IFIP/IEEE IM 2019, Washington DC, U.S.A., April 8-12, 2019

Blockchain Fundamentals – An Assessment of Their Broad Feasibility

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

With many thanks to T. Bocek, M. Franco, C. Killer, M. Knecht, G. Parangi, S. Rafati, B. Rodrigues, E. Scheid, E. Schiller, and others

Fundamentals
Assessment
Challenges and Risks

© 2019 UZH, CSG@IfI

The Decentralized “Internetification“ of Life

Physical Objects

TELEGRAMSTOP.COM T.C.C. ★ WORLDWIDE ★ SERVICING MOST CONTINENTS.

TELEGRAM

MXT344 ORIG LONDON UNITED KINGDOM

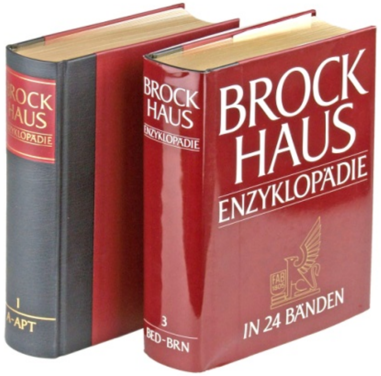
SENT 16 SEP 2010 10025

KATHERINE LONESTAR
77 PILKINGTON PLACE BEDFORD HILLS NY 10507

DARLING KATHERINE -(STOP)- JOURNEY ON THE CONTINENT HAS BEEN LONG AND ARDUOUS -(STOP)- TRAIN WAS INVADED BUT WE HELD THEM OFF WITH OUR CONVERSATION HAHAHA THE FOOLS -(STOP)- ARRIVING SANTA MARINA RAILWAY STATION ON THE TWENTY FOURTH -(STOP)- EXPECT A WELCOME RECEPTION

CAPTAIN DANIEL PERKINS 7.47 PM

Telegram



Encyclopedia

Money

↓ *Ended Dec 29, 2017 in Belgium*

Since mid 70’s, RFC 524

↓

Since 2001

↓

DigiCash®
www.e-gold.com
Second Life
L$
Linden Dollar

Since 2009

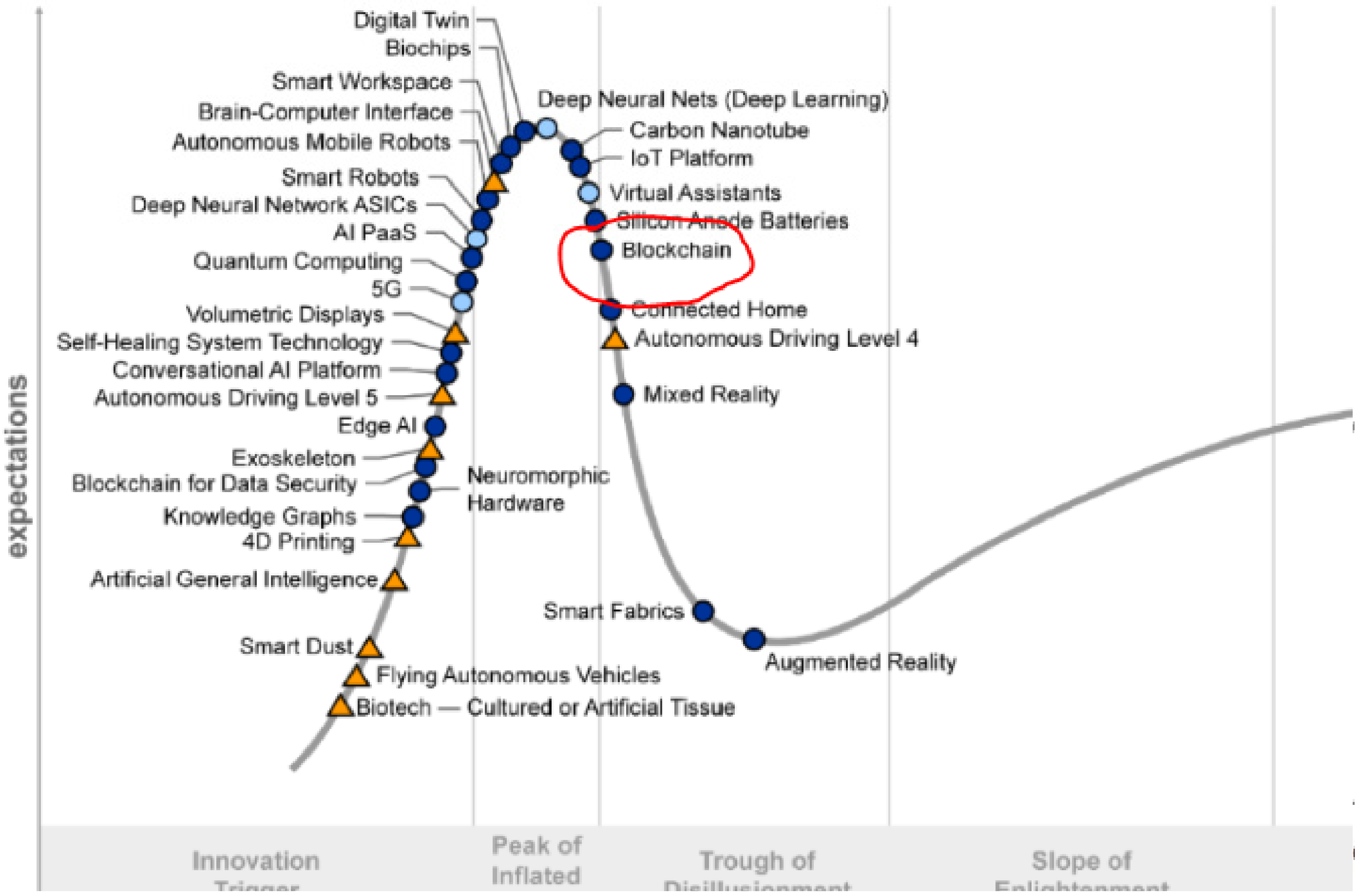
Bitcoins

Digitized Representations

All systems operated as open, networked, and distributed systems!

“A” Certain Blockchain Perception ...

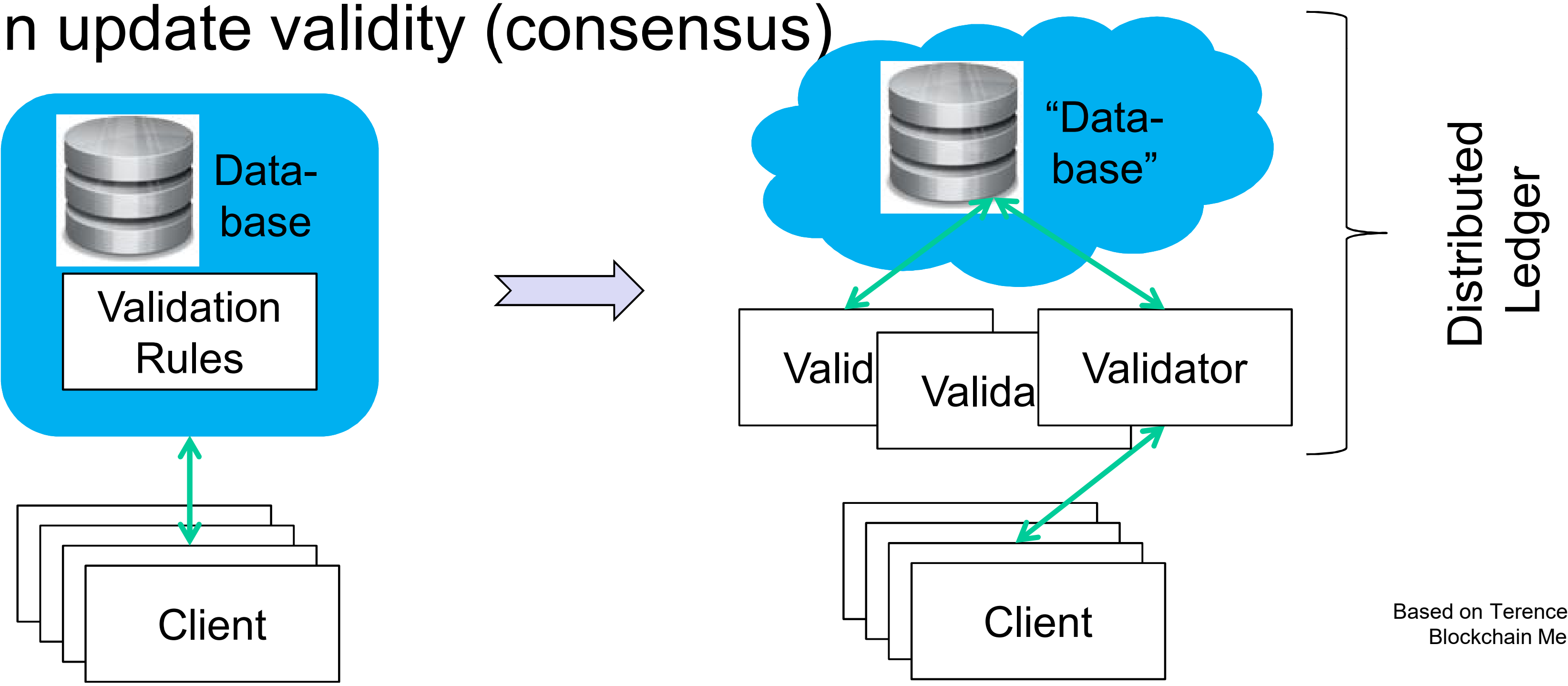
- Blockchain on the Gartner Hype Cycle (2016, 2017, and 2018)



2018

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 agreements of an update validity (consensus)



Based on Terence Spies:
Blockchain Mechanics

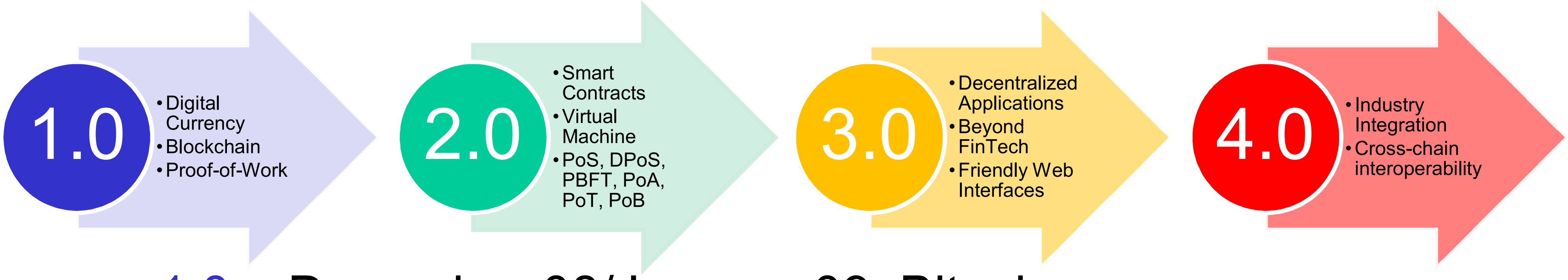
© 2019 UZH, CSG@IfI

Blockchain Definition

- Distributed Ledgers (DL) or Blockchains (BC)
  - Decentralized and public digital ledgers, transparently and permanently storing records across a network based on a consensus algorithm without modifying previous blocks
    - Digital record of who-owns-what (token, asset) w/o a central storage
      - 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 (distributed system)
    - Access to ledgers by everyone (public, permissionless) or more recent by dedicated stakeholders only (private, permissioned) 🔓 or 🔒
      - Writing = persisting “incoming” data (token, asset) on ledger
- Key advantages of BCs
  - Immutable, traceable, no intermediary, open to everyone, and preventing “double spending” (relevant for assets/tokens)

Blockchain Eras and Evolution

- ❑ 4 different BC eras are running in parallel today

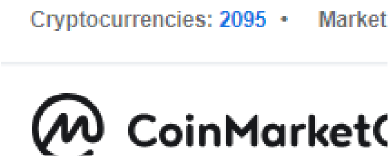


1.0
- Digital Currency
- Blockchain
- Proof-of-Work

2.0
- Smart Contracts
- Virtual Machine
- PoS, DPoS, PBFT, PoA, PoT, PoB

3.0
- Decentralized Applications
- Beyond FinTech
- Friendly Web Interfaces

4.0
- Industry Integration
- Cross-chain interoperability



Cryptocurrencies: 2095 • Market

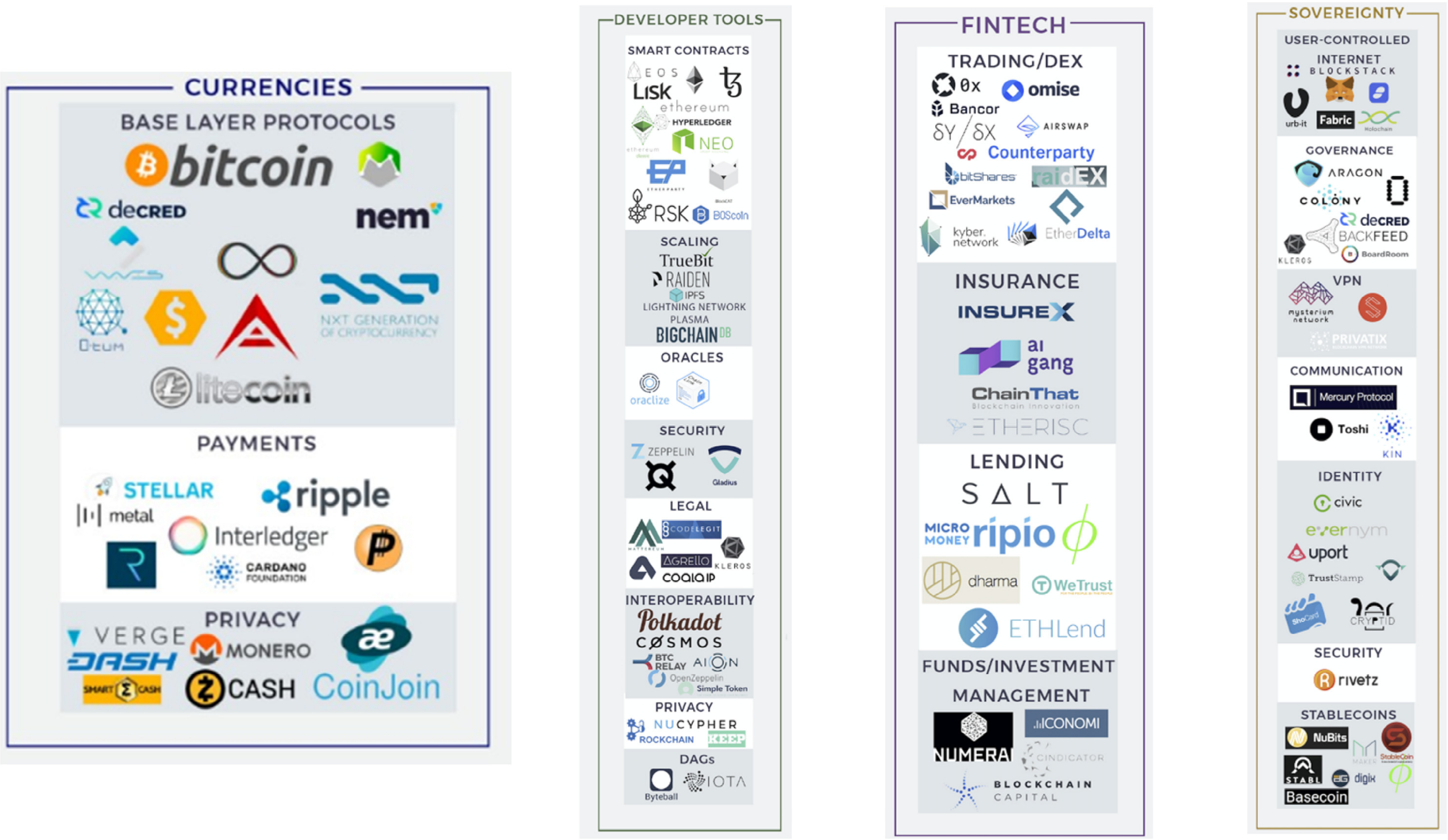
CoinMarketC

– 1.0 – December 08/January 09: Bitcoins
  - More than 2100 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

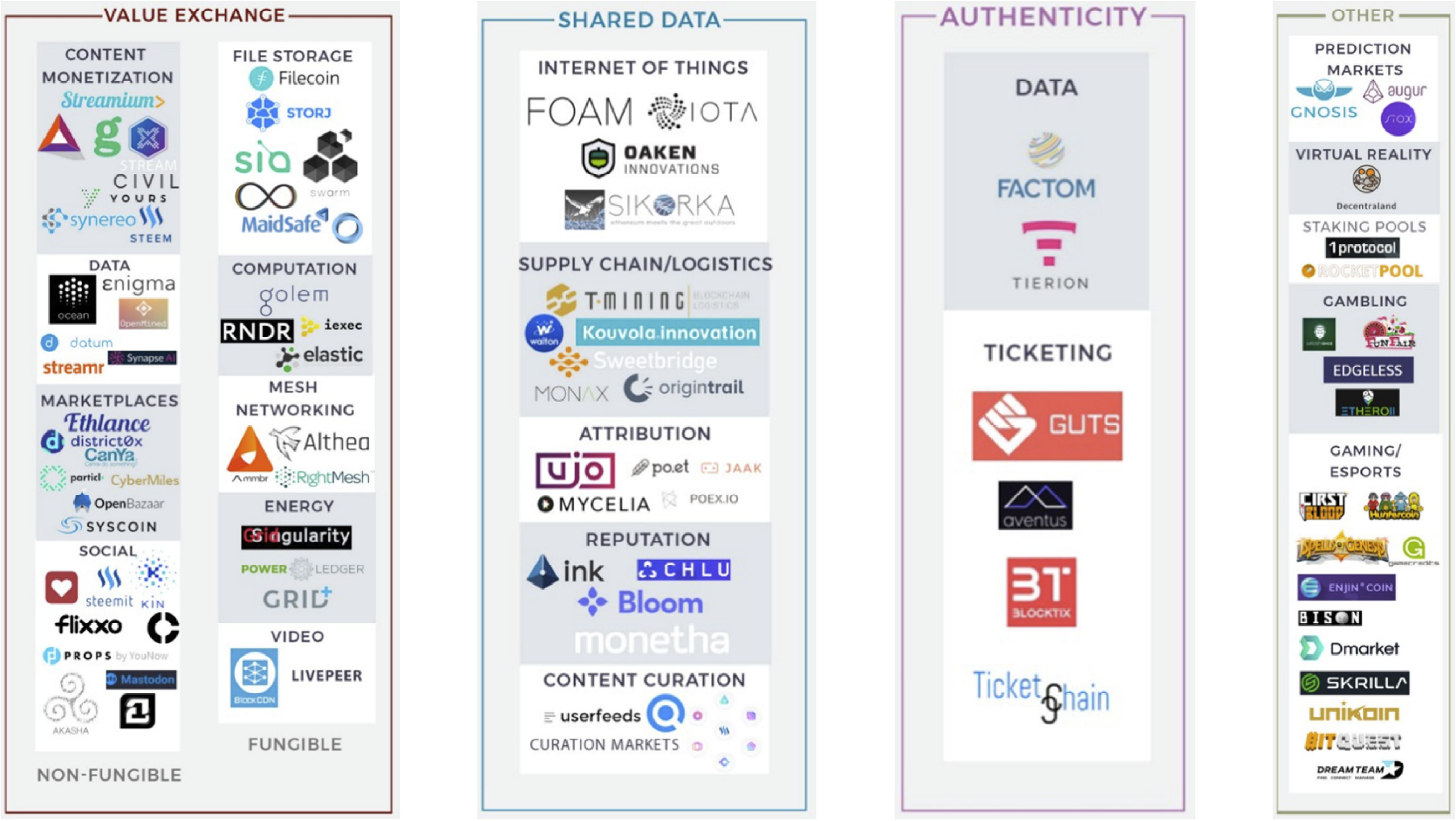
  - Running on peer-to-peer network, all data transparent and tamper-proof
– 4.0 – App. 2015: BC ecosystems and industrial integration
  - Countless Blockchain projects in many fields
    – FinTech, supply-chain, governmental, identity, …

Blockchain Fields (1)



: https://medium.com/@josh_nussbaum/blockchain-project-ecosystem-8940abababaf27

Blockchain Fields (2)



: https://medium.com/@josh_nussbaum/blockchain-project-ecosystem-8940ababaf27

CSG@UZH Blockchain Research

- Coinblesk – A real-time Bitcoin payment Android app (2014-2016)
- Blockchains for Coldchains (temperature, IoT) – modum.io SME founded (ICO in Sept 2017: 13.5 mil US$, KYC'ed) (since 2015)
- Foodchains – Tracing and tracking (since 2015)
  - Swiss Federal Office for Agriculture: highly quality diary products tracing
- Collaborative DDoS Mitigation Based on Blockchains (since 2016)
- Edu Chain: Blockchains for UZH certificates and diploma checks (2017-2018)
- Cryptocurrency Bazo from scratch (since 2017)
  - Proof-of-Stake, mobile light client, blockchain-based loyalty program
- Blockchain-based E-Voting (since 2017)
  - Privacy, verifiability, auditability, secure cast-as-intended
- Smart Contract-based Frameworks (since 2017) – IoT pollution mgt.
- Studies on "Off-chain Data Storage Tools", "Identity Management"
  - Steady support of startups: modum.io, ScienceMatters, ICOnator

Mechanisms for Distributed Agreement

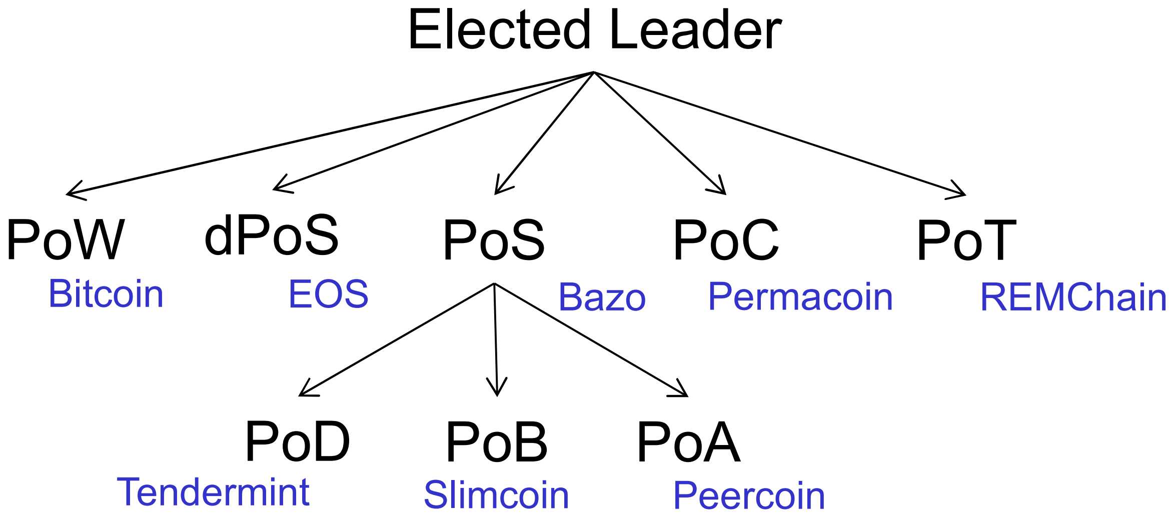
- ❑ Distributed consensus algorithms

- ❑ The key characteristics
  - – Uniform agreement
    - No two nodes decide differently
  - – Integrity
    - No node decides twice
  - – Validity
    - If a node decides on value *v*, then *v* was proposed by some node
  - – Termination
    - Every node that does not crash eventually decides on some value

https://pradeeploganathan.com/blockchain/consensus/

Consensus Mechanisms (1)

- ❑ Classical Consensus Models
  - – Crash failure models → honest nodes failing
  - – Byzantine Failure Tolerance (BFT) HyperLedger (SOLO, Kafka mechanisms), Stellar
    - Capacity of a system to handle or survive unreliable situations, failures
    - Practical BFT (PBFT): small fraction of nodes as Byzantines (dishonest)
- ❑ Elected Leader Models



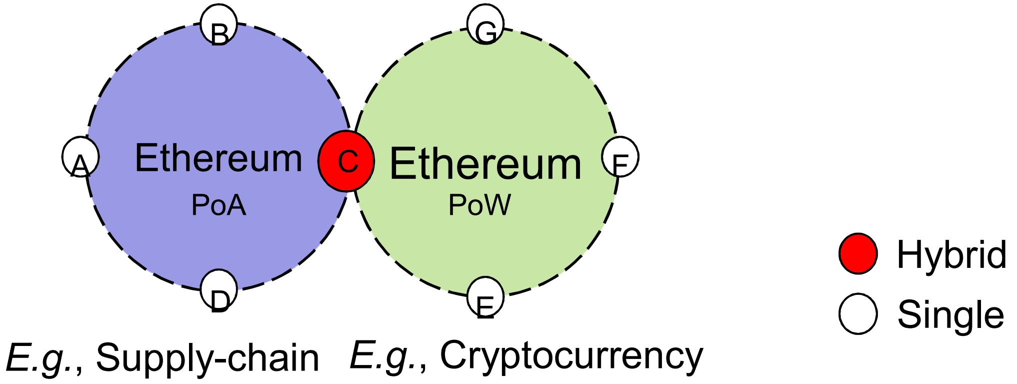
PoX: Proof-of-X, where *X*=

A: Age
B: Burn
C: Capacity (storage)
D: Deposit
S: Stake
T: Trust
W: Work
d: delegated

© 2019 UZH, CSG@IfI

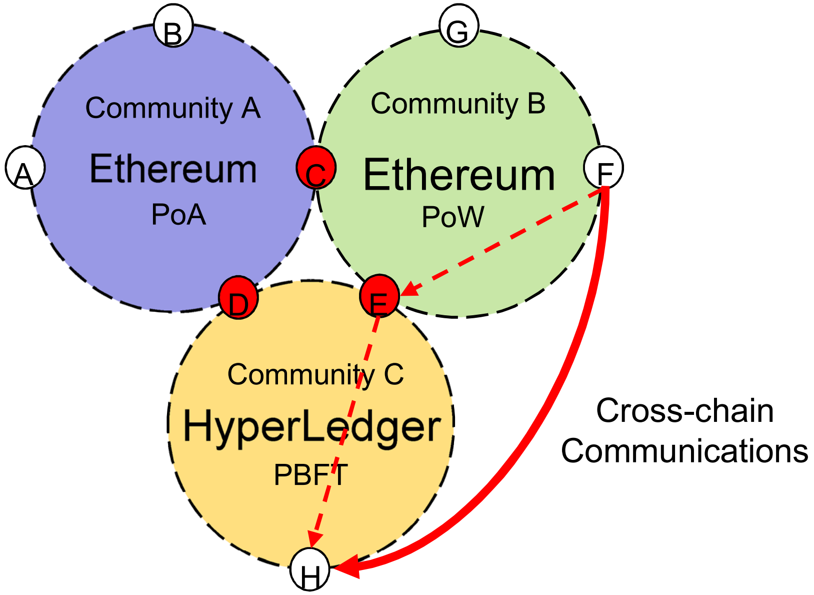
Consensus Mechanisms (2)

- Hybrid Consensus Models
  - Using a single consensus results in limitations
    - Combination of different consensus mechanisms



E.g., Supply-chain *E.g.*, Cryptocurrency

- Hybrid Sharding
  - System can be organized into shards (communities)
    - Cross-chain communications
    - Applied by CSG's Bazo BC



Now skipping all further details on

who-owns-what w/o a central storage relations,
Merkle trees and blocks,
ingredients and transaction handling,
chain pruning, and
disintermediation

… , but be flagged on:

Blockchain Types

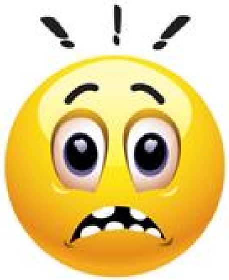
- A public/permissionless blockchain
  - BC open to any stakeholder (no relations)
    - → Contributions to the processing of transactions and blocks
  - No dependency on any prior identity of any kind
  - Examples: Bitcoin “Grandfather BC”, Ethereum, …

The real and only blockchain!

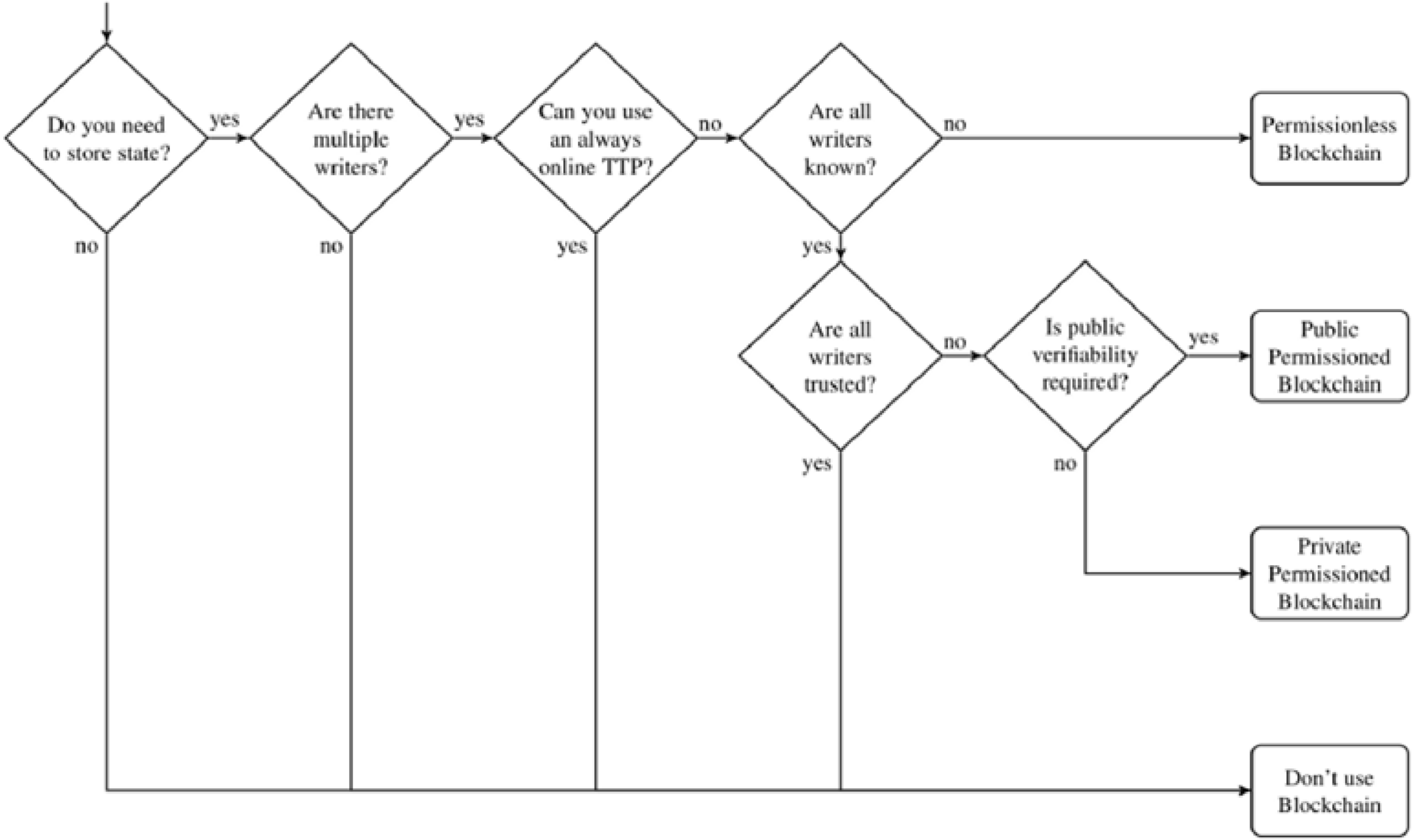
- A private/permissioned “blockchain”, better a DL
  - Chain open to permissioned (known) stakeholders
    - Transaction processing is accessible, processed, and validated by those stakeholders only, who are known to the BC “creator/owner”
    - → Contributions count according to the rules the BC applies
  - Examples: Hyperledger, Corda, consortium-based, …

No real blockchain: limited stakeholders!

Blockchain Assessment



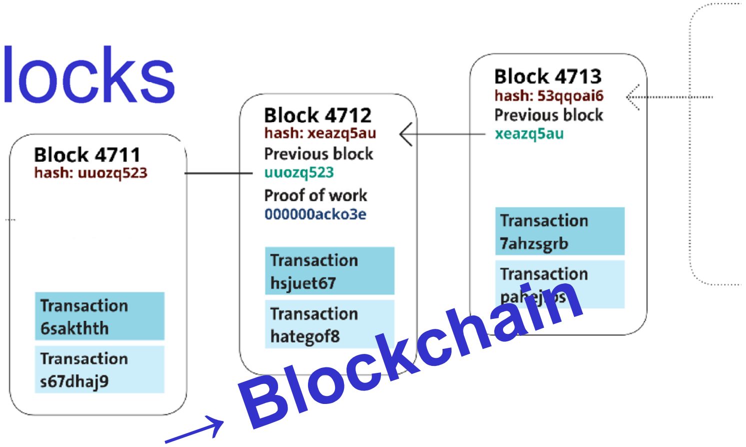
Blockchain Demand “Checker”


Do you need to store state?
yes
no
Are there multiple writers?
yes
no
Can you use an always online TTP?
no
yes
Are all writers known?
no
yes
Are all writers trusted?
no
yes
Is public verifiability required?
yes
no
Permissionless Blockchain
Public Permissioned Blockchain
Private Permissioned Blockchain
Don’t use Blockchain

K. Wüst, A. Gervais, 2017

Blockchain Operations

- Transactions (content) collected in blocks
  - New blocks created regularly (blocktime)
- 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
  - *E.g.*, 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

BC Operations' Assessment

- ❑ Trust (depends on consensus mechanism, cryptography)
  - – "No" power to change or delete previously persisted block
    - Auditability, traceability for data of a transaction
- ❑ Decentralization (full autonomy)
  - – No-one "owns", no single instance controls the BC
    - Immutability, no single-point-of-failure
- ❑ Integrity
  - – State of a transaction cryptographically secured (signed)
    - Privacy depends on handling of the blocks/transactions content
- ❑ Sustainability
  - – Depending on the consensus mechanism

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

“Active” database!

- SCs first mentioned in 1996

> 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

- SCs alone are not “smart”
  - They need an infrastructure (“technology“)
  - A blockchain forms ***the*** ideal, distributed basis for SCs
- Ethereum: BC with Turing-complete SC language (Solidity)

SC's Assessment

- Trust (depends on consensus mechanism, cryptography)
  - – "No" power to change or delete previously persisted SC
    - Auditability, traceability for the processing of data of a transaction
- Decentralization (full autonomy)
  - – No single instance controls the processing of a SC
    - Immutability, no single-point-of-failure
- Integrity
  - – State of SC and processing results cryptographically secured
- Costs
  - – Depend on the SC and the exchange value of tokens in use
- Legal relevance of "coded", more general contracts?

Challenges & Risks

What’s the following?

18f8ab5e9a5c7e9f3a0c570d56abc37f

The 256 bit private key of *your* asset, the apartment located at Pennsylvania Avenue Northwest, Washington DC!

18f8ab5e9a5c7e9f3a0c570d56abc37f

BC Advantages and Drawbacks

Selection only!

Characteristics	Advantages	Drawbacks	Remarks
Distributed	No central control, no “master” needed	No central control, no “master” exists	Censorship vs. conflict resolution!
Unknown stakeholders	Everyone can participate	Lacking control of participants’ “writes”	Application-specific needs
Open, transparent	No hiding possible	Stakeholders’ activities publicly viewable	Application-specific needs
Immutable	Once persisted, persisted forever	Wrongly deployed SC(s) not retractable	Realistic for “useful” SCs? GDPR?
Append-only	No deletions	Growing in size	GDPR compliance?
Traceable	Proof of actions	No hiding of actions	Error handling?
Technical aspect	Effective	Efficiency, energy dem.	Sustainability?
Economic aspect	Cryptocurrency (fully elect., decen.)	Impacts on economic stability, currencies, …	Survivability of too many “tokens” or “coins”?
Legal aspect	Contracts without intermediary	“Unknown” conflict resolution instance(s)	No jurisdictional borders, enforceability?

Blockchain to Database Comparison

		Blockchains (BC)	Databases (DB)
Operations	Operations	Insert, read	Insert, read, delete, update
	Replication	Full replication	*E.g.*, master-slave model
	Consensus	Majority of nodes agree on outcome of transactions	Distributed transactions
	Invariants	Any node can validate transactions	DB manager in charge of validation
Characteristics	Disintermediation	Fully reached for public BCs Partially reached private BCs	Central management (logical view), while physical distribution possible
	Performance	Still limited for public BCs “Increasing” for private BCs	All scales reachable
	Reliability	As distributed systems can be	Based on failover and redundancy mechanisms applied
	Integrity	Dependent on consensus protocol	Typically based on ACID principle
	Confidentiality and Privacy	Partially reachable for public BCs Fully reachable for private BCs	Dependent on access control regime and storage regulations of DB
	History	Fully achieved since start	Only partially, DB archiving function

Public Blockchain Challenges

Selection only!

Solutions seem possible

- How to handle reliably tangible (non-digital) assets in BC?
  - A token is represented in bits vs. property/real estate as physical items
- Sustainability: Energy efficiency of consensus mechanisms?
  - Energy consumption for Bitcoin BC alone in 2017 ≈ Iceland‘s production
- Scalability: BC throughput as a number of transactions per second, volume of data persisted in Mega (?) bytes, costs?
  - *E.g.*, BC sizes grow faster than the density of HDDs/SSDs
  - BC (always) better than a (distributed) data base? Exorbitant costs?
- Identity management (users, objects) and anonymity
- Standardized APIs for switching BCs for BC-based dApps
  - *E.g.*, in contrast, databases from different vendors offer “similar” APIs
- Many economic effects of BC-based cryptocurrencies unknown
  - Role of national “e”-currency, interrelationships of about 2100+ cryptocurr.
- Legal/regulative compliance, societal/governmental acceptance

© 2019 UZH, CSG@IfI

Public Blockchain Risks

Selection only!
Fundamental concerns

- ❑ BCs' "true semantics" depend on the input received!
- ❑ BCs' security, privacy, and reliability
  - Unknown attack vectors (& 51% attack), Programming errors in SCs
  - Alternative consensus mechanisms beyond PoW? Security at stake?
  - – The breaking of currently used security algorithms
    - Long-term storage? Quantum Computing impacts?
  - – Privacy: persisted data at stake? GDPR?
    - – The right to forget vs. immutability
    - – Transparency (public knowledge of BC) vs. privacy (private data)

GDPR: General Data Protection Regulation

- ❑ Networking infrastructure's reliability (critical infrastructures)
  - Lacking Internet connectivity for a "longer" period of time?
- ❑ Economic/legal risks (cryptocurrency/tokens/coins, BC)
  - Fraudulent profitability projections, volatility, dispute resolutions

Conclusions

1. Blockchains ***do*** show a logical evolution of linked lists, however, public BCs “exaggerate” processing demands
   - Especially Proof-of-Work (PoW), but this ensures immutability

2. The technical future of blockchains is based on ***security ingredients*** of today’s technology, however, long-term storage/security management is not known by now
   - *E.g.*, unknown impact of quantum computing (certainly on all IT!)

3. Blockchains show ***no revolution***, but a typical Computer Science (Abstract Data Type) **evolution** of linked lists
   - The “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.