The Use of Blockchains in Commercial Applications and their Related Telco Challenges

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

With many thanks addressed to M. Franco, C. Killer, S. Rafati, B. Rodrigues, E. Scheid, and E. Schiller

Universität Zürich[UZH]

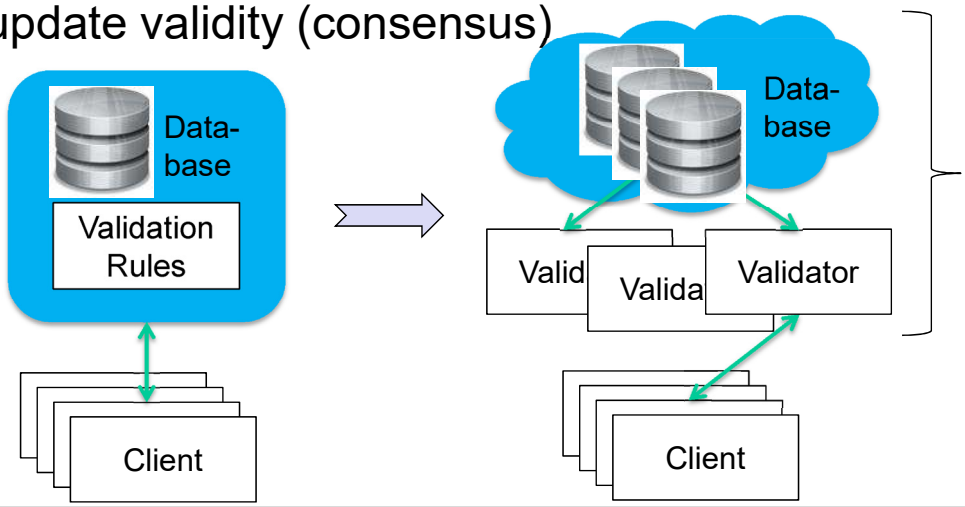
Blockchains
Applications
A Telco Review

CSG
Communication Systems Group

Key Principles

Key Idea: "Replacing" (Central) Databases

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



Based on Terence Spies: Blockchain Mechanics

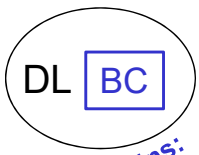
DL/BC Types and Terminology – Simplified

- Private permissioned 

  - Read/write/consensus restricted to authorized nodes (pre-defined stakeholders)
  - "Enterprise-grade" DL

- Public permissioned 

  - Write/consensus restricted to authorized nodes (pre-defined stakeholders)
  - Read open to everyone
  - "Controlled collaborative" DL



No real blockchains: "restricted" stakeholders capabilities!

- Private permissionless
  - Write/consensus restricted to authorized nodes (pre-defined stakeholders)
  - Read partially open 

  - "Consortium-grade" DL

- Public permissionless 

  - Read/write/consensus open to everyone
  - No restrictions and full transparency
  - "Public" BC, **the** BC

The real and only blockchain (BC)!

Definition

- [Distributed Ledgers (DL) or] Blockchains (BC)
  - "Private" BC
  - "Public" BC

  - Digital records of who-owns-what w/o a central storage
  - Consensus Mechanism (CM) ensures that each node's copy of the ledger is identical to every other node's copy

  - Write access to BCs by miners or validators (with data from any asset owner) for transactions via CM and cryptographic signatures, read access at no "costs"

- Key advantages of (public) BCs
  - Immutable, traceable, and preventing "double spending"

"Who-owns-what" Records/Smart Contracts

- A digital asset = an electronic representation, *e.g.*, file
  - Inherently bears the exclusive right of use of this file
- A token (digital token) = digital asset
  - Issued by stakeholder, giving right to participate within network
- A coin (digital coin) = electronic representation of value
  - Specifically designed to represent digital "money" within a network of stakeholders, typically the BC, and beyond

⇨ One can buy a token with a coin, but generally not a coin with a token.

- A Smart Contract (SC) resides inside transactions
  - = code executed "on record" and validated on every node
  - *E.g.*, SCs specify to withdraw, escrow, refund, or transfer coins

Blockchain Ingredients

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

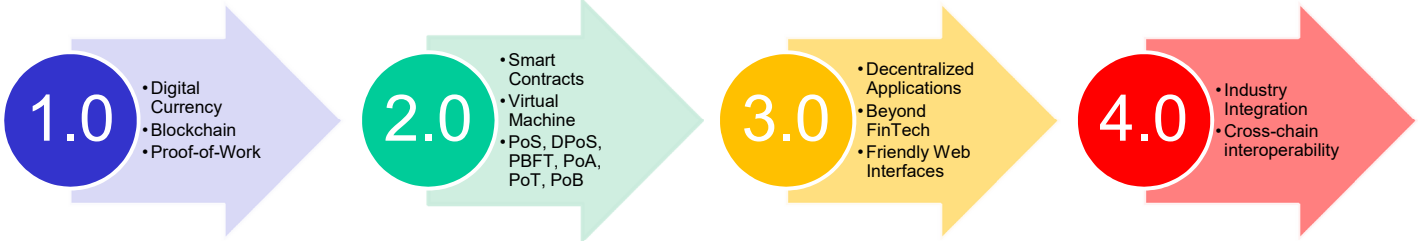
- Internet
  - Networked infrastructure for everyone
  - Distributed system with arbitrary users and devices (nodes)
    - Peer-to-peer (overlay network) communication paradigms: protocol
    - Storage capabilities for “any”-sized data volumes

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

Applications

Blockchain Eras and Evolution

- 4 different BC eras are running in parallel today



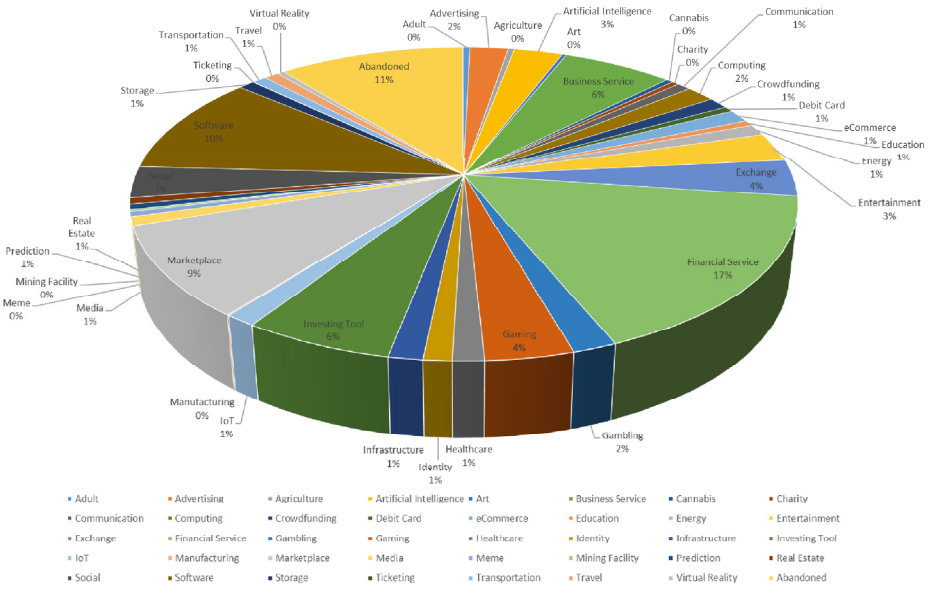
  - 1.0 – December 08/January 09: Bitcoins
    - More than 2900+ cryptocurrencies available today
  - 2.0 – 2012-14: Ethereum, Smart Contracts, Solidity, …
  - 3.0 – April 2012: Decentralized Apps (dApps) – "Satoshi Dice"

https://hackernoon.com/dapp-and-things-you-need-to-know-4f50853a4cb7

    - Running on peer-to-peer network, all data transparent and tamper-proof
  - 4.0 – App. 2015: BC ecosystems and industrial integration
    - Countless Blockchain projects in many fields
      - FinTech, supply-chain, governmental, identity, …

Overview on Cryptocurrencies

- Overview with app. 2900+ cryptocurrencies
  - Based on app. 40+ platforms



Cryptocurrencies: 2493 · Markets: 20293 ·

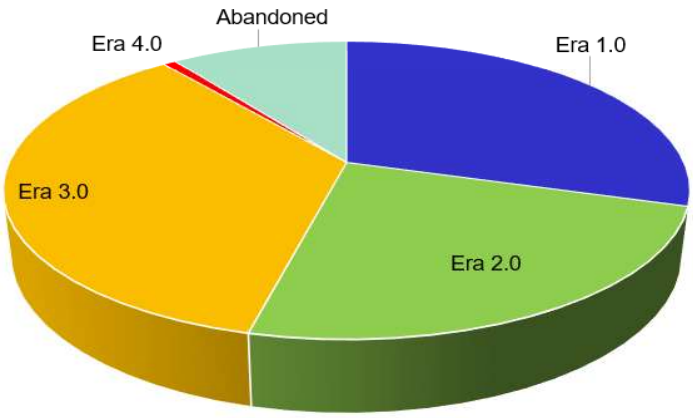
CoinMarketCap

https://coinmarketcap.com/

Application Domains Grouped by BC Eras

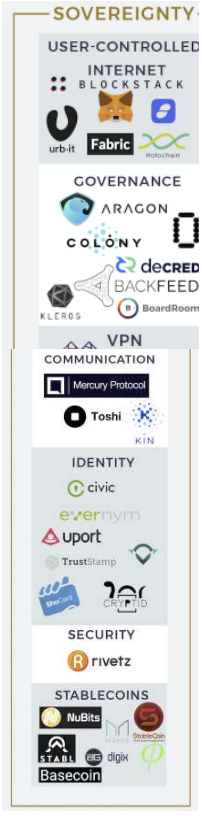
- Similarly, BC projects/domains grouped in Eras
  - Cryptocurrencies and digital finance sector is still dominant
  - However, dApps represents the major number of projects

- Era 1.0 (Finance)
  - 738 projects, 30%
- Era 2.0 (Smart Contracts)
  - 602 projects, 24%
- Era 3.0 (dApps)
  - 884 projects, 35%
- Era 4.0 (Integration)
  - 18 projects, 1%
- Abandoned
  - 248 projects, **10%**

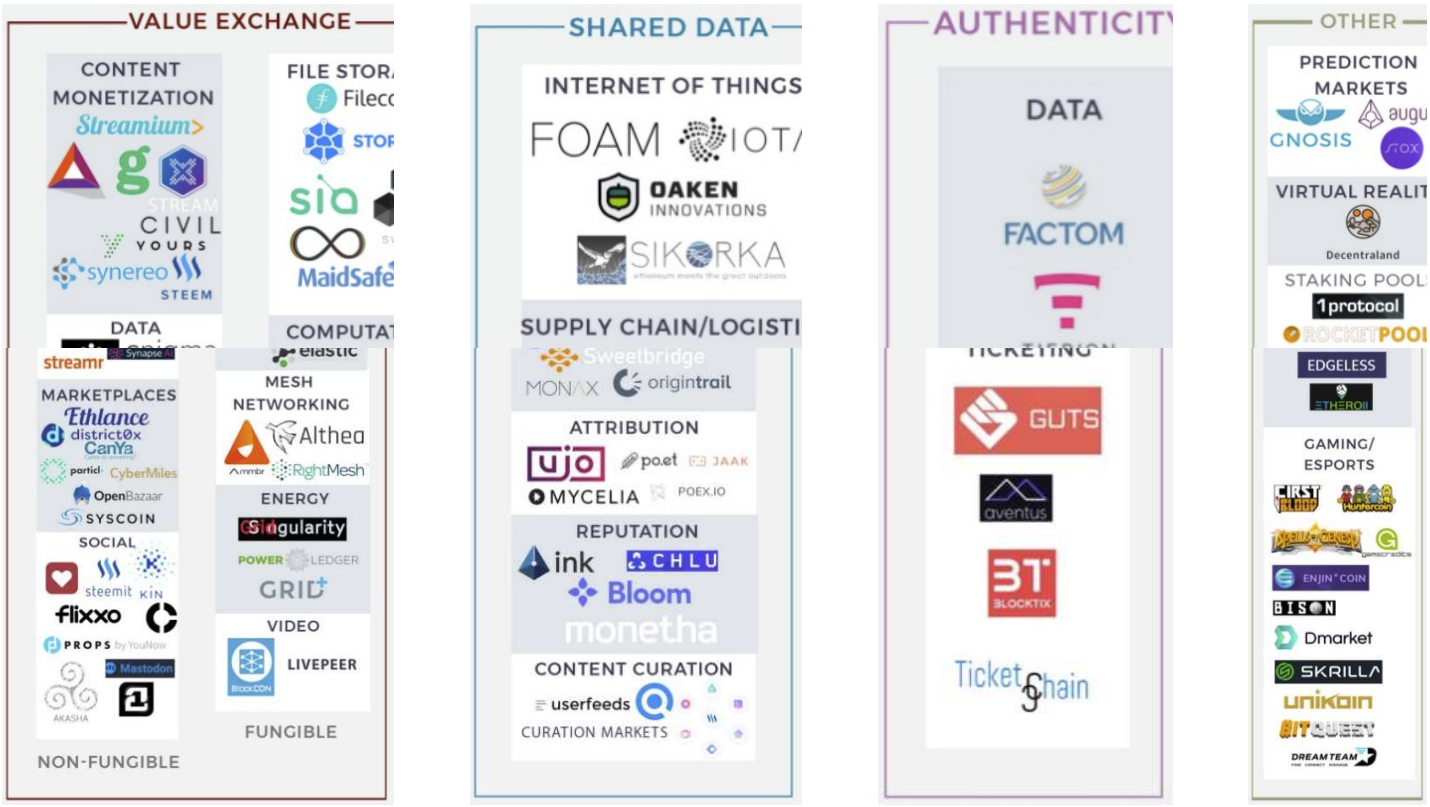


Missing more integration!!

Current Application Domains (1)



Current Application Domains (2)



A Telco Review

Neither Good* nor Bad*, Only “as is”!

* “Good” or “bad” qualifications can be determined from results of evaluations, which depend heavily on models and assumptions!

What's the following?

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

All electronic, algorithmic creation!

A Bitcoin Address in the Pay-to-PubkeyHash (P2PKH) Format

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

… being derived from
A = RIPEMED160(SHA256(K)) with
K ≙ public key of a private-public key pair

What's the following?

18f8ab5e9a5c7e9f3a0c570d56abc37f

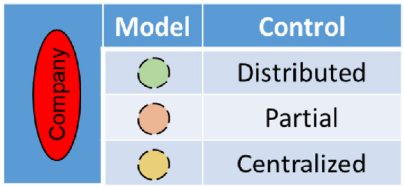
The 256 bit private key of *your* physical asset, the top floor apartment located at 5th Avenue, New York, U.S.A.

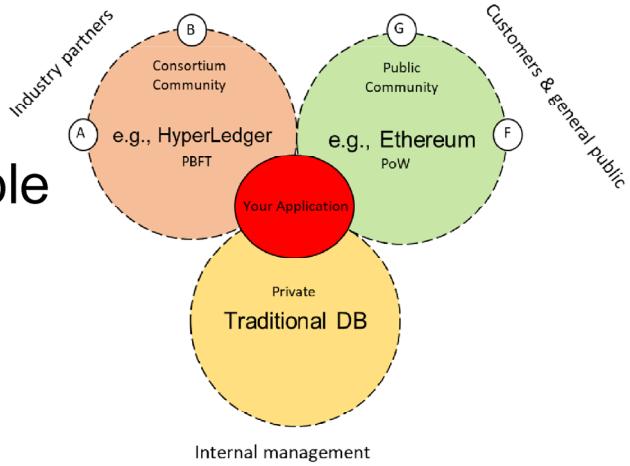
18f8ab5e9a5c7e9f3a0c570d56abc37f

How can someone guarantee that the public part of this key will be "attached" immutably to *your* top floor apartment?

Distributed vs. Centralized (Telco) Control

- Distributed control based on elected leader (*e.g.*, PoW)
- Partial control via selected leaders (*e.g.*, PoA, PBFT)
  - Telco may run a "trusted" consensus node (a selected leader)
- Centralized control (via telco) based on trust (*e.g.*, traditional databases), following co-location model
- Multiple combinations possible





PoW: Proof-of-Work, PoA: Proof-of-Authority, PBFT: Practical Byzantine Fault Tolerance

Application Domains and Role of Telco

Application Domain	Blockchain (BC) Era	BC or Distributed Ledger (DL)	Read (R) and Write (W) Permissions	Mining Permissions (Role of Telco)
Currencies	1.0	BC	Public R/W	All nodes
Developer Tools	2.0	BC	Public R/W	All nodes
FinTech	3.0	DL	Private R/W	Selected nodes
Sovereignty	3.0	DL	Private R/W	Selected nodes
Value Exchange	3.0	DL	Public R, Private W	Selected nodes
Shared Data	3.0	DL	Public R, Private W	Selected nodes
Authenticity	3.0	DL	Public R, Private W	Selected nodes
Networking	3.0	BC	Private R/W	Selected nodes
Interoperability	4.0	BC	Public R/W	Selected nodes

Potential Telco Opportunities

*Based on a general observation, characteristics of specific projects within each application domain may vary

Telco and Distributed System Impact Factors

Influencing Factor	Network (Telco)	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.

Conclusions

1. Blockchains ***do*** show a logical evolution of linked lists, however, public BCs “exaggerate” processing demands
   - By design: Proof-of-Work (PoW), but this ensures immutability
   - Note: Telcos not involved in “digital record” or assets as such
2. Public read/write/consensus (BC) ***very different*** than private write/consensus with Distributed Ledgers (DL)
   - BCs with basically no impacts on telcos, but “expensive”
   - All DLs show possible telco services, especially for enterprise-grade, consortium-grade, and controlled-collaborative DLs
3. Blockchains show ***no revolution***, but a typical Computer Science (Abstract Data Type) **evolution** of linked lists
   - But “distribution” of consensus ***does not always*** make sense
     - Any system as of the past has ***not*** been replaced fully by a BC

Thank you for your attention.