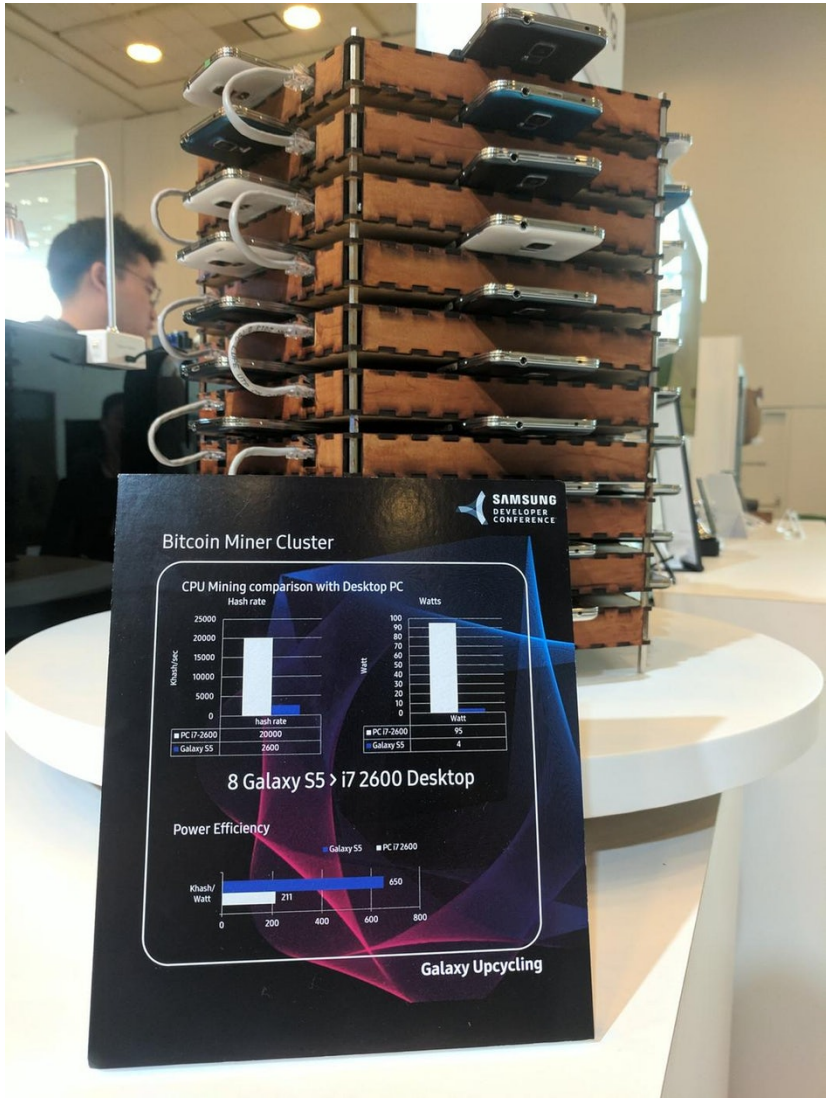
Blockchain technologies

András Pataricza

Budapest University of Technology and Economics

pataric@mit.bme.hu

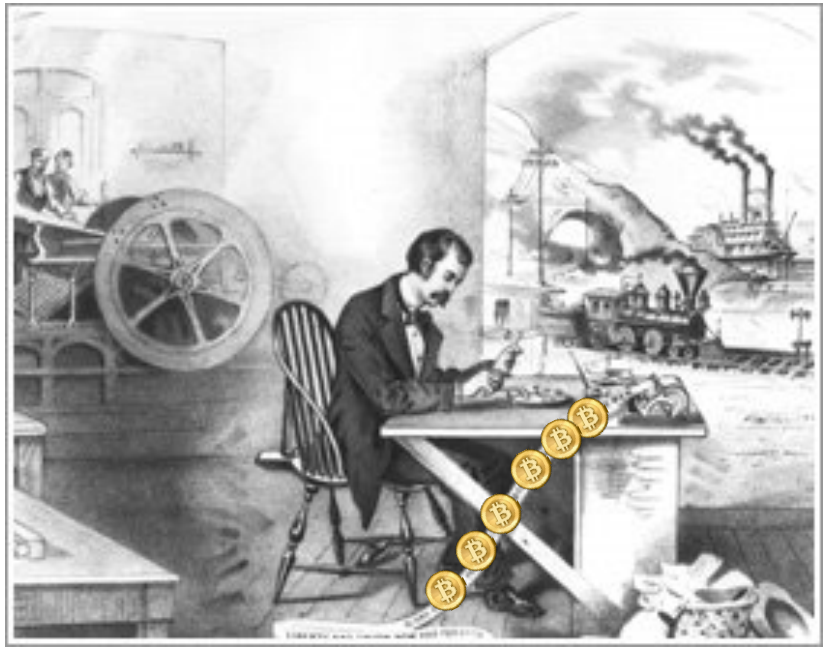
Gold digging then and now?



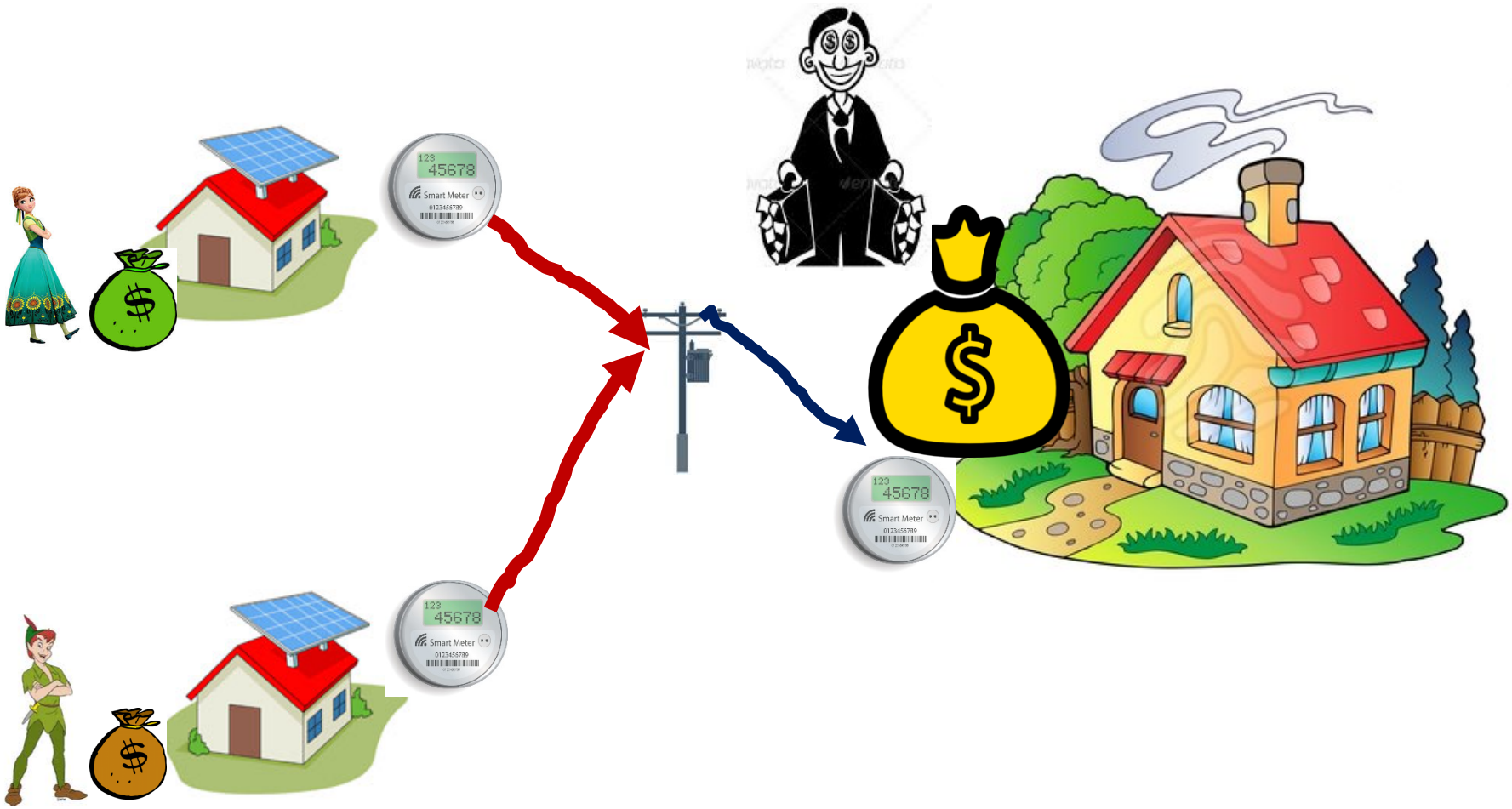
Bitcoin vs. Blockchain

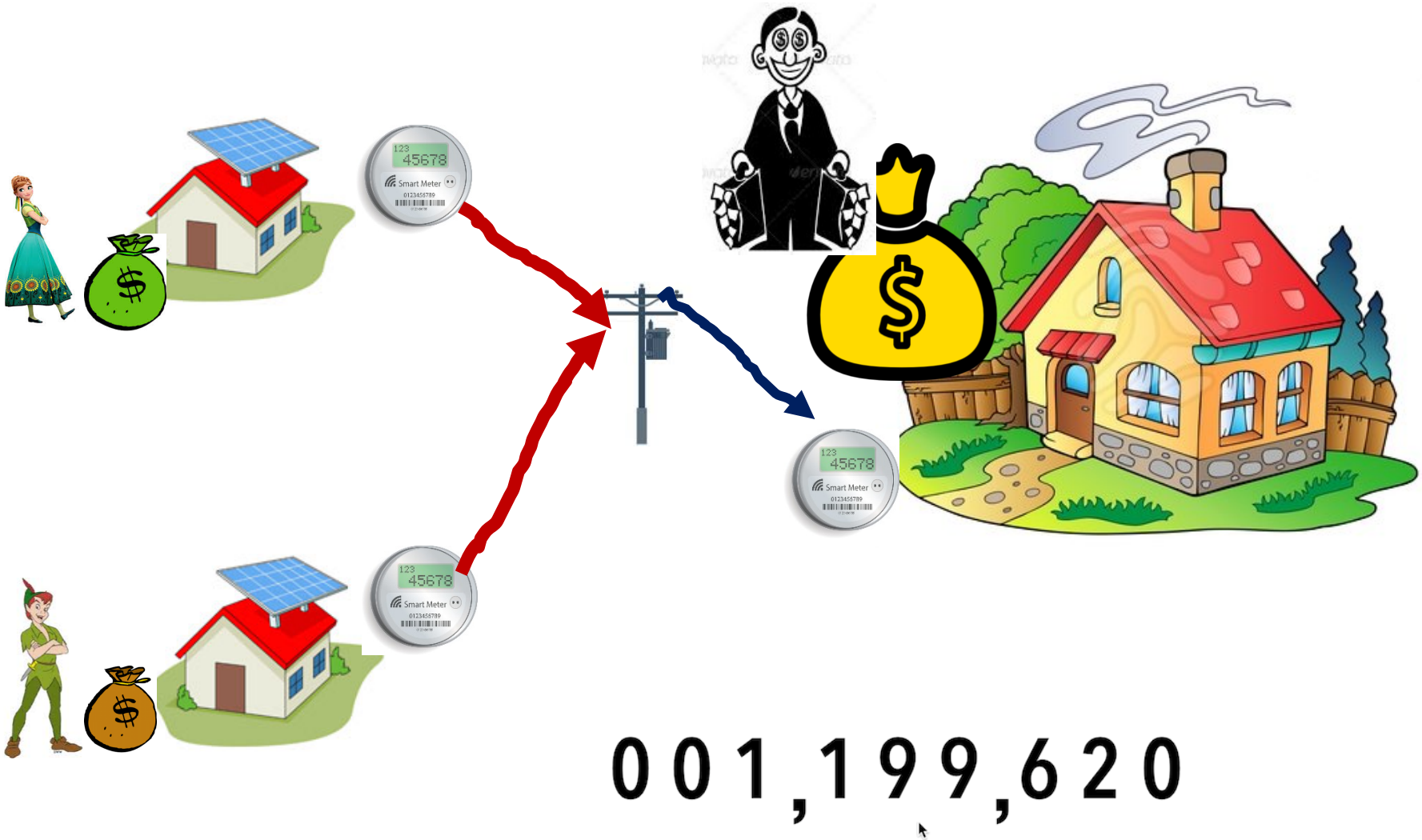
I am not a miner…

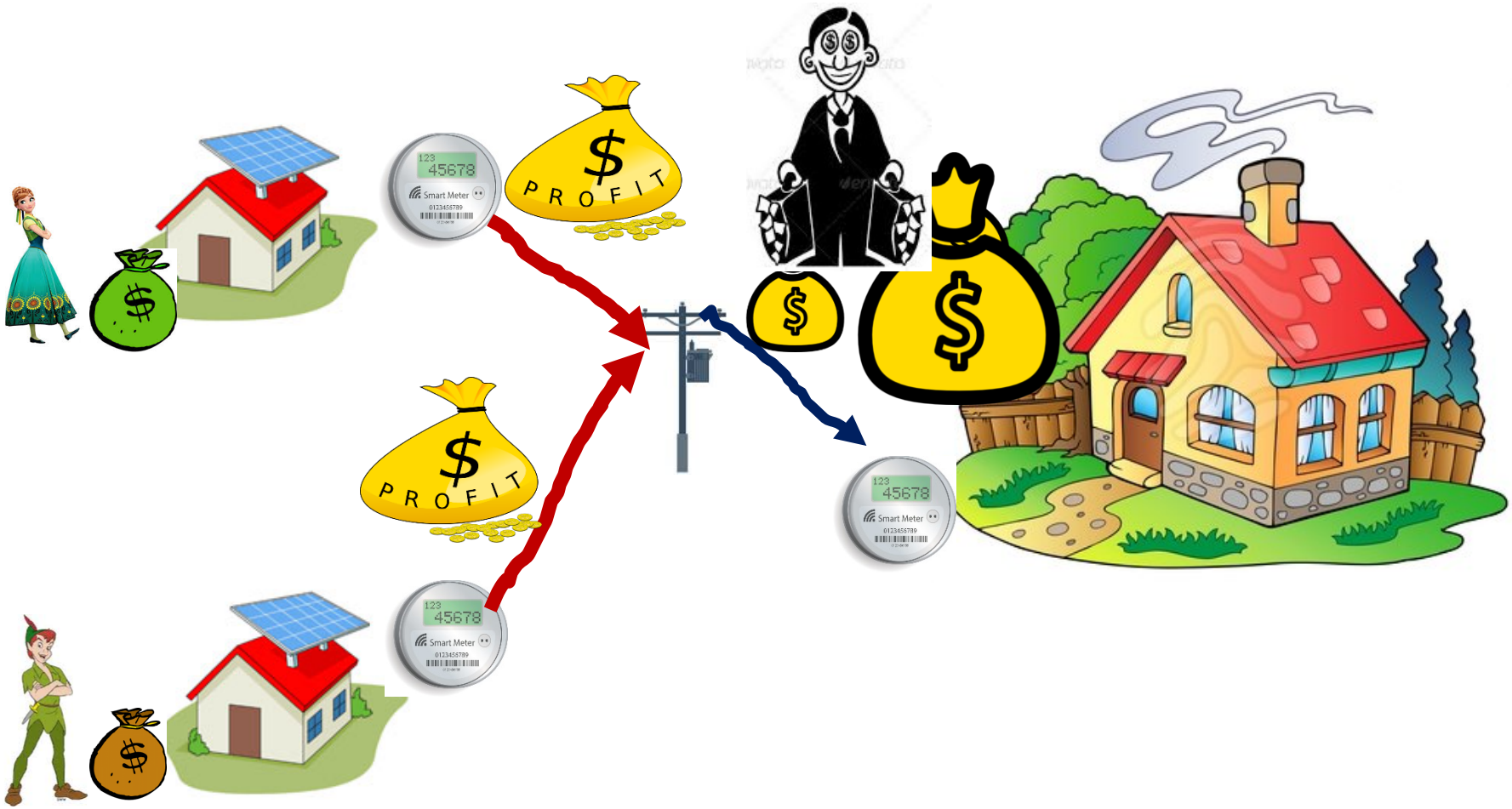
There is more money in cooperation

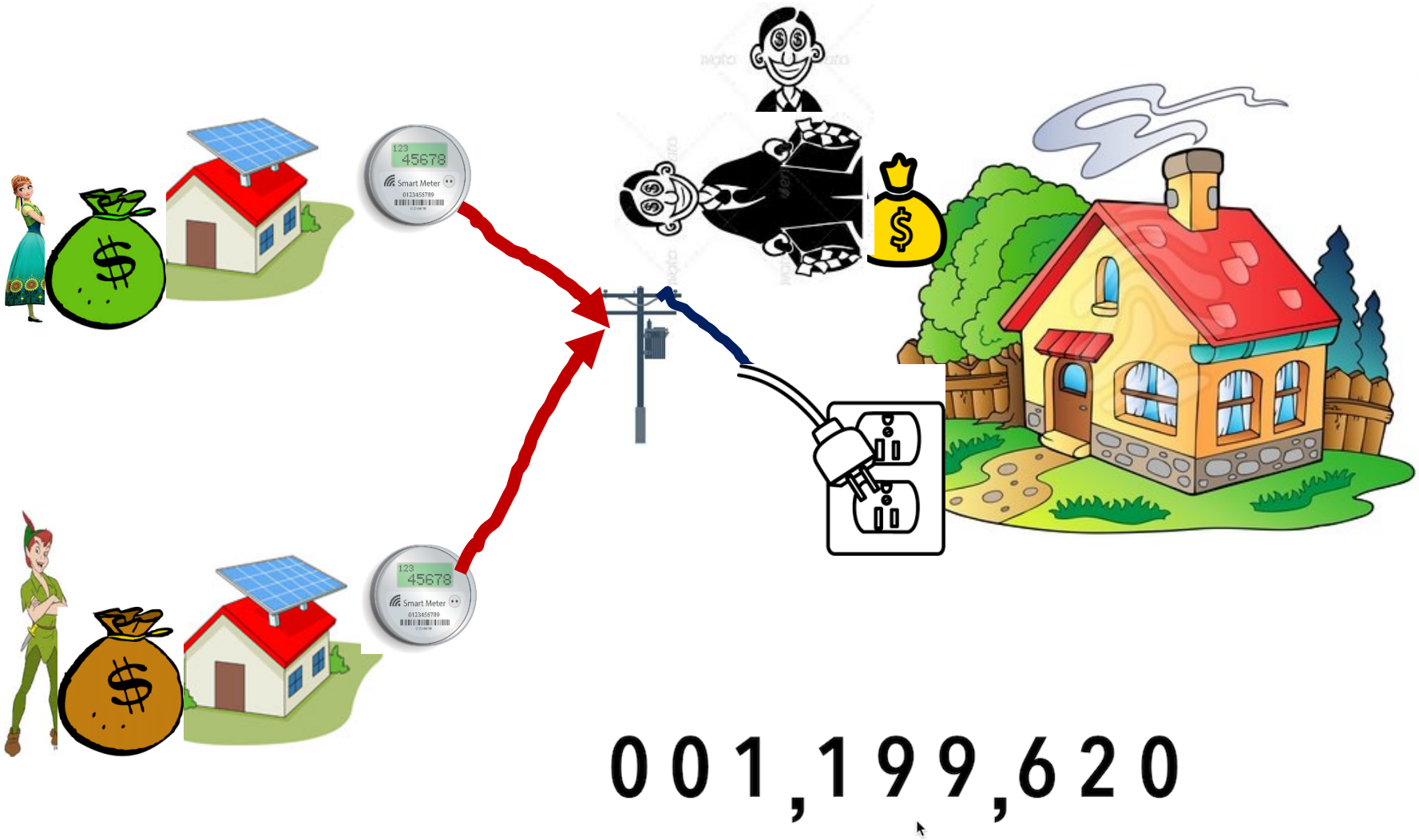


A distributed, collaborative production-financial system based on trust


123
45678
Smart Meter
0123456789
123
45678
Smart Meter
0123456789
123
45678
Smart Meter
0123456789

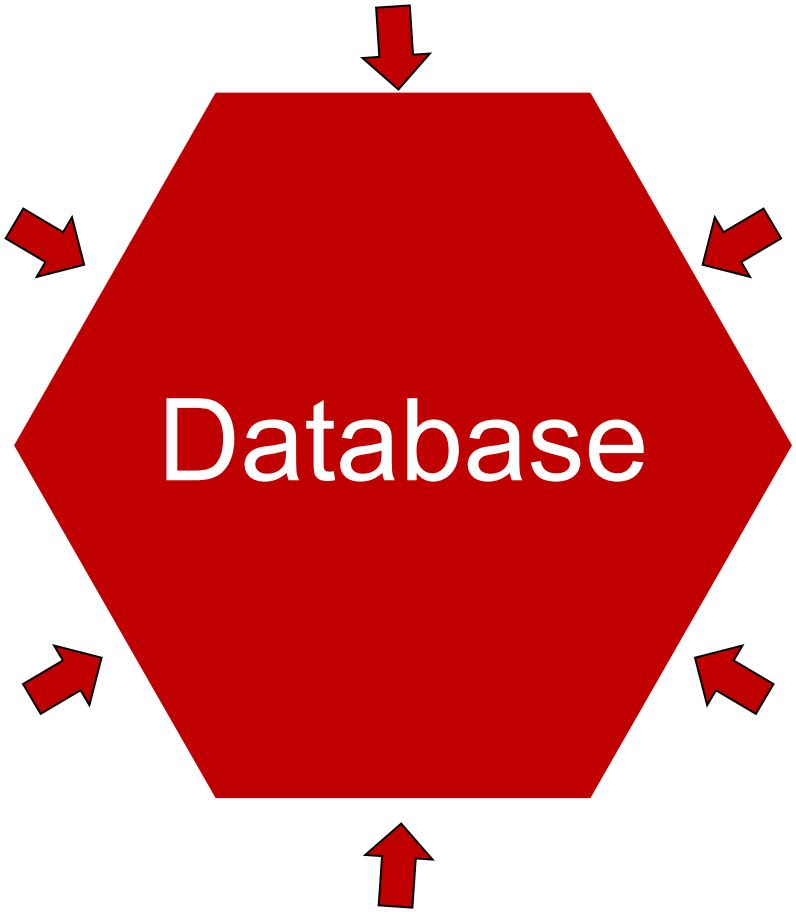

123
45678
Smart Meter
0123456789
001,199,620

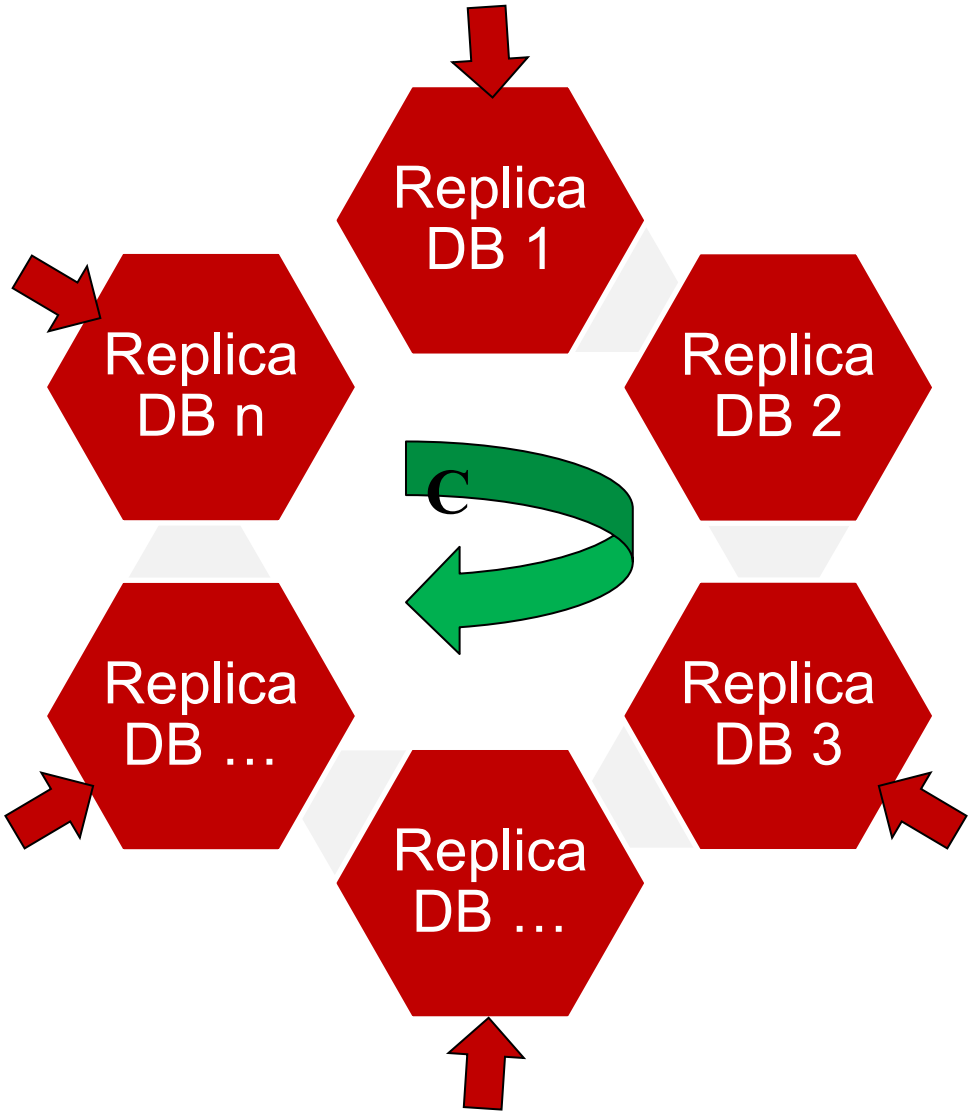

123
45678
Smart Meter
0123456789
$
PROFIT


123
45678
Smart Meter
0123456789
123
45678
Smart Meter
0123456789
001,199,620

BLOCKCHAIN FOUNDATIONS

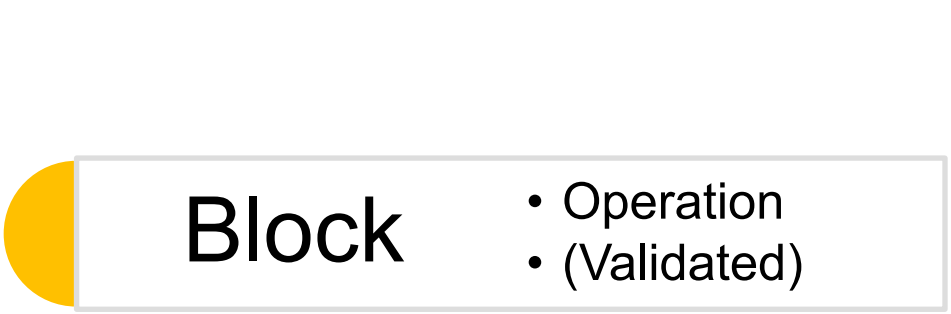
From replicated databases…

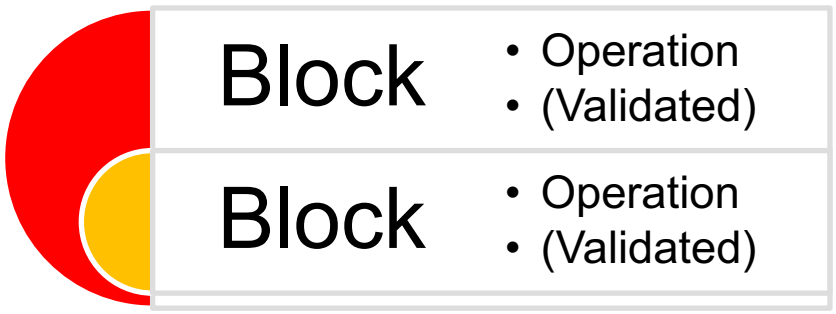




Blockchain=block+chain

Block: validated transaction sequence protected by a hash
Distributed databases
State synchronization by simultaneous execution
Strict determinism





Blockchain

Four elements characterize Blockchain

Replicated ledger

- History of all transactions
- Append-only with immutable past
- Distributed and replicated

Cryptography

- Integrity of ledger
- Authenticity of transactions
- Privacy of transactions
- Identity of participants

Consensus

- Decentralized protocol
- Shared control tolerating disruption
- Transactions validated

Business logic

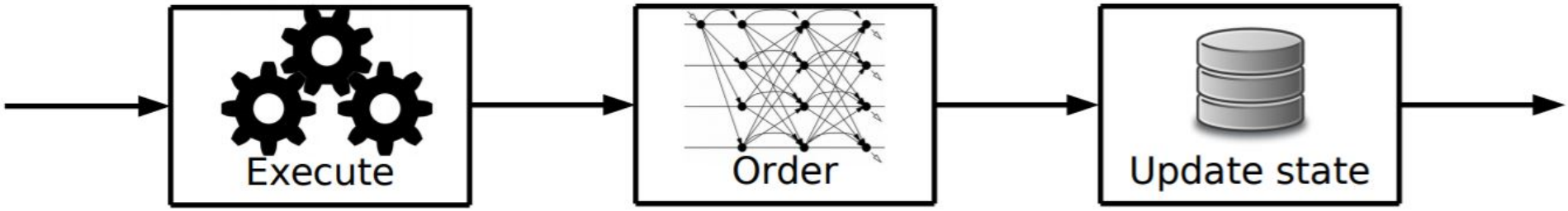
- Logic embedded in the ledger
- Executed together with transactions
- From simple "coins" to self-enforcing "smart contracts"

5

C. Cachin: Hyperledger Fabric V1. Workshop on Blockchain Technology and Theory,16 October 2017, Vienna: http://blockchain-workshop.net/talks/cachin.pdf

HYPERLEDGER FABRIC V1 ARCHITECTURE

Hyperledger 1.0



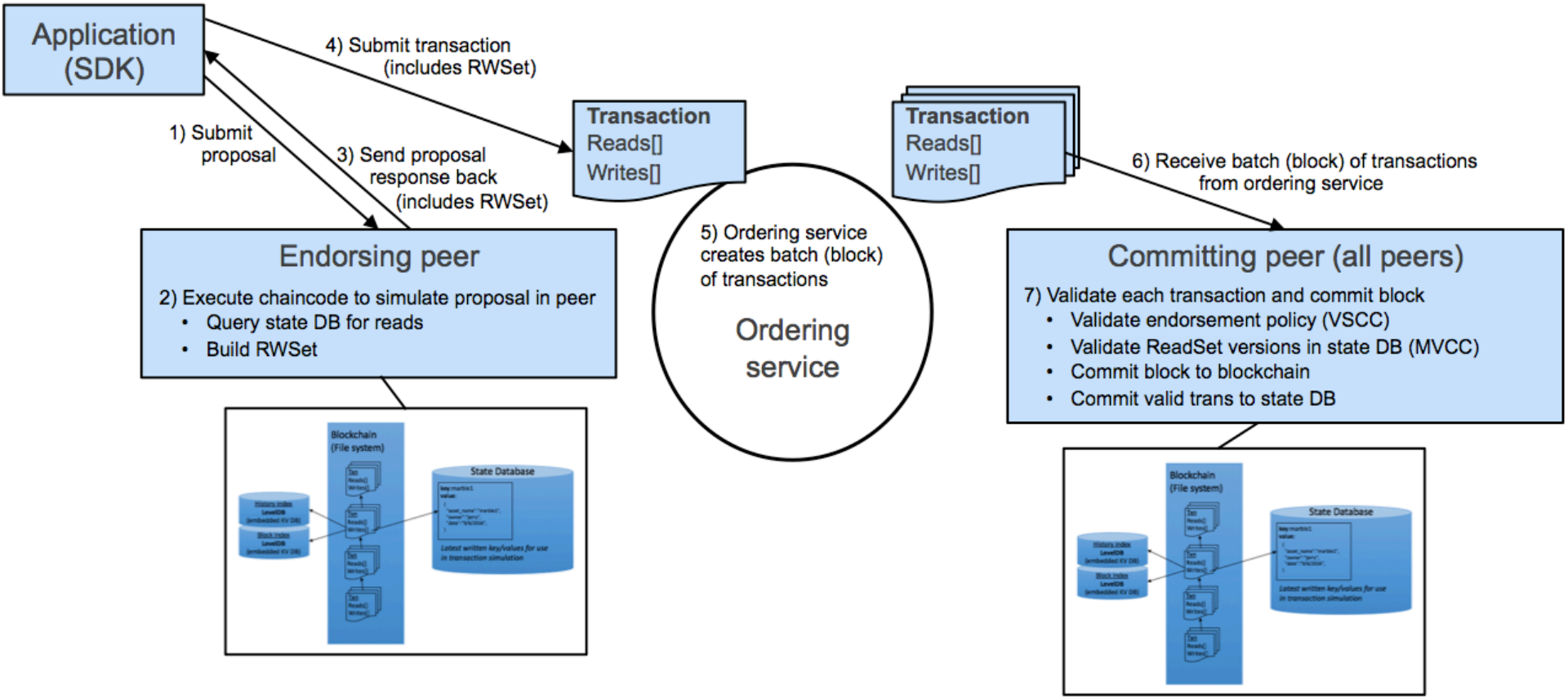
- Simulate op. and endorse
- RW-set
- Nodes differ per application

- Order RW-sets
- Stateless con-sensus service

- Validate RW-sets
- Eliminate conflicting ops.
- State kept by all nodes

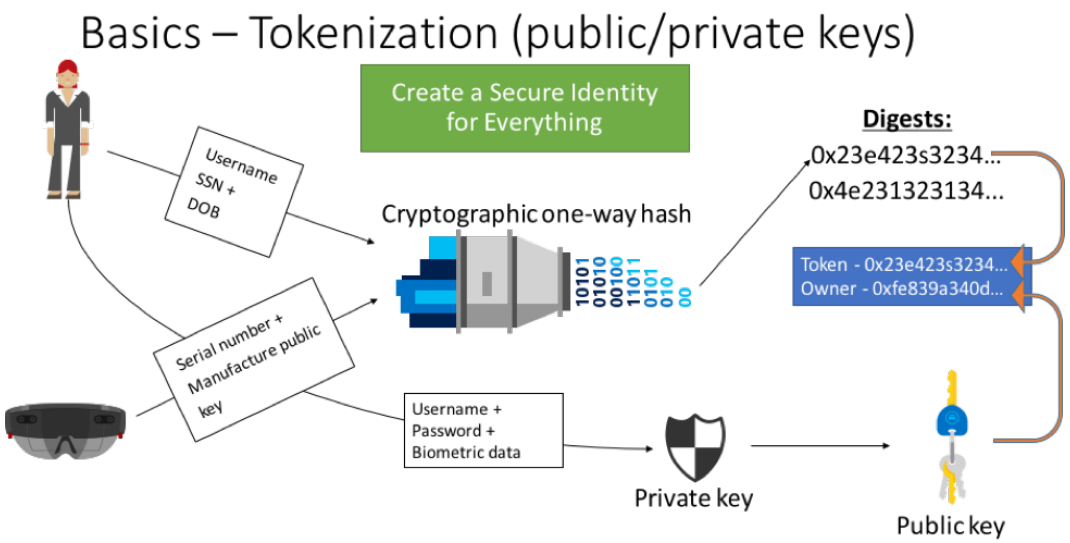
C. Cachin: Hyperledger Fabric V1. Workshop on Blockchain Technology and Theory,16 October 2017, Vienna: http://blockchain-workshop.net/talks/cachin.pdf

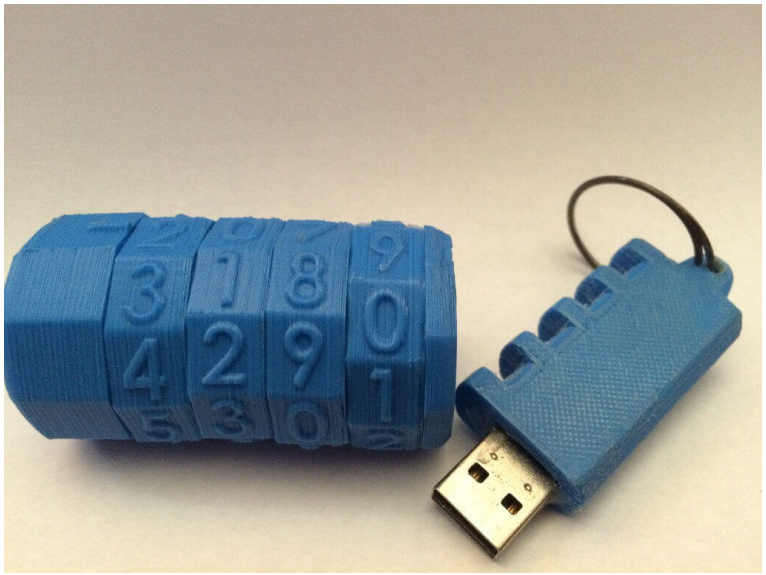
Transaction Lifecycle

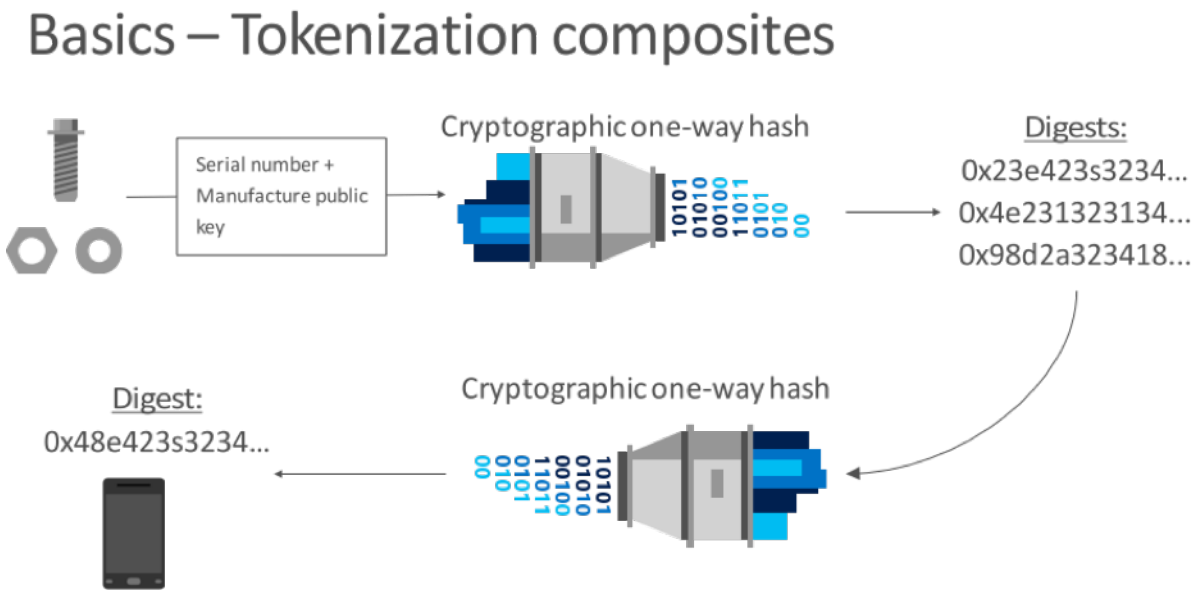


Source:
https://www.ibm.com/developerworks/cloud/library/cl-top-technical-advantages-of-hyperledger-fabric-for-blockchain-networks/index.html

Cryptographically Tokenized Assets

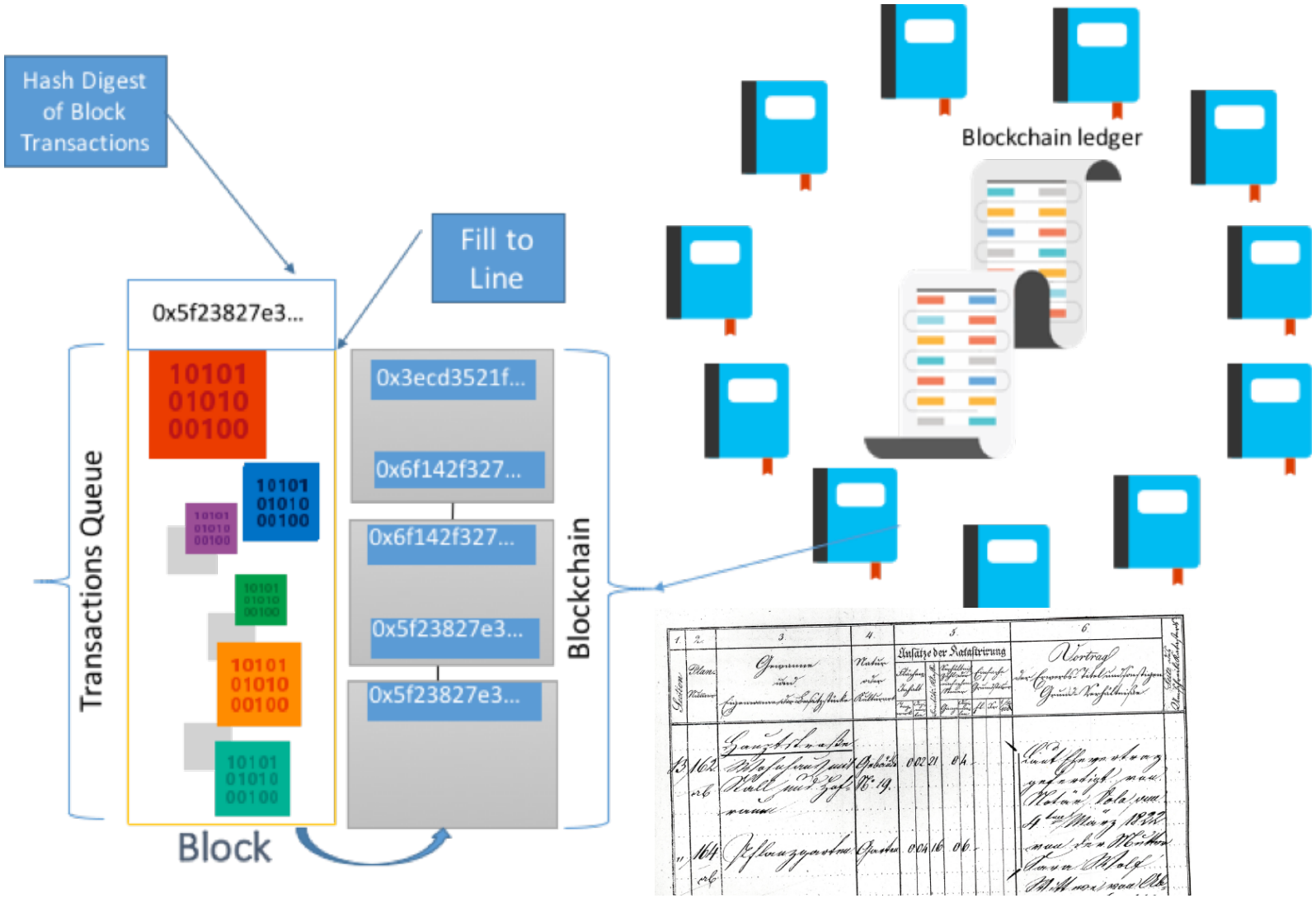






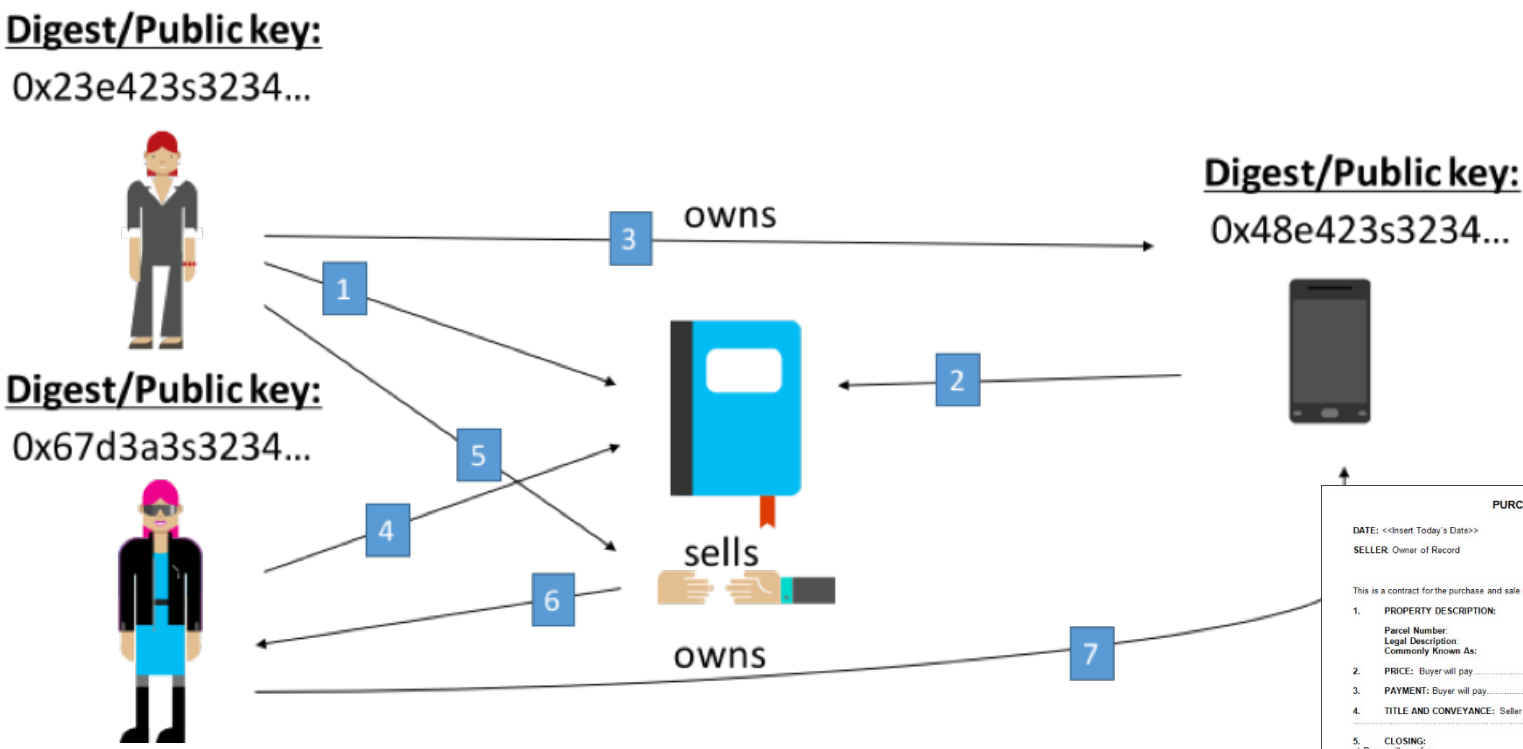
Source: Introducing Project "Bletchley" *Marley Gray, Principle Architect PM - Microsoft - Azure Blockchain Engineering*

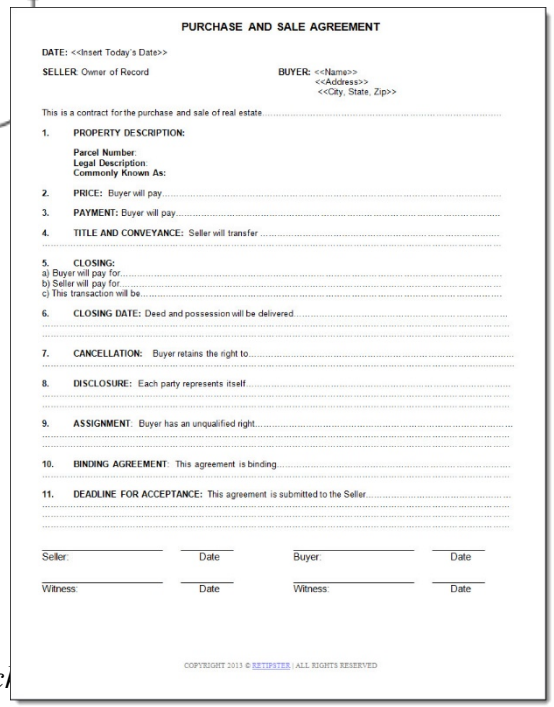
Blockchain = Cryptographically Authentic, Shared, Distributed Ledger



Source: Introducing Project "Bletchley" *Marley Gray, Principle Architect PM - Microsoft - Azure Blockchain Engineering*

Interaction flow-smart contracts





PURCHASE AND SALE AGREEMENT

DATE: <<Insert Today's Date>>

SELLER: Owner of Record

BUYER: <<Name>>
<<Address>>
<<City, State, Zip>>

This is a contract for the purchase and sale of real estate.

1. PROPERTY DESCRIPTION:
Parcel Number:
Legal Description:
Commonly Known As:
2. PRICE: Buyer will pay
3. PAYMENT: Buyer will pay
4. TITLE AND CONVEYANCE: Seller will transfer
5. CLOSING:
a) Buyer will pay for
b) Seller will pay for
c) This transaction will be
6. CLOSING DATE: Deed and possession will be delivered
7. CANCELLATION: Buyer retains the right to
8. DISCLOSURE: Each party represents itself
9. ASSIGNMENT: Buyer has an unqualified right
10. BINDING AGREEMENT: This agreement is binding
11. DEADLINE FOR ACCEPTANCE: This agreement is submitted to the Seller

Seller: Date Buyer: Date
Witness: Date Witness: Date

COPYRIGHT 2013 © RETIPSTER | ALL RIGHTS RESERVED

Source: Introducing Project "Bletchley" *Marley Gray, Principle Architect PM - Microsoft - Azure Blockc*

Use cases

Harvard Business Review

INFORMATION & TECHNOLOGY

The Promise of Blockchain Is a World Without Middlemen

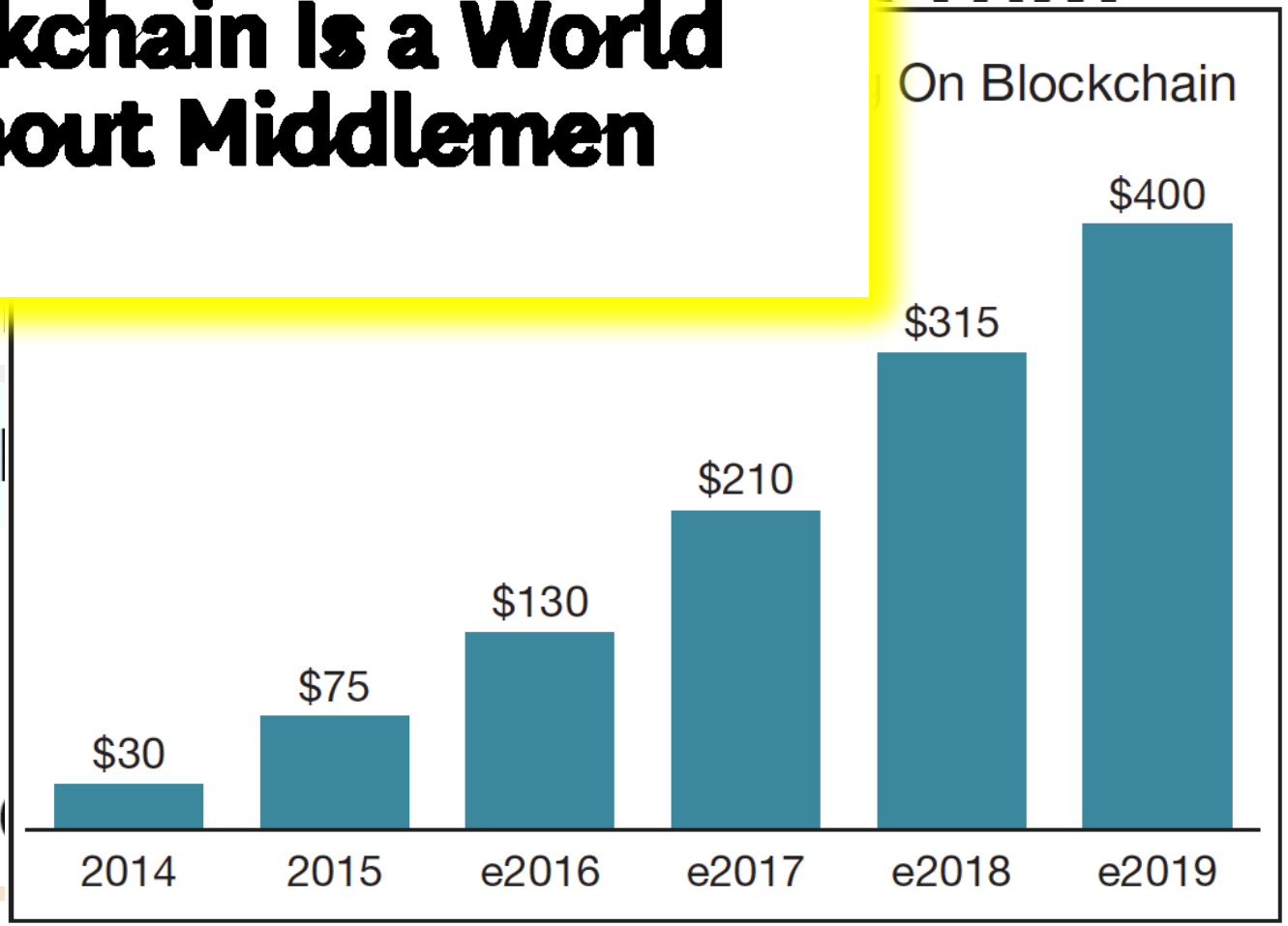
by Vinay Gupta

MARCH 08, 2017

...l Do

...stem

...On Blockchain



So... Blockchai...

Pa...

News

Dao.Casino

Gambling E...

Source: Aite Group

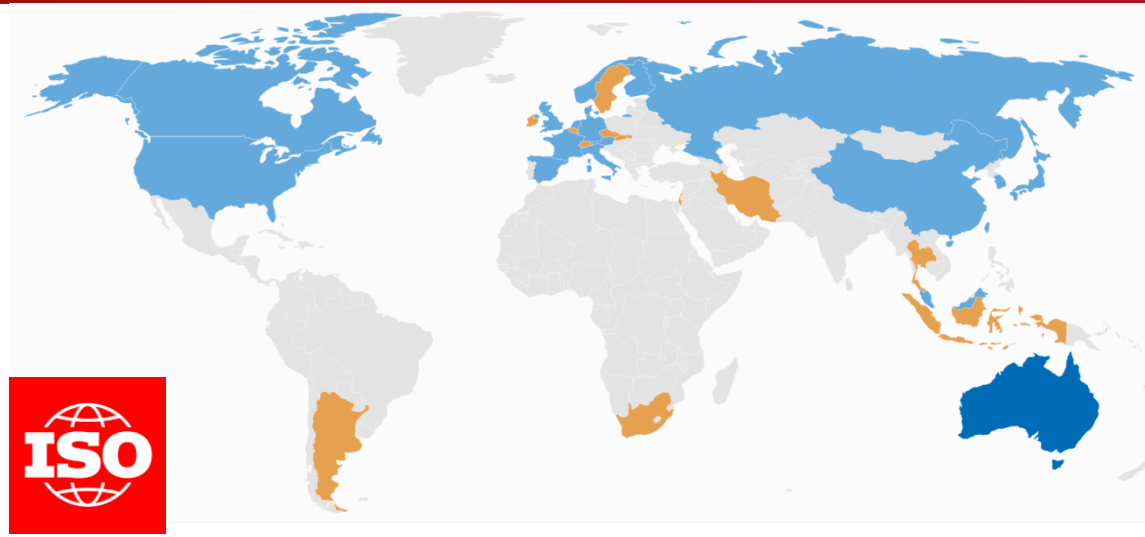
e: estimate

Standardization

ISO/TC 307: Blockchain and electronic distributed ledger technologies

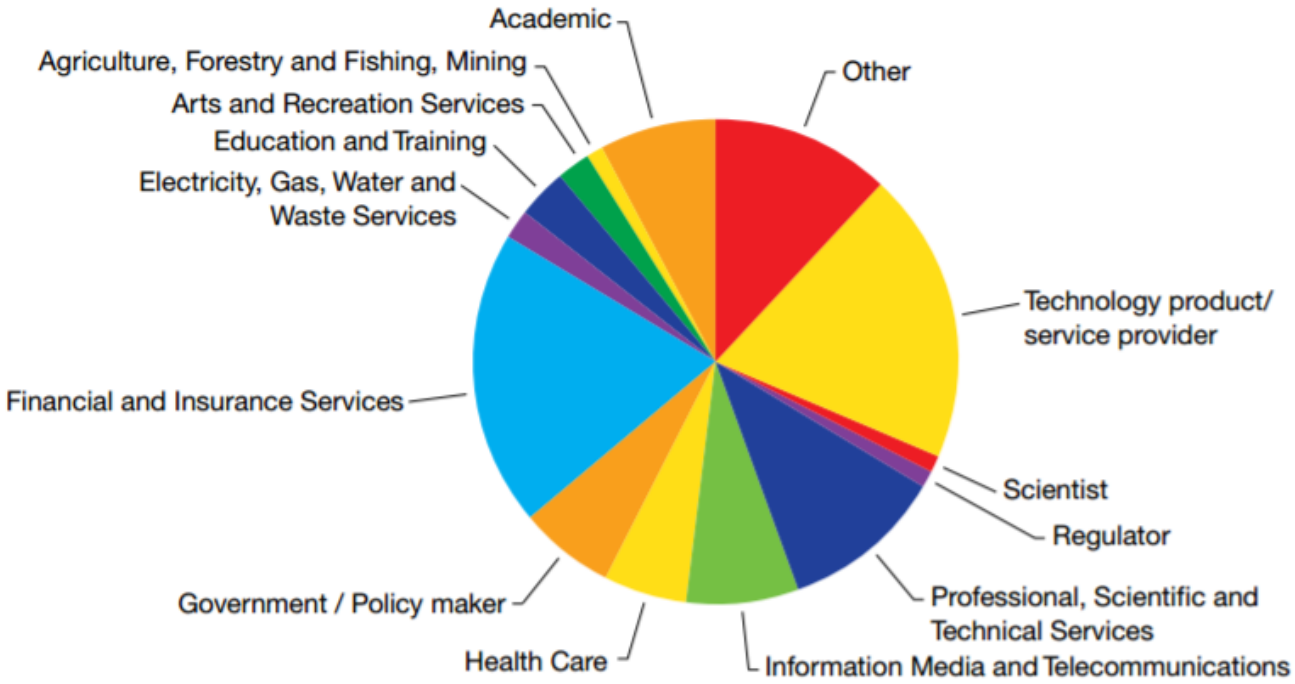
INTEROPERABILITY, LEGAL BACKROUND REQUIREMENTS

Survey



ISO

Respondents by sector of economic activity

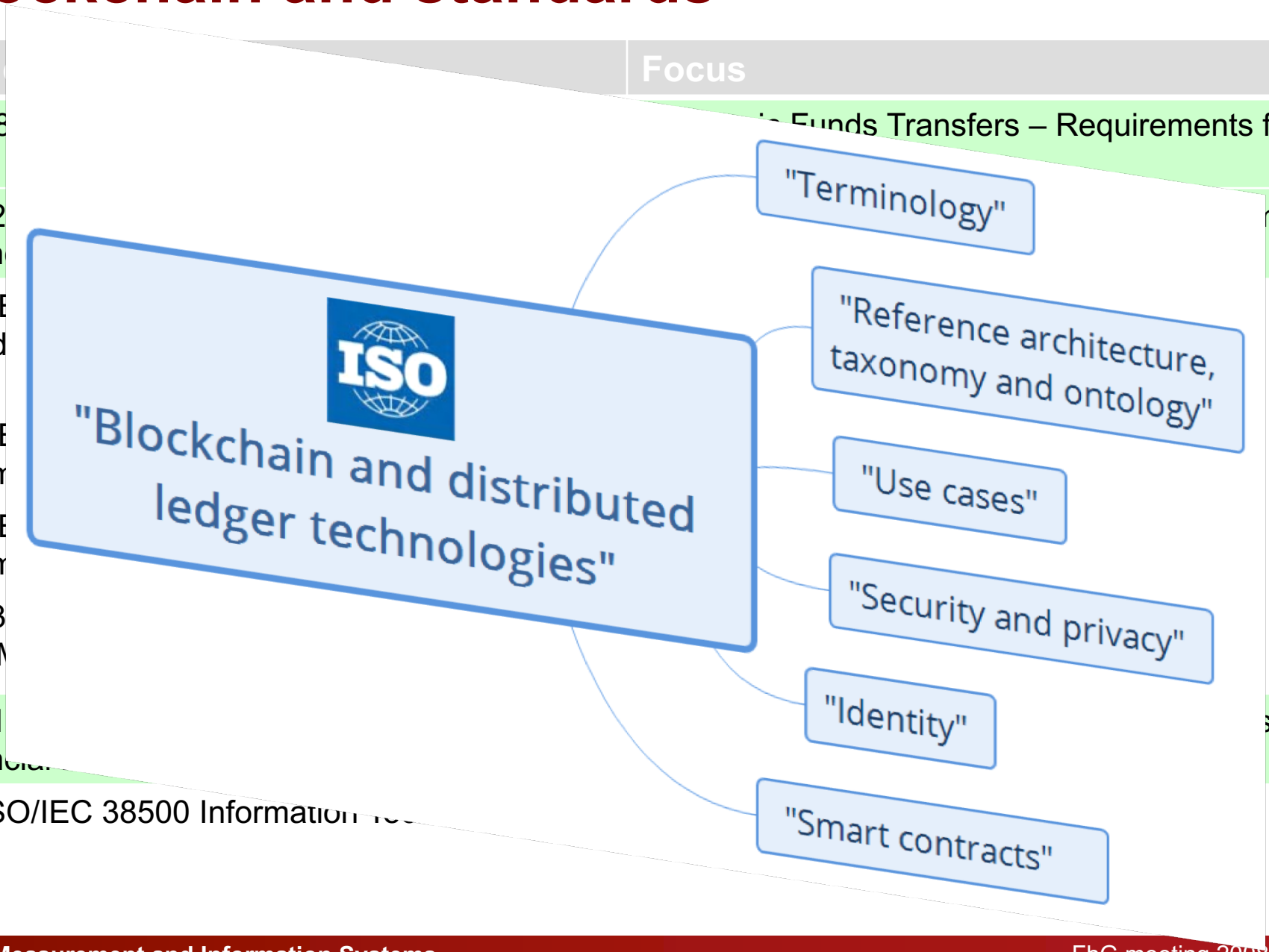


Source: Blockchain survey, Standards Australia analysis

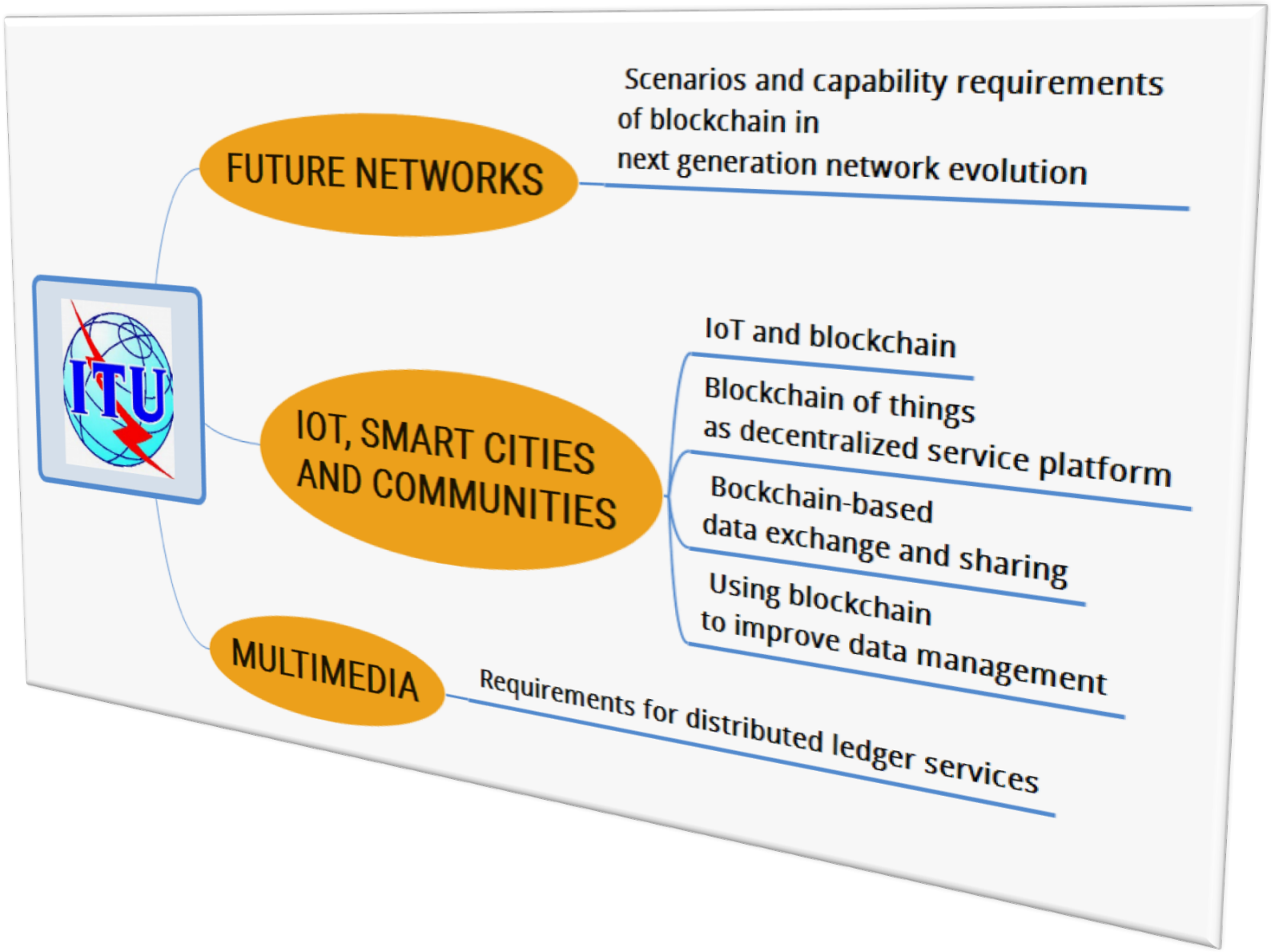
- Priorities
  - Terminology
  - Privacy
  - Governance
  - Interoperability
  - Security
  - Risk

Blockchain and standards

Stan	Focus
AS 28	...Funds Transfers – Requirements for
ISO 2 Finan	...ne
ISO/IE Cloud	
ISO/IE Inform	
ISO/IE Inform	
ISO 3 Risk M	
ISO 1 Financ	...s
AS ISO/IEC 38500 Information ...	



Towards smart-*



Governmental use

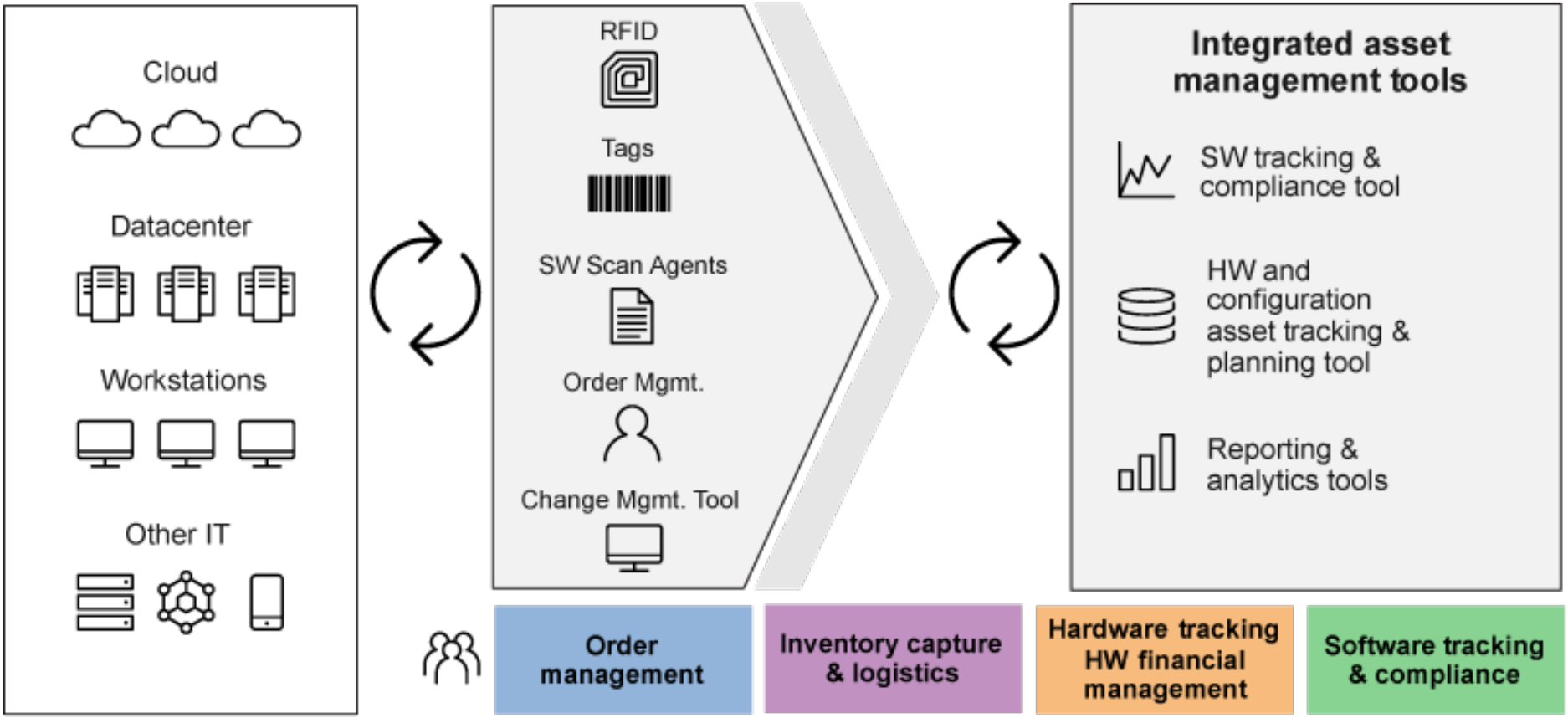
Government services that survey respondents would like to see using blockchain technologies to improve efficiencies and public access

Land Transfers and Property Title registrations	72.1%
Personal Identification and Passport Documentation	68.9%
Management of Health Records	65.6%
Vehicle Registrations	54.1%
Welfare Distribution and Monitoring	37.7%
Urban planning; wider pedestrian sidewalks, increased times for crossings	21.3%
Public Transport Scheduling	16.4%

Source: Blockchain survey, Standards Australia analysis

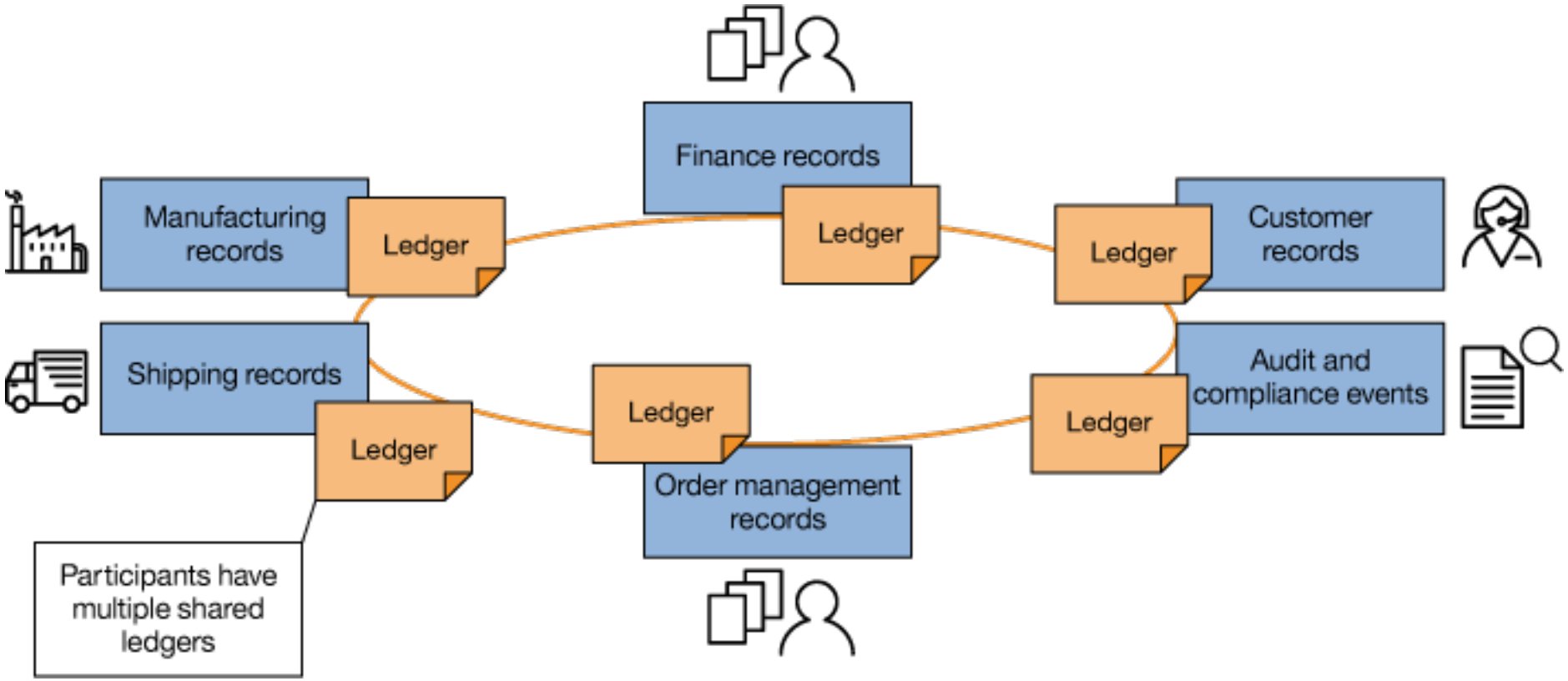
ASSET MANAGEMENT

IBM asset management



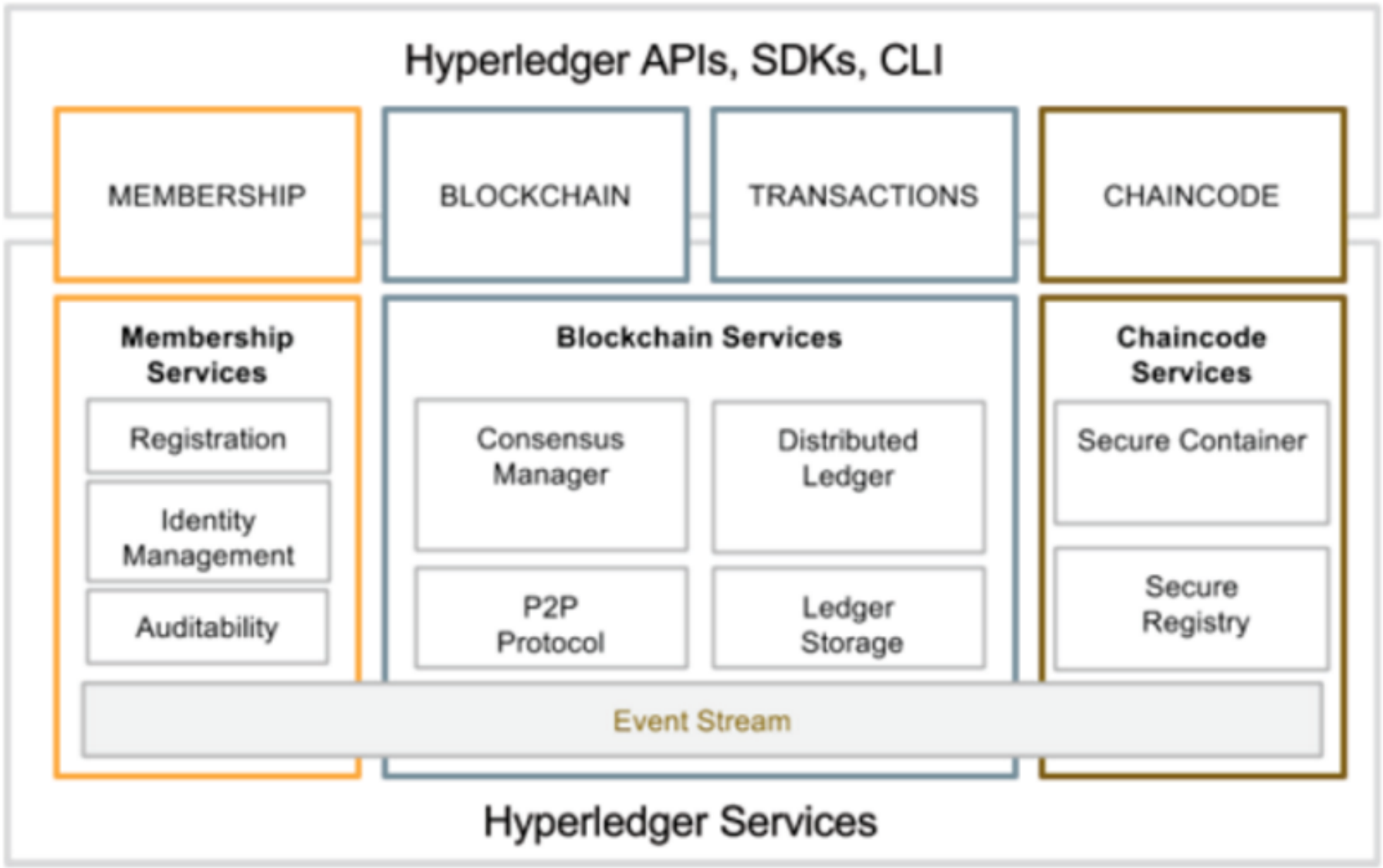
Source: IBM DeveloperWorks

Ledgers…



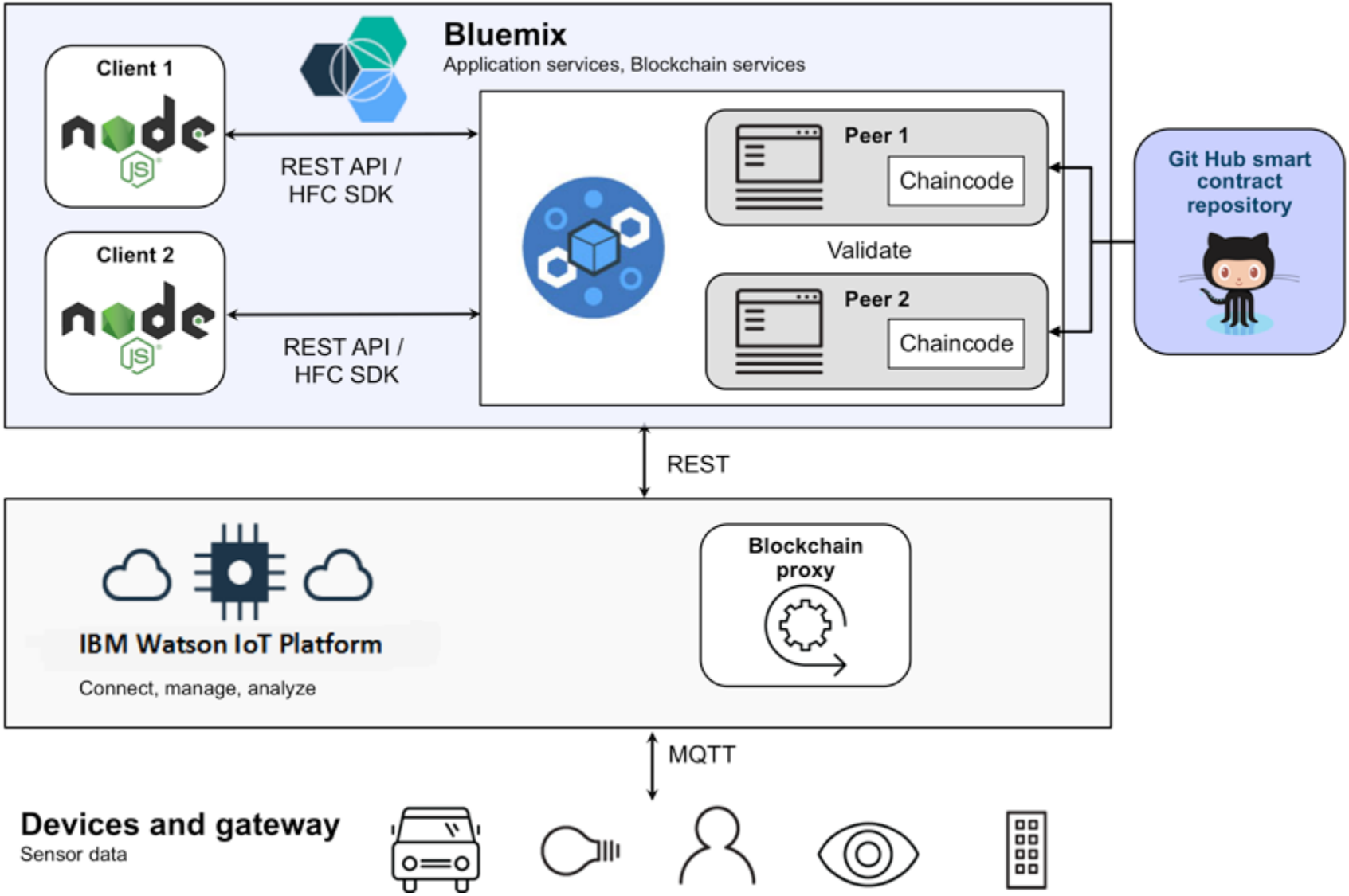
Source: IBM DeveloperWorks

Service map



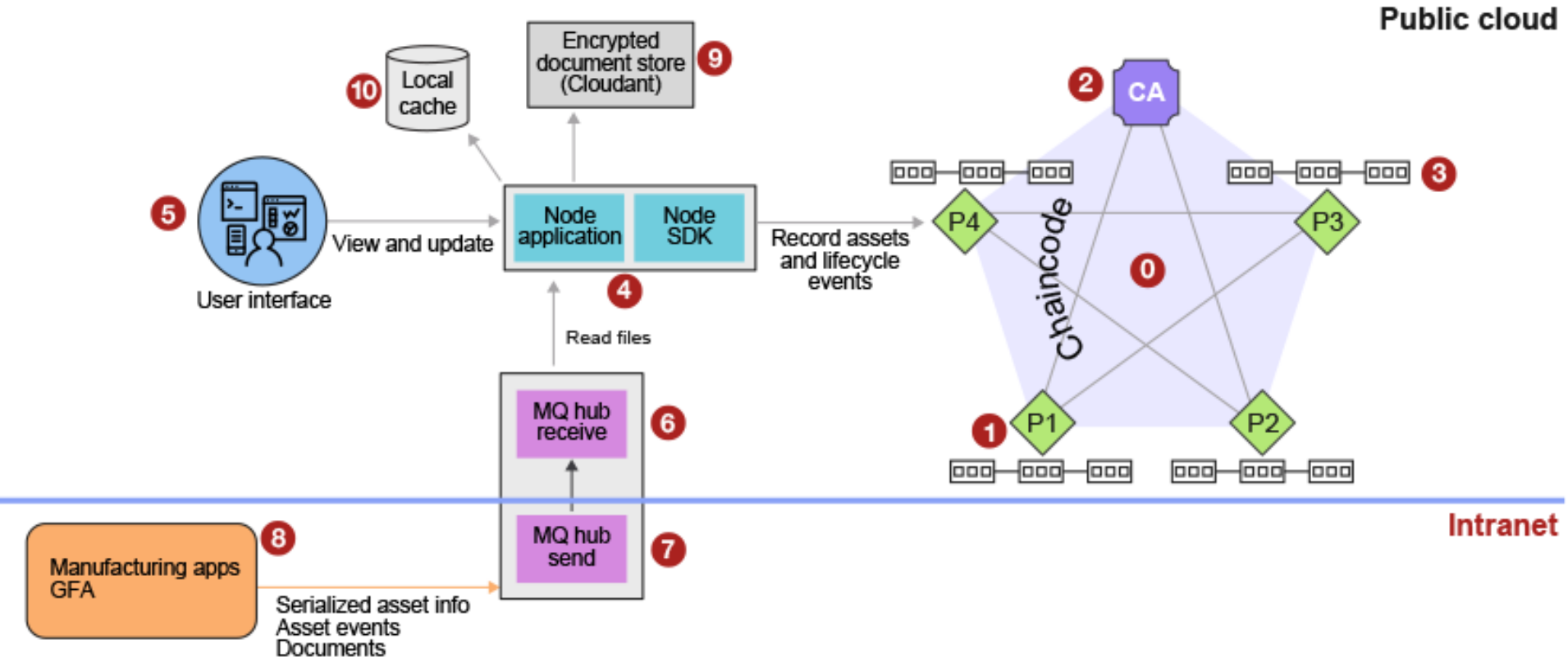
Source: IBM DeveloperWorks

Integrating the physical world



Source: IBM DeveloperWorks

Architecture



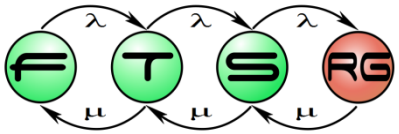
Source: IBM DeveloperWorks

TOWARDS OPEN-SOURCE

Linux Foundation: Blockchain Frameworks

- FABRIC: foundation for developing blockchain applications
  proposed by Tamas Blummer (DAH) and Christopher Ferris (IBM)
- Iroha: distributed ledger for infrastructural projects
- Sawtooth Lake: modular blockchain suite
- Burrow: permissionable smart contract machine.
- COMPOSER: collaboration tool for building blockchain business networks,
- Blockchain Explorer: web app view/query blocks, transactions, chain codes
- Cello: deploying a Blockchain-as-a-Service

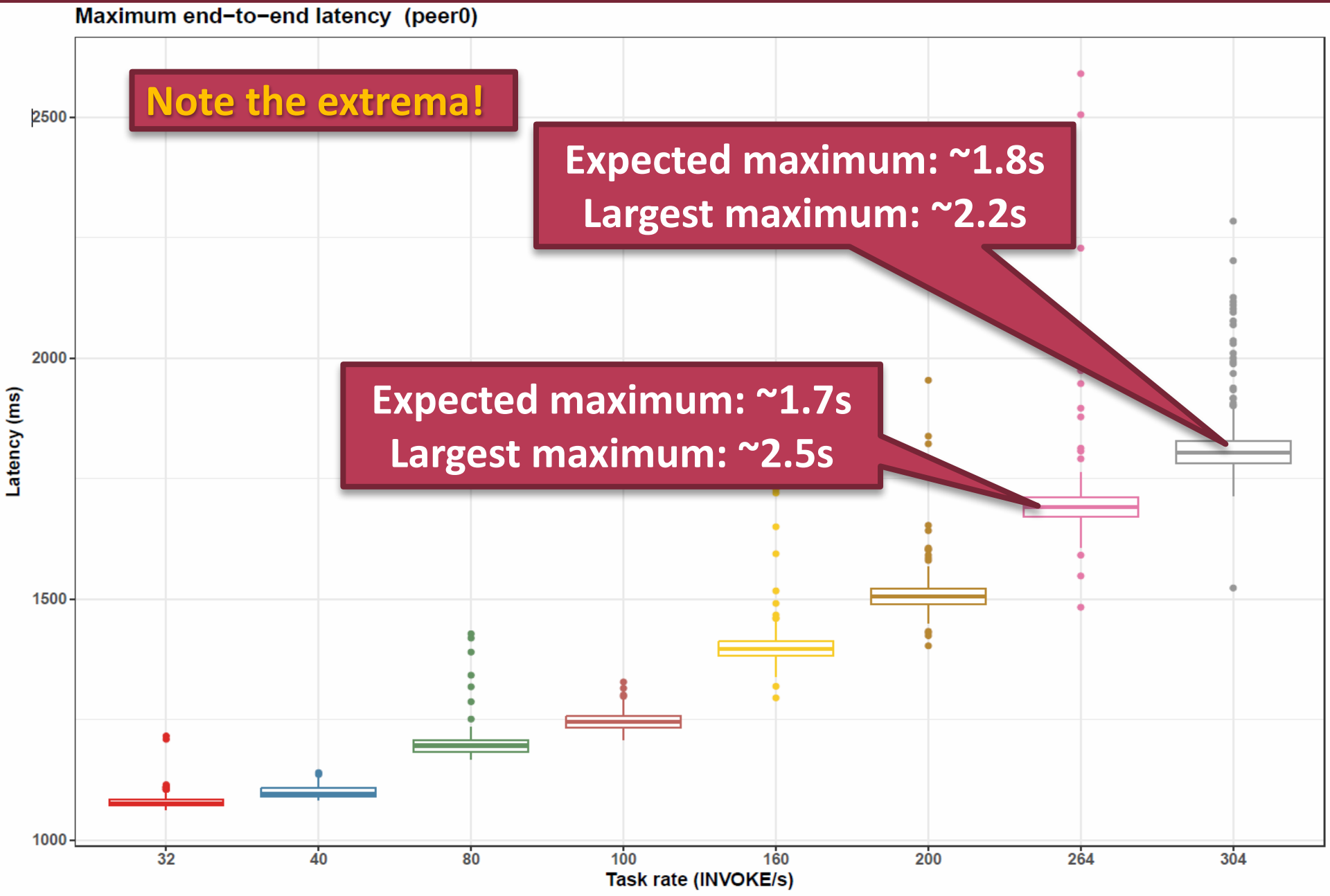
HYPERLEDGER PROJECT



A joint project

PERFORMANCE BENCHMARKING AND MODELING OF THE HYPERLEDGER FABRIC

End-to-end latency – MAX/s



BUSINESS PROCESS EXECUTION ON BLOCKCHAIN PLATFORMS

Blockchainification”

- Porting existing solutions to blockchain platforms
- Similar to „cloudification”

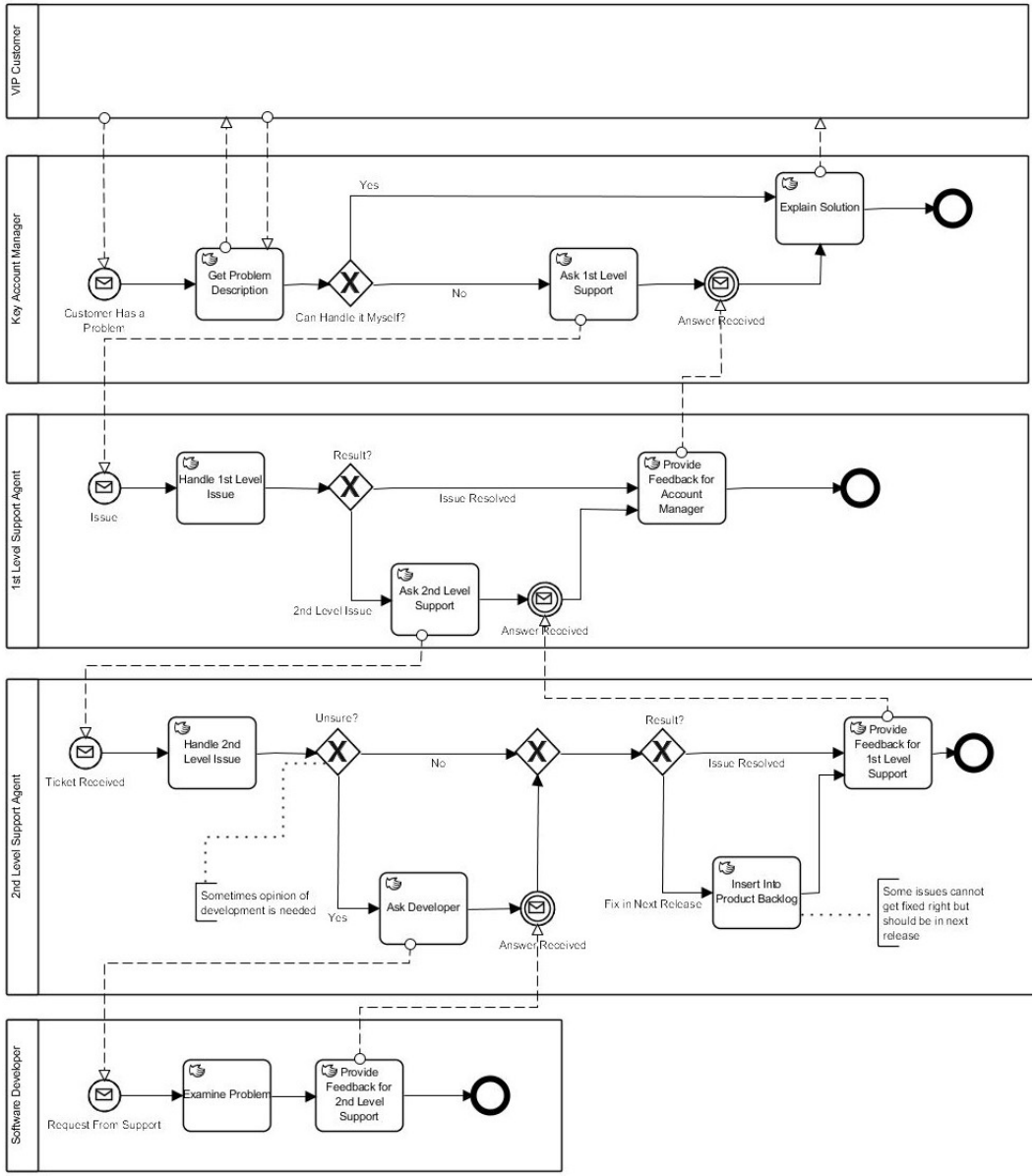
Motivation

- Aspects of business processes
  - High level definition of
  - Managing collaborations
  - Between different participants
  - Executed in a centralized way ☹
- Aspects of enterprise blockchain platforms
  - Managing transactions
  - According to „Smart Contracts”
  - Between different participants
  - In a robust, decentralized, secure way ☺

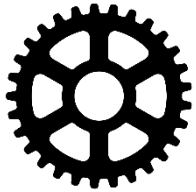
Motivation

- Model driven engineering
  - Higher abstraction levels
  - Increased productivity
    - Reuse of standardized models
    - Simplifying design phase
  - Increased automation during development
  - Easier quality assurance
    - Model validation, model checking, model-based testing
- „

BPMN Elements



Participants



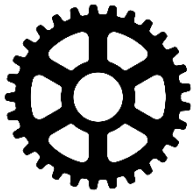
Tasks

Data

Control flow

BPMN Elements in Blockchain Platforms

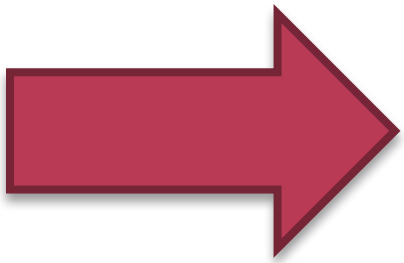
Participants



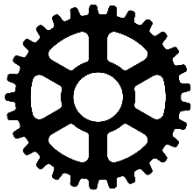
Tasks

Data

Control flow



Organizations in the network



Transactions on the blockchain

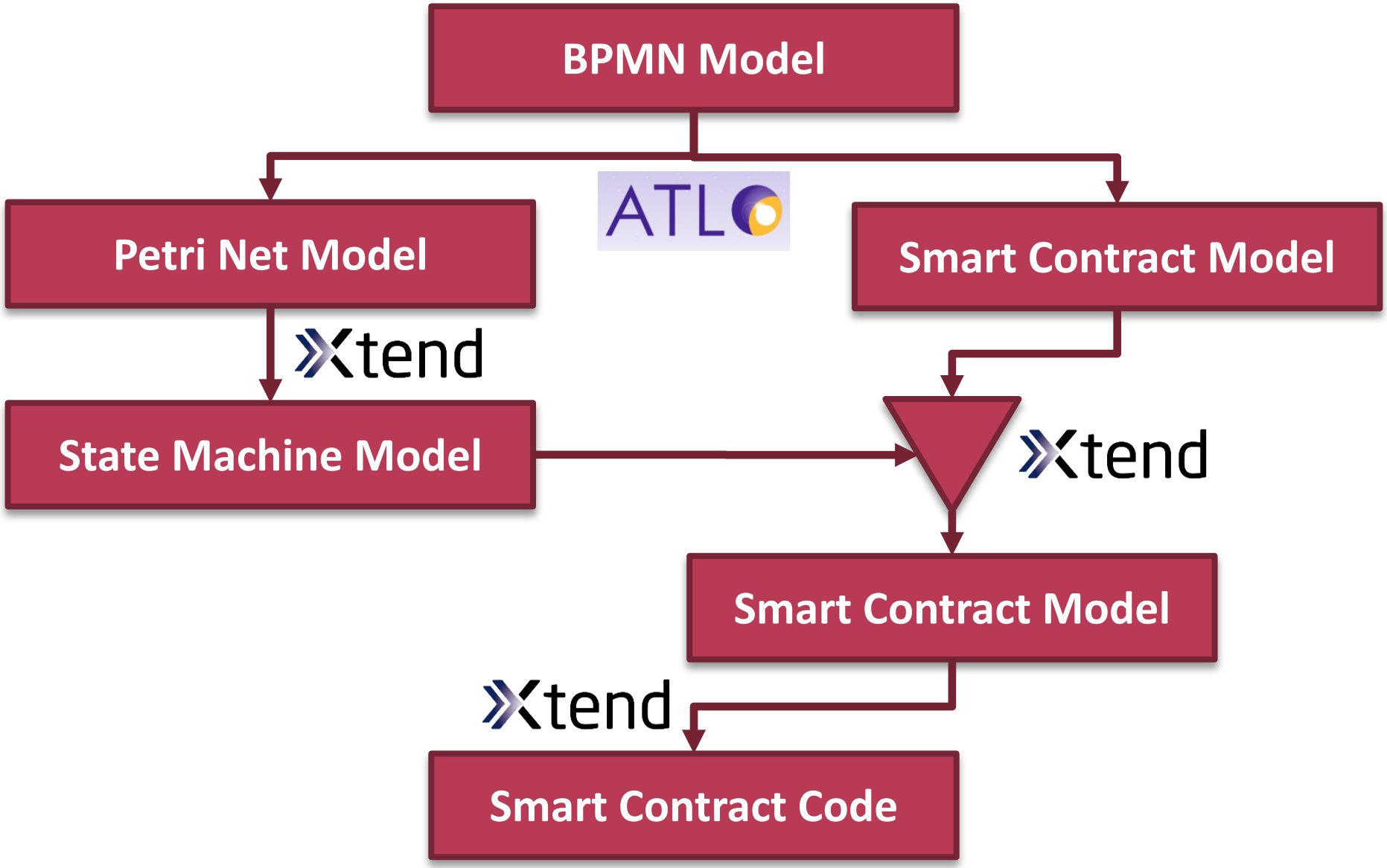
Data model in the „Smart Contract”

Constraints in the „Smart Contract”

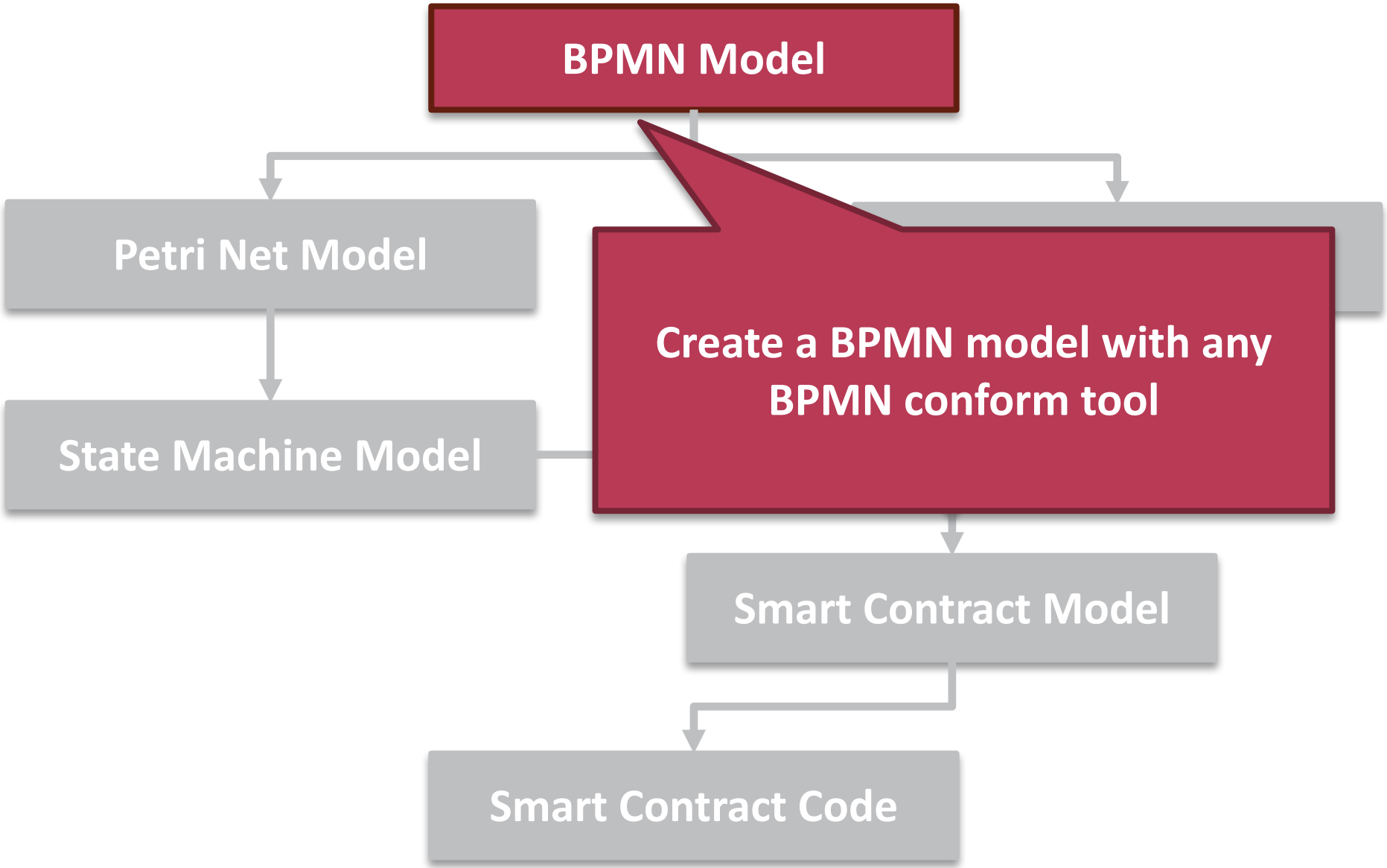
Goals

- Dedicated „Smart Contract” for a business process
  - Cannot trust general execution engines
    - Hard to verify correctness
    - Unnecessary overhead
    - Non-trivial integration with blockchain
  - Easier traceability between code and specification
- Automate parts of the implementation
  - Generate „boilerplate” code
    - Cumbersome, error-prone to implement
  - Leave only the business logic for manual implementation
    - Skeleton for business logic
    - Integration of existing business logic implementation?

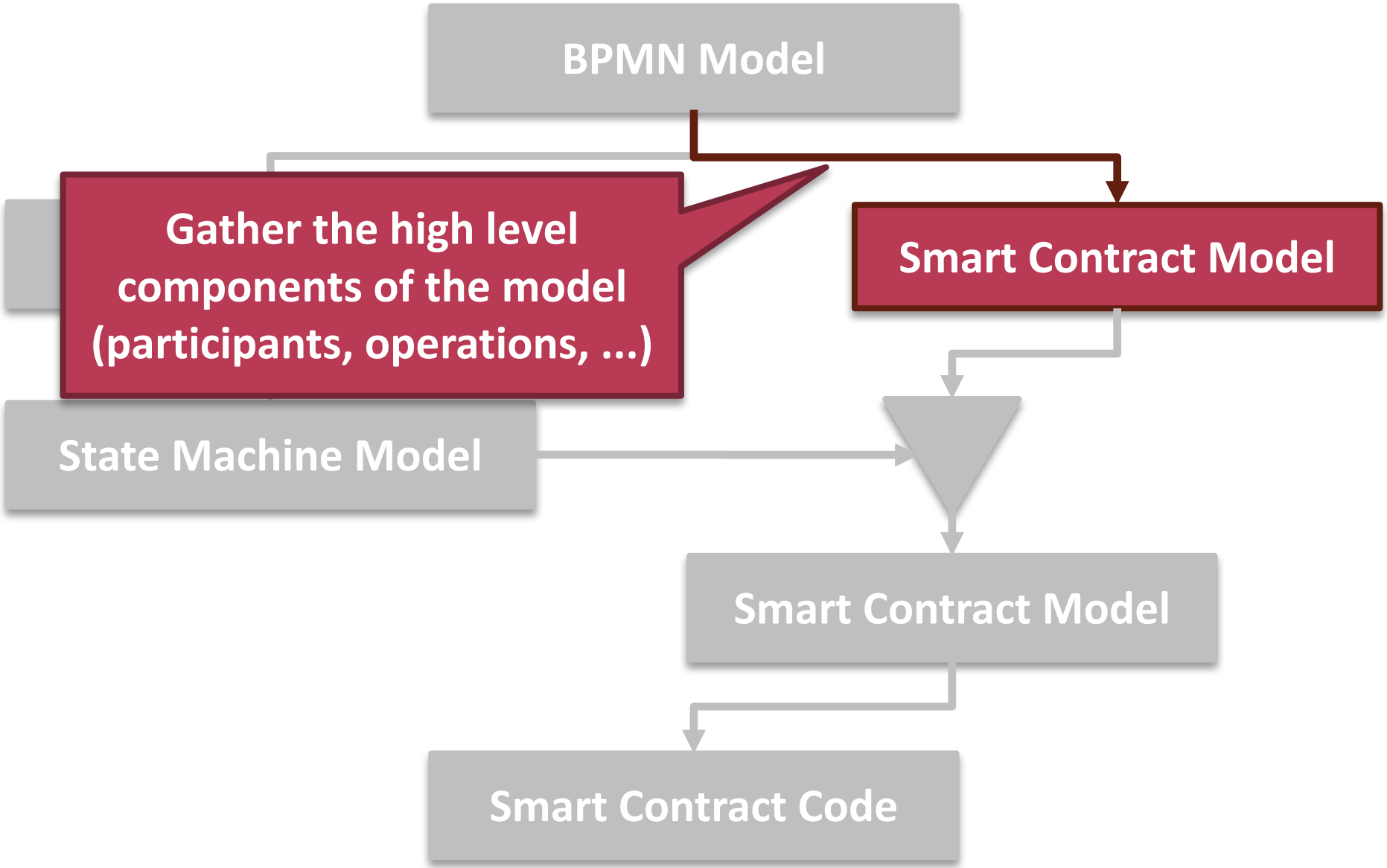
Transformation Workflow



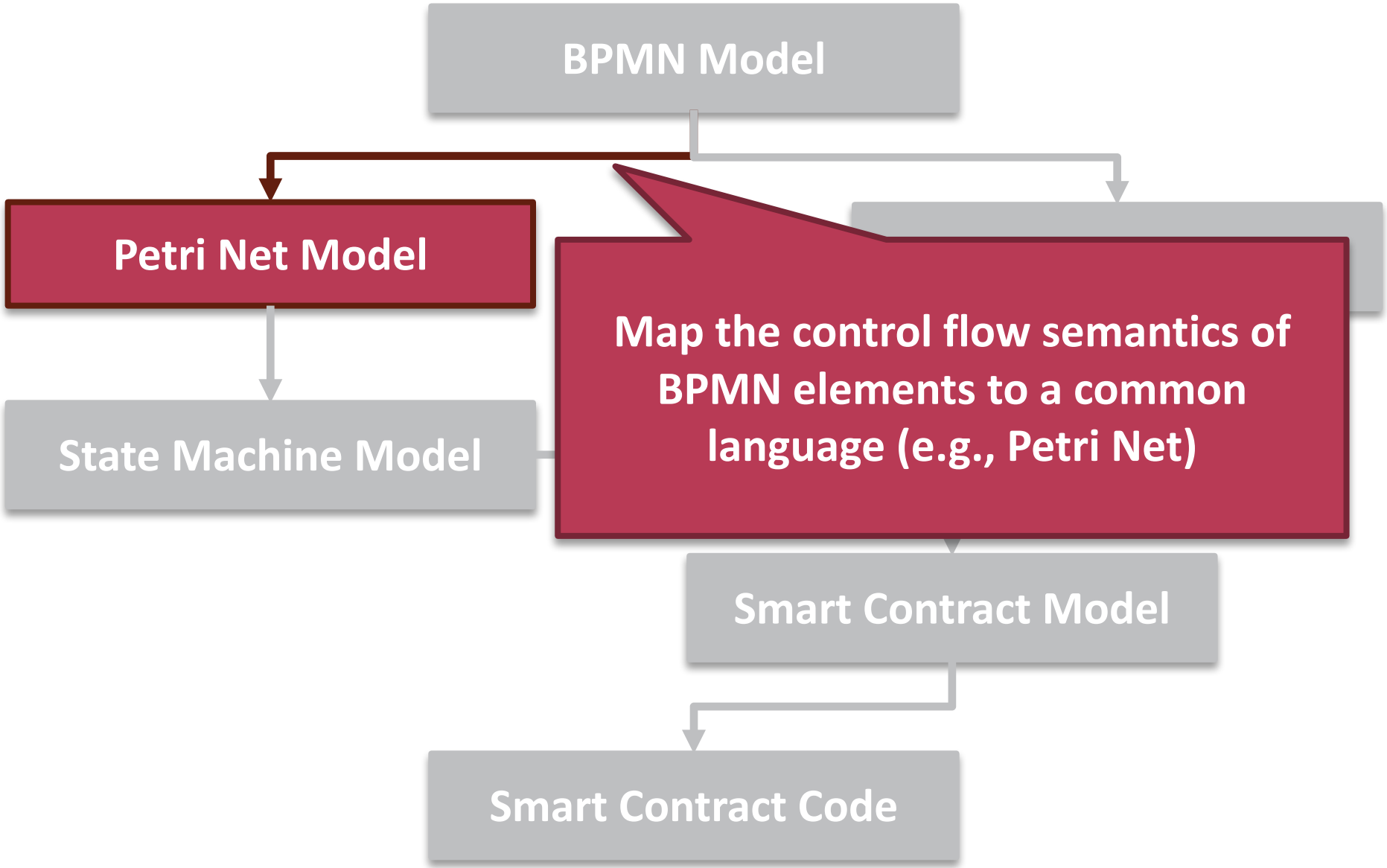
Transformation Workflow



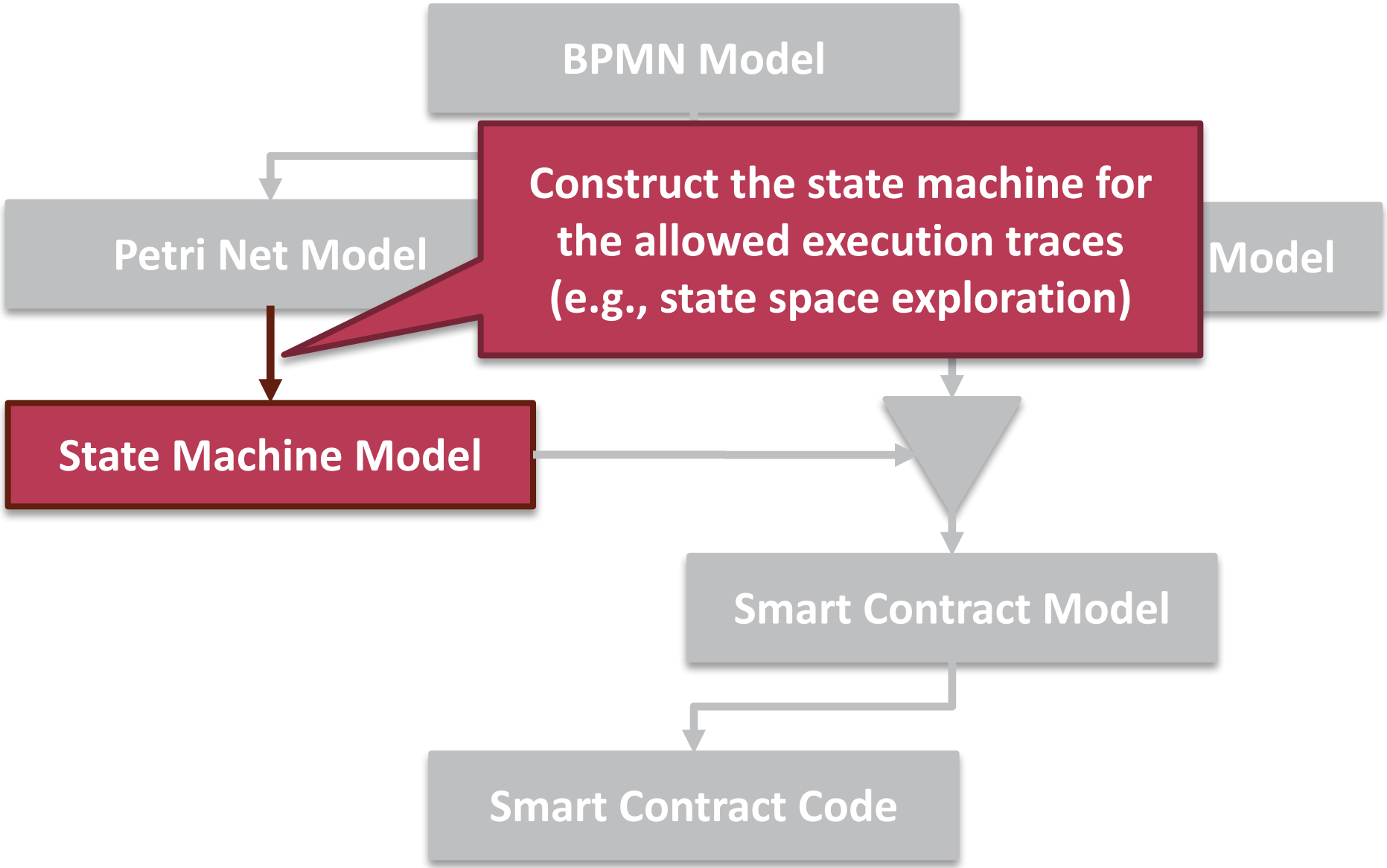
Transformation Workflow



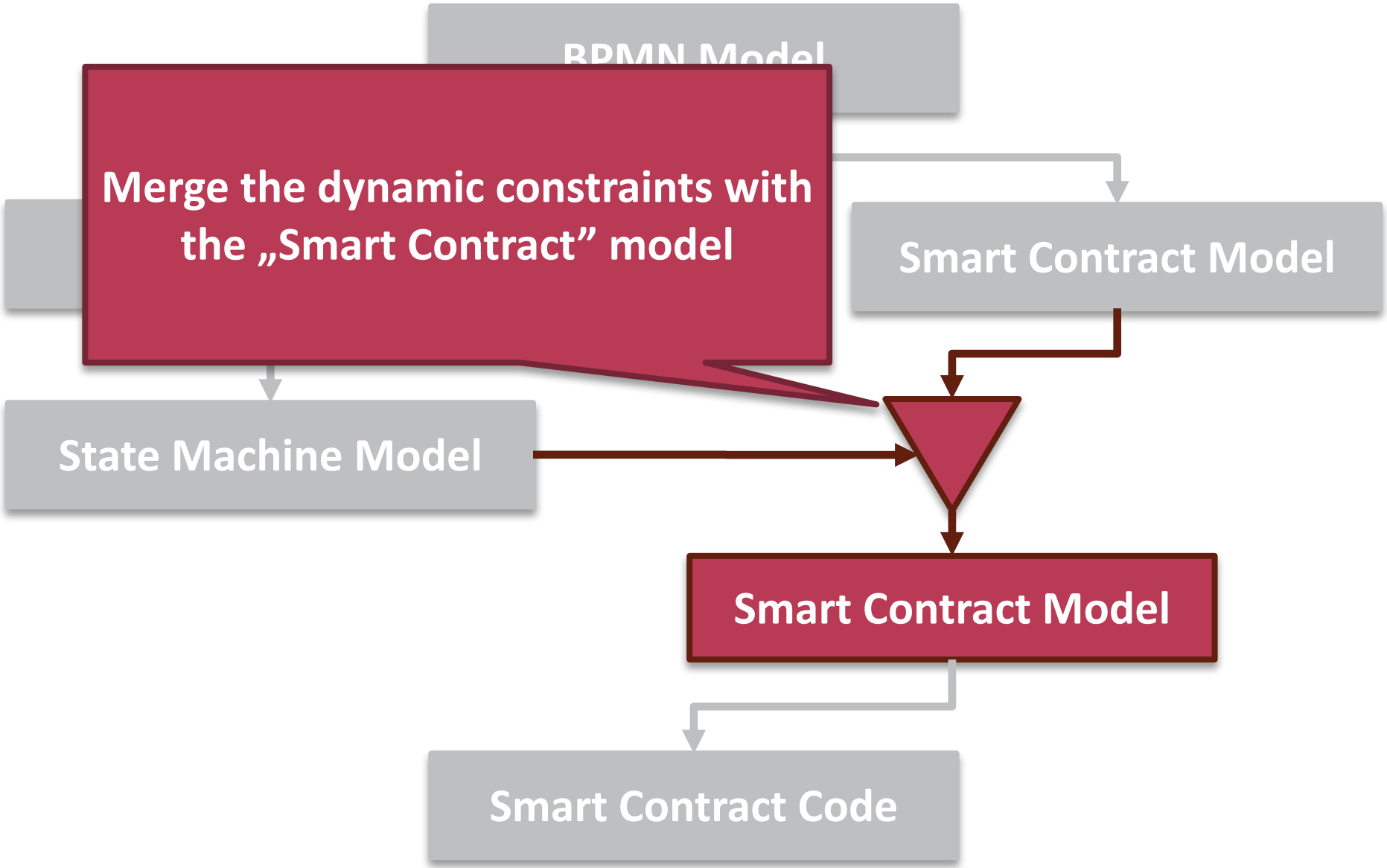
Transformation Workflow



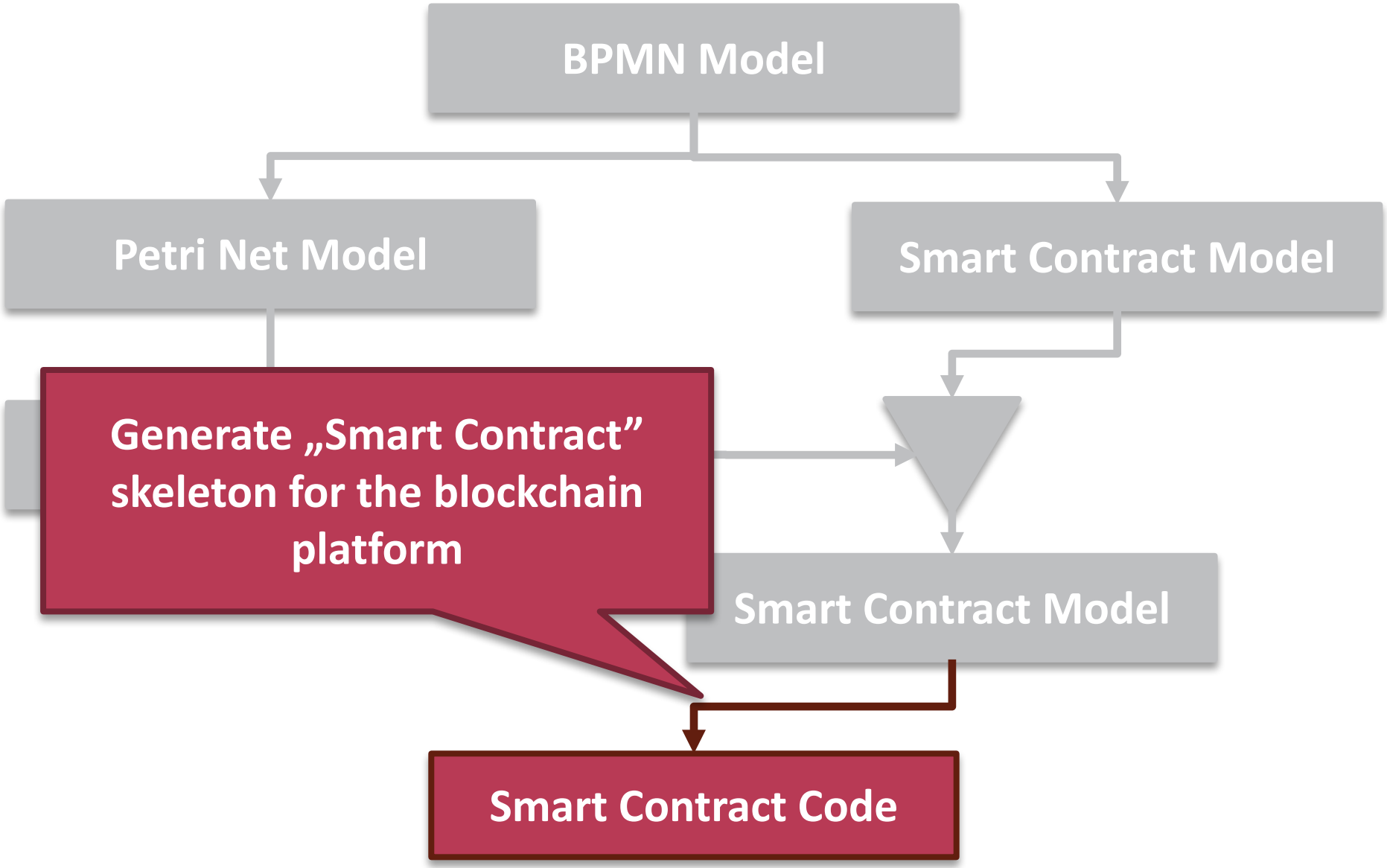
Transformation Workflow



Transformation Workflow



Transformation Workflow



Summary

- Blockchain
  - Distributed system
  - Security
  - Fault-tolerance
  - Interoperability
  - Throughput
  - Coverage of business
- THIS IS THE NEXT IT REVOLUTION

- Cooperation as a service