WS on Blockchain and Smart Contracts: Technology, Applications, and Legislation
Université de Neuchâtel, Switzerland, November 15, 2018

Blockchain Applications and their Applicability

Bruno Rodrigues
Communication Systems Group CSG
Department of Informatics IfI
University of Zürich UZH
rodrigues@ifi.uzh.ch

With many thanks to Thomas Bocek, Sina Rafati, Eder Scheid, Burkhard Stiller, and others

University of Zurich[UZH]

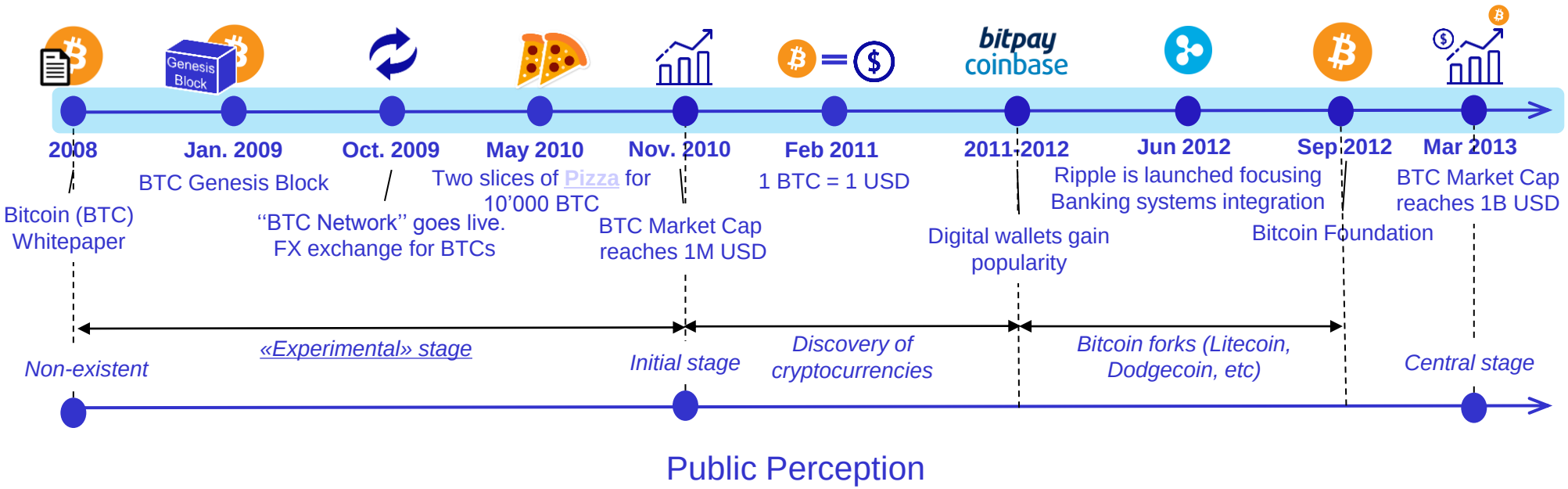
Introduction
Blockchain Basics
CSG Applications
Blockchain Applicability
Conclusions

CSG
Communication Systems Group

Introduction

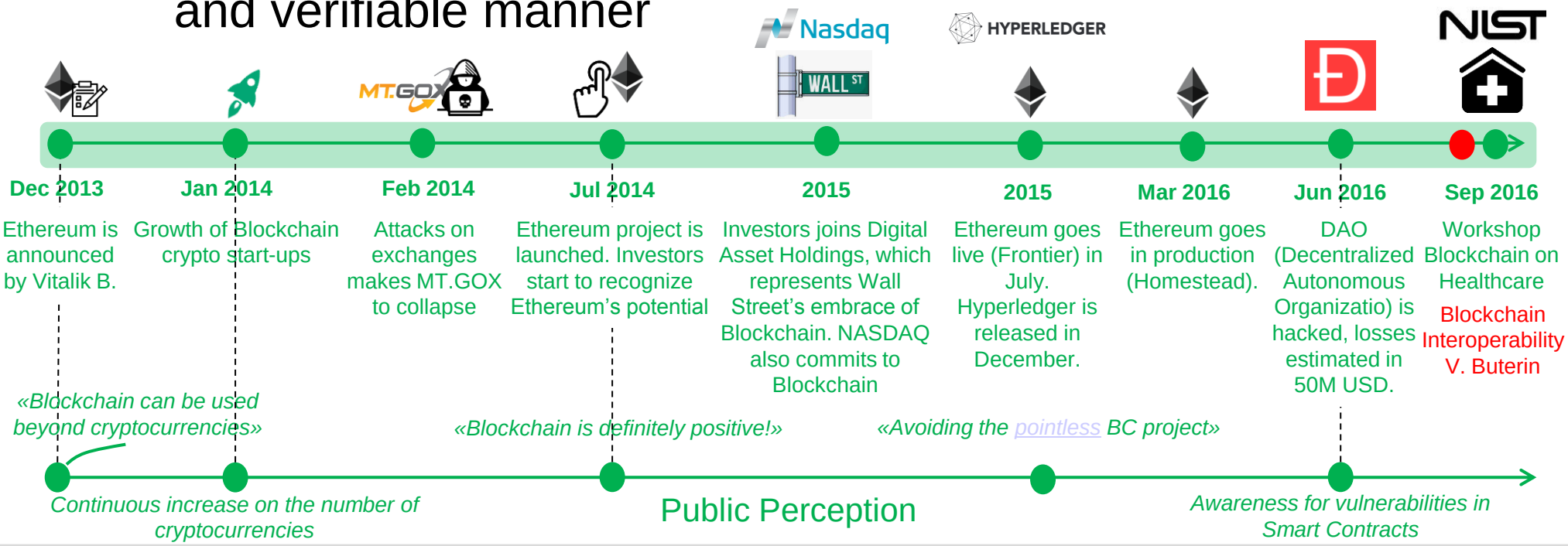
Blockchain 1.0

- Digital Currency
  - Decentralized payment system
  - Bitcoin as the father of digital currencies
    - Still, not much awareness of (other) Blockchain capabilities
  - Proof-of-Work (PoW)



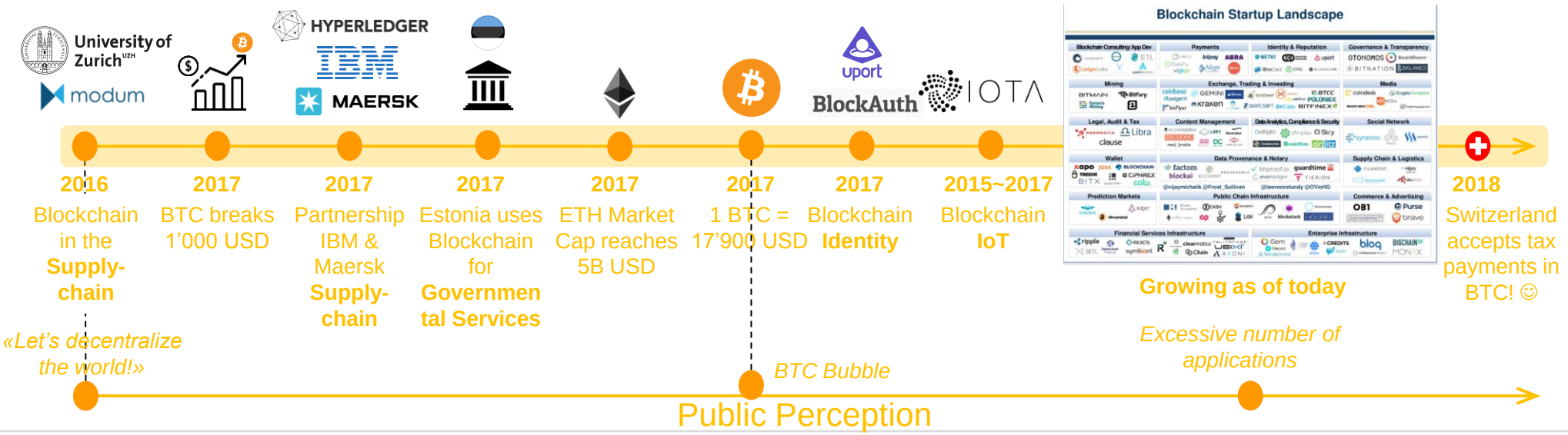
Blockchain 2.0

- Smart Contracts
  - Ethereum unlocks the blockchain potential beyond cryptocurrencies
  - Blockchain is able to run computer programs in a transparent and verifiable manner



Blockchain 3.0

- Decentralized Applications (DApps)
  - Production stage:
    - Large number of applications
  - Scalability/Performance issues:
    - Need for performance → new consensus protocols
    - Need for storage → off-chain storage tools



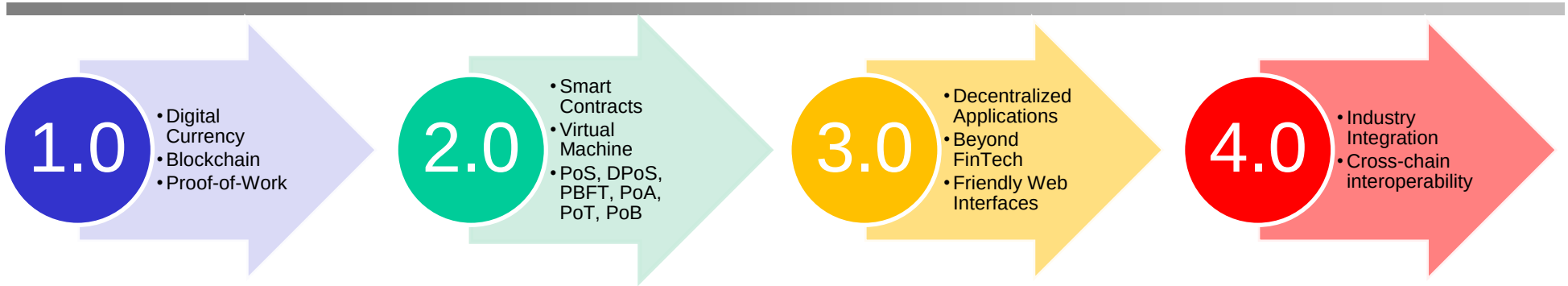
Blockchain 4.0

- Ecosystem and Industry Integration
  - Making blockchain effective in industry
  - Decentralized and disconnected blockchain networks
    - Vendor-specific blockchain technology, interoperable chains
  - Need for standardization

As of today

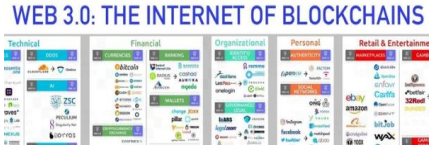
origintrail
wanchain
COSMOS INTERNET OF BLOCKCHAINS
ARK.io
Ambrosus
BLOCKONOMI
aelf.
HERDIUS
Seele
blockstack
AION The Third Generation Blockchain Network
INTERLEDGER Payments across payment networks
MULTIVERSUM HERE TO STAY
Polkadot.
CROWD MACHINE

The Blockchain Evolution



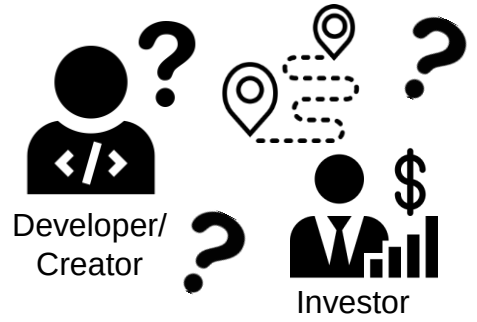
- The different “eras” are running in parallel
- There are more than 2000 cryptocurrencies available as of today.
  - And the list is still growing

- Countless Blockchain projects in many areas (supply-chain, health-care, governmental, identity, cross-chain interoperability, etc).



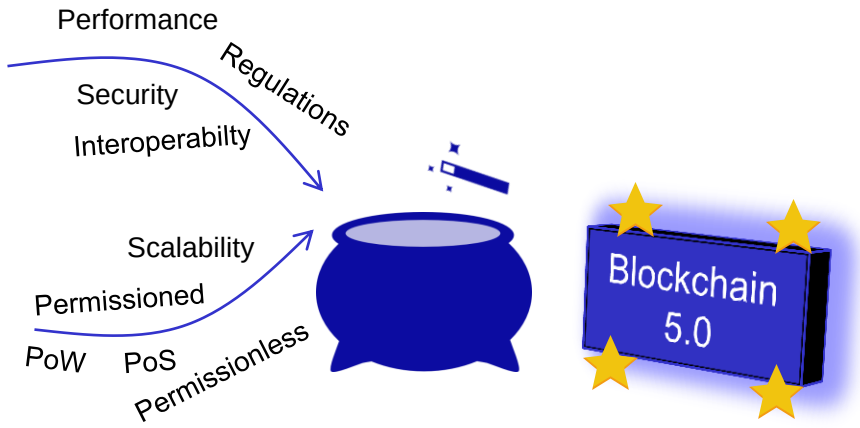
Driving Questions

- How and under which conditions to use Blockchain?
  - Creator or investor points-of-view
- Is there right or wrong? A roadmap for blockchain usage?
  - There is no simple answer…



Application — *"What are the application requirements?"*

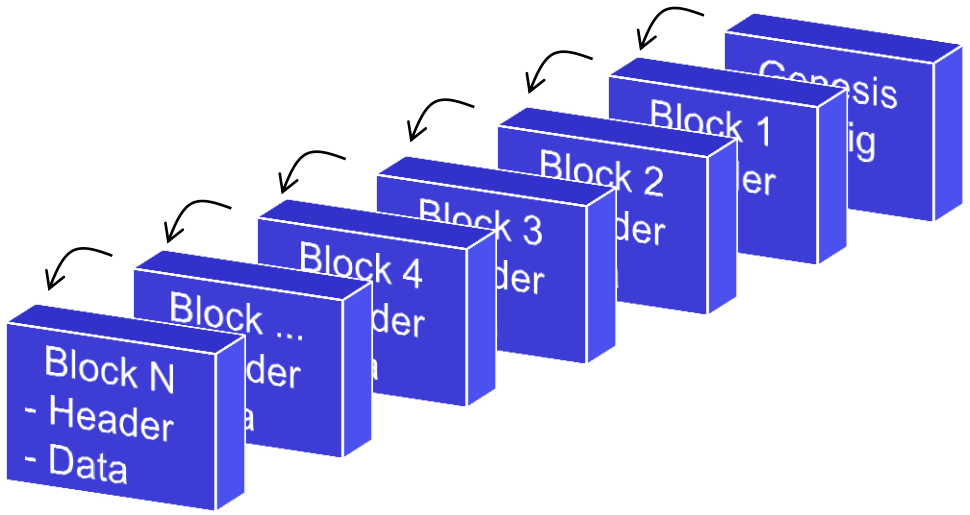
Blockchain — *"What the different types of blockchain can offer you?"*



Blockchain Basics

Definition

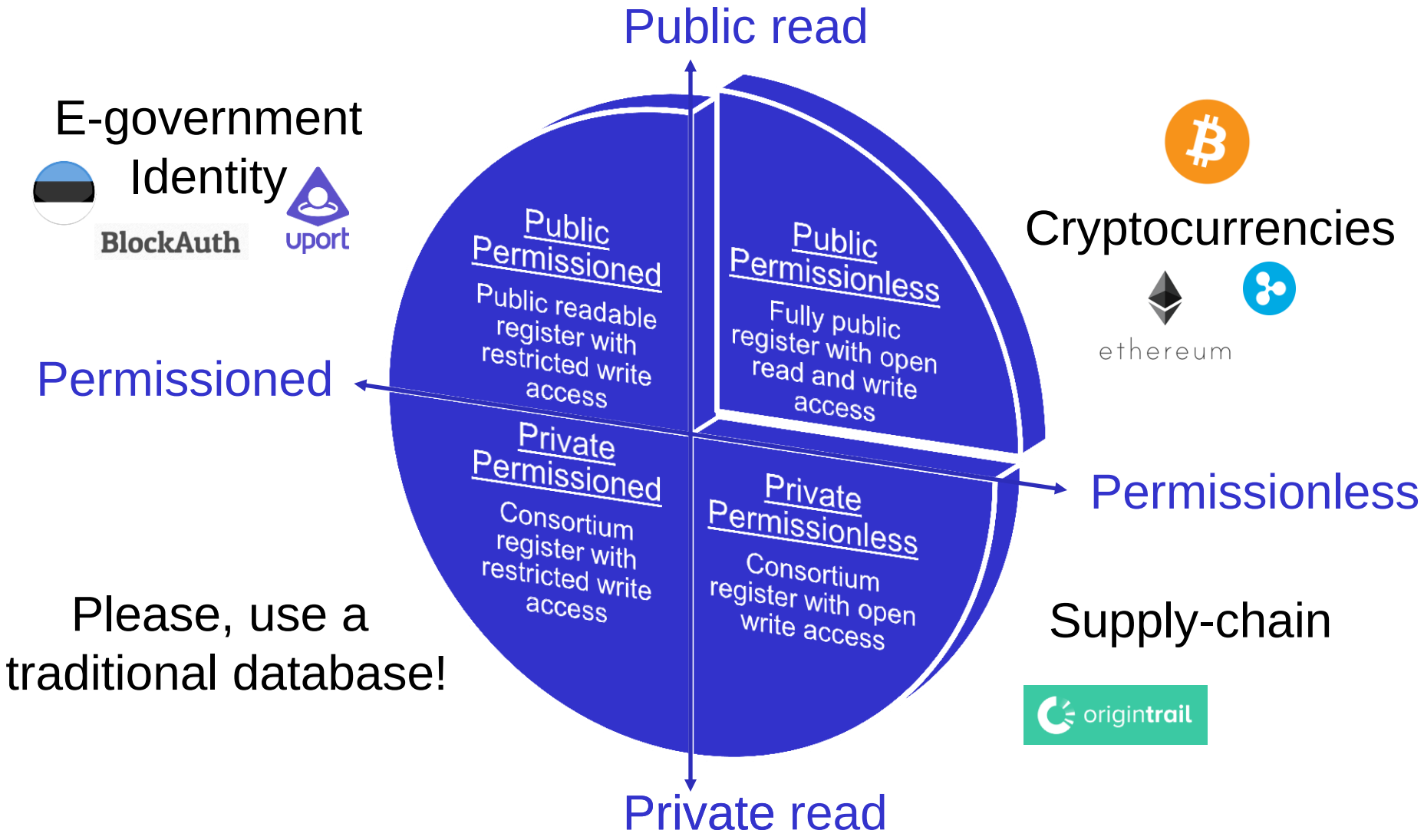
- A Blockchain in its "*pure*" form is a decentralized and public digital ledger that transparently and permanently record blocks of transactions across computers based on a consensus algorithm without modifying the subsequent blocks.



ethereum

bitcoin

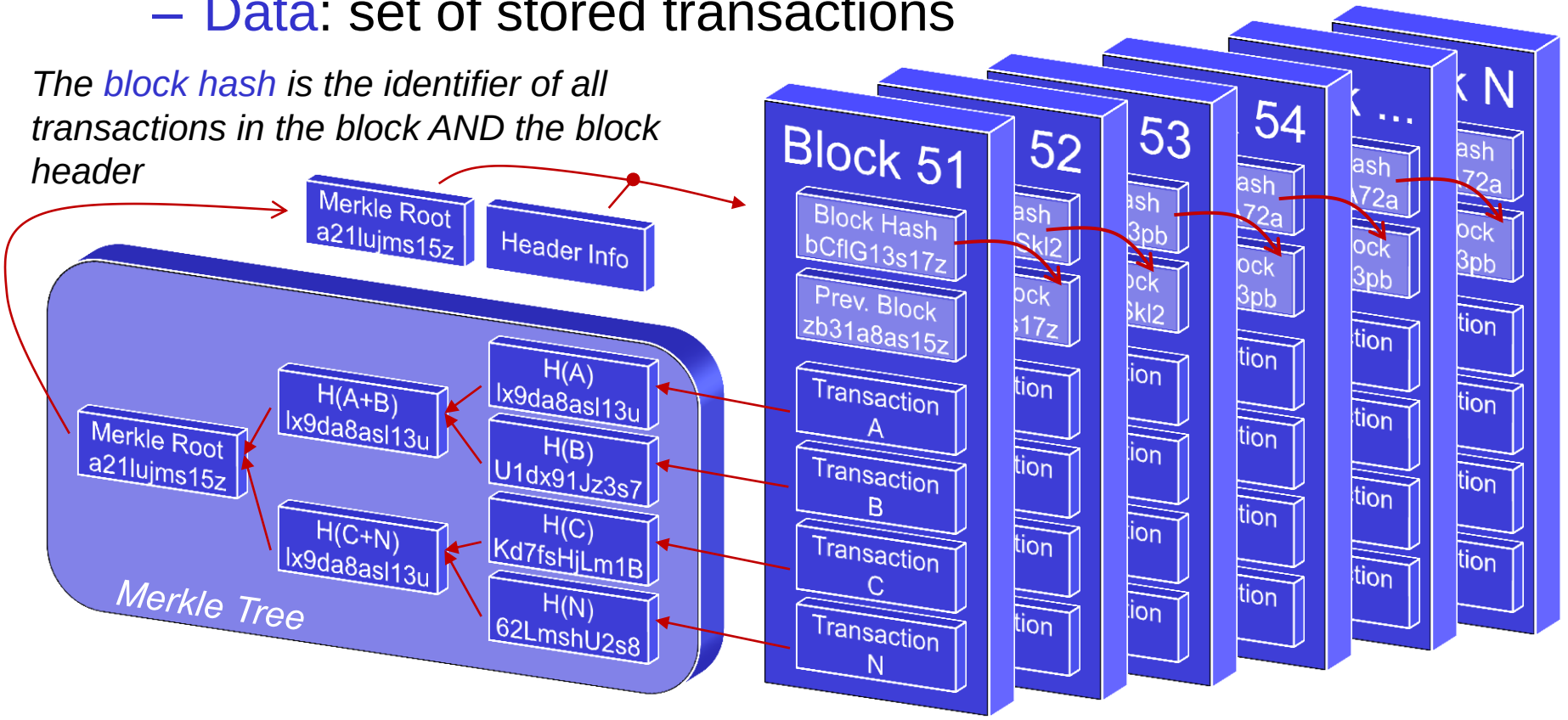
Permissions and Transparency



Block

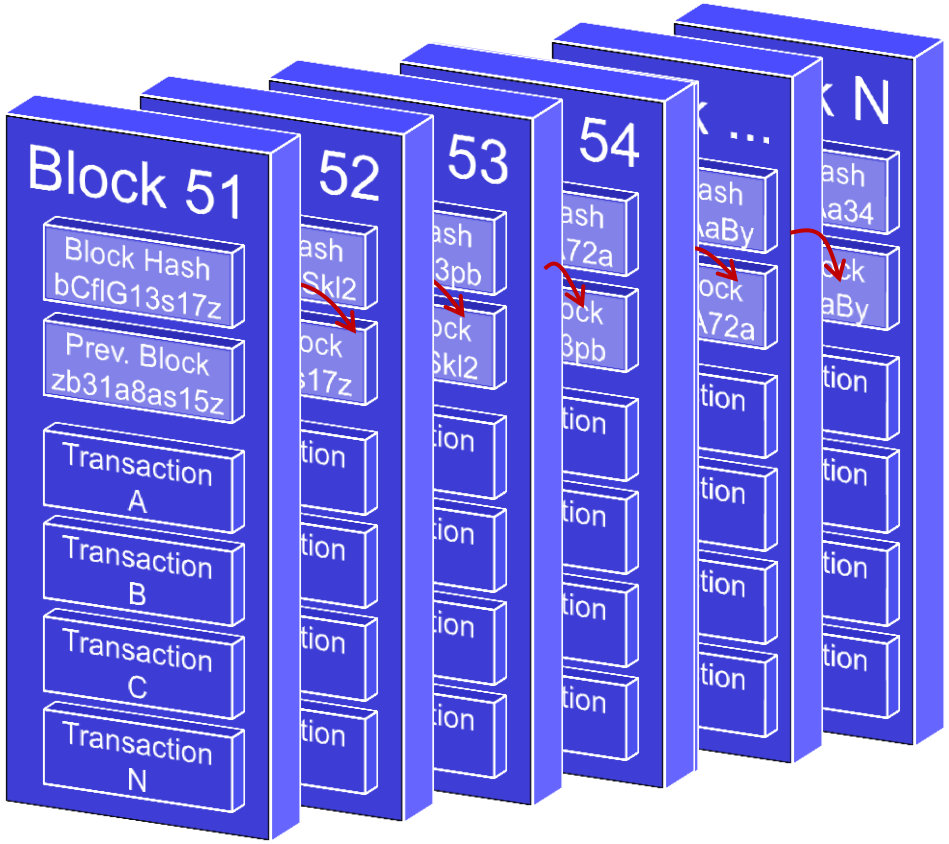
- A block is a structure to store data (transactions)
  - Header: information to identify the block.
  - Data: set of stored transactions

The block hash is the identifier of all transactions in the block AND the block header

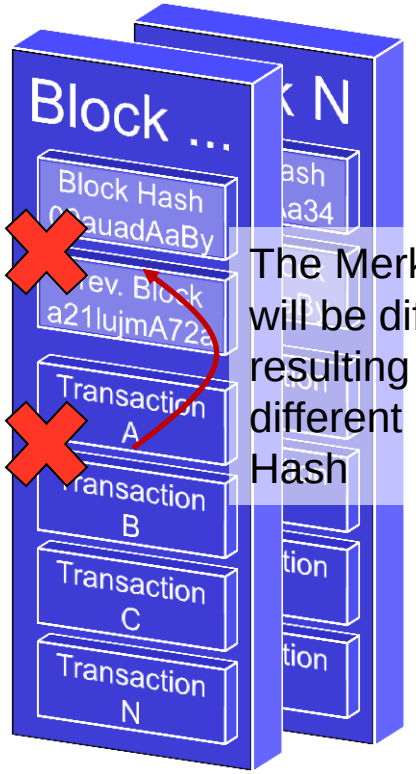


Merkle Tree

- In practice, the Merkle Tree guarantees immutability



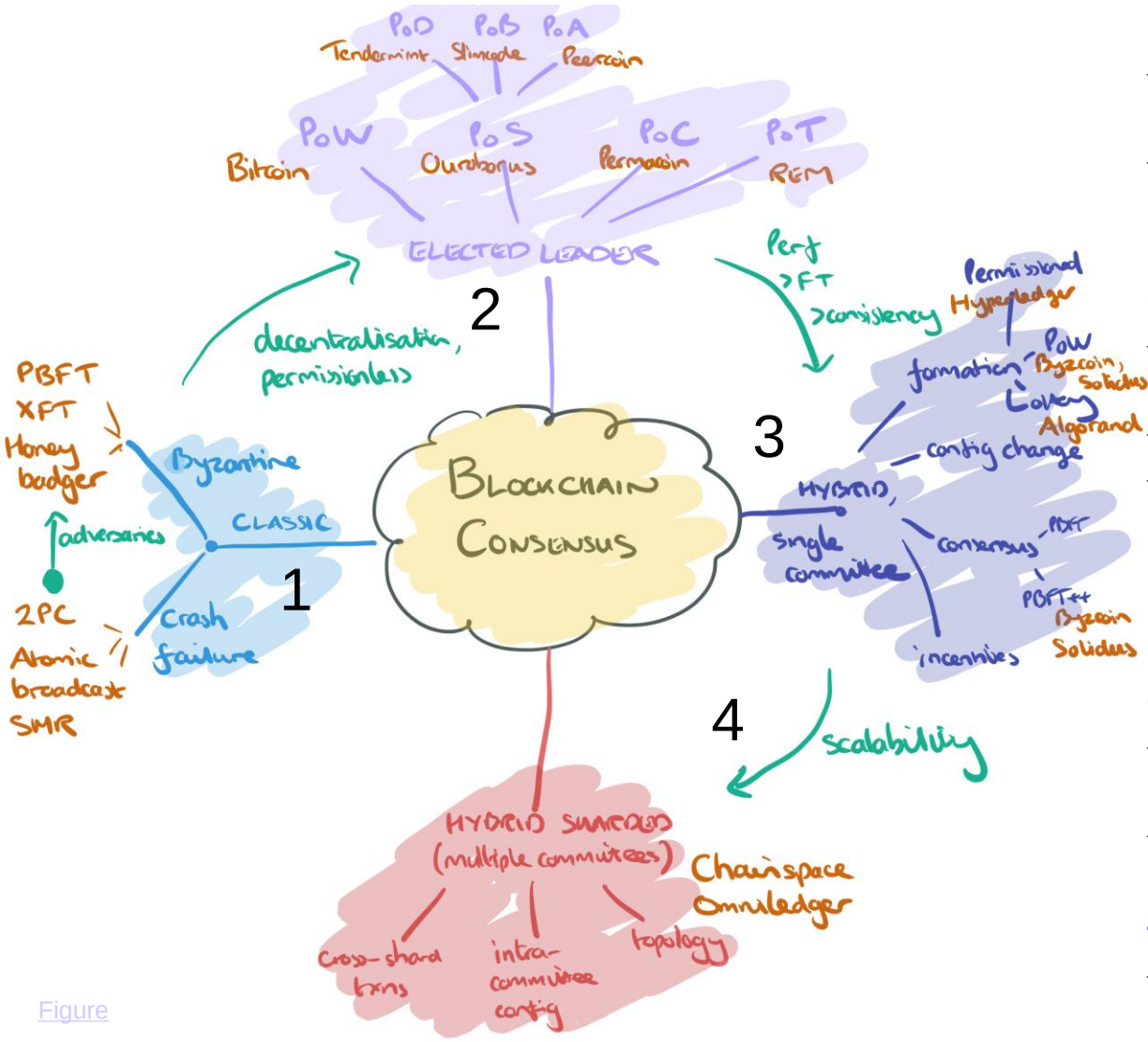
Then, a parallel (forked) chain is created



The Merkle Root will be different resulting in a different Block Hash

Imagine if one wants to remove/change a transaction

Level of Decentralization



Figure

1. Classical Consensus Models
   - Crash failure models → honest nodes failing
   - Byzantine failure model → able to tolerate a portion of malicious nodes
2. Elected Leader
   - Probabilistic elected leader (e.g., who can find the hash first?)
   - Most known Proof-of-Work (PoW)
   - Also, Proof-of-Stake (value held on the chain and its variants), Proof-of-Capacity (PoC), Proof-of-Burn (PoB), Proof-of-Authority (PoA), etc.
3. Hybrid Consensus Models
   - Single consensus has many limitations
   - Combine different consensus mechanisms
4. Hybrid Sharding
   - System is divided into shards (communities)
   - Cross-chain communications

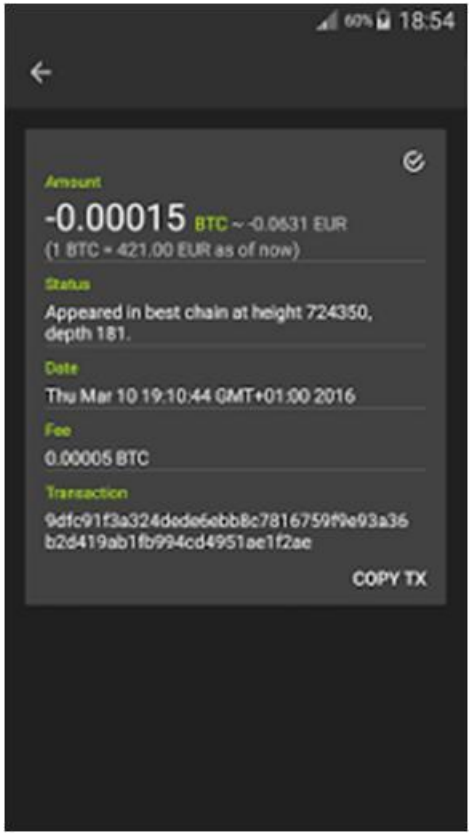
Key Blockchain Characteristics

- Permissions (write/read)
  - Fully: everyone in the world can participate (W/R)
  - Partially: selected public can participate (W/R)
- Transparency
  - Members can access the history of transactions
- Permanent storage, *i.e.,* immutability
  - Transactions cannot be removed
- Level of decentralization
  - Fully: consensus with elected leader
  - Partially: consensus with selected leader(s)

CSG Applications

CSG‘s Coinblesk Application

- Real-time bitcoin payments (Android app)
  - Use case: merchant/customer and person/person with online Bitcoin payments
  - 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 work on reduction of transaction fees, adding clearing



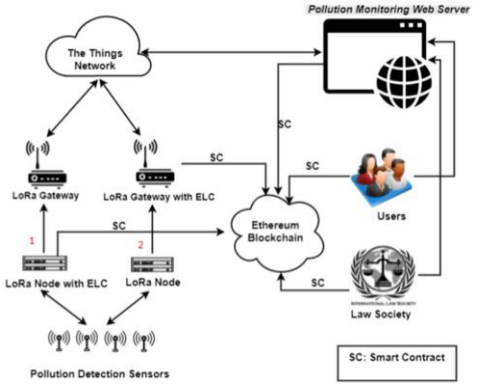
Discontinued: https://play.google.com/store/apps/details?id=com.coinblesk.client&hl=en

CSG‘s SC-based Contracting Applications

- IoT-based pollution monitoring
  - Blockchain-based automated measuring, storing, and monitoring via sensors via the Ethereum Light Client

ethereum

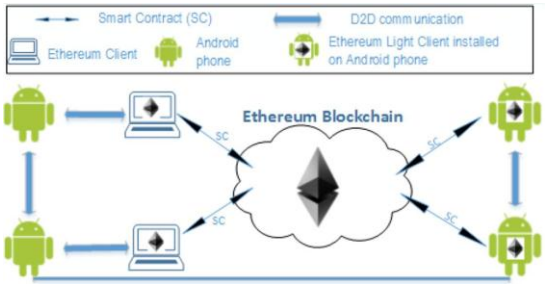
- SCs used since 2017 to define pollution thresholds based on international specs
  - CO, CO_2, ph, turbidity



  - Employs IoT protocols LoRaWAN (TTN)
    - Reduced power consumption, range to 200 km
- Flexible, light weight trading contracts
  - Ethereum Light and Full Client applicable
  - SCs used (since 2017) to set/get information

ethereum

- Deposits, traded objects, contract parties’ ID
- Enhanced user privacy



CSG‘s and modum.io‘s Architecture

- 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

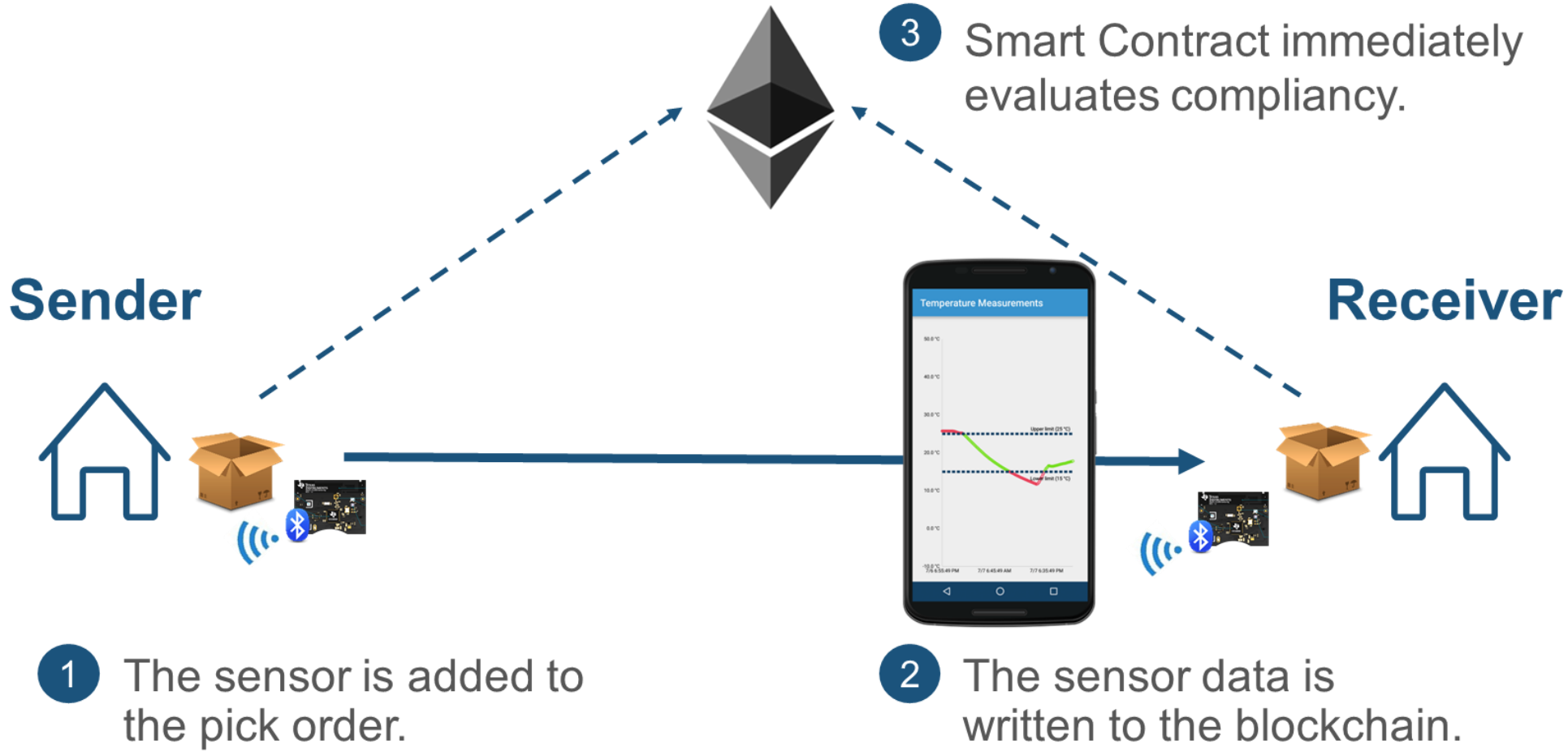
  - Architecture developed enables storing of temperature data monitored and executing smart contracts on those upon arrival

ethereum

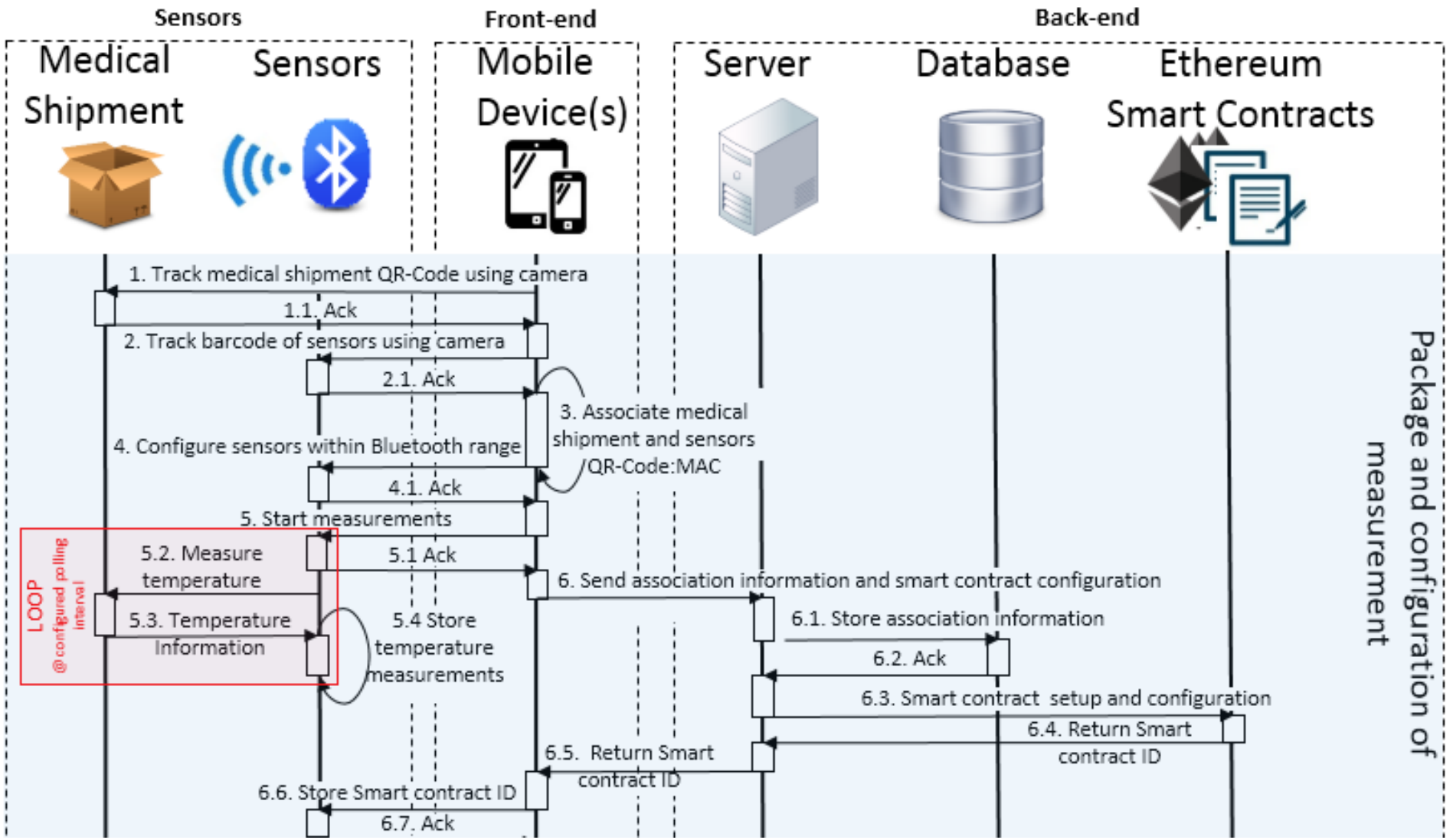
    - UZH prototype based on certified (temperature) sensor and Ethereum
  - Swiss SME modum.io raised in Sept 2017 13.5 M US$ (ICO)

ICO: International Coin Offering

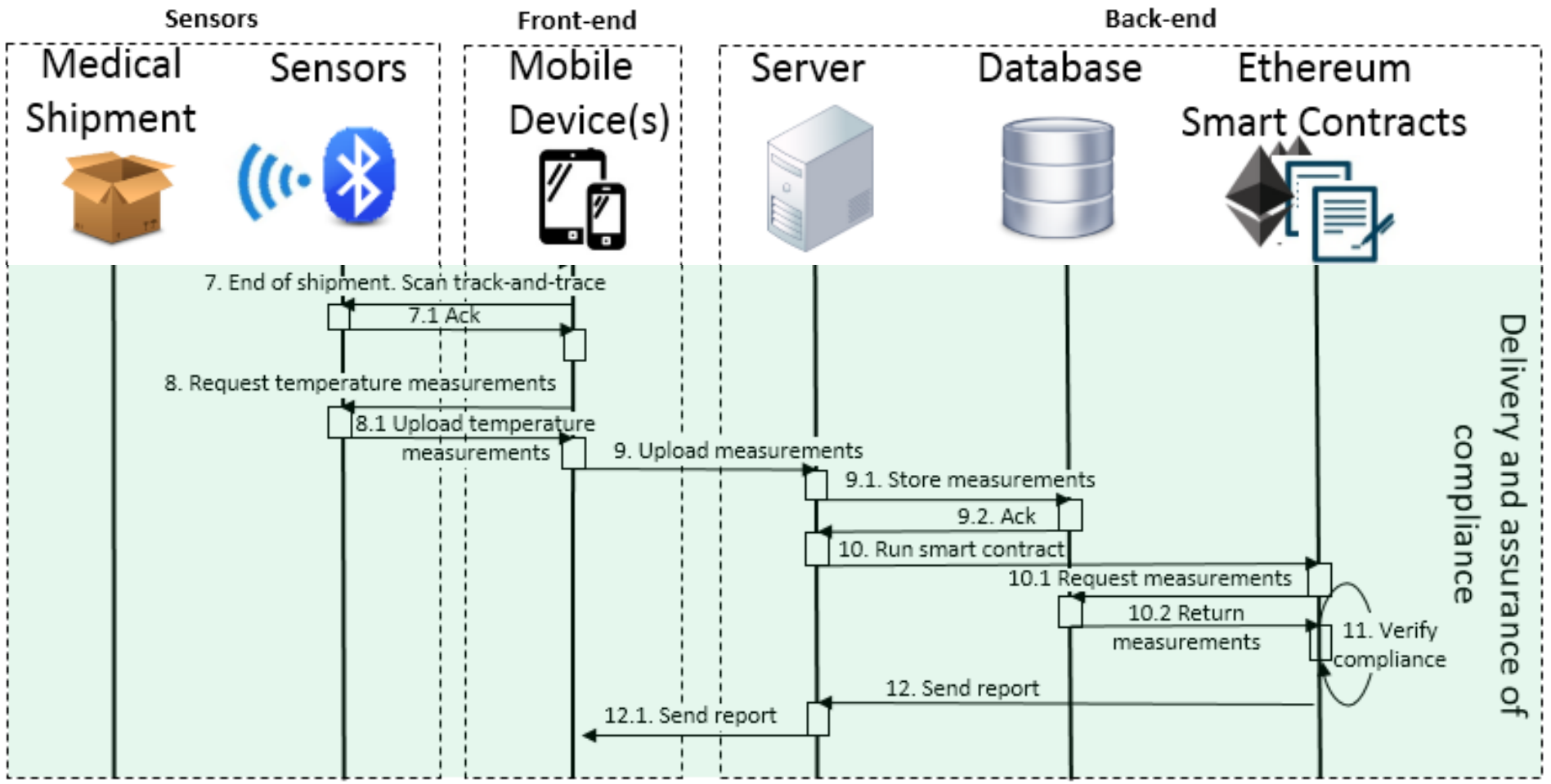
Modum.io Workflow



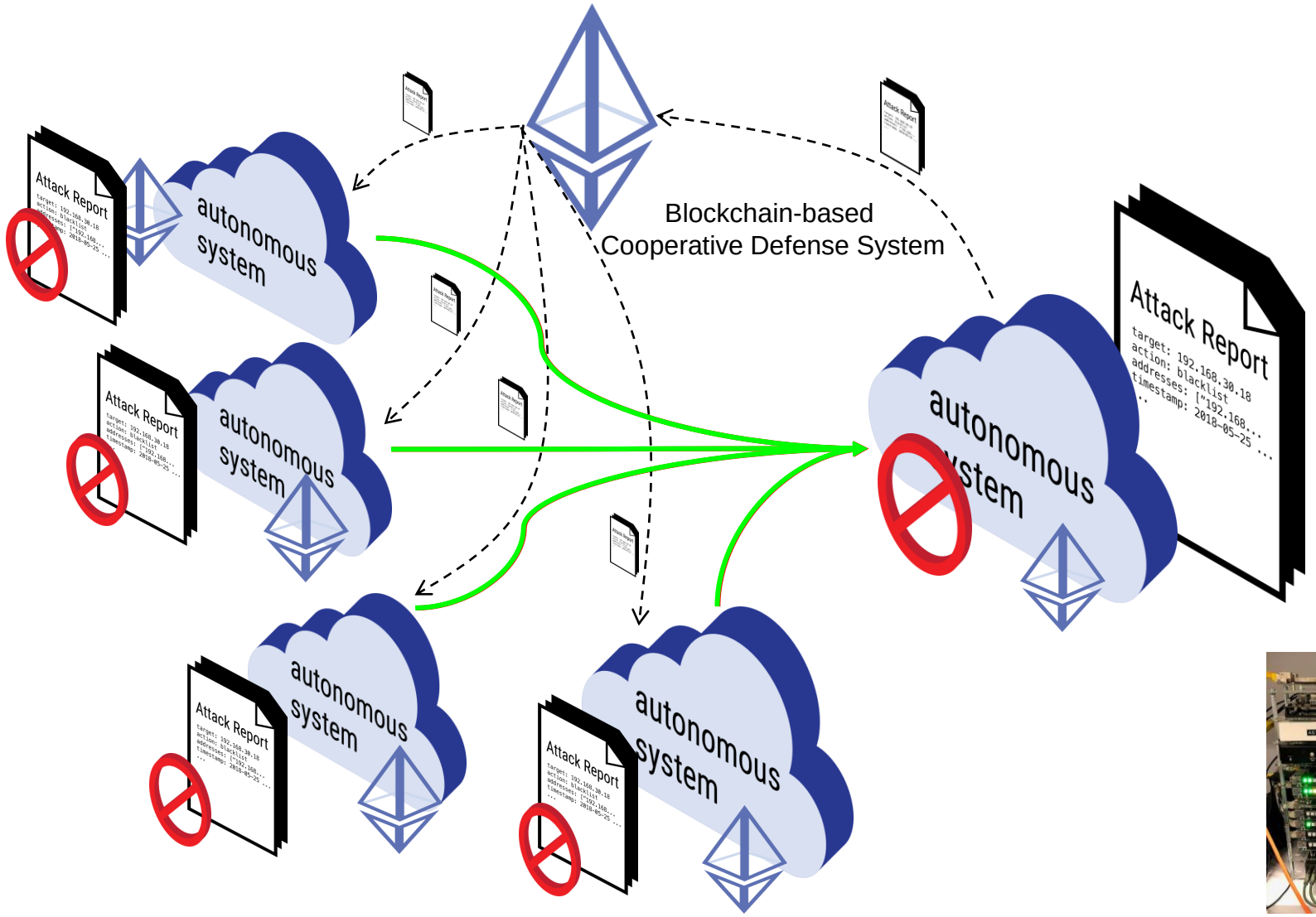
Modum.io Sequence Diagram (1)



Modum.io Sequence Diagram (2)



Collaborative DDoS Mitigation



Further CSG BC Projects

- Blockchains for Coldchains (KTI Project) – running
- Smart Cow Paddock Journal – 2016/17
  - Blockchain-based “Direktzahlungen”
- BLW: Foodchain Project – running
- Cryptocurrency Bazo from Scratch – running
  - Proof-of-Stake, mobile light client, blockchain-based loyalty program
- Blockchain-based E-Voting – running
  - Privacy, verifiability, and auditability
- Studies – since 2016
  - Performance Analysis of Blockchain Off-chain Data Storage Tools
  - Comparative Study on Identity Management Methods Using Blockchains
- Steady support of startups: modum.io, sciencematters, ICOnator

modum sciencematters ICONATOR

Blockchain Applicability

When to use (or not) Blockchain?

Posted November 22, 2015 by Gideon Greenspan in Private blockchains.

Avoiding the pointless blockchain project

How to determine if you've found a real blockchain use case

Do you need a Blockchain?

Karl Wüst
Department of Computer Science
ETH Zurich
karl.wuest@inf.ethz.ch

Arthur Gervais
Department of Computing
Imperial College London
a.gervais@imperial.ac.uk

The Use of Blockchains: Application-Driven Analysis of Applicability

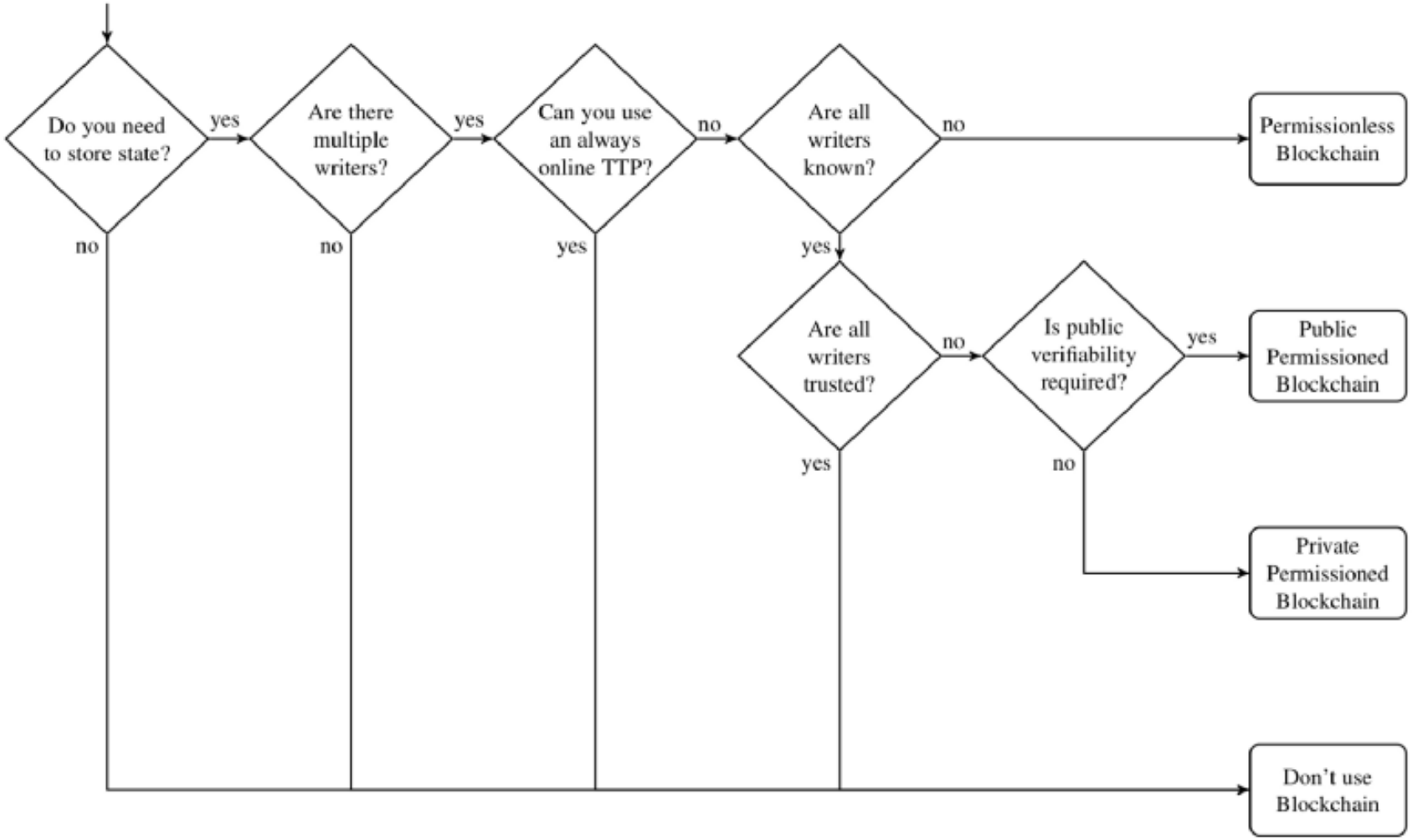
Bruno Rodrigues, Thomas Bocek, Burkhard Stiller
Communication Systems Group (CSG), Department of Informatics (IfI), Universität Zürich (UZH), Zürich, Switzerland

G. Greenspan (2015)

Key Points	When to use BC	Traditional DBs
Database	Shared	Centralized, Shared
Multiple writers	Multiple writers	Single or multiple
Absense of trust	Database with multiple non-trusting writers	Trust
Disintermediation	No trusted intermediaries	Trusted intermediary
Transaction interaction	There is a dependency between transactions	Trust the intermediary to mediate interactions
Set the rules	Clear rules applied to all writers	Different rules based on roles/groups of writers
***Pick your validators**	Trust in the validation scheme (single entity or democratic)	
***Back your assets**	Translation of digital assets into the real world	

***Recommendations**

K. Wüst, A. Gervais (2018)



K. Wüst, A. Gervais (2018)

- Performance and scalability requirements impacts of alternative BC solutions and data bases in comparison

	Permissionless Blockchain	Permissioned Blockchain	Central Database
Throughput	Low	High	Very High
Latency	Slow	Medium	Fast
Number of readers	High	High	High
Number of writers	High	Low	High
Number of untrusted writers	High	Low	0
Consensus mechanism	Mainly PoW, some PoS	BFT protocols (e.g. PBFT [6])	None
Centrally managed	No	Yes	Yes

BFT: Byzantine Fault Tolerance
PBFT: Practical Byzantine Fault Tolerance

Application Trade-offs (B. Rodrigues, T. Bocek, B. Stiller, 2018)

- Based on Blockchain characteristics:
  - Performance vs Reliability
    - BC offers slow throughput but more robustness than traditional DBs
  - Confidentiality vs Transparency
    - More transparency (trust) and less confidentiality
  - Distributed vs centralized control
    - No central authority (PoW) or trusted nodes (PBFT)
- Limited storage
- Unknown regulations
  - Different countries, different regulations
- Lack of standards
  - Blockchain 4.0 target

Public Blockchain Challenges

- How to handle reliably tangible (non-digital) assets in BC?
  - A Bitcoin is represented as 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 2000+ cryptoc.
- Legal/regulative compliance, societal/governmental acceptance

Public Blockchain Risks

- BCs' "true semantics" depends 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)
- 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. There is ***no general formula*** to determine conflict-free, whether a blockchain makes sense or not
   - The analysis of different blockchain variations ***and*** concrete application requirements is a must
2. The technical future of blockchains is based on ***security ingredients*** of today's technology, however, long-term storage and security management is not known by now
   - *E.g.*, unknown impact of quantum computing (on all IT!)
3. Blockchains show ***no revolution***, but a typical Computer Science (Abstract Data Type) **evolution** of linked lists, but
   - 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.

Questions?