Blockchains' Impact on Networking and Distributed Systems

Burkhard Stiller
Communication Systems Group CSG
Department of Informatics Ifl
University of Zürich UZH
stiller@ifi.uzh.ch

With many thanks to Thomas Bocek, Sina Rafati, Bruno Rodrigues, Eder Scheid, and others

Universität Zürich[UZH]

Blockchains
Applications
Impacts & Consequences

CSG
Communication Systems Group

ifi

The “Internetification“ of Life

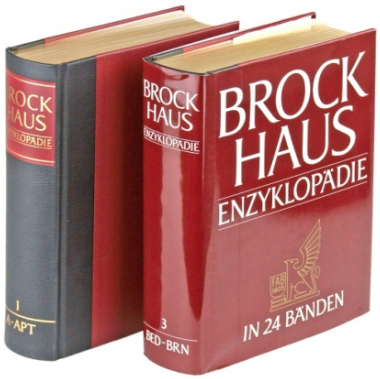
Physical Objects

Telegram

Ended Dec 29, 2017 in Belgium

Digitized Representations

Since mid 70’s, RFC 524



Encyclopedia

Since 2001

Money

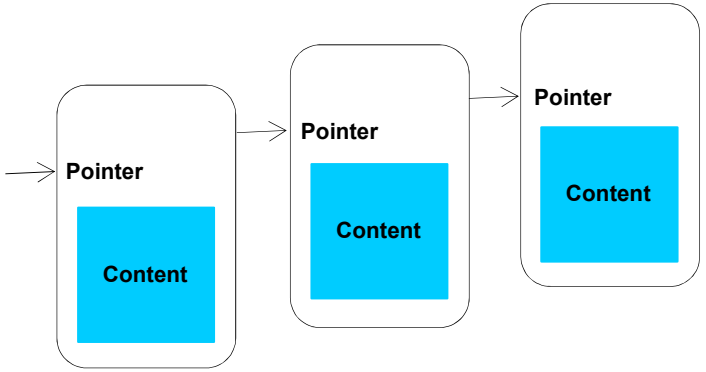
Since 2009

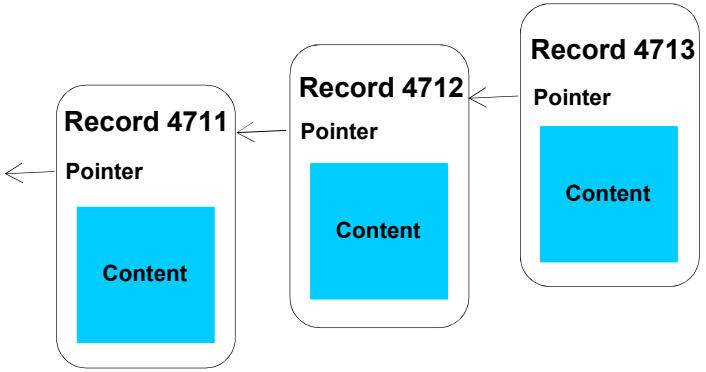
Bitcoins

All systems operated as networked and distributed systems!

Digression – Data Type “Linked List”

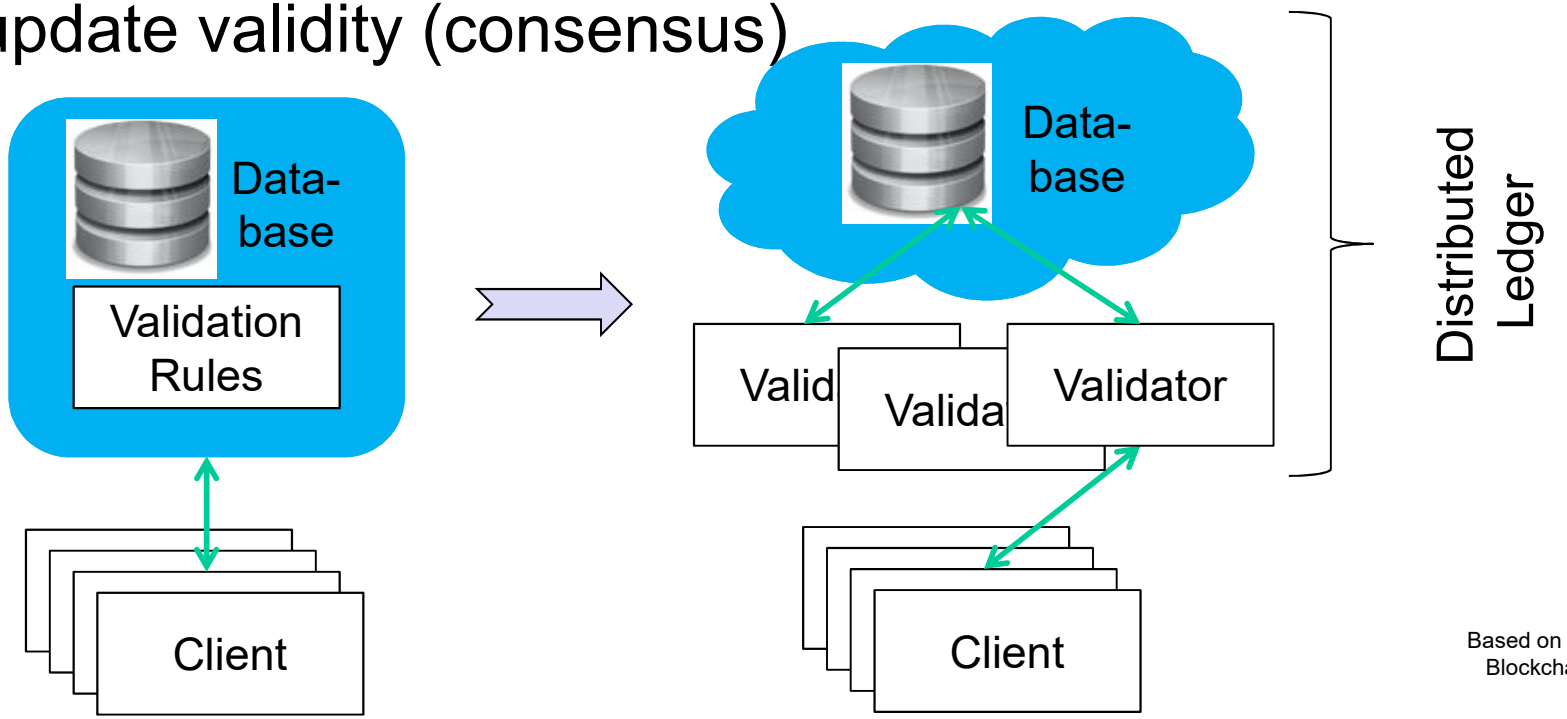
- Linear collection of data elements (records)
  - Linear order of records is given by pointers to the next record
  - Data structure as a group of nodes represents an implicit sequence
  - Example: backward linked list
  - Data structure as a group of nodes represents an explicit sequence due to record identifiers added





Key Idea: “Replacing” (Central) Databases

- Distributed Ledgers replace clients’ access-protected writes to an authoritative database via validation rules by a distributed consensus of many validators
  - where the database’s state depends on majority agreement of update validity (consensus)



Based on Terence Spies:
Blockchain Mechanics

Blockchain Definition

- Distributed Ledgers (DL) or Blockchains (BC)
  - Digital record of who-owns-what w/o a central storage
    - Records are organized in blocks, unchangeably chained (cryptography)
  - Consensus algorithm ensures that each node's copy of the ledger is identical to every other node's copy
  - Access to ledgers by miners with large compute power (PoW) to and from any asset owner for transactions via cryptographic signatures

    PoW: Proof-of-Work
    - Persist "incoming" data (token=asset) on private/public ledger
    - Read/offer "outgoing" data to other stakeholders (non-private)
- Key advantages of BCs
  - Immutable, traceable, and preventing "double spending"





Blockchain Ingredients

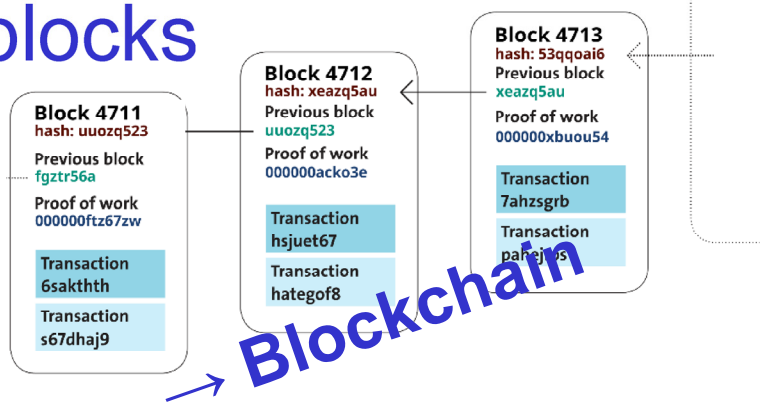
- Public key cryptography and hashes
  - Asymmetric approach for arbitrary users
    - Ensures validation and authentication (in turn authorization)

- Internet
  - Networked infrastructure for everyone
  - Distributed system with arbitrary users and devices (nodes)
    - Peer-to-peer (overlay network) communication paradigms
    - Storage capabilities for “any”-sized data volumes

- Incentives
  - Supporting rewards for participants’ tasks performed within an overlay network by a “protocol” enabling communications
    - Ensures participation of anyone (potentially untrusted stakeholders)

Blockchain Operations

- Transactions (content) collected in blocks
  - New blocks created regularly
- A block contains a hash of and a pointer to the previous block …



- Consensus mechanism required to determine the block to be integrated into this blockchain
  - Public blocks contain solved crypto puzzles (PoW)
    - *E.g.*, a form of partial hash collisions (SHA256)

- Creation of valid blocks performed by anyone (reward)
  - Computational expensive → Avoids double spending
  - Mining ≡ confirmation of blocks ≡ solving crypto puzzles

ifi

Blockchain Data Structure in Detail

- BCs are a backward-ordered, linear list of blocks
  - Chain starts with genesis block to which others are back-linked
- Blocks contain (at least)
  - Transaction data (content, payload)
  - Pointer to and a hash of the previous block
  - Cryptographically hashed value of crypto puzzle (result of PoW)
  - Time stamp
- BC's structural and technical characteristics
  - Chain may show side chains, but only one valid branch finally
    - Chronological order guaranteed by previous block's hashes
  - A BC network is organized as a peer-to-peer network
    - Overlay topology may change, replicas of BC are hold on multiple nodes, exchanges of new blocks performed within that overlay, anyone to join

Blockchain Types

- A public/permissionless blockchain

The real and only blockchain!

  - BC open to any stakeholder
    - → Contributions to the processing of transactions and blocks
  - No dependency on any prior identity of any kind
  - No need for any previous relationship of stakeholders
- A private/consortium/permissioned "blockchain"

  - Chain open to permissioned (known) stakeholders
    - Transaction processing is accessible, processed, and validated by those stakeholders only, who are known to the BC "creator/owner"
    - → Contributions count according to the rules the BC applies

No blockchain, limited stakeholders!

- A hybrid blockchain

  - Certain processing steps open, others restricted to known stakeholders

Smart Contracts

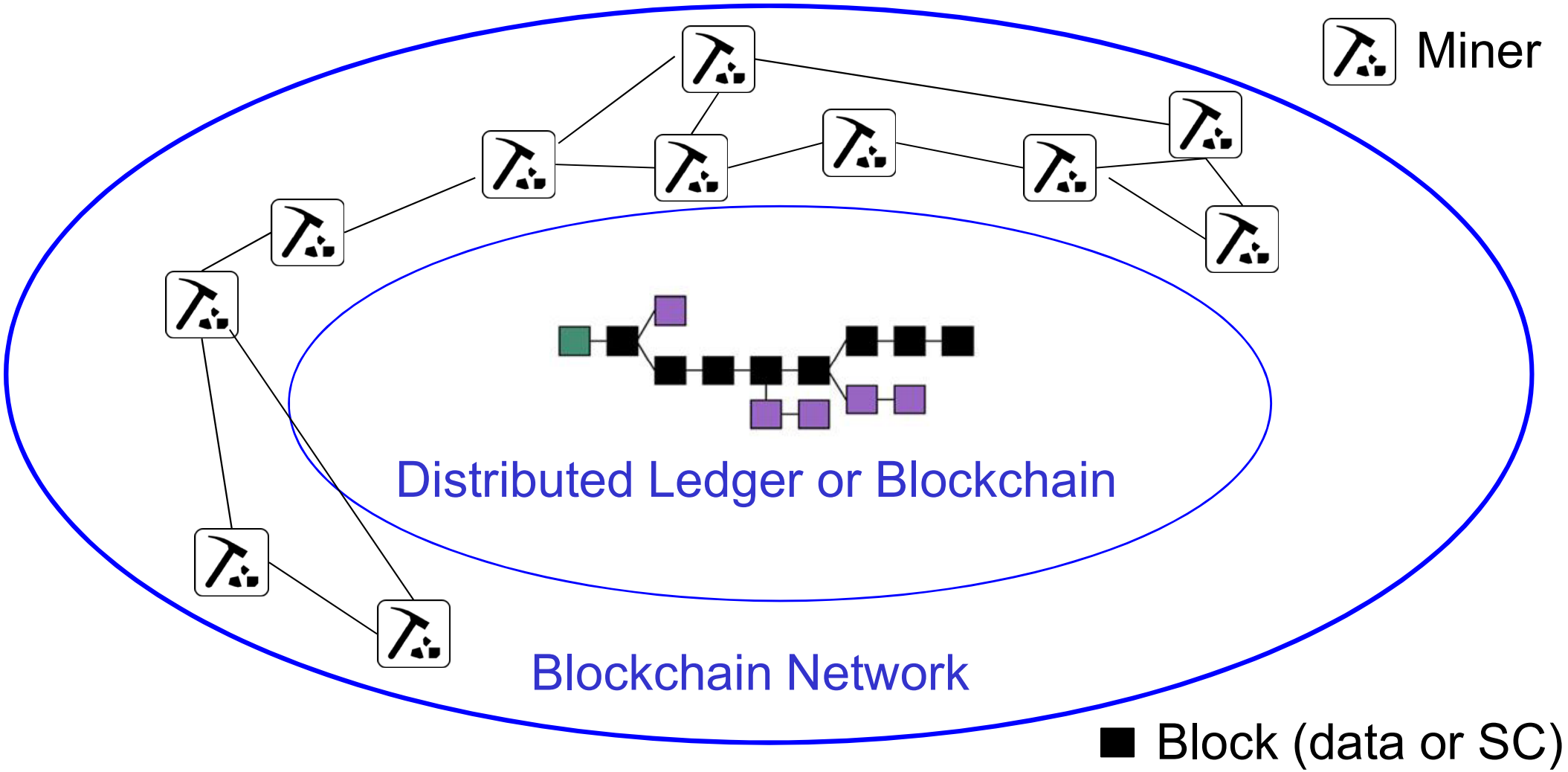
- A Smart Contract (SC) may reside inside transactions
  - Executed & validated on every node upon persisting that block
    - *E.g.*, for Bitcoins (blockchain-based cryptocurrency) SCs specify how to withdraw, escrow, refund, or transfer BTC from A to B
- SCs first mentioned in 1996

"Active" database!

> A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of [a] smart contract['s] design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs.
>
> N. Szabo

- Smart contracts alone are not "smart"
  - They need an infrastructure ("technology")
  - A blockchain forms ***the*** ideal, distributed basis for SCs
- The legal relevance of "coded", more general contracts?

Key Blockchain Terminology (1)



Chain: Backward-linked list of cryptography-based (hash-secured) pointers to previous blocks

Key Blockchain Terminology (2)

- Miners
  - Those BC members, who run machines to solve crypto puzzles
  - Their reward in case of a successful inclusion are tokens of BC
    - *E.g.*, in case of the bitcoin BC the reward is BTC
- Mining (Process)
  - The process of BC members trying to solve the crypto puzzle and adding the respective new block onto the BC
- Consensus
  - State reached where the majority of members of the same P2P network agrees on the same mining output
  - This state of the consensus is secure and tamper-resistant, immutable with respect to the blocks, and their data is persisted

Applications

Examples

Only very specific ones …

Main BC Example 1: Bitcoin

- Bitcoin is an **experimental** cryptographic (digital) currency
  - Bitcoin is fully peer-to-peer (no central entity, trustless)

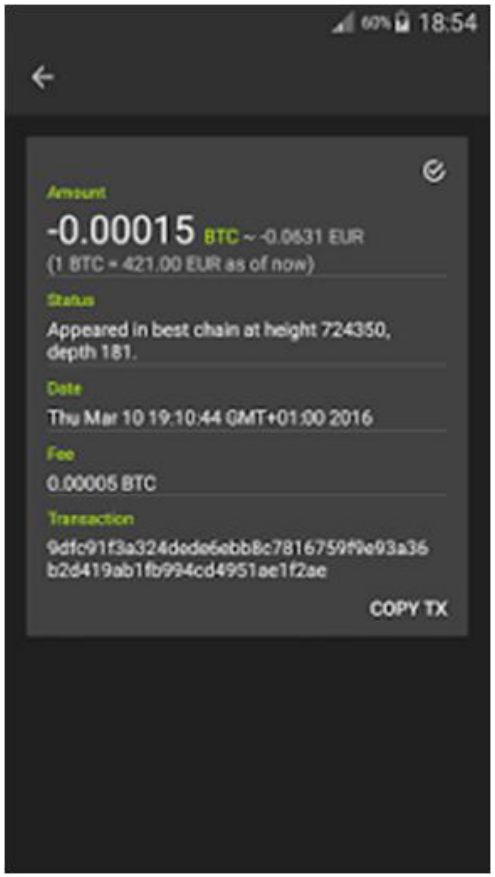
    → Blockchains applied to reach this goal (sic!)
  - 1st Bitcoin issued on January 3, 2009
- Key characteristics
  - Maximum of 21 million BTC
  - Every transaction broadcast to all peers (every 10 min, P2P)
    - Every peers knows all transactions (~125 GByte as of today)
    - Maximum of 7, real life 3-4 transactions per second (1 MB block size)
  - Validation (consensus) by Proof-of-Work (PoW)
    - Partial hash collisions (SHA-256), thus, very difficult to fake this PoW
    - Absolutely no double-spending
  - Bitcoin user account controlled by private key

Main BC Example 2: Ethereum

- General purpose smart contracts based on blockchain
  - Ether = token (cryptocurrency), payment of tx fees, no limitation
    - Formed as a decentralized P2P network
    - Ethash algorithm and Ghost protocol (fencing off pool mining)
    - Block creation time at 12 s
    - Mining similar to bitcoins except for block halving (here every 4 y) and rewarding scheme
    - Applies Turing-complete SCs (language: Solidity), dApps
      - Ethereum Virtual Machine (EVM) , Ethereum Light/Full Clients
      - SC on ethereum verify or auto-enforce any type of bus./legal agreement
      - “gas” needed to ensure the execution of a SC
    - 2 account types
      - User account controlled by private key or contracts controlled by code
  - Beta Frontier July 15; Homestead Release March 16; DAO fork, mid 16; Byzantium October 17; Constantinople 18 (expected)

UZH‘s Coinblesk Application

- Real-time bitcoin payments (Android app)
  - Use case: merchant/customer and person/person with online Bitcoin payment
  - Transaction time < 1 s (multi-sig, registered)
    - Device build-in NFC and Bluetooth LE
  - Merchant with regular trade-back to US$ (decreasing BTC volatility)
    - Refund transaction for service disruptions
  - Successful field tests at UZH cafeterias
    - Started in 2014, presented in 2016 at CeBIT in Hannover, Germany
  - Add’l work on reduction of transaction fees, adding clearing



https://play.google.com/store/apps/details?id=com.coinblesk.client&hl=en

UZH‘s and modum.io‘s Architecture “Blockchains for Coldchains (BC4CC)”

- Pharmaceutical sector
  - More than 200 million yearly shipments of medical drugs inside of the EU and associated countries

  - 100% monitoring of transport required due to EU regulation
    - “Good Distribution Practice of medicinal products for human use” (GDP 2013/C 343/01) since January 2016

    - Package: Postal 6 CHF, cooled transport 35 CHF → app. cost factor 6
- Solution

modum

  - Swiss SME modum.io raised in 2017 in an ICO 13.5 M US$
  - Architecture developed enables storing of temperature data monitored and executing smart contracts on those upon arrival

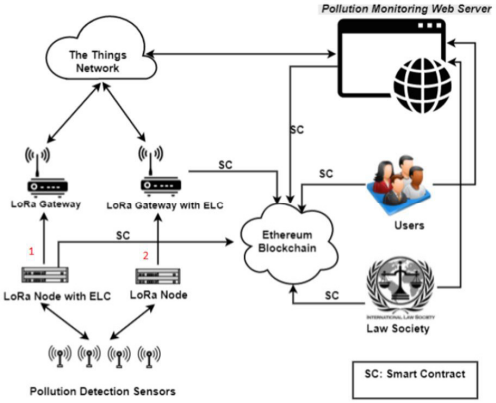
ethereum

    - UZH prototype based on certified (temperature) sensor and Ethereum

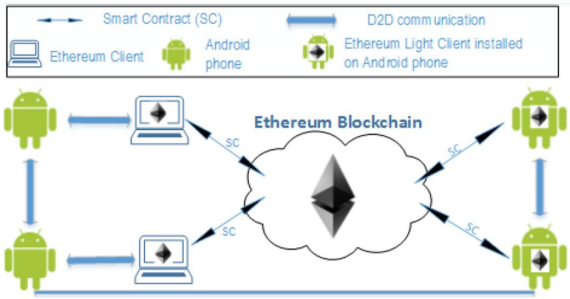
UZH‘s SC-based Contracting Applications

- IoT-based pollution monitoring → IEEE/IFIP Man2Block 2018 Workshop: Poster on Friday

  - Blockchain-based automated measuring, storing, and monitoring via sensors via the Ethereum Light Client
    - SCs used since 2017 to define pollution thresholds based on international specs
      - CO, CO_2, ph, turbidity
  - Employs IoT protocols LoRaWAN (TTN)
    - Reduced power consumption, range to 200 km



- Flexible, light weight trading contracts → IEEE/IFIP NOMS 2018 Demo just after this keynote
  - Ethereum Light and Full Client applicable
  - SCs used (since 2017) to set/get information
    - Deposits, traded objects, contract parties’ ID
    - Enhanced user privacy



Impact & Consequences

(Direct) Impact Factors

Influencing Factor	Network	Distributed System	Remarks
Access: Public BC	In principle unaffected	Very many nodes possible	The ***real*** BC case
Access: Private BC	Unaffected	Typically “centralized”	“No” BC
Cryptography	-	Compute load affected	Mechanisms’ break?
BC size	Larger throughput	-	-
Consensus mechanisms	Availability essential	PoW: high compute load	Problem of energy efficiency unsolved
Incentive/reward mechanisms	Availability necessary	Number of nodes in BC network affected	-
Creation of blocks	Load affected	Compute load affected	-
Block size	Load affected	Compute load affected	-
Smart Contracts	-	Compute load affected	-
Governance	Affected	Affected	In multiple facets

Based on an incomplete survey, but originating from an investigation of those applications developed ourselves.

Example: Current Transaction Durations

- Bitcoin Cash: 615 s
- Bitcoin: 504 s
- Litecoin: 135 s
- Ethereum: 15 s
- Ripple (XRP): 4 s
- EOS: 1.5 s

Sample effect of BCs very visible by the user!

Bitcoin report, March 2018, http://www.bitcoin.report.de

EOS "provides accounts, authentication, databases, asynchronous communication, and the scheduling of applications across many of CPU cores or clusters. The resulting technology is a blockchain architecture that ***may ultimately scale*** *to millions of transactions per second, eliminates user fees, and allows for quick and easy deployment and maintenance of decentralized applications, in the context of a* ***governed*** *blockchain", thus a private BC.*

https://globalcoinreport.com/eos-strides-towards-recovering-its-record-against-bitcoin/

Blockchain Interoperability

- Projects using or providing a platform for interoperable chains

Blockchain	Area	Interoperability Type
Origintrail.io	Supply-chain	Sidechain/Relay
Ælf (ELF)	General purpose	Sidechain/Relay
Wanchain	Finance	Hash-locking
Herdius	Finance	Notary-scheme
Cosmos	General purpose	Sidechain/Relay
Aion	General purpose	Hash-locking
Polkadot	General purpose	Sidechain/Relay
Ark.io	General purpose	Sidechain/Relay
Crowdmachine	Cloud-computing	Sidechain/Relay
Blockstack	Identity	Sidechain/Relay

Consequences (1)

- BCs in general
  - Handling of tangible (non-digital) assets: proof of asset's ownership? "Secure" mapping of tangible to digital asset?
  - Societal and governmental acceptance?
    - Cryptocurrency bans, ICO illegal activities, asset mapping fraud
- BC "technology", including SCs
  - Breaking of applied security algorithms (long-term storage, if signing algorithm will be broken?)
    - Security impacts due to alternative consensus mechanisms?
  - Unknown attack vectors and programming errors
    - Privacy: persisted data at stake? General Data Protection Regulation?
  - Efficiency of consensus mechanisms
    - Energy consumption for Bitcoin alone in 2017 ≈ Iceland's production
  - Standardized APIs for switching applications on top of BCs

Consequences (2)

- General BC operations
  - Scalability: Throughput as a number of transactions per s? Volume of data persisted, not Bytes but MB?
    - Note: BC sizes grow faster than density of HDDs/SSDs!
  - Delay: Latency of persisting steps, block sizes?
    - Bitcoin blocks running out of capacity and having to wait hours and sometimes days for transactions to get confirmed
  - Implications on privacy: access rights and management?
  - Lacking Internet connectivity for a “longer” period of time?
- Economics
  - Stability of coin/token value against fiat currency: volatility?
  - No prevention of making fraudulent profitability projections
  - Role, interrelationships of more than 1500 cryptocurrencies?

Conclusions

1. Blockchains ***do not*** have a relevant impact on general networking, however, “unreliable” networks do have an impact on the BC
   - Especially in case of longer outages
2. Blockchains ***do not*** have a relevant impact on Distributed Systems, however, the full decentralization is (very) costly (PoW) or still not secure (other Po”X”)
   - Especially (in case of PoW) BC-related energy demands
3. Traditional Network and Service Management methods ***apply***, however, long-term security management is key
   - Transparency vs. anonymity, performance vs. sustainability
4. BCs show **no** revolution, but an evolution of linked lists
   - Any system as of the past had not been replaced in full by a BC

Modulo “measurable” effects, but at no impact

Thank you for your attention.