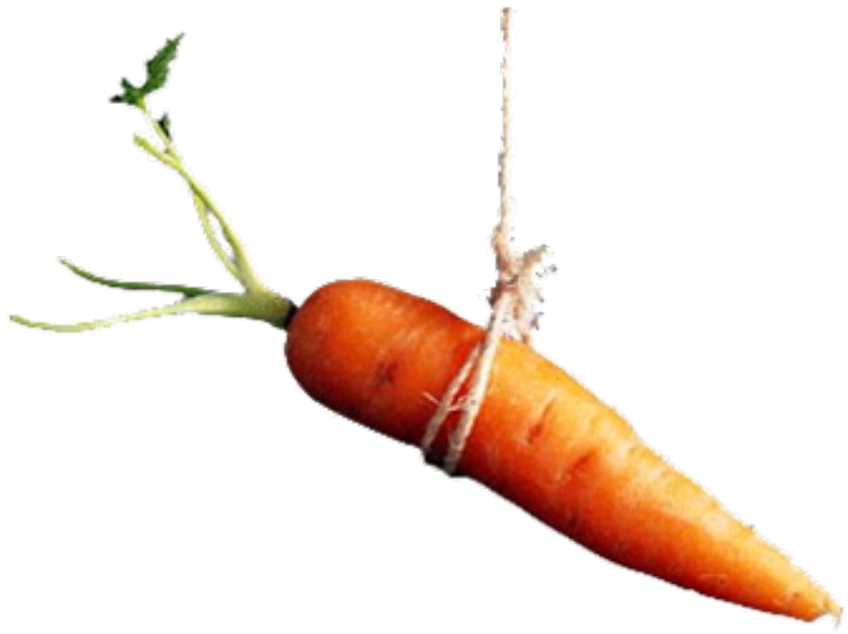
The more the merrier!

- Unforgeable history
  Spread to the network
- Majority consensus
  Spreading to the network
- Forming consensus
- Proposed events

Design choices

Identity

Consensus
and
Consistency



Incentives

Identity management

- Who can join?
  - Propose valid transactions
- Who can mine?
  - Define transaction order
- Anonymity
  - Zero knowledge identities
  - Ephemeral public keys
  - Pseudonyms
  - (Potentially) certified public keys

Identity: Fundamentals

- May an identity have *negative* value?
  - You need the real world / certification
    - or entry barrier as high as highest negative value
- Is *collusion* (Sybil attack) a threat?
  - You are likely to need the real world
- Can one benefit from *affecting the order*?
  - You may need the real wold for mining

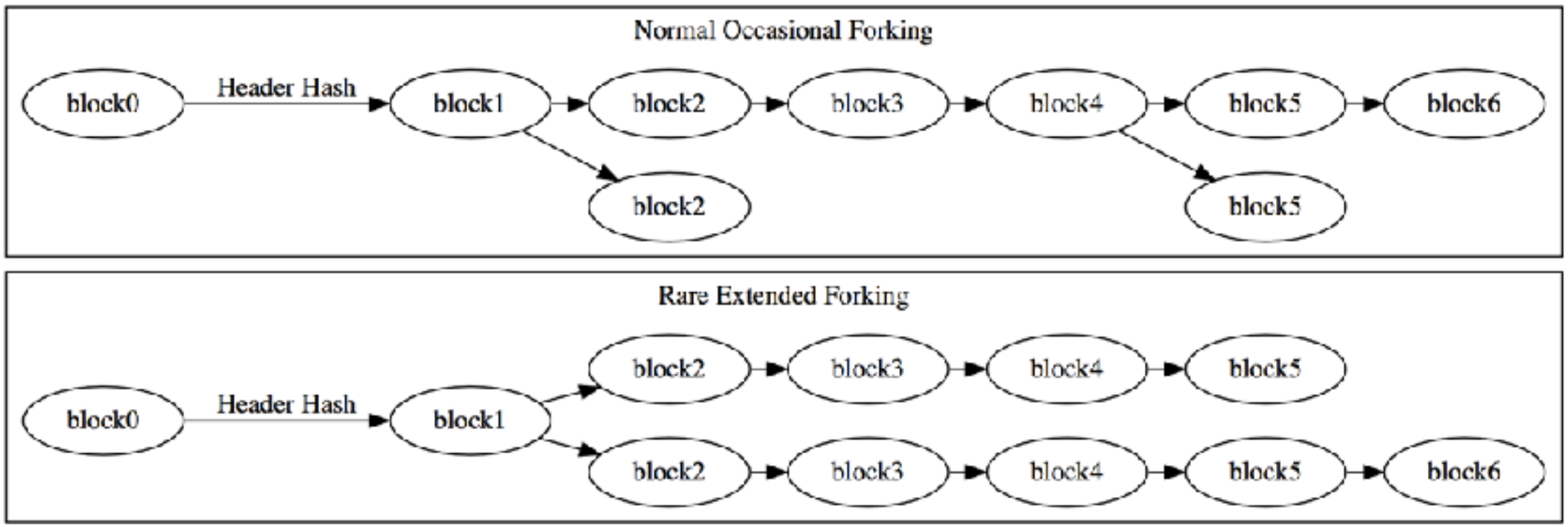
Consistency

- Is full order / consistency really a must?
  - How fast do you need full consistency?
    - E.g. bitcoin reaches full consistency only in about an hour

- Can you remodel you problem to partial order / eventual consistency?
  - or can you do without the block chain?

Consensus

- Usually meaning: No block chain **forks** …



- … but requires rethinking
with partial order or weak consistency

Incentives

- Verification requires work
  - Check transaction chains, signatures, identities, …
- Remember the added value?
  - “If it is in the ledger, I can believe in it”

Incentives

- How to make sure there is the ledger?
  - Who have the incentive to contribute it?
  - Who have an incentive to contribute in 10 years? In 30 years?

- How to make sure everything in the ledger has been verified?
  - How to punish the lazy bookkeeper?

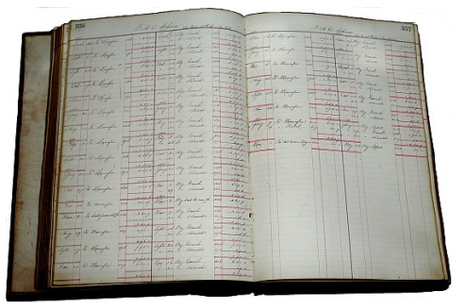
Some incentive models

- Get paid through block mining (bitcoin)
  - Mining creates new “money”
- Get explicitly paid in the transactions
  - Value explicitly transferred to the miners
- Make it the only way to make transactions
  - Each transaction verifies some others randomly
  - Likely to work only with partial oder

A layered model

Blockchain layer	Main function	Analogue Internet layer
Contracts	Contract semantics	RESTful
Blocks	Complete order	TCP
Transactions	Partial order Partial contracts	IP
Storage and network	Distribute and store	Ethernet / L2

Block chain summary



- Ordered transactions
- Open ledger
- Design choices
  - Identity
  - Consistency & consensus
  - Incentives
- Layered model
- The more the merrier!

Outline

- Block chains
  - Open ledger
  - Accumulation of events
  - Design choices
    - A layered model
- Internet of Things
  - Accumulation of data aka Context Model
  - Value bearing transactions
- Information Centric networking
  - Decentralised storage and multicast
- Putting Blockchains, IoT and ICN together

Things

IoT ledgers

- Accumulating data or metadata
- Combining value and real world

Accumulation of data or metadata

- Blockchain as an open event log
  - Where to get the context for the data?
- Blockchain as an open meta data log
  - Platform for data provenance transactions
- Benefits
  - Undeniability (but that you can get also otherwise)
  - Reduced verification costs
  - Open access — increased awareness

Controlling IoT devices

Think of onions — multiple layers of security

Combining value and real world

- IoT actuation affects the real world
  - Transition of real world states, e.g.
    - giving an item from a vending machine
    - transferring a container (next slide)
    - …
- Combine the real world "state change" and the virtual world state change

Transfer of liability: Passing a container

- Who is responsible?
  - Recognising environment
    - Record changes to blockchain
- I am now responsible!
  - Acknowledging liabilities
- Three parties:
  - Holders and the container

Transactions with value

- Digital transfer of value
  - Usually real world transfer of ownership

- Digital transfer of liability
  - Often real world transfer of possession

- Contracts with ambiguous value
  - E.g. derivative contracts; any IoT examples?

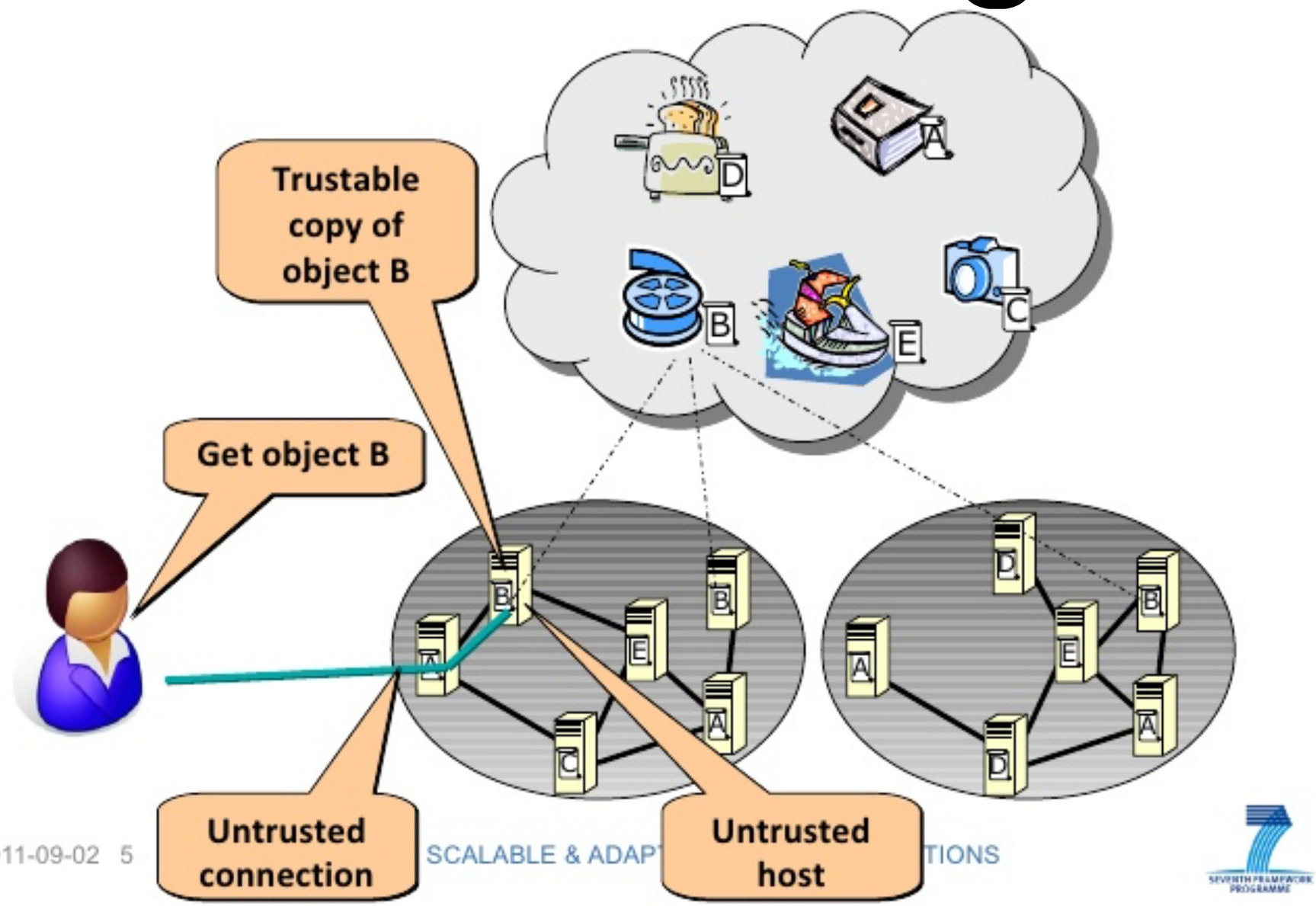
Business and threat models

- Remember our identity discussion?
  - May an identity have negative value?
    - Is there any danger of collusion?
- Denial of service and / or flooding models
  - Limited ability to add events to the ledger
- And other considerations…

Outline

- Block chains
  - Open ledger
  - Accumulation of events
  - Design choices
    - A layered model
- Internet of Things
  - Accumulation of data aka Context Model
  - Value bearing transactions
- Information Centric networking
  - Decentralised storage and multicast
- Putting Blockchains, IoT and ICN together

Information Centric Networking



- Decentralised Content Delivery Network (CDN)

ICN necessities & benefits

- Necessities
  - Secure naming of data
  - Ability to verify data integrity
- Benefits
  - Retransmitting data less often
    - Multicasting and “caching”
  - Data may be moved more easily
  - DoS attacks harder to implement

ICN challenges

- Secure naming
  - How the client knows the secure name
- Incentives and compensation
  - How to compensate for “caching”?
    - Decentralised storage?
    - Actual data delivery?
- (There are other technical challenges, but they are beyond the scope here)

Combining block chains, IoT, and ICN

- Block chains
  - Open decentralised ledger
    - Capturing events and liabilities
- Information Centric Networking
  - Decentralised storage of info
- Internet of Things
  - Events linking digital and real

Summary:
Some thoughts

- "Blockchains" are a *social* phenomenon
  - Nothing technically spectacular, the technology has existed 15+ years
- *Open ledger* may change the world
  - Reduces information asymmetries
- Combining blockchains, ICN and IoT seems like a potentially interesting approach

Questions?

Objections?

Anything else?