Blockchains – A Valuable Commercial Contribution or a Romanticized Technology Playground?

Prof. Dr. Burkhard Stiller
Communication Systems Group CSG, Department of Informatics IfI
University of Zürich UZH
stiller@ifi.uzh.ch

Many thanks are addressed to Dr. T. Bocek, B. Rodrigues, and S. Rafati
Introduction

- **Databases**
  - Data organized in schemata
  - Access control for users and the “SysAdmin” (trusted root)
    - Centralized, physical, and trusted servers are maintained
    → Potentially central point of failure, loss, or misuse
  - SQL-based systems
    - MySQL, MariaDB, PostgreSQL, Oracle DB, MSSQL, ...
  - NoSQL-based systems
    - Hadoop/HBase, Cassandra, MongoDB, Redis, ...

© 2017 UZH, CSG@Ifi
Decentralization

- Decentralized databases
  - Available and used in production
  - Every copy runs on a trusted node
  - But, users (stakeholders) are known/registered

- Can data be stored fully decentralized and handled reliably between non-trusted stakeholders?
  - Unstructured or structured data
  - Access control by “all” without a central root
  - Storage “across the world” by anyone
  - No central point of failure, redundant copies in place, non-trusted participants, detectable misuse
Blockchain Definition and Basics

- **Distributed Ledgers** or **Blockchains** (technology)
  - Digital record of who-owns-what w/o a central storage
    - Ledger is replicated among nodes in a distributed network

- **Consensus algorithm** ensures that each node’s copy of the ledger is identical to every other node’s copy

- Access to ledgers from **asset owners** for transactions via cryptographic signatures and by **miners** with large compute power (PoW) to
  - persist “incoming” data (token=assets) on a (private or) public ledger
  - read/offer “outgoing” data to any other stakeholder (non-private)

- **Advantages** of distributed ledgers:
  - Unforgeable, traceable, and preventing “double spending”
Blockchain Operations

- Transactions collected in blocks
  - New blocks created regularly
- A block contains a pointer to the previous block → Blockchain!
- Consensus mechanism required to determine the block to be integrated into the blockchain
  - Public blocks typically contain solved crypto puzzles
    - *E.g.*, a form of partial hash collisions (SHA256)
- Creation of valid blocks is called mining (reward)
  - Computational expensive → Avoids double spending
  - Mining ≡ confirmation of blocks ≡ solving crypto puzzles
Smart Contracts

- A **Smart Contract** (SC) resides inside transactions
  - Executed and validated on every node
  - In **Bitcoin** (a blockchain-based crypto-currency), SCs specify how to withdraw, escrow, refund, or transfer BTC from A to B
- SCs first mentioned in 1994

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.

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

© 2017 UZH, CSG@ifi
First Practical and General Smart Contracts

- SCs for a crypto-currency, e.g., the Bitcoin scripts
  - Are not Turing-complete
  - Show slow developments and slow feature integration
  - Are characterized by slow consensus finding in its community

- General purpose SCs are needed
  - Ethereum enables Turing-complete SCs
    - Beta Frontier July 2015, Homestead Release March 14, 2016,
    - Hard fork July 20, 2016 after DAO (investor-directed venture capital fund)
  - Permissioned blockchains based on Ethereum
    - Monax (Eris:db) with an additional permission layer
  - Other non-Ethereum-based (target on fast clearing, settlement)
    - Originally R3 Corda: fintech members, “quieter” since mid 2017
Applications
Application Example 1 – Bitcoin

- **Bitcoin** is an *experimental* cryptographic currency
  - Bitcoin is fully peer-to-peer (no central entity, trustless)
  - **Blockchains** applied to reach this goal (sic!)
  - 1\textsuperscript{st} Bitcoin issued on January 3, 2009

- **Key characteristics** (for a maximum of 21 million BTC)
  - Every transaction broadcast to all peers
    - Every peers knows all transactions (~160 GByte as of Nov 2017)
    - Maximum of 7, real life 3-4 transactions per second (1 MB block size)
  - Validation by Proof-of-Work (PoW) consensus mechanism
    - Partial hash collisions, thus, very difficult to fake this type of PoW

- **2\textsuperscript{nd} Hard fork** on Oct 25, 2017 into “Bitcoin gold“
  - To be “mineable“ by more people with less powerful hardware
## Application Domains – Examples

<table>
<thead>
<tr>
<th>Domain</th>
<th>Assets</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Governmental services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Registry of deeds, eVoting, …</td>
<td>X</td>
<td>(X)</td>
</tr>
<tr>
<td><strong>Trading/banking services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Diamonds, cash-heavy, …</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Copyright</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Authorship, ownership, …</td>
<td>X</td>
<td>(X)</td>
</tr>
<tr>
<td><strong>Data and identity management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Records, processes, compliance</td>
<td>X</td>
<td>(X)</td>
</tr>
<tr>
<td><strong>“Chain” support/IoT services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Supply, food, energy, …</td>
<td>(X)</td>
<td>X</td>
</tr>
<tr>
<td><strong>Entertainment</strong></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Cryptocurrencies</strong></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

© 2017 UZH, CSG@ifi
Application Example 2 – Coldchains

- **Pharmaceutical sector (supply chain)**
  - 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: Post 6 CHF, cooled transport 35 CHF → cost saving’s factor 6
    - 60% of medical drugs are not even temperature-sensitive!

- **Solution (incl. vendors, logistic, wholesale, authorities)**
  - Blockchain-based Coldchains (BC4CC) to store temperature data monitored, execute smart contracts on those upon arrival
    - Direct authority access, unknown stakeholders can participate

© 2017 UZH, CSG@ifi
Blockchains for Coldchains Architecture

Developed by CSG@IfI, serves as foundation for modum.io UZH start-up

© 2017 UZH, CSG@IfI
Perceptions and Findings

(preliminary – as of today)
General Perception of Blockchains

- **Stakeholders** involved in (public) blockchains are
  - everyone on the globe (potentially) with Internet access
  - unknown to each other, without any central authority

- **First “appearance” of blockchains**
  - In the context of Bitcoin in 2009
    - First real and experimental crypto-currency
  - Transactions determine data of payments to be persisted, while solving the double spending of electronic “coins”

- **Generalization of non-trusted stakeholder interactions for unforgeable data persistence**
  - Considered to be a disruptive technology?
Concerns and Risks (1)

- **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 as “illegal activity”, asset mapping fraud

- **Technology**
  - **Breaking** of applied **security algorithms** (long-term storage, if signing algorithms will be broken?)
    - Security impacts due to alternative consensus mechanisms?
  - Unknown attack vectors and **programming errors**
    - Privacy: persisted data at stake?
  - **Efficiency** of consensus mechanisms
    - Energy consumption for Bitcoin alone required in 2015 ≈ Mühleberg’s energy production
Concerns and Risks (2)

- **Operations**
  - **Scalability**: Throughput as number of transactions per sec? Volume of data persisted, not bytes but MB? Chain sizes grow faster than density of HDDs/SSDs!
  - **Delay**: Latency of persisting steps, block sizes?
  - Implications on **privacy**: access rights and management?
  - Lacking Internet **connectivity** for a “longer” period of time?
  - **Standardized APIs** for switching applications on top of blockchains at minimal costs (“lock-in” effects?)

- **Economics**
  - **Stability** of coin/token value against fiat currency: volatility?
  - No prevention of making **fraudulent profitability projections**
  - Role, **interrelationships** of more than 1000 crypto-currencies?
Observations

- Distributed apps show a larger coordination effort
- Blockchain’s cost/benefit perspective (incentives)
  - Costs: known in advance (e.g., HW, VM, network, setup, or fees)
  - Benefits: less “central” infrastructure plus “unknown” soft factors
- Once risks are mitigated and legal/regulatory constraints are known, apps may benefit from blockchains, but
  - How to address value destruction problems?
  - ICO vs. traditional emission rules may harm?
  - Country-specific rules will become “international” obstacles?
- Dedicated apps maintaining inherently digital assets do show a much larger (disruption) potential
  - Solving the “media break” may increase this potential
Important to Remember

- Blockchain (technology) is potentially able to:
  - change existing legal contracts including a or multiple trusted third party(ies), *e.g.*, by “replacing”
    - Banks as transaction mediator for fund/Fintech transfers
    - Notaries as mediation of two or more stakeholders, incl. enforcement
  → Trusted communications (incl. documents) are persisted, but *no counseling* is stored

- persist *digital* assets, but not limited to (?) including, *e.g.*:
  - Property, driving licenses, art, diamonds, meat, objects, ...
  → Trusted communications & persisted storage of assets could offer automated operations of ownership and validity checks, *but* lack the proof-of-ownership due to secure mapping problems of tangible assets to digital tokens.

© 2017 UZH, CSG@ifi
Thank you for your attention.