Blockchain - Demystified

Oriental University, Indore

06 November 2020

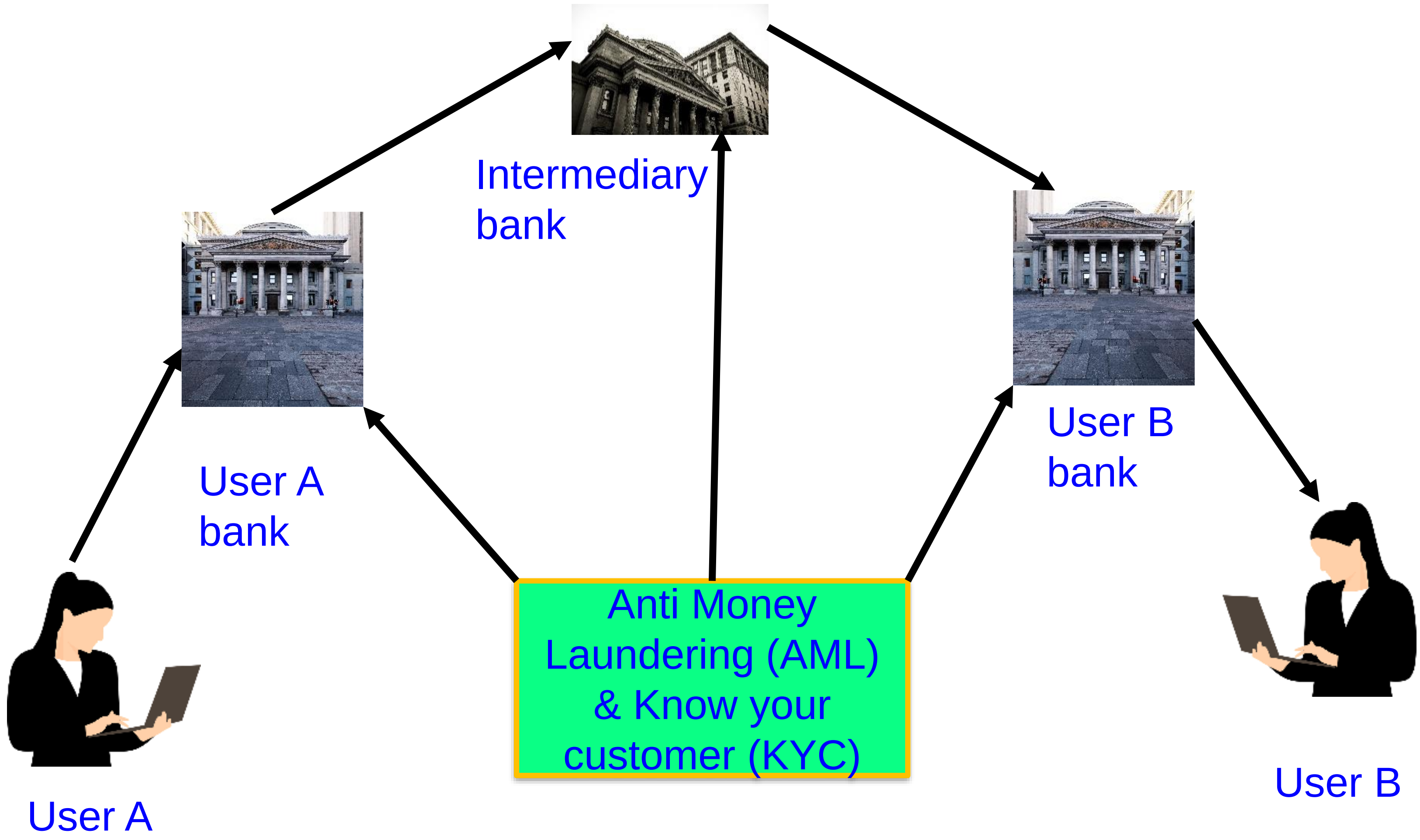
Saraju P. Mohanty
University of North Texas, USA.
Email: saraju.mohanty@unt.edu
More Info: http://www.smohanty.org

Talk Outline

- Blockchain Introduction
- Blockchain Consensus Algorithms
- Blockchain Applications
- Smart Agriculture
- Blockchain Challenges
- Blockchain for Business
- Hardware for Blockchain
- Software Simulation of Blockchain
- Conclusions and Future Directions

Introduction –
Banking → Cryptocurrency

Traditional Banking System



Traditional Banking System

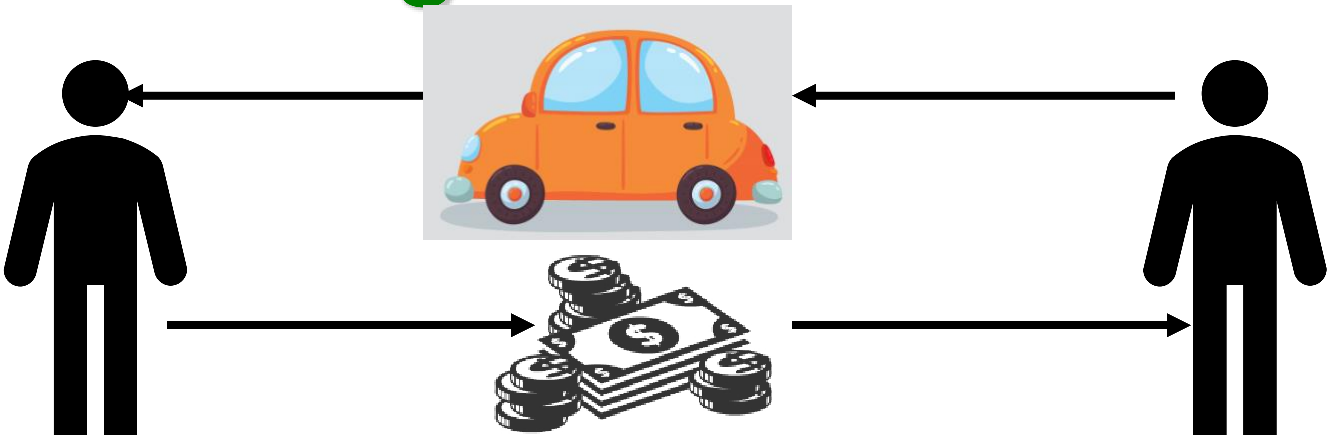
Issues in Banking system

- Transaction fees
- Delay
- Central authority
- Fraud
- Walk-In transactions

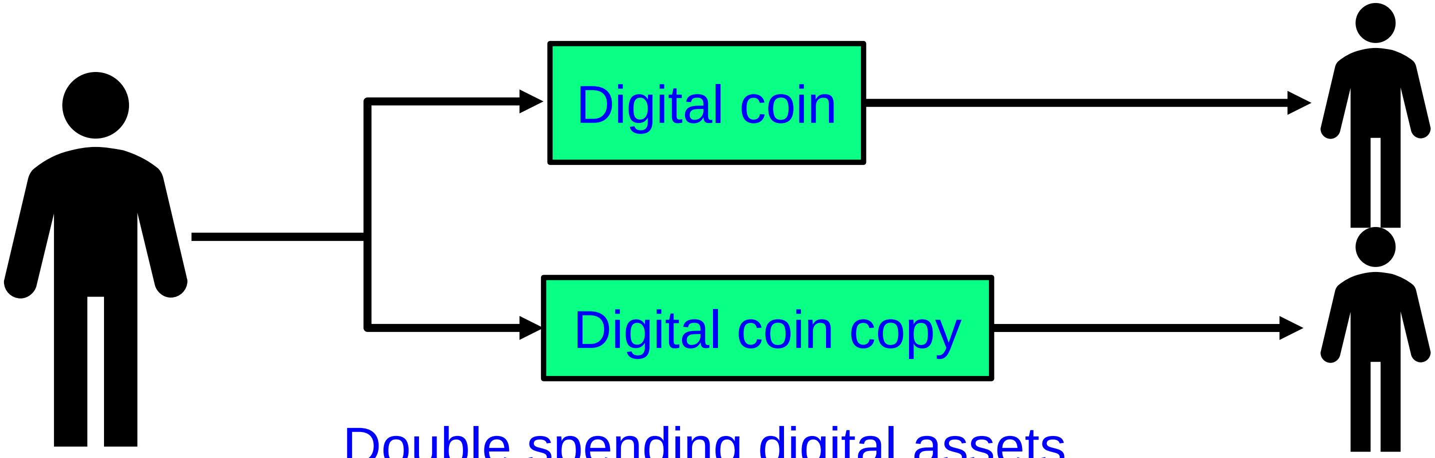
Digital Assets

- Digital asset can be anything of value, such as the combination to your home safe, a secret password, a list, a message, electronic cash, a document, a photo, and so on.
- Encryption + Decryption = Cryptography
- Digital Assets + Cryptography = Cryptocurrency
- Cryptocurrency + Economics = Cryptoeconomics

Double Spending may Happen in Digital Assets



Traditional exchange of physical money – No Double Spending



Double spending digital assets

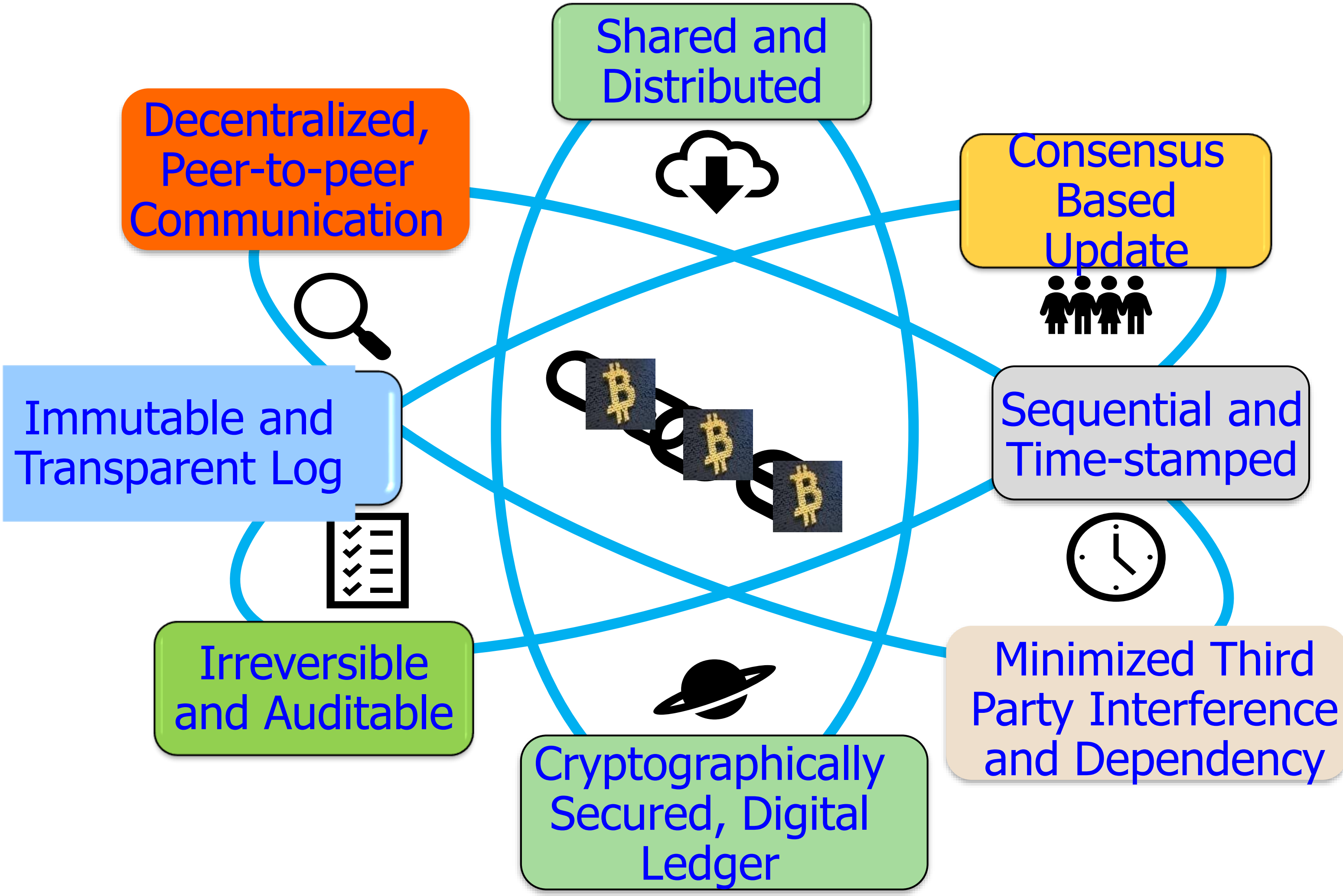
Blockchain Technology

What is Blockchain

What is Blockchain?

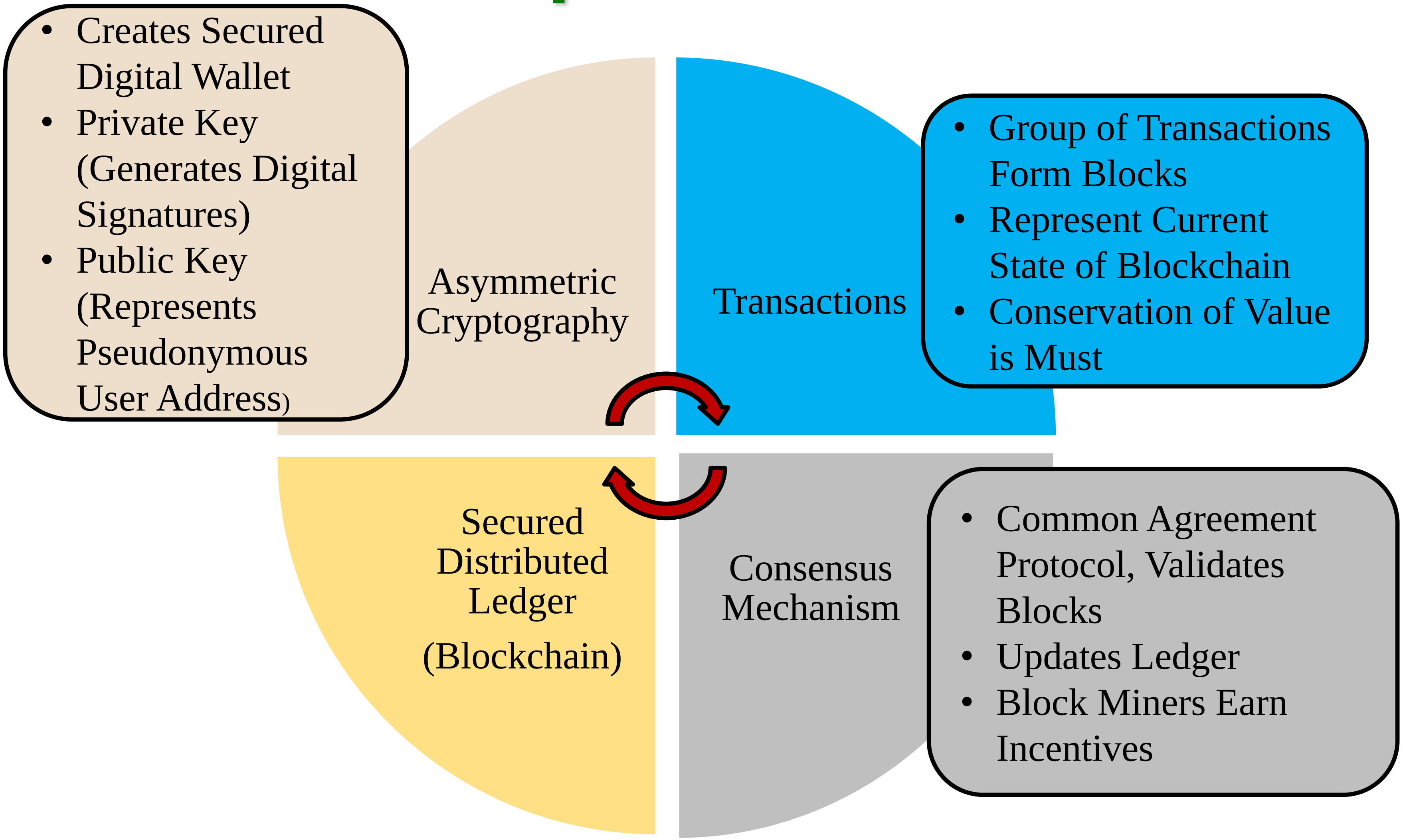
- Technical Definition: A blockchain is a linked list that is built with hash pointers instead of regular pointers.
- Socio–Political–Economic Definition: A blockchain is an open, borderless, decentralized, public, trustless, permission less, immutable record of transactions.
- Financial – Accounting Definition: A blockchain is a public, distributed ledger of peer-to-peer transactions.

Blockchain Characteristics



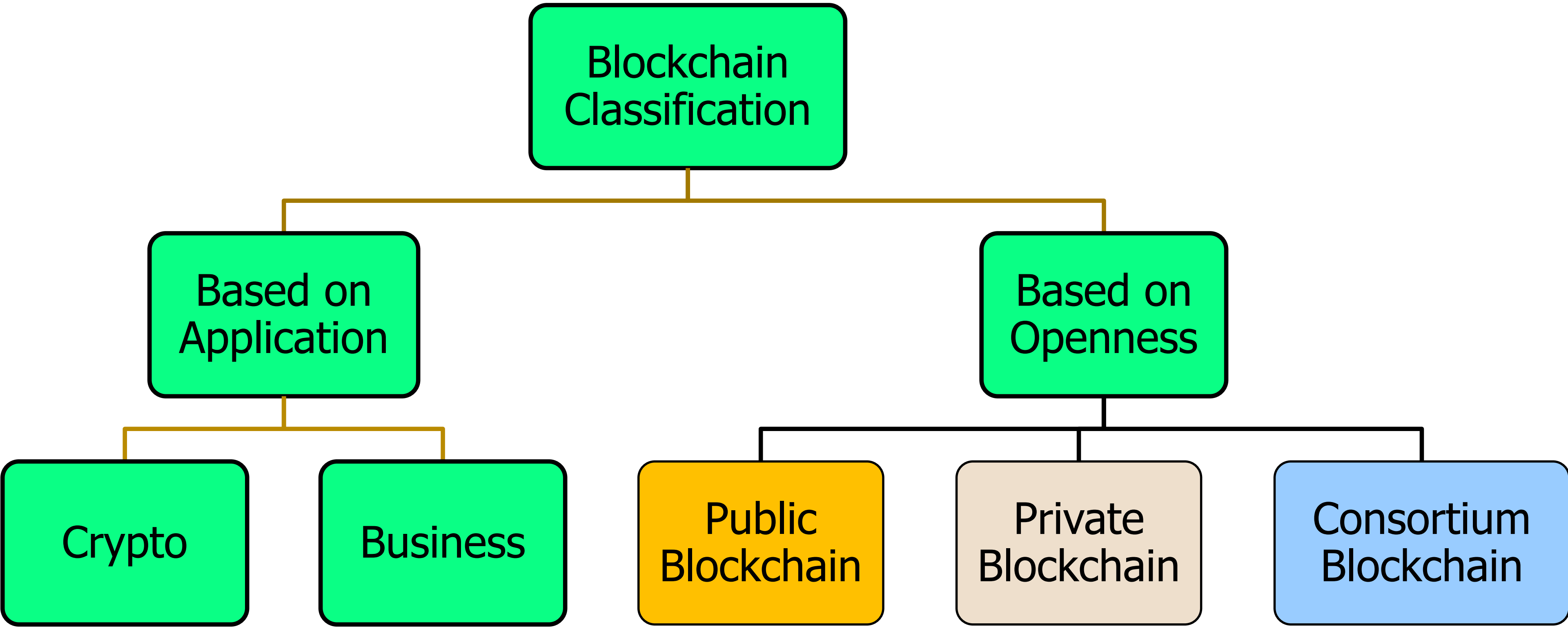
Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, “The Blockchain as a Decentralized Security Framework”, *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 2, March 2018, pp. 18--21.

Different Aspects of Blockchain

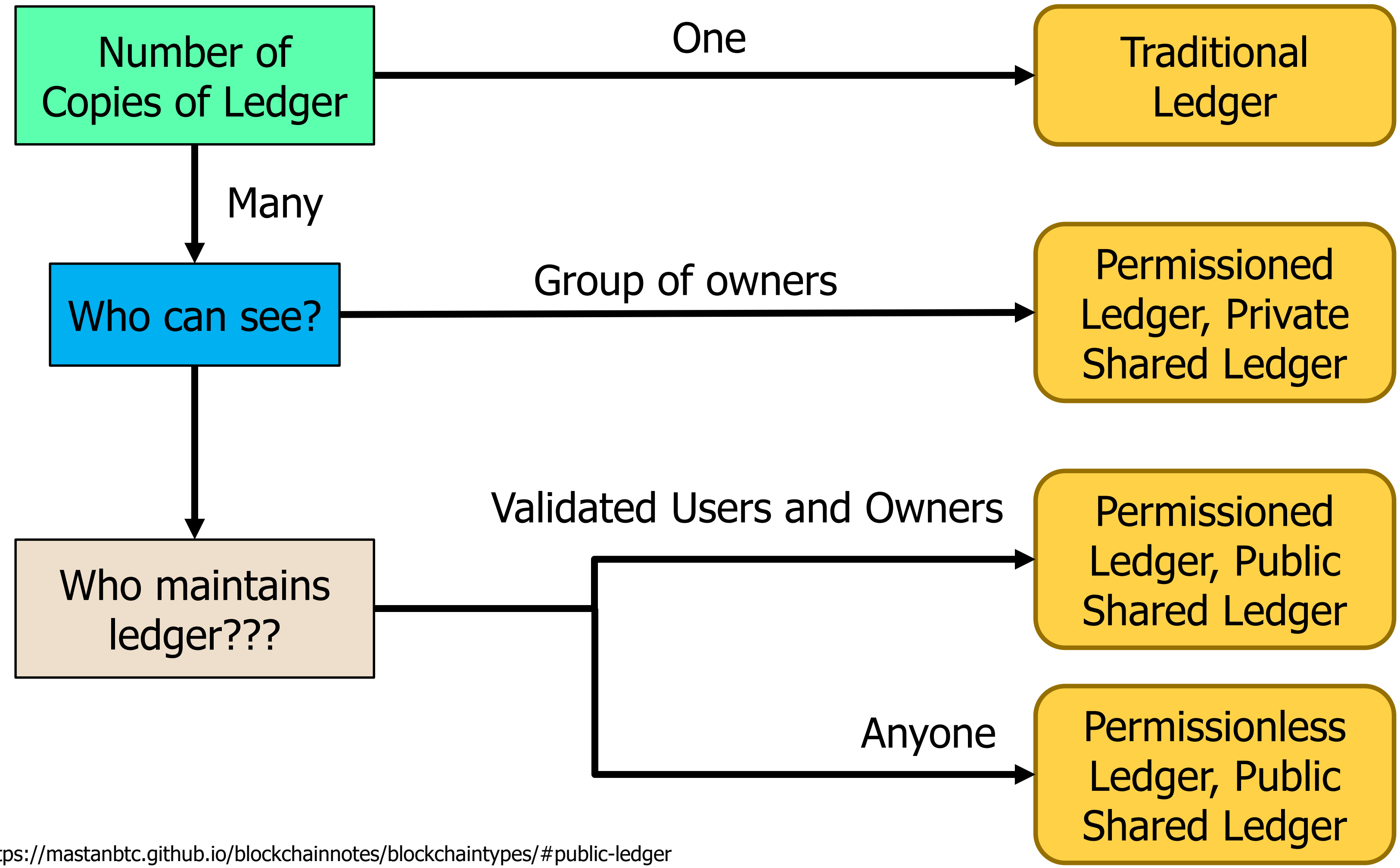


Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you Wanted to Know about the Blockchain", *IEEE Consumer Electronics Magazine*, Volume 7, Issue 4, July 2018, pp. 06--14.

Classification of Blockchain

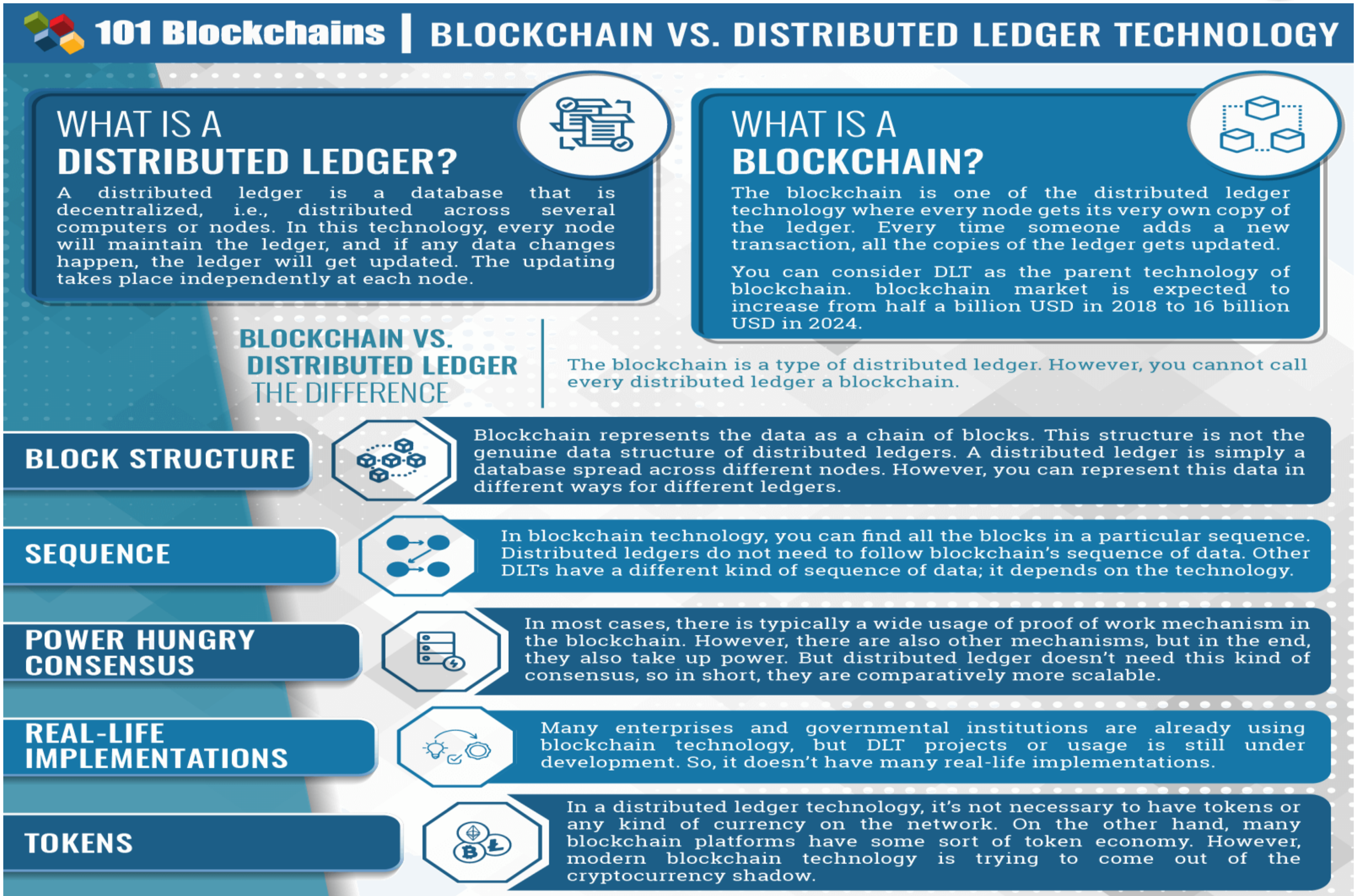


Private vs Public Ledger



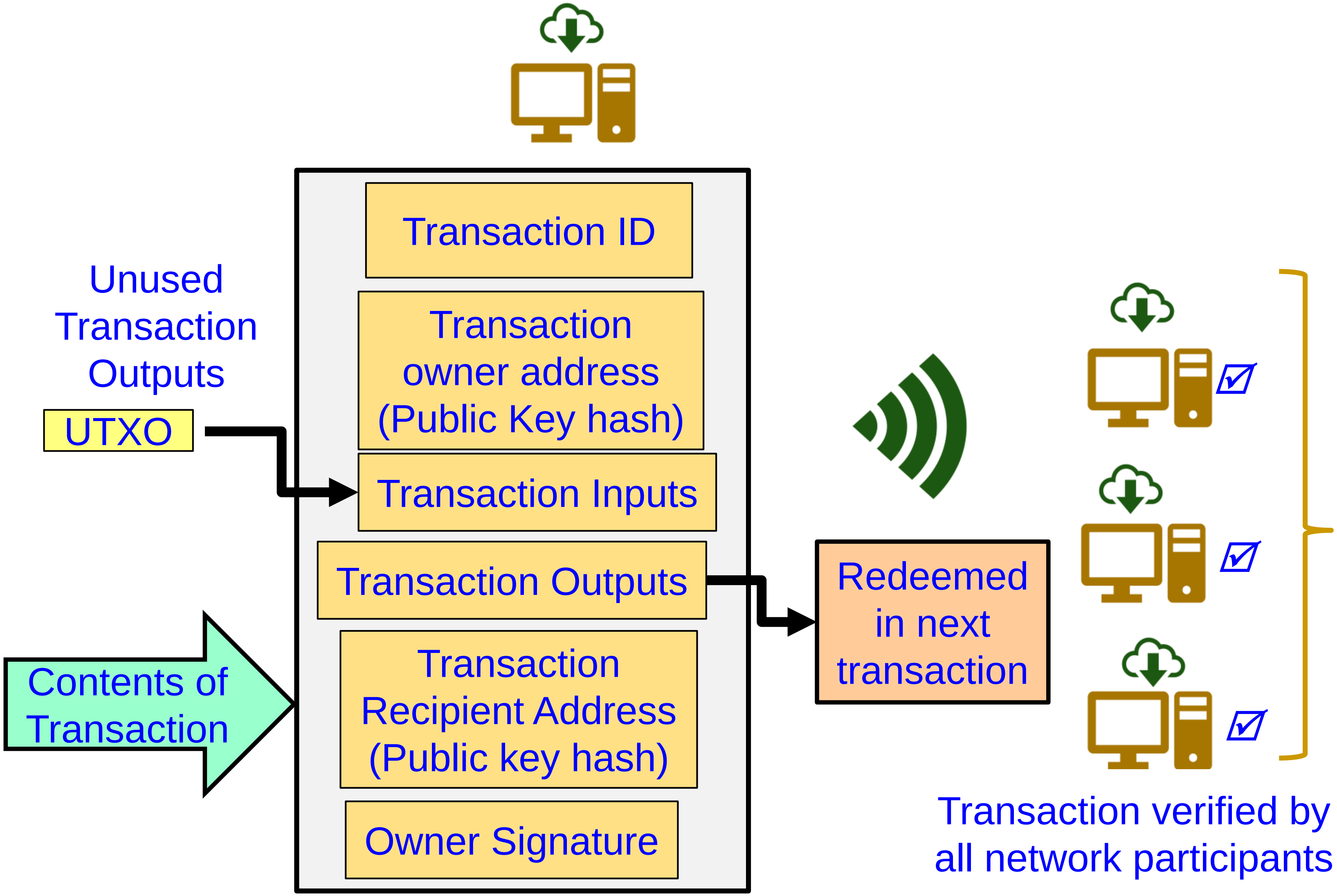
https://mastanbtc.github.io/blockchainnotes/blockchaintypes/#public-ledger

Blockchain vs. Distributed Ledger



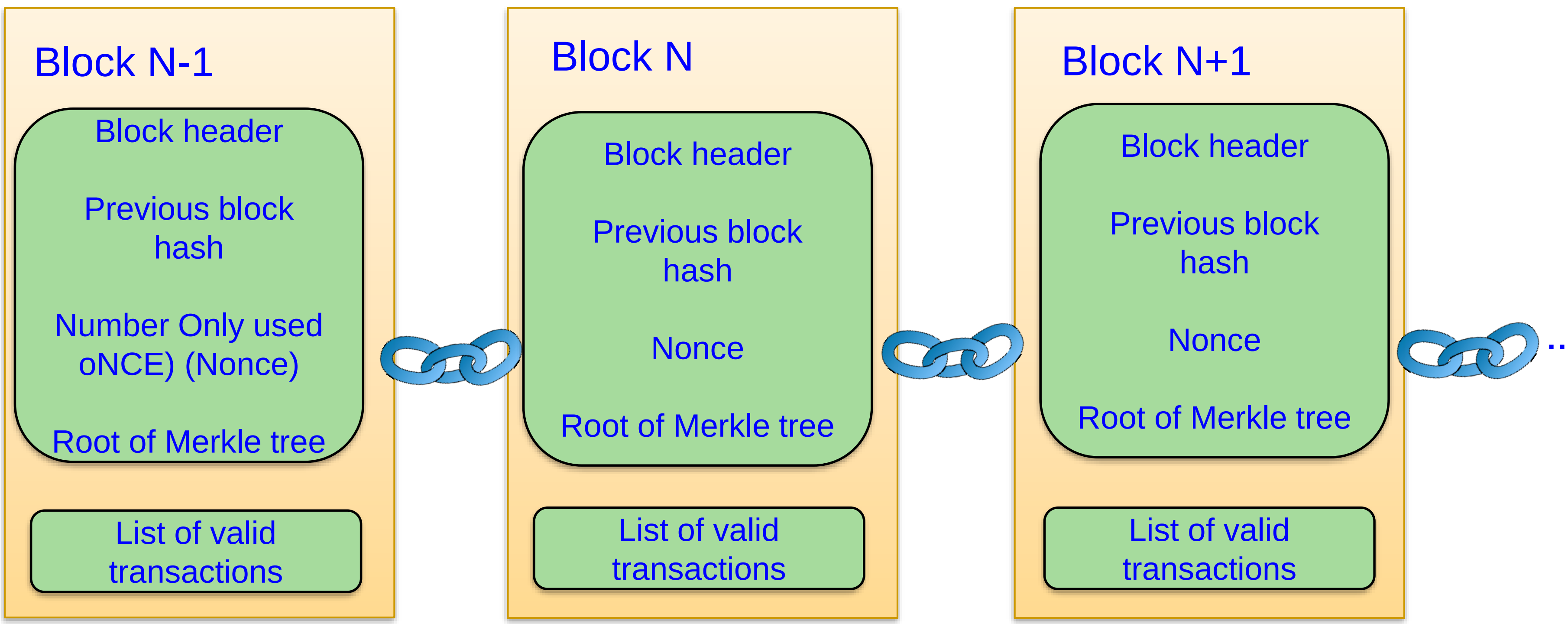
Source: https://101blockchains.com/blockchain-vs-distributed-ledger-technology/

Contents of a Transaction



Transaction verified by
all network participants

Blockchain Structure



Crypto Mining and Miners

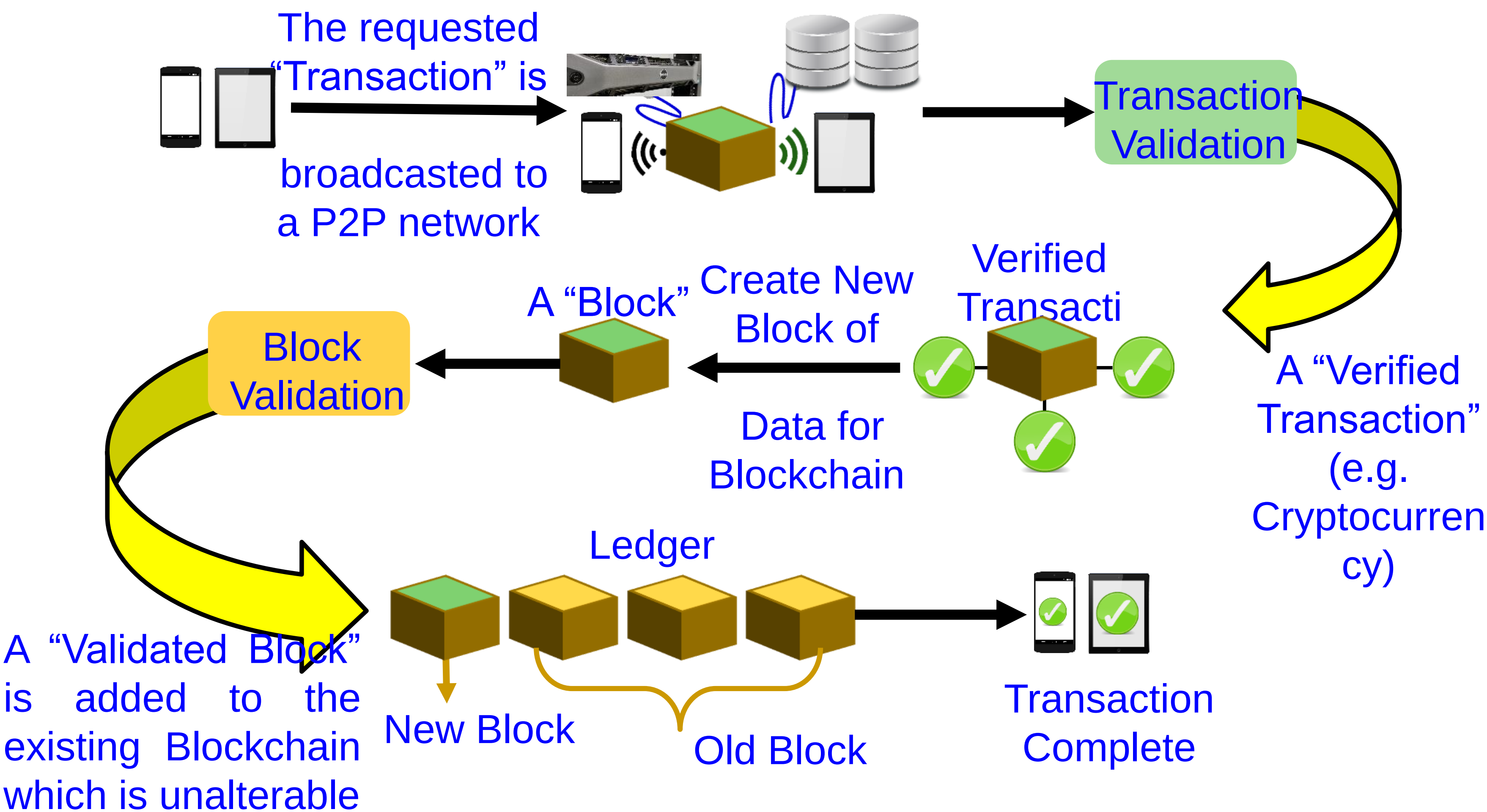
- To prevent double spending all the peers in P2P network is carrying a shared ledger.
- A peer can use this to verify the transactions and help in adding records to ledger.
- Such process is called crypto mining and those peers are called crypto miners.
- Miners will be awarded with some rewards for the work.

Consensus Mechanism

- As blockchain deals with untrusted peers sharing a ledger, there is a need for rules that will ensure security and data integrity.
- An agreement in the network to operate properly even in events of failure.
- This will also determine the rewards to do the work of storing and creating transactions in the network.

How Blockchain Works?

Blockchain - Working Model

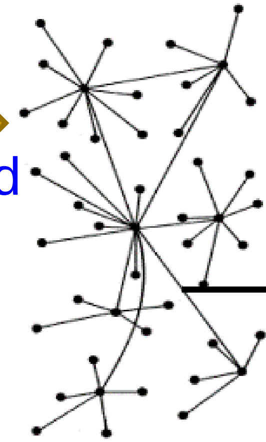


Source: Deepak Puthal, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, and Gautam Das, "Everything you Wanted to Know about the Blockchain", *IEEE Consumer Electronics Magazine*, Vol. 8, No. 4, pp. 6--14, 2018.

Transaction Generation

Transaction is requested by a node

Broadcasted to a P2P network of nodes



P-2-P Network

Users in same network know address of each other

It is called as input transaction: has amount to be transferred + recipient's bitcoin (BTC) address

Input Transaction

Public Key Hash of receiver: 'A' BTC address

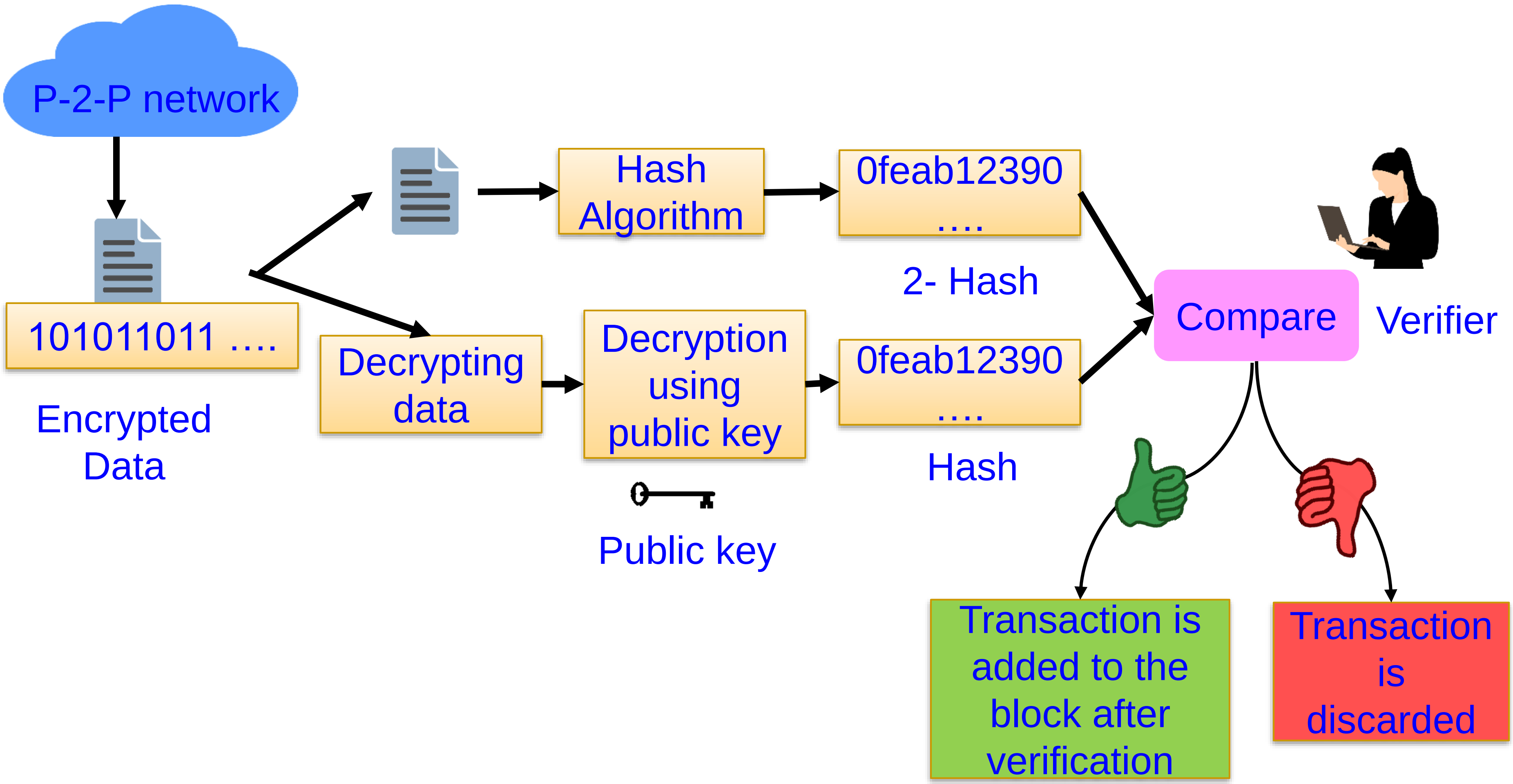
Hashing (e.g. SHA-256)

Unique Transaction identity

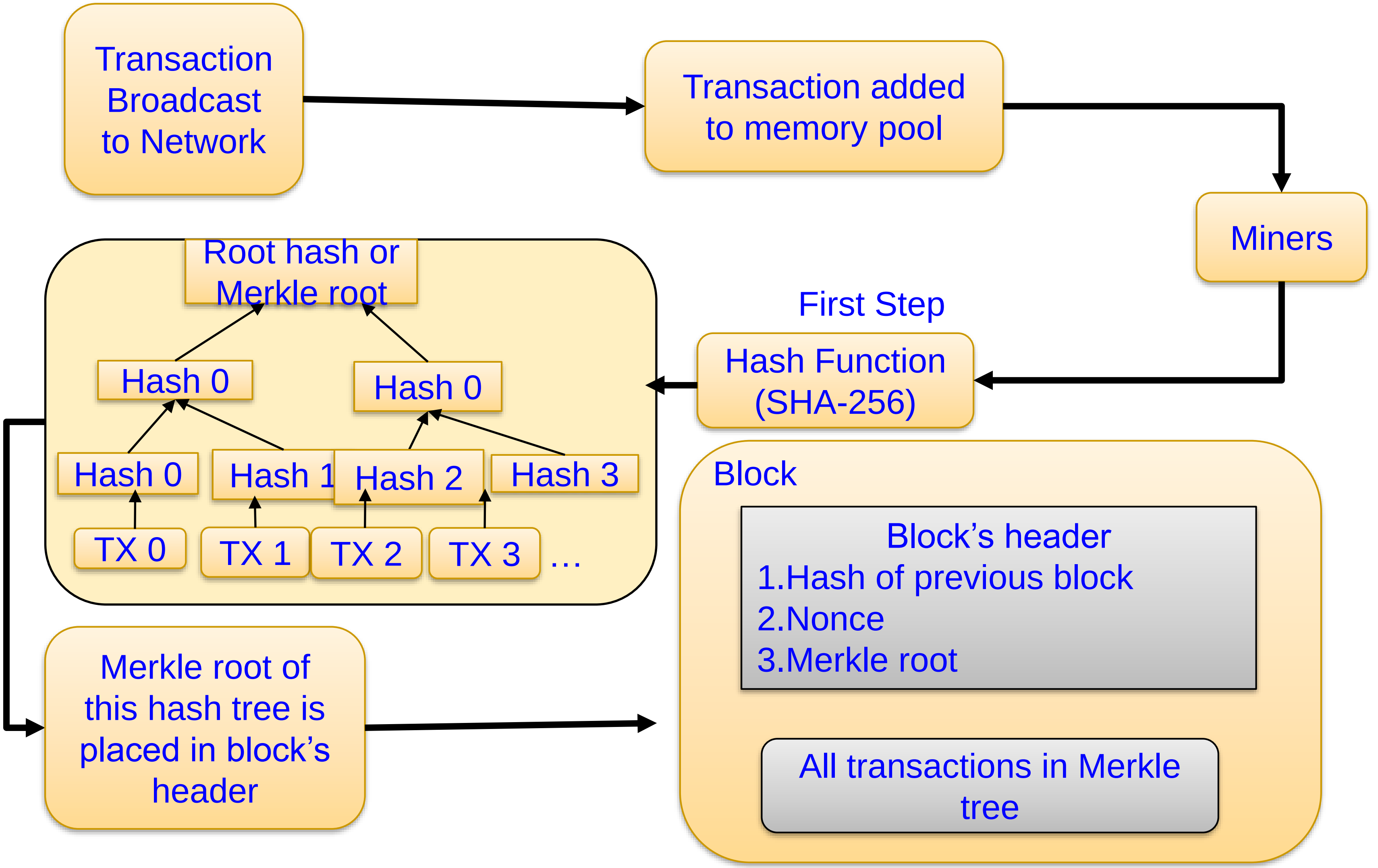
Sender's Private key

Digital Signature

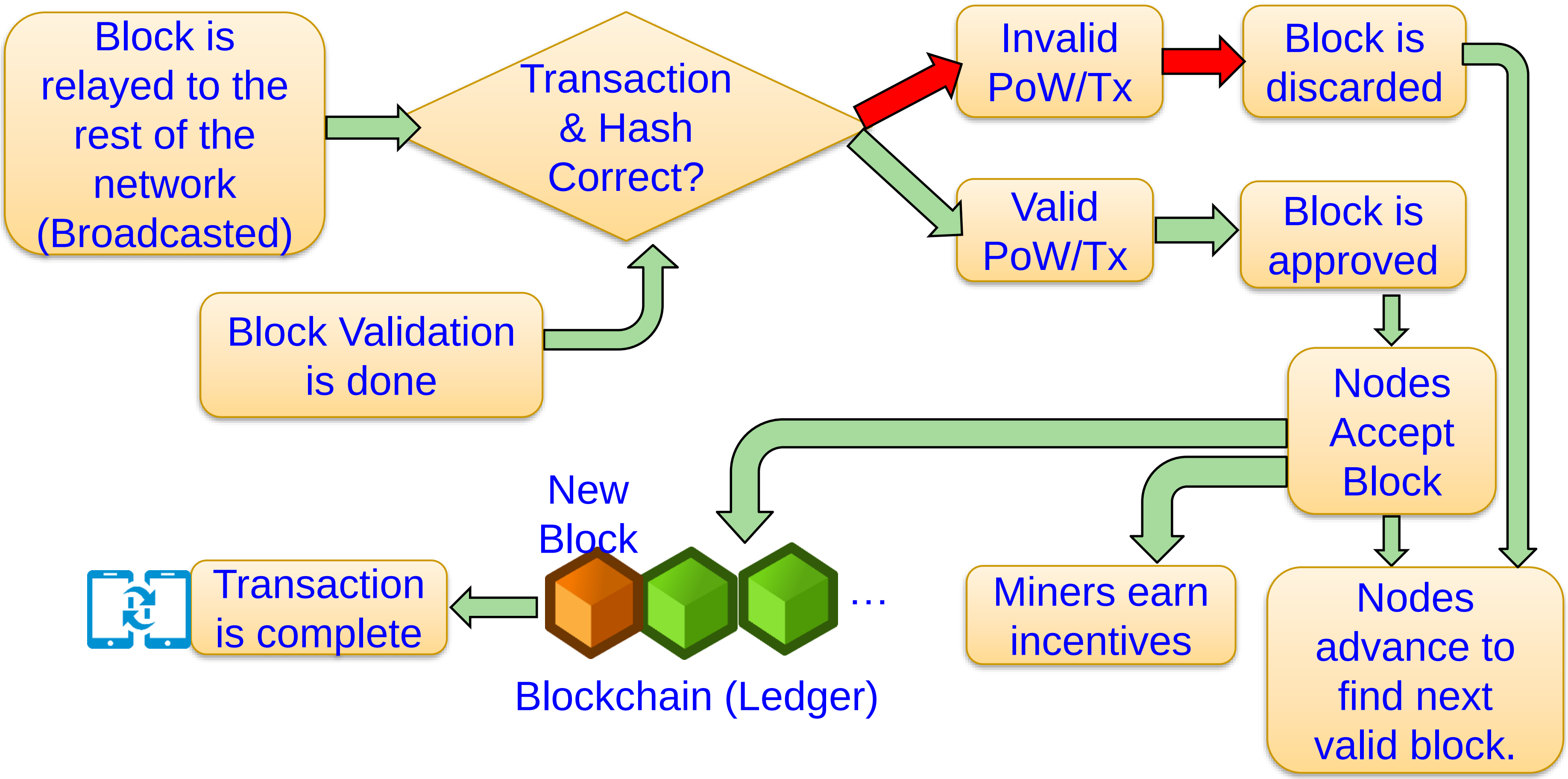
Transaction Validation



Block Generation



Block Validation

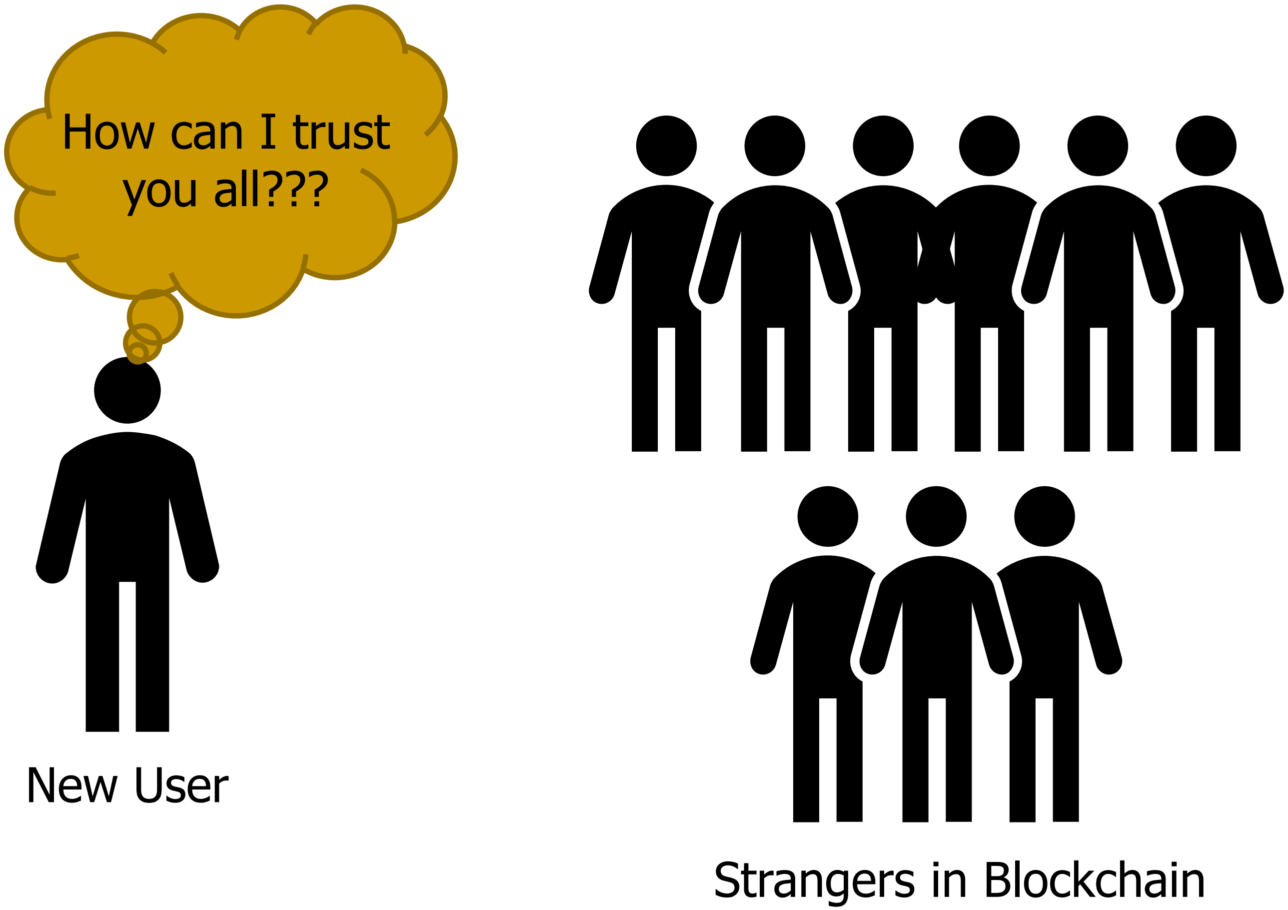


Transaction Verification

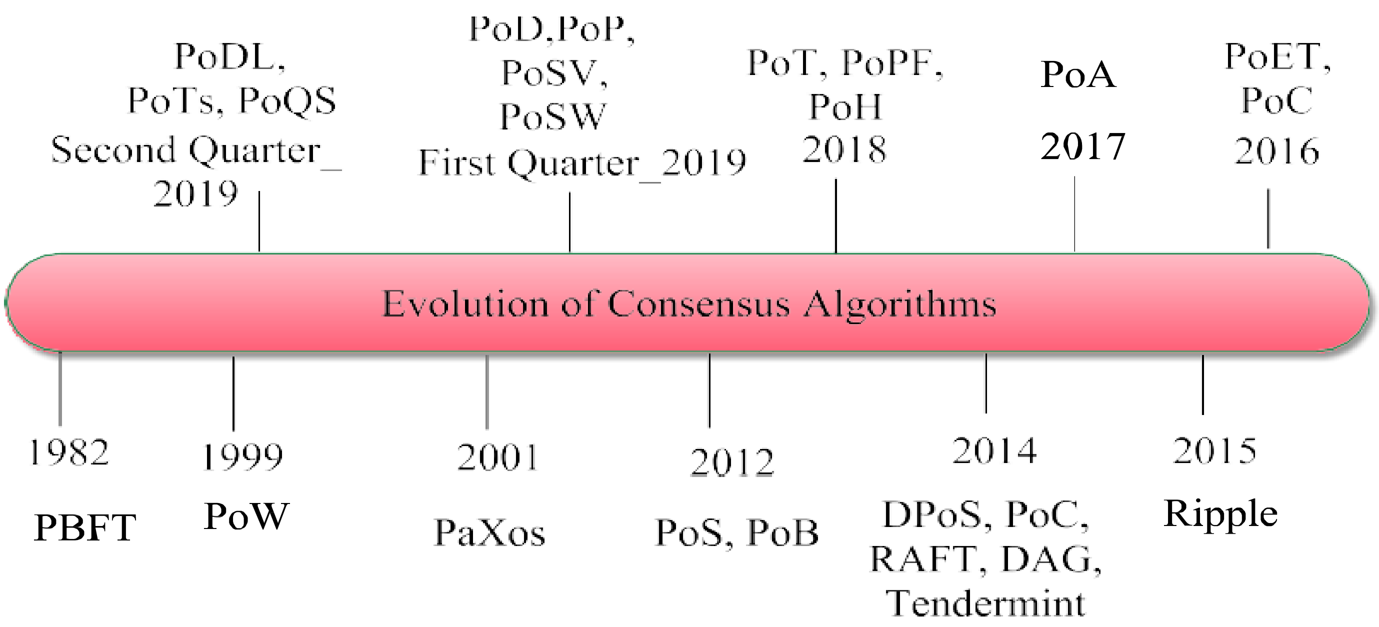
- General nodes are not required to store all the transactions
- Only block headers are stored
- To verify a transaction
  - Get the latest longest chain
  - Obtain the Merkle branch linking the transaction to block
  - If the node is accepted and block is created, transaction is verified

Blockchain Consensus Algorithms

Trust in Blockchain

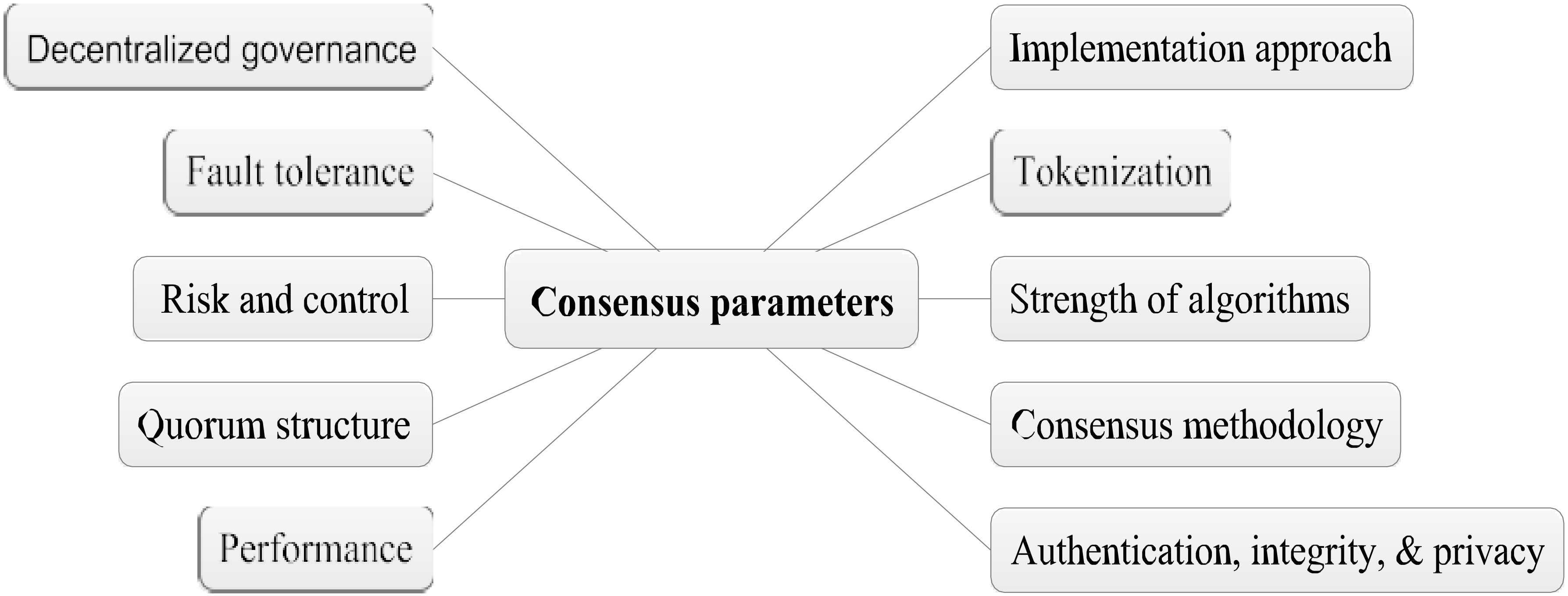


Blockchain Consensus Algorithm - Timeline



Source: U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh and W. Hong, "A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems," in *IEEE Access*, vol. 8, pp. 54371-54401, 2020, doi: 10.1109/ACCESS.2020.2981415.

Blockchain Consensus - Parameters



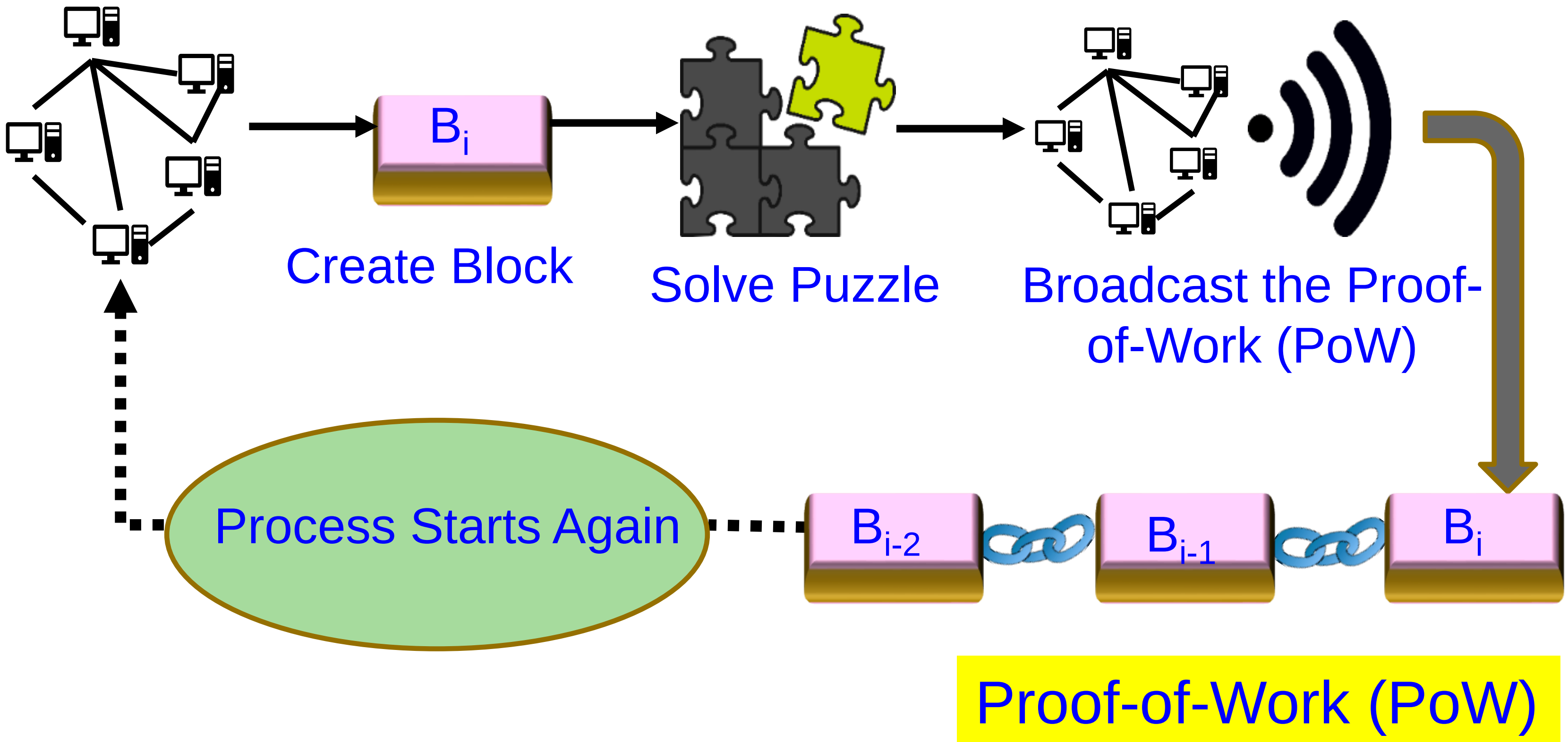
Source: U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh and W. Hong, "A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems," in *IEEE Access*, vol. 8, pp. 54371-54401, 2020, doi: 10.1109/ACCESS.2020.2981415.

Consensus Algorithm Types

Blockchain Consensus Algorithm

- **Validation Based**
  - Proof of Work (PoW)
  - Proof of Stack (PoS)
  - Proof of Activity (PoA)
  - Proof of Relevance (PoR)
  - Proof of Elapsed Time
- **Voting Based**
  - Ripple
  - Proof of Vote
  - Proof of Trust
- **Authentication Based**
  - Proof of Authentication (PoAh)
  - Proof of PUF-Enabled Authentication (PoP)

Proof-of-Work (PoW)

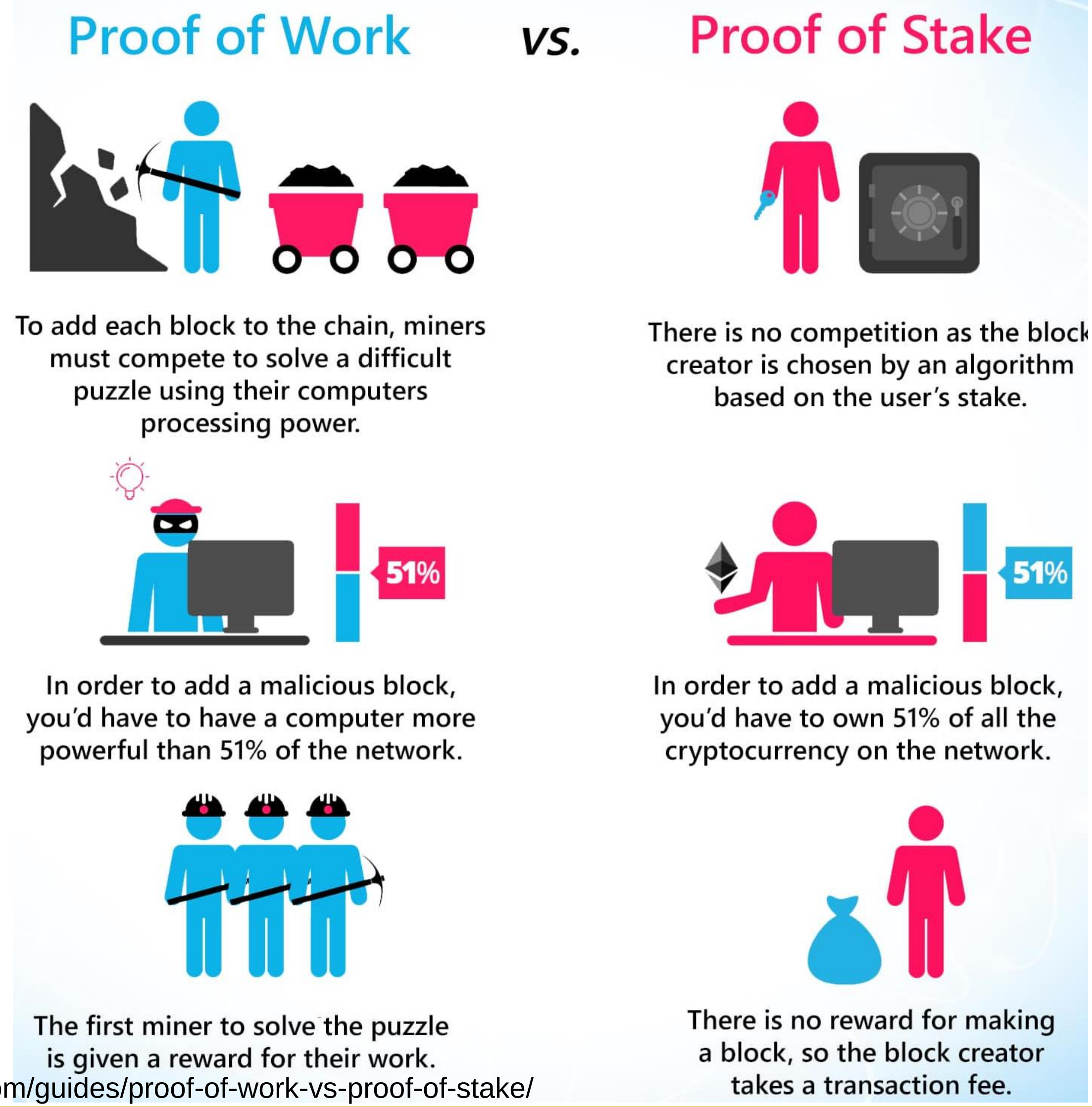


Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, “PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and DataSecurity in the Internet of Everything(IoE)”, arXiv Computer Science, arXiv:1909.06496, Sep 2019, 37-pages.

Proof-of-Stake (PoS)

- Stake of coins instead of mining
- Creator of new block is chosen randomly by various combinations of wealth and age of stake
- Coin age is used to select the node
  - Coin age= number of coins * number of days coins are held
- Once a block is signed by elected node, coin age for that node will go back to zero and start again
- No mining rewards, only transaction fees.

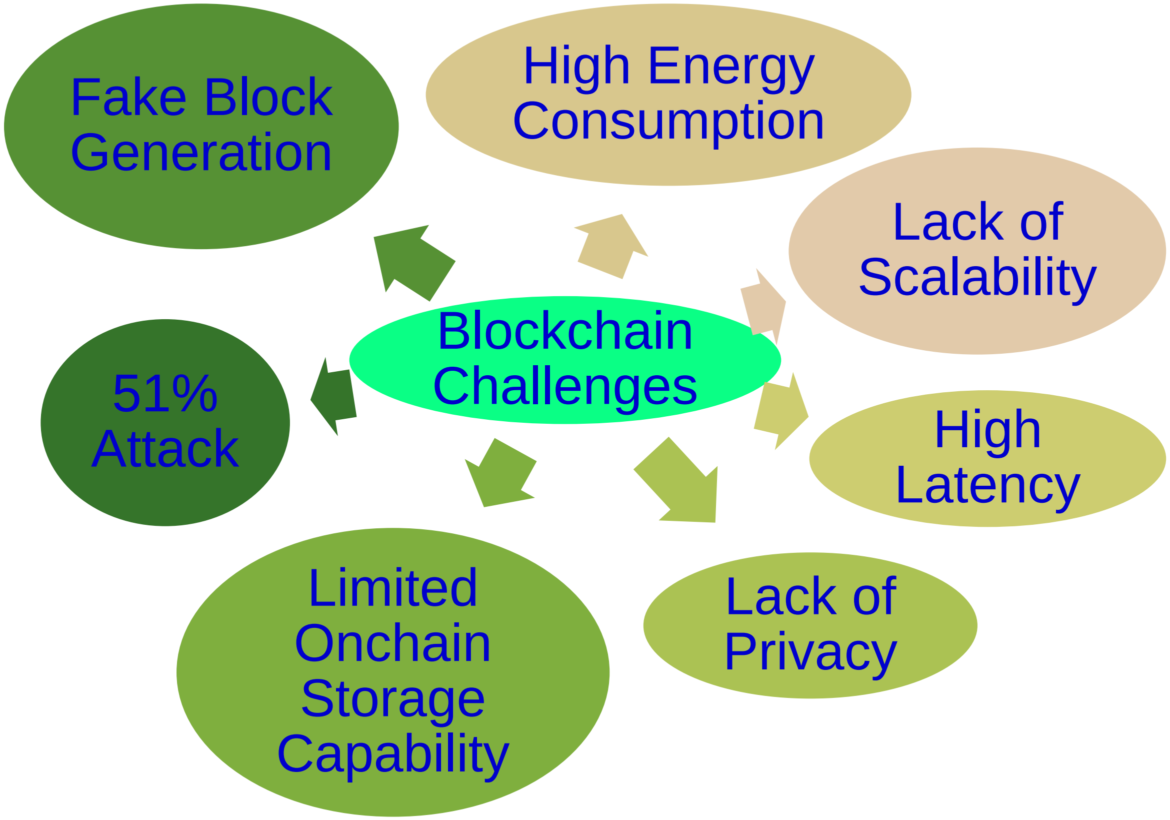
PoW Vs PoS



Source: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

Blockchain Challenges

Blockchain has Many Challenges



July 2018

Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, “Everything you Wanted to Know about the Blockchain”, *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 4, July 2018, pp. 06--14.

Blockchain Energy Need is Huge

Energy for mining of 1 bitcoin

Energy consumption 2 years of a US household

Blockchain Energy Need is Huge

Energy consumption for each bitcoin transaction = 80,000X

Energy consumption of a credit card processing

Energy aspect of bitcoin

Embodied Energy: Manufacturing equipment

- Decreases overtime
- Returns to scale

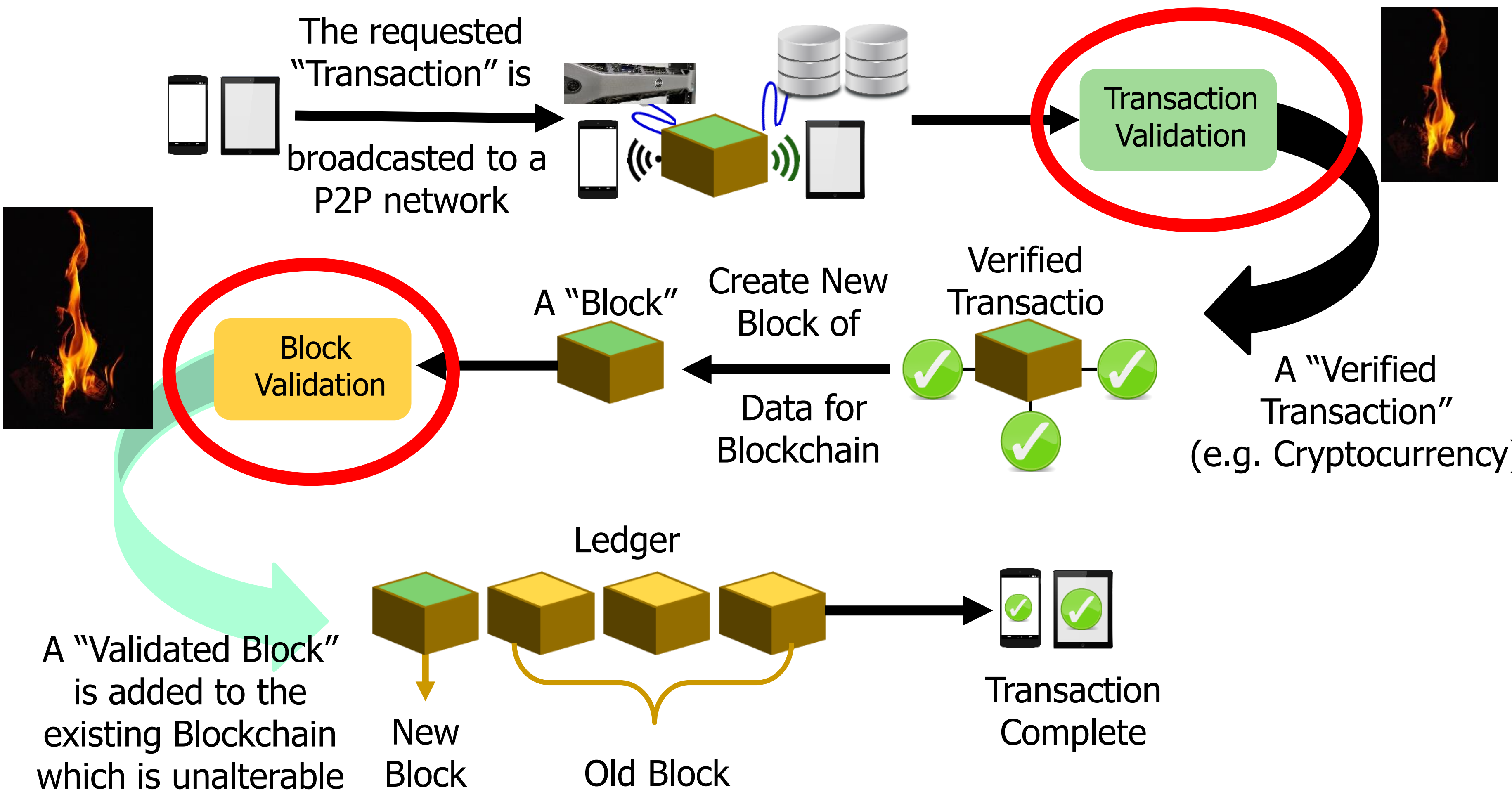
Electricity: Computations of algorithms

- Increases overtime
- Returns to scale

Cooling: Protection of equipment

- Increases with scale of mining rig

Blockchain Challenges - Energy



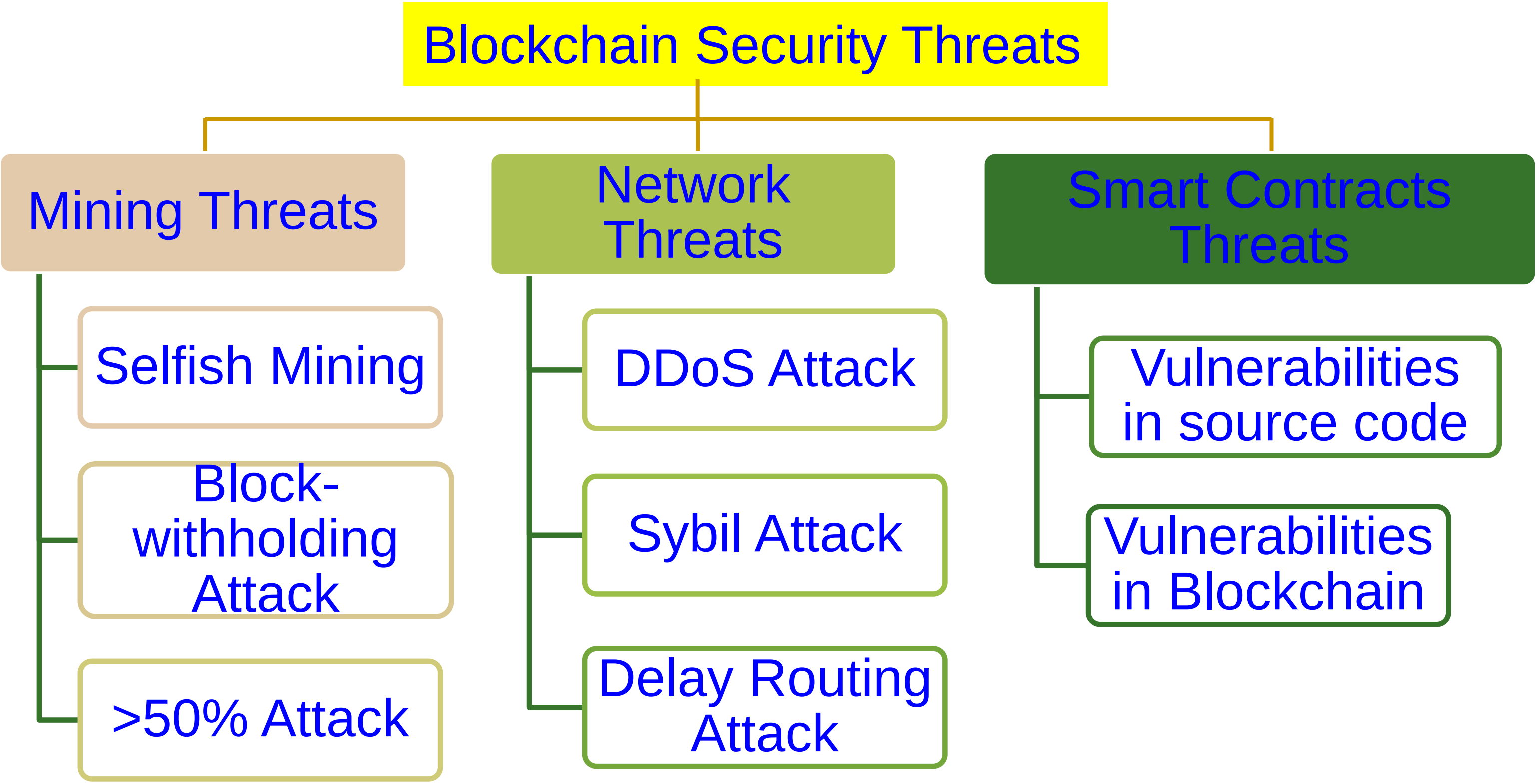
Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you Wanted to Know about the Blockchain", *IEEE Consumer Electronics Magazine*, Volume 7, Issue 4, July 2018, pp. 06--14.

Blockchain has Security Challenges

Selected attacks on the blockchain and defences		
Attacks	Descriptions	Defence
Double spending	Many payments are made with a body of funds	Complexity of mining process
Record hacking	Blocks are modified, and fraudulent transactions are inserted	Distributed consensus
51% attack	A miner with more than half of the network's computational power dominates the verification process	Detection methods and design of incentives
Identity theft	An entity's private key is stolen	Reputation of the blockchain on identities
System hacking	The software systems that implement a blockchain are compromised	Advanced intrusion detection systems

Source: N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, "Secured by Blockchain: Safeguarding Internet of Things Devices," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 28–34, May 2019.

Blockchain Security Threats

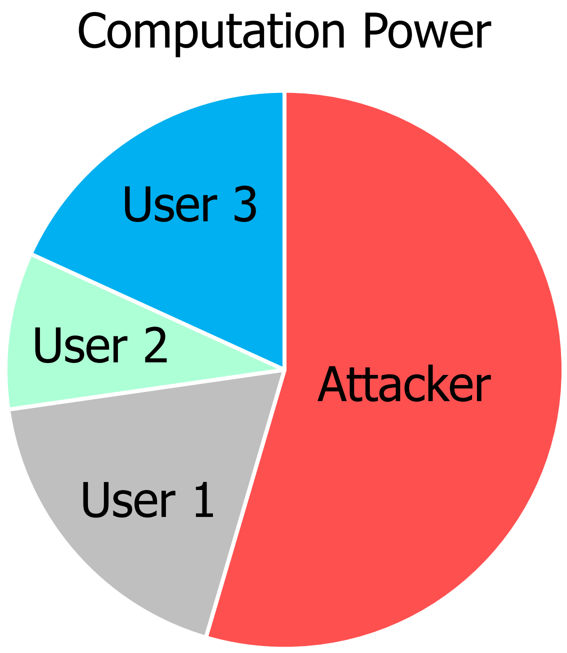


Blockchain has Serious Privacy Issue

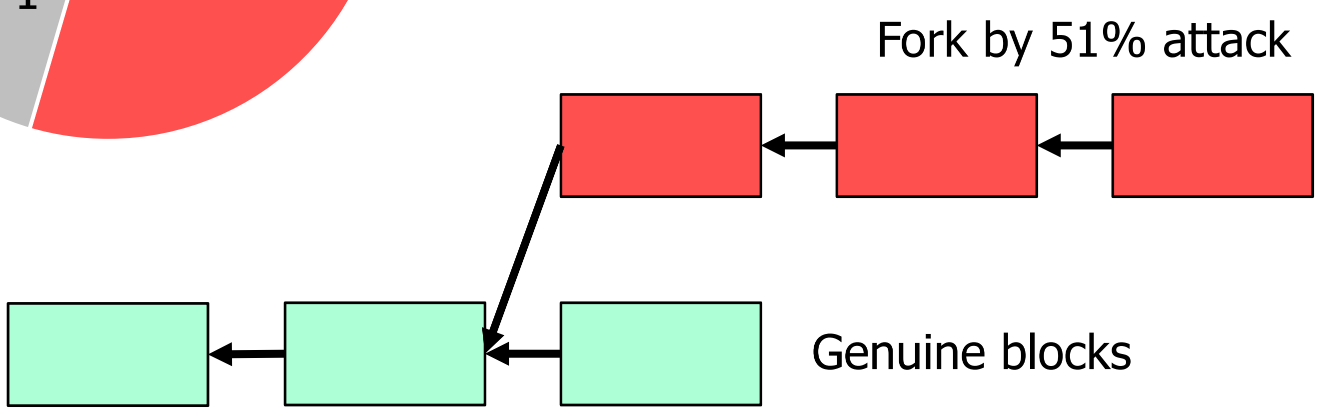
	Bitcoin	Dash	Monero	Verge	PIVX	Zcash
Origin	-	Bitcoin	Bytecoin	Bitcoin	Dash	Bitcoin
Release	January 2009	January 2014	April 2014	October 2014	February 2016	October 2016
Consensus Algorithm	PoW	PoW	PoW	PoW	PoS	PoW
Hardware Mineable	Yes	Yes	Yes	Yes	No	Yes
Block Time	600 sec.	150 sec.	120 sec.	30 sec.	60 sec.	150 sec.
Rich List	Yes	Yes	No	Yes	Yes	No
Master Node	No	Yes	No	No	Yes	No
Sender Address Hidden	No	Yes	Yes	No	Yes	Yes
Receiver Address Hidden	No	Yes	Yes	No	Yes	Yes
Sent Amount Hidden	No	No	Yes	No	No	Yes
IP Addresses Hidden	No	No	No	Yes	No	No
Privacy	No	No	Yes	No	No	Yes
Untraceability	No	No	Yes	No	No	Yes
Fungibility	No	No	Yes	No	No	Yes

Source: J. Lee, "Rise of Anonymous Cryptocurrencies: Brief Introduction", IEEE Consumer Electronics Magazine, vol. 8, no. 5, pp. 20-25, 1 Sept. 2019.

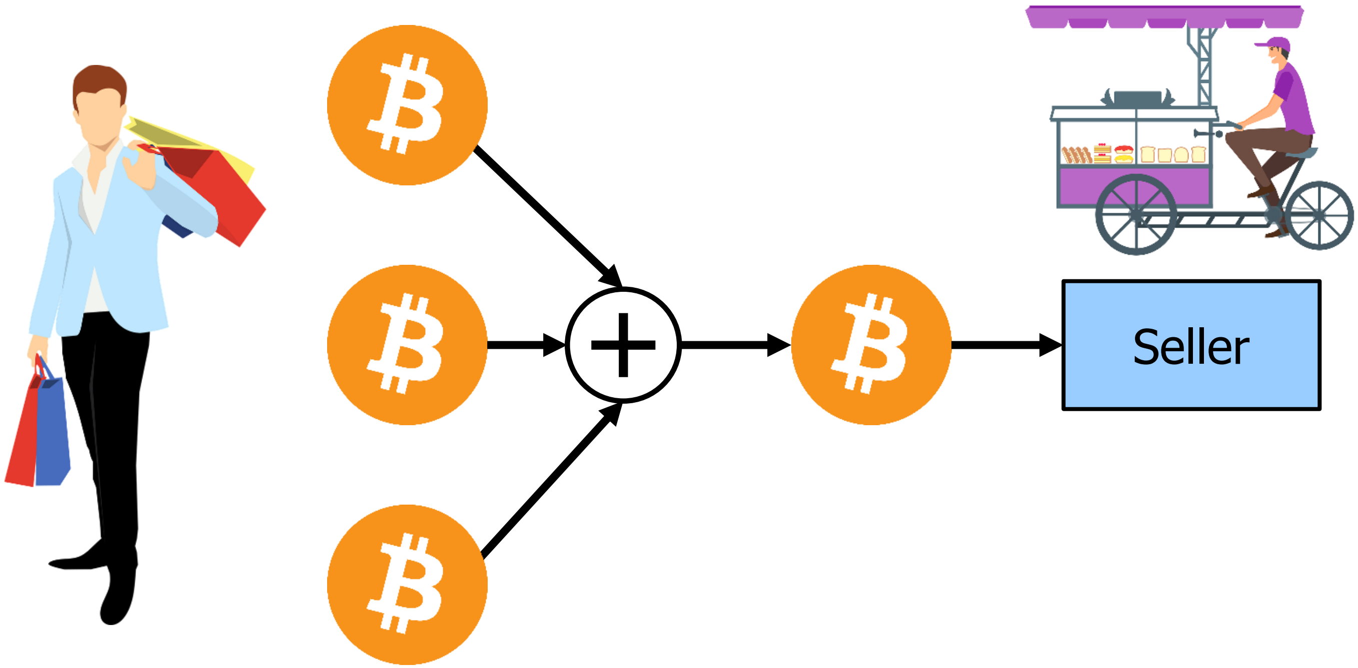
Blockchain - 51% Attack



With >50% computation power, attacker can create fork with fraudulent data.



Blockchain Challenges – Anonymity Can be Broken



With careful analysis, anonymity can be broken

Blockchain Scalability Issue

- Since Blockchain is an immutable and irreversible database, the blockchain will grow over time.
- The amount of data stored will bring up other problems such as the power consumed while searching or analyzing the huge database.

Blockchain Latency Issue

- Latency is another challenge caused by the huge amount of data.

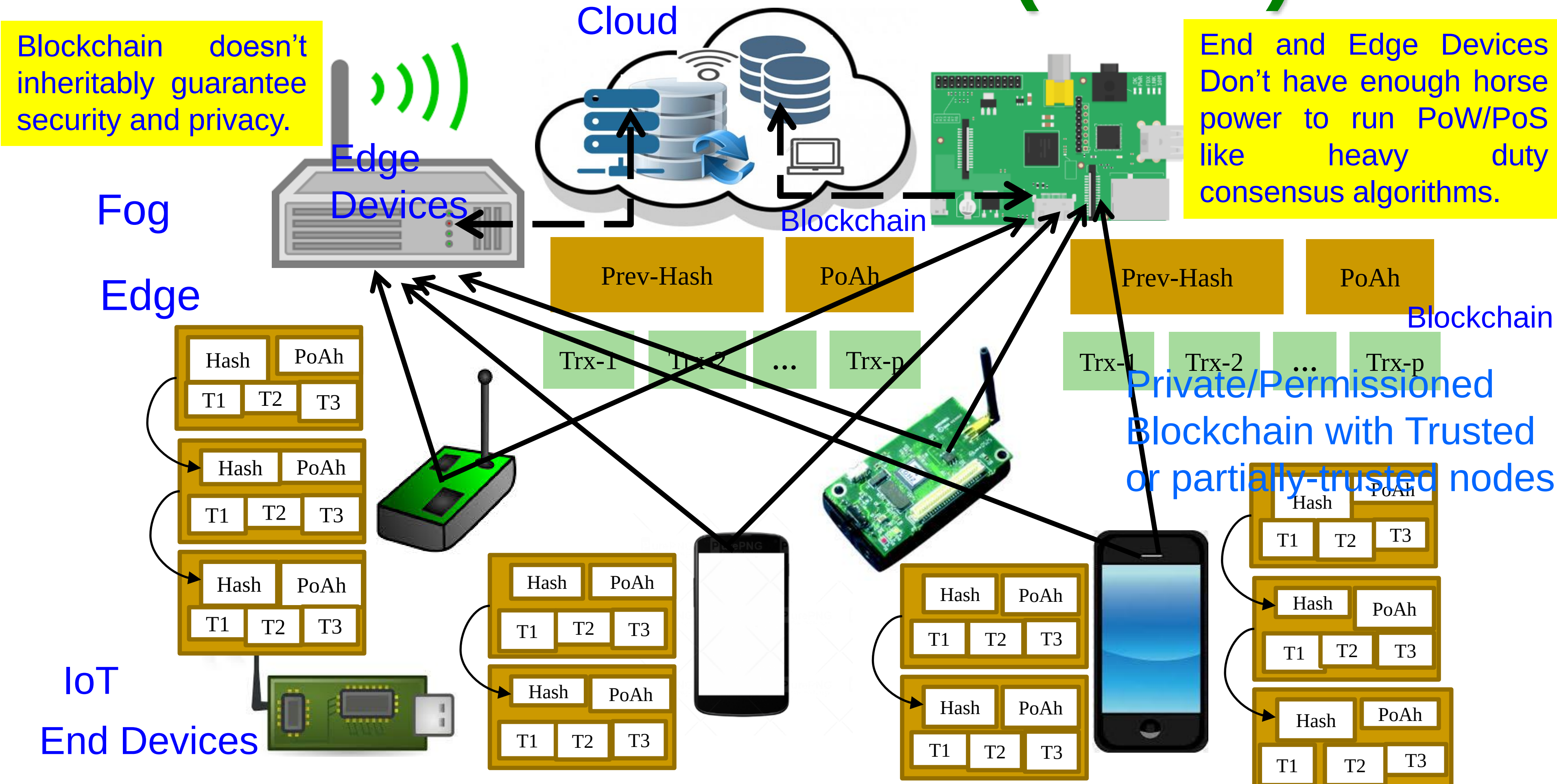
Blockchain Memory Usage

- A transaction is charged based in the amount of data
- Multiple transactions needed for larger files to break them into chunks and send multiple transactions
- This will increase cost in terms of base transaction fee, fee per byte of data
- All these factors limited amount of data to be stored on the blockchain
- Solution: Usage of hash to be stored on the blockchain and actual data to be stored off-chain like RDBMS and File sharing systems

Some of our Blockchain Solutions

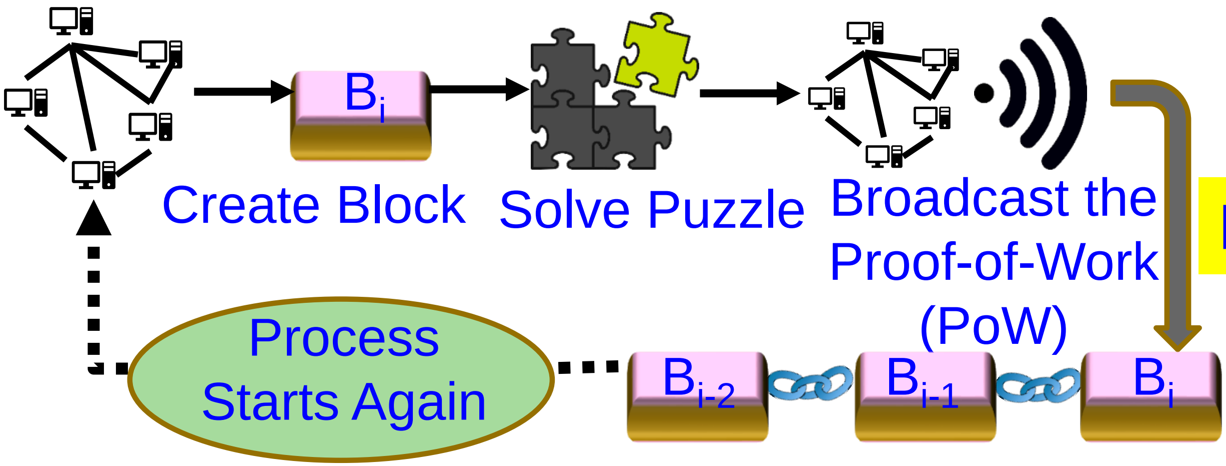
PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for Large-scale IoT Frameworks

IoT-Friendly Blockchain – Proof-of-Authentication (PoAh)



Source: D. Puthal and S. P. Mohanty, "Proof of Authentication: IoT-Friendly Blockchains", *IEEE Potentials Magazine*, Vol. 38, No. 1, January 2019, pp. 26--29.

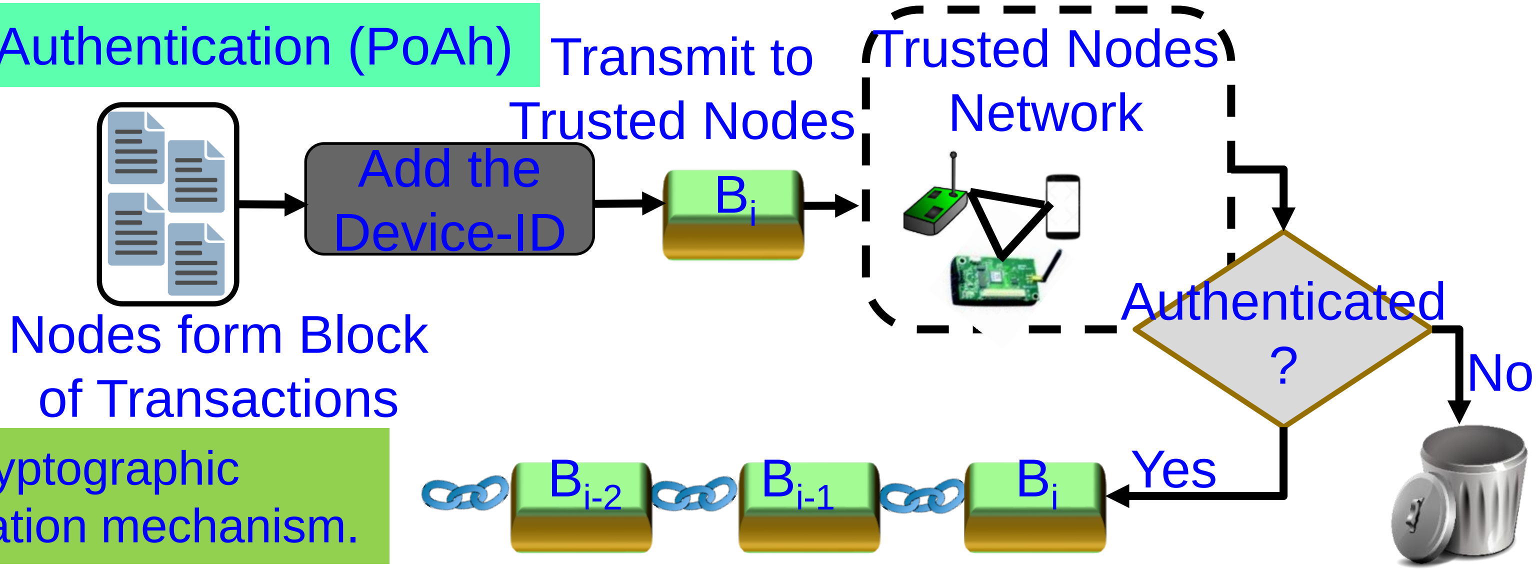
Our Proof-of-Authentication (PoAh)



Proof-of-Work (PoW)

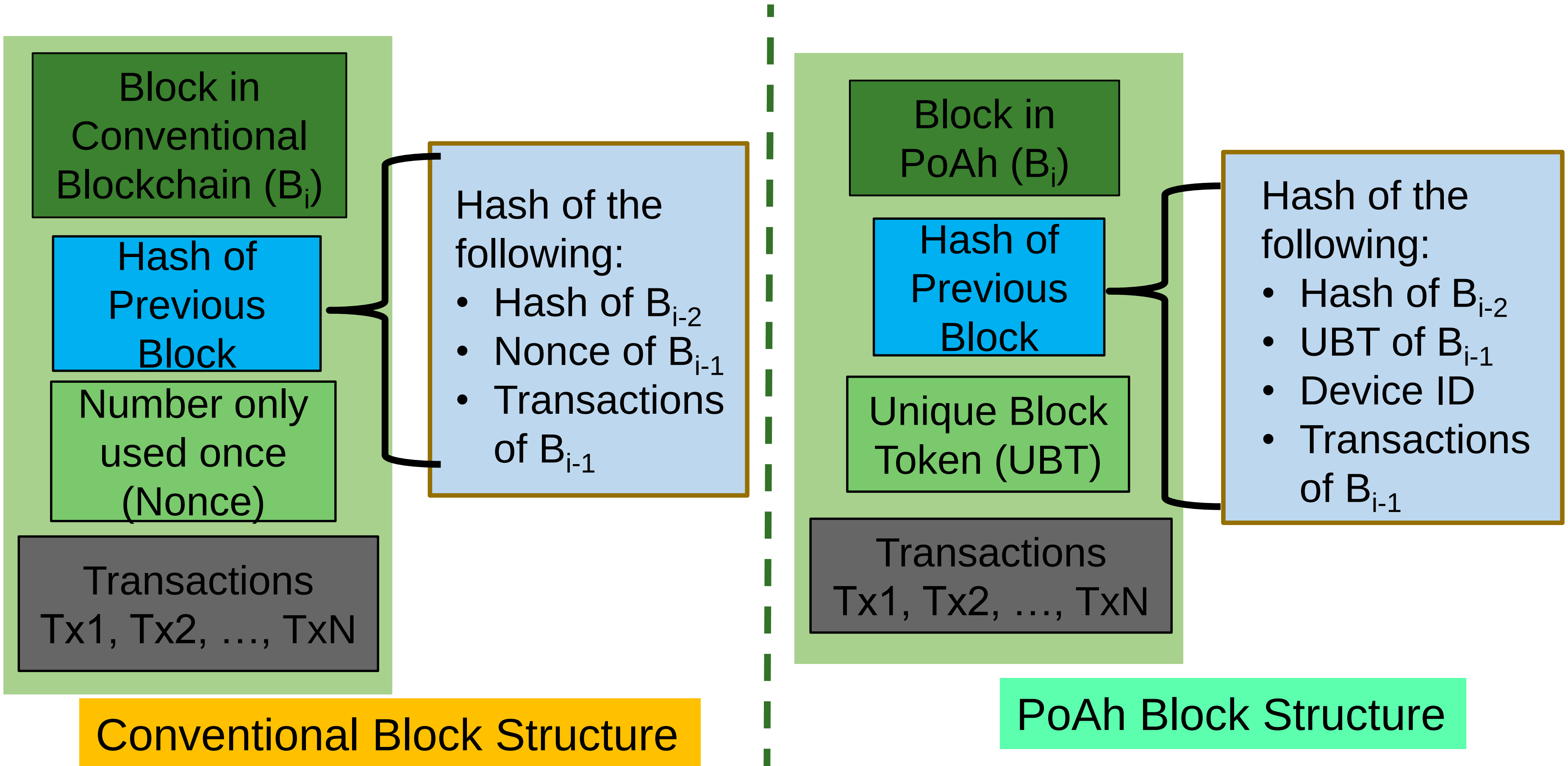
Eliminates cryptographic "puzzle" solving to validate blocks.

Proof of Authentication (PoAh)



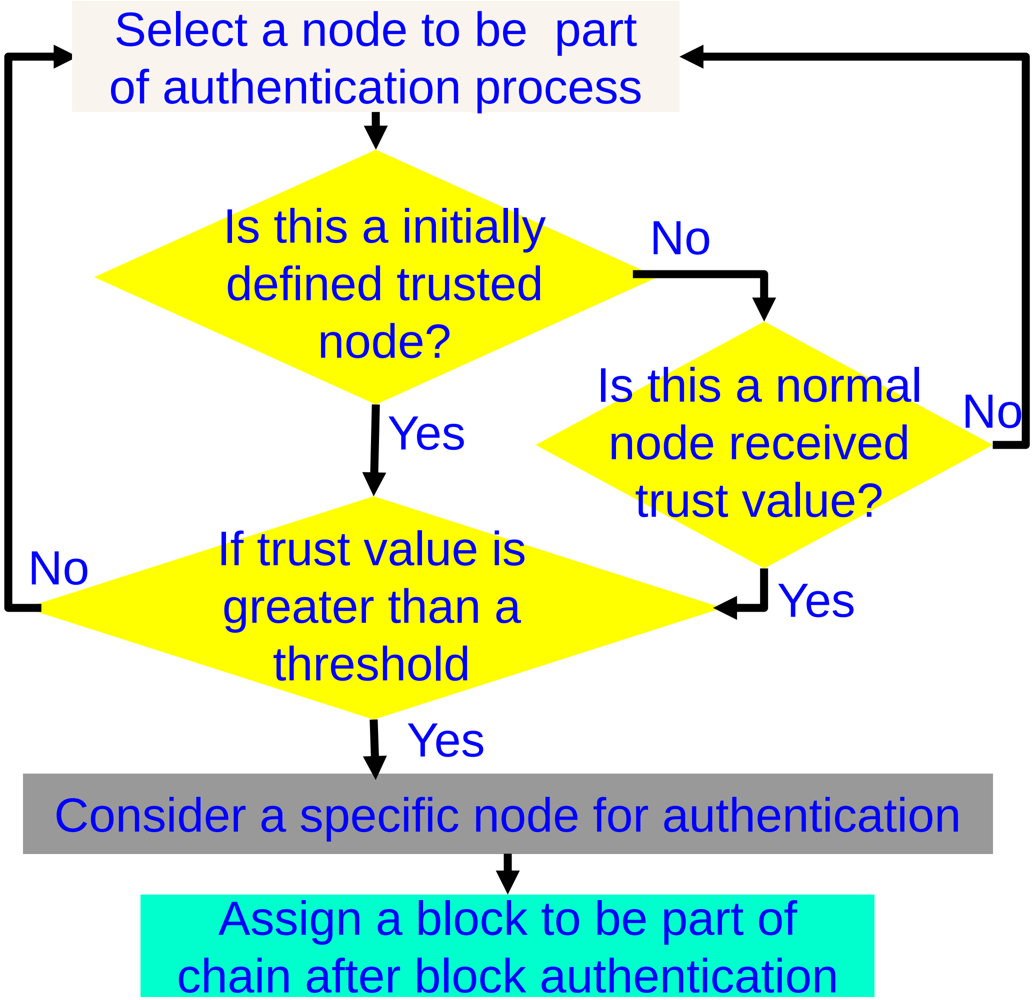
Uses a cryptographic authentication mechanism.

Our PoAh-Chain: Proposed New Block Structure



Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and DataSecurity in the Internet of Everything(IoE)", arXiv Computer Science, arXiv:1909.06496, Sep 2019, 37-pages.

Our PoAh: Authentication Process

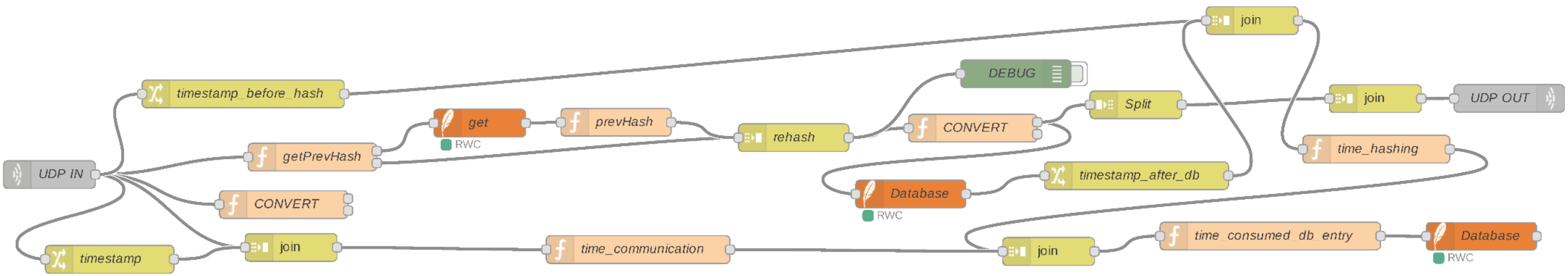


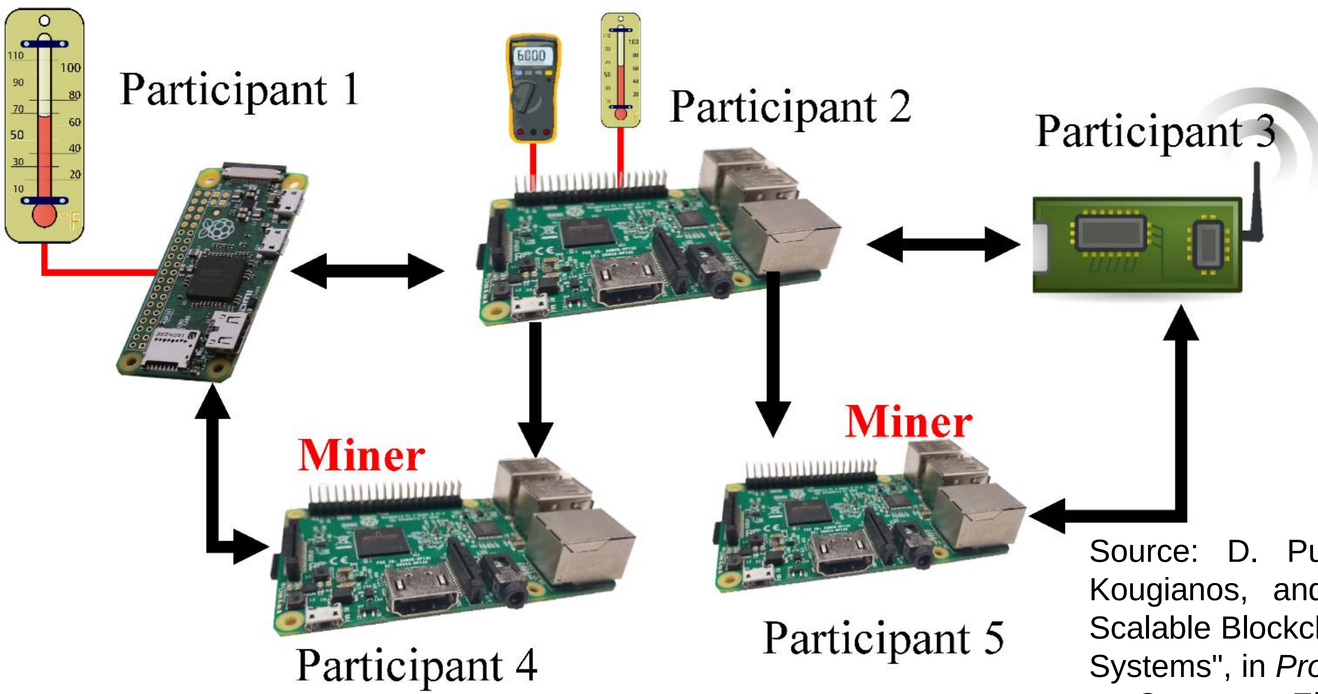
Steps to find a Trusted Node which will Authenticate a Block.

Algorithm 1: PoAh Block Authentication

Provided:
All nodes in the network follow SHA-256 Hash
Individual node has Private (PrK) and Public key (PuK)
Steps:
(1) Nodes combine transactions to form blocks
    $(Trx^{+}) \rightarrow$ blocks
(2) Blocks sign with own private key
    S_{PrK} (block) $\rightarrow$ broadcast
(3) Trusted node verifies signature with source public key
    V_{PuK}(block) $\rightarrow$ MAC Checking
(4) If (Authenticated)
    Block||PoAh(ID) $\rightarrow$ broadcast
    H(block) $\rightarrow$ Add blocks into chain
(5) Else
    Drop blocks
(6) GOTO (Step-1) for next block

IoT Simulators - Node-RED - Example

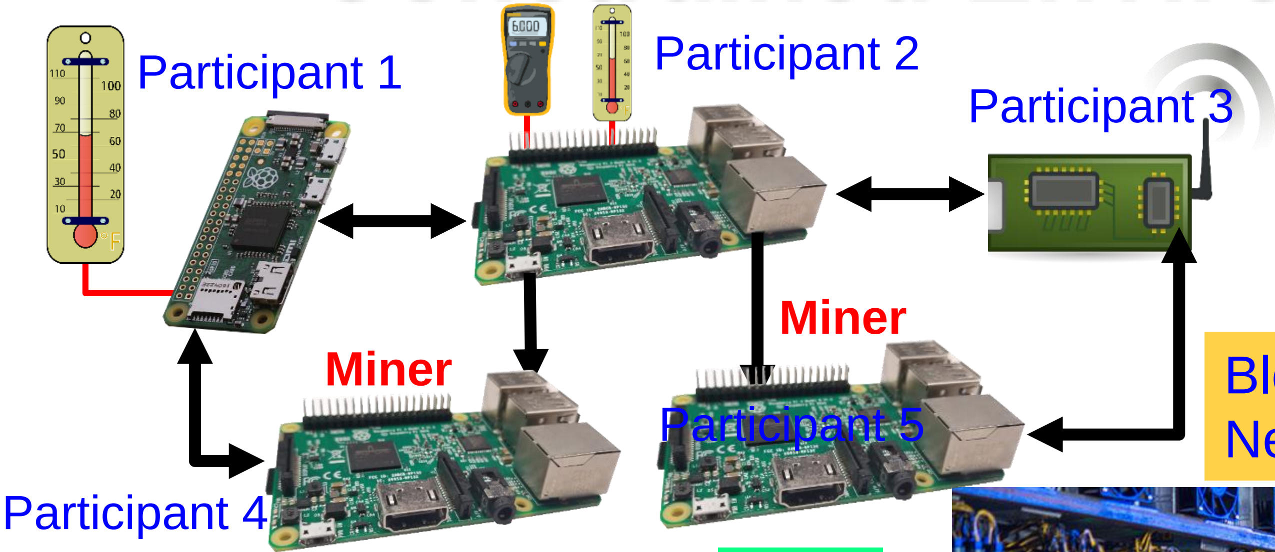




Simulation: Proof-of-Authentication (PoAh) based IoT Friendly Blockchain

Source: D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems", in *Proc. of 37th IEEE International Conference on Consumer Electronics (ICCE)*, 2019.

Our PoAh-Chain Runs in Resource Constrained Environment



Blockchain using PoW Needs Significant Resource

Our PoAh-Chain Runs here

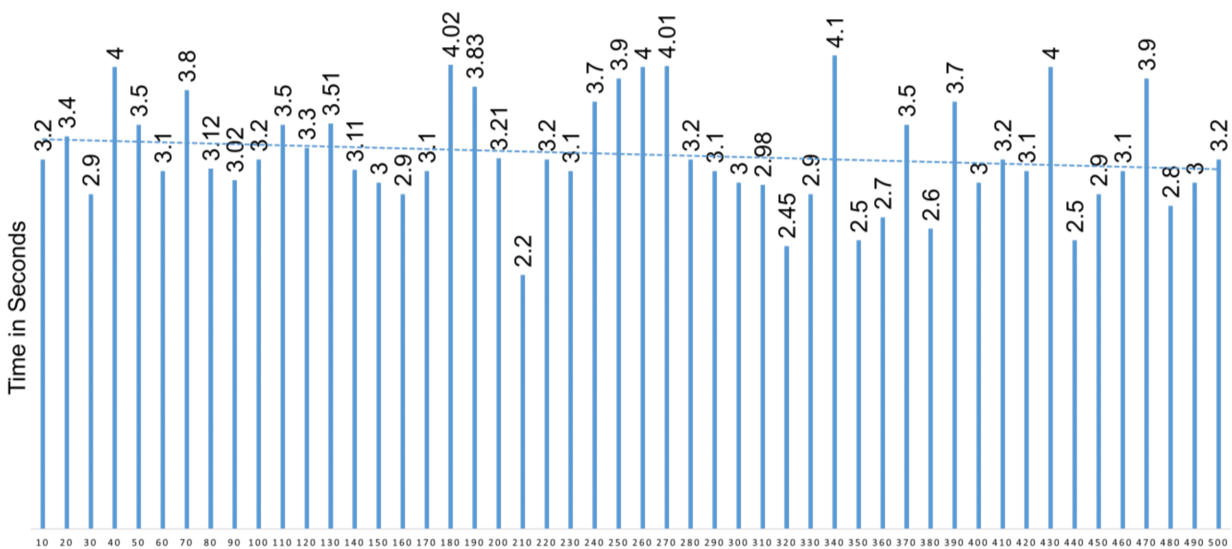
5 W

Source: https://www.iea.org/newsroom/news/2019/july/bitcoin-energy-use-mined-the-gap.html

500,0000 W

Our PoAh is 200X Faster than PoW While Consuming a Very Minimal Energy

Consensus Algorithm	Blockchain Type	Prone To Attacks	Power Consumption	Time for Consensus
Proof-of-Work (PoW)	Public	Sybil, 51%	538 KWh	10 min
Proof-of-Stake (PoS)	Public	Sybil, Dos	5.5 KWh	
Proof-of-Authentication (PoAh)	Private	Not Known	3.5 W	3 sec

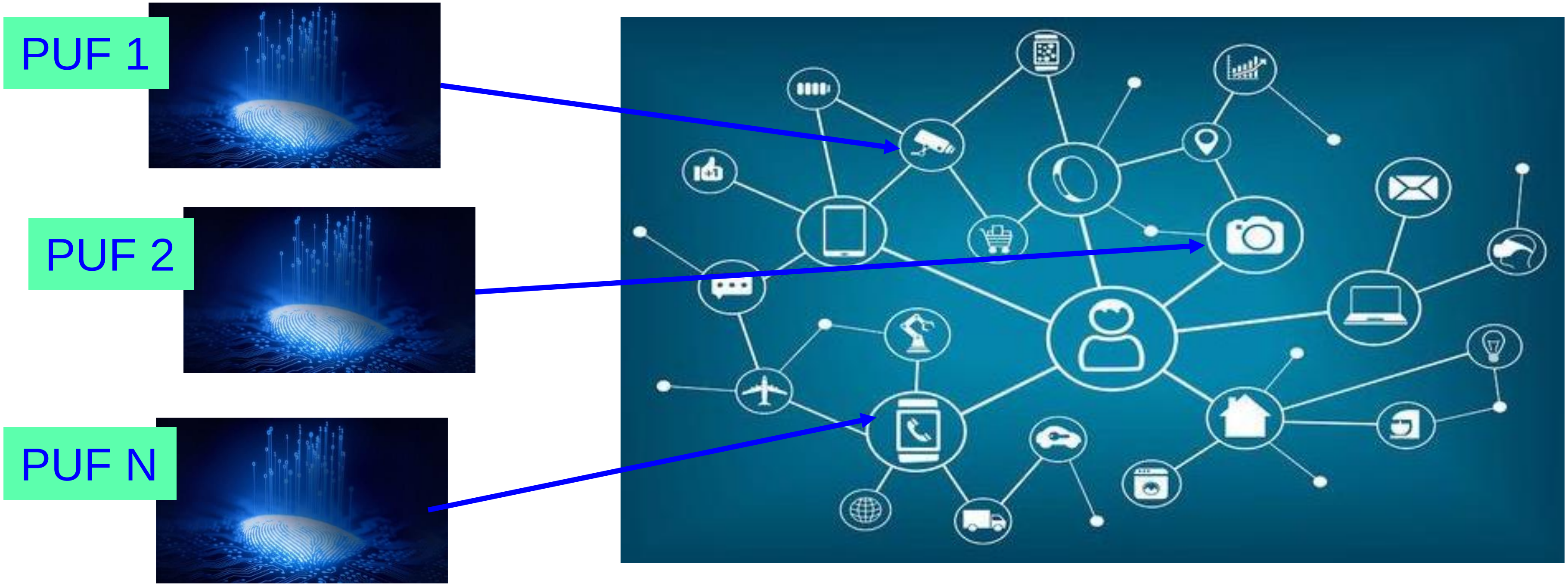


PoAh Execution for 100s of Nodes

Source: D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems", in *Proc. 37th IEEE International Conference on Consumer Electronics (ICCE*), 2019.

PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)

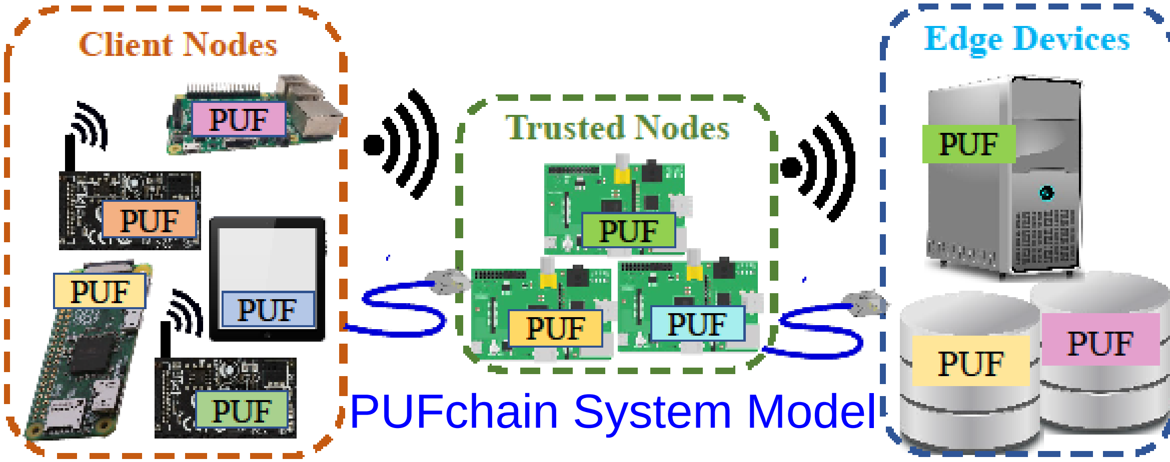
We Proposed World's First Hardware-Integrated Blockchain (PUFchain) that is Scalable, Energy-Efficient, and Fast



Challenges and Novel Contribution

- Challenges for blockchain to adopt in IoT architecture
  - Scalability
  - High computational requirement
  - High Power consumption
- A high level of security by integrating Hardware assisted security module
  - A hybrid oscillator arbiter PUF module is used
  - Key generated is used for cryptography
- A novel consensus mechanism for IoT environment, proof-of-PUF-Enabled Authentication (PoP)
  - PUF keys are used in cryptography
  - Keys are not transmitted over network

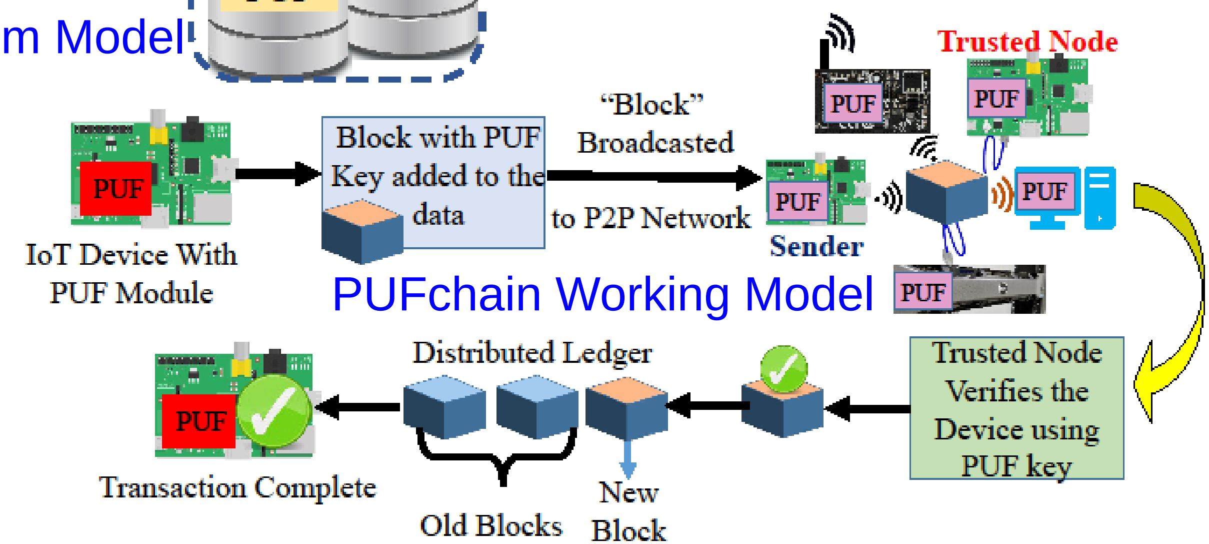
PUFchain: The Hardware-Assisted Scalable Blockchain



PUFchain System Model

Can provide:
Device, System, and Data Security

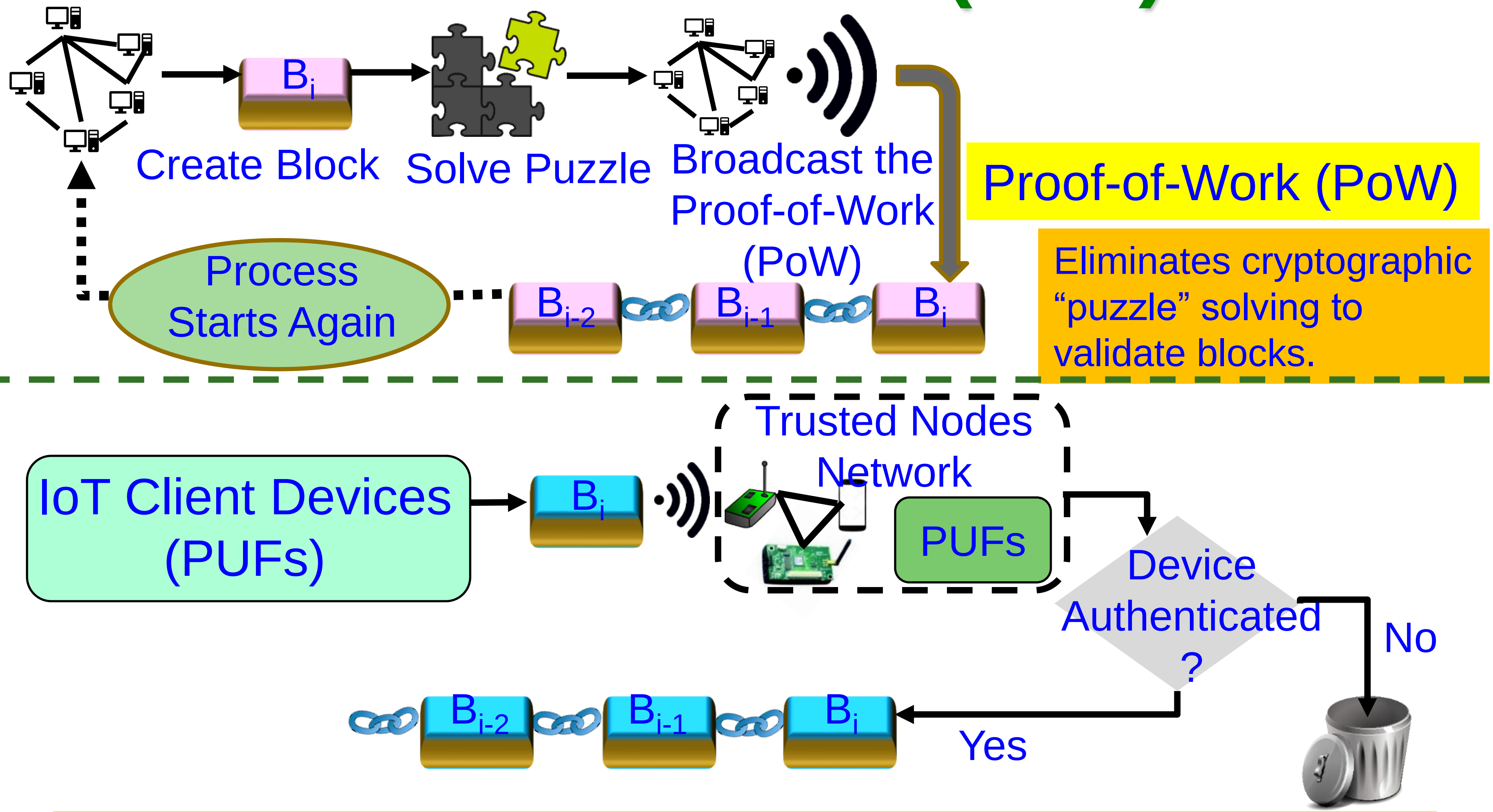
PUFChain 2 Modes:
(1) PUF Mode and
(2) PUFChain Mode



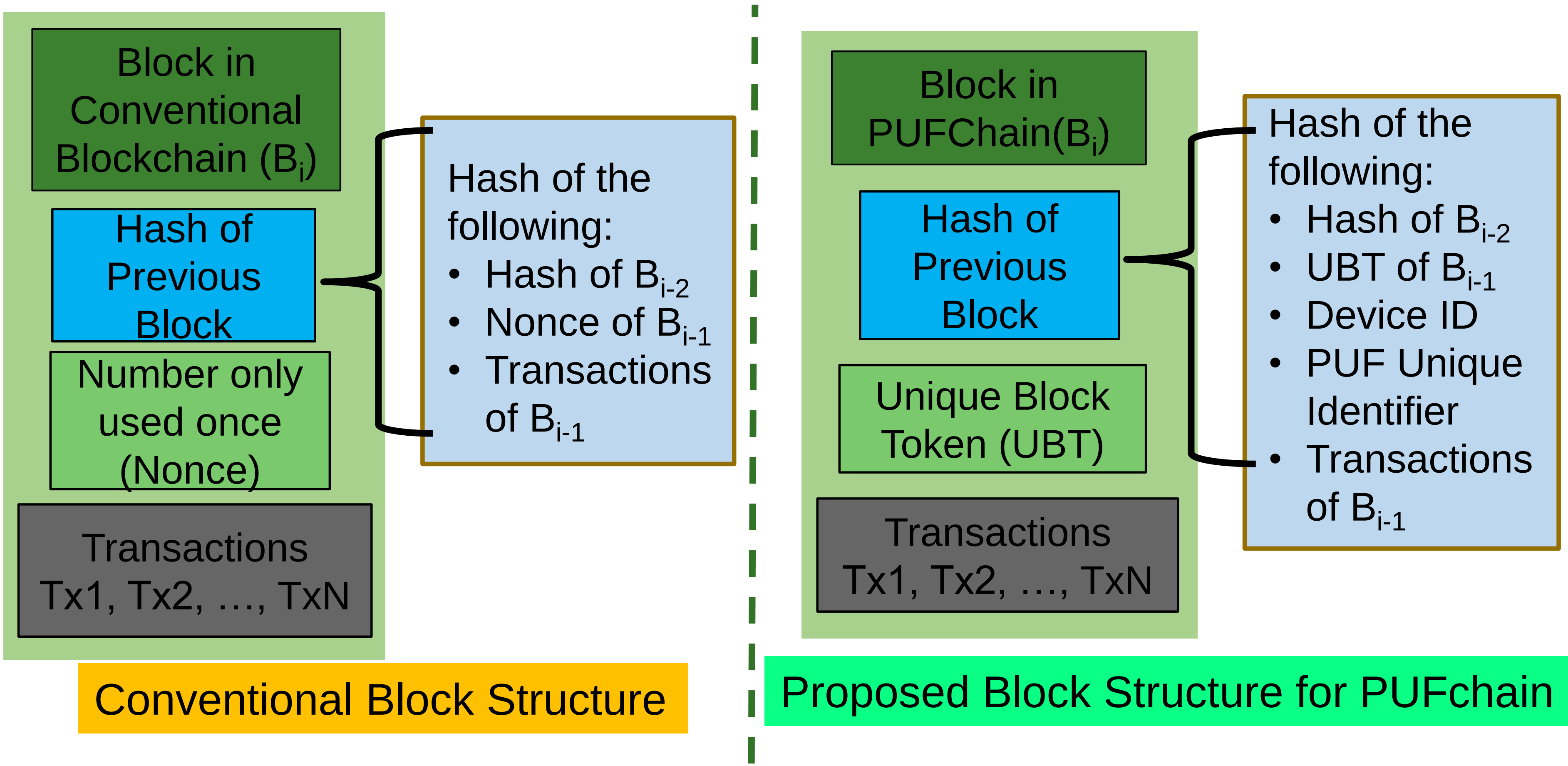
PUFchain Working Model

Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. in Press.

Our Proof-of-PUF-Enabled-Authentication (PoP)



PUFchain: Proposed New Block Structure

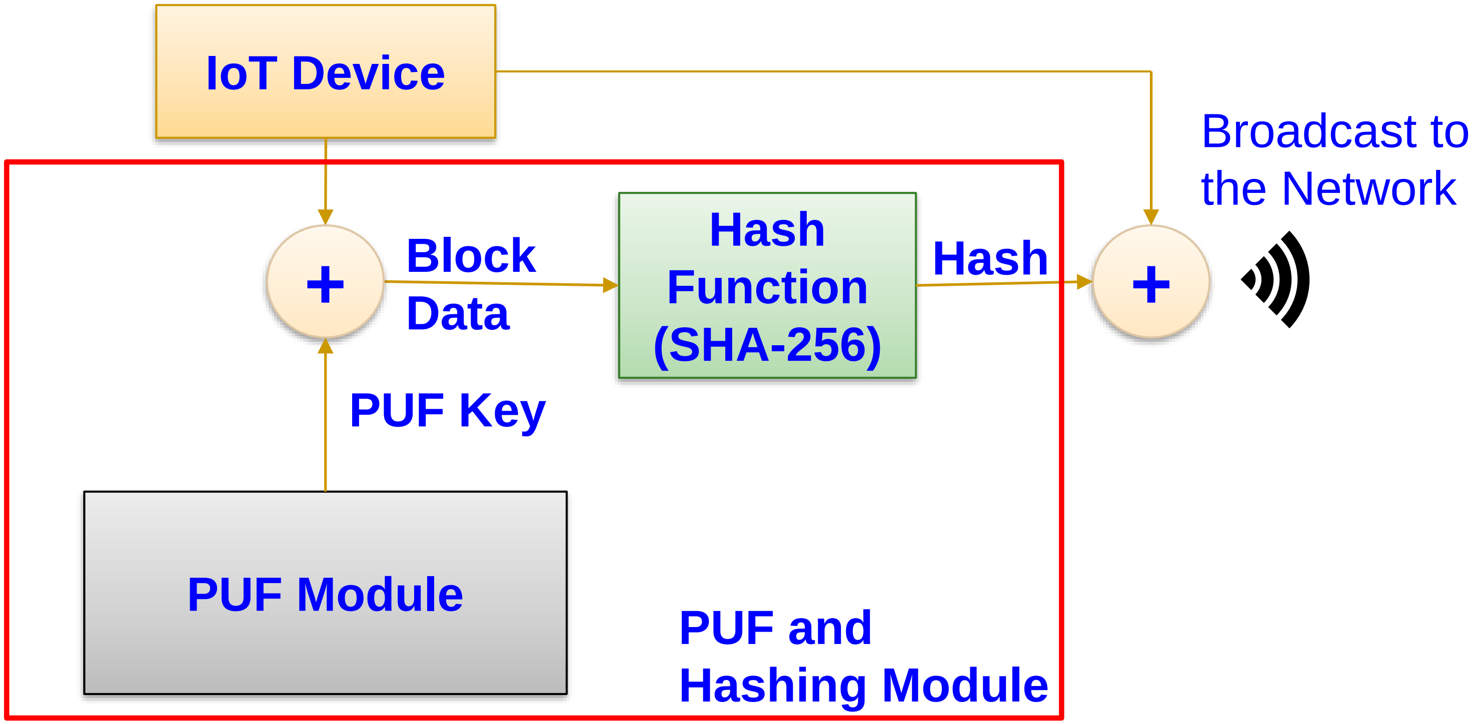


PUFchain node

- Contains PUF module and hashing module attached to IoT device
- PUF Module
  - PUF module is responsible for generating unique key for IOT device
  - PUF key uses process variations during manufacturing process to generate device fingerprints
  - Key is not fixed and depends on challenge posed to the PUF module
  - Key is not transmitted over the network
- Hashing Module
  - Makes uses of the unique key generated from PUF module
  - Off-loads computational overhead on the IoT device

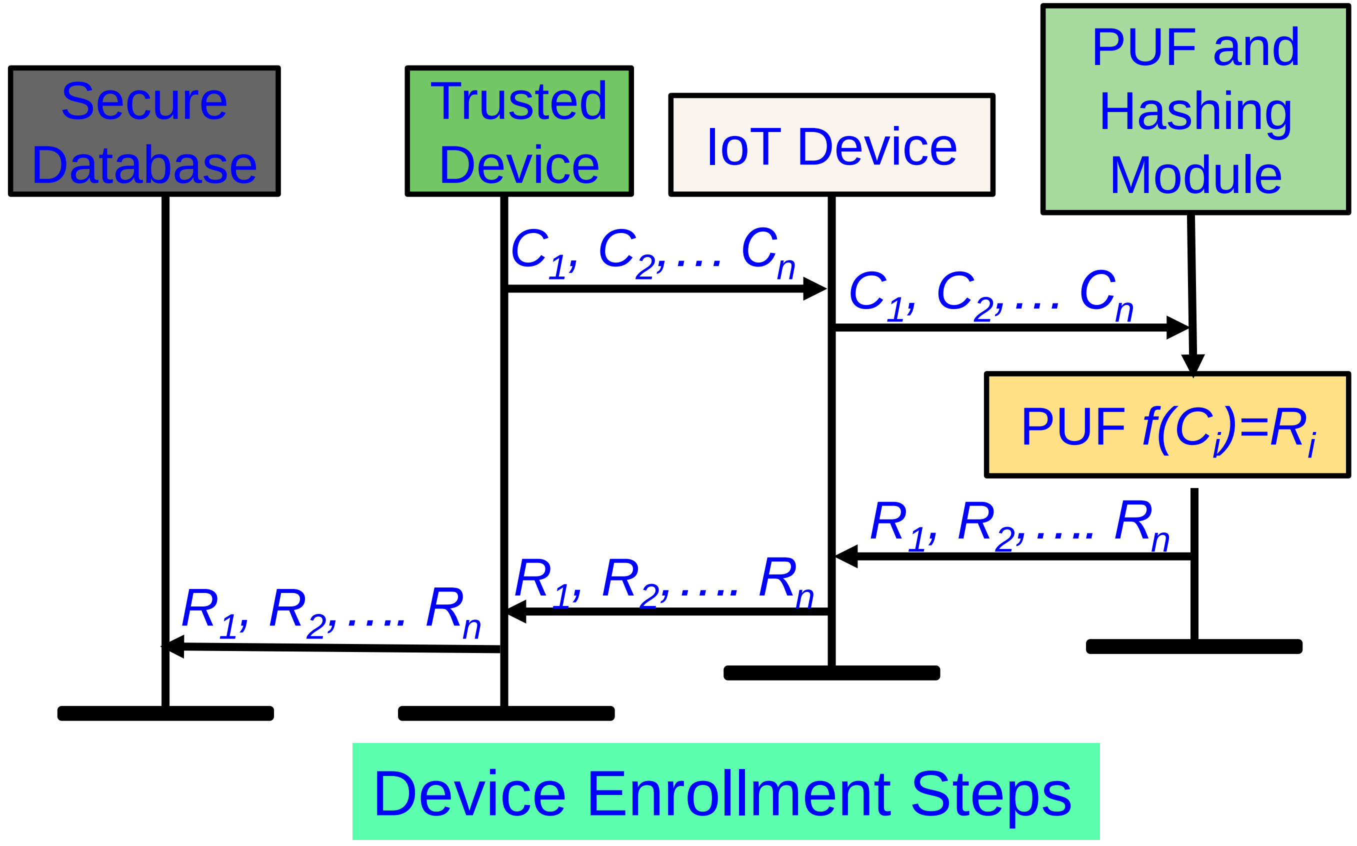
PUFchain – A Typical Node

Node in A PUF – Chain Environment



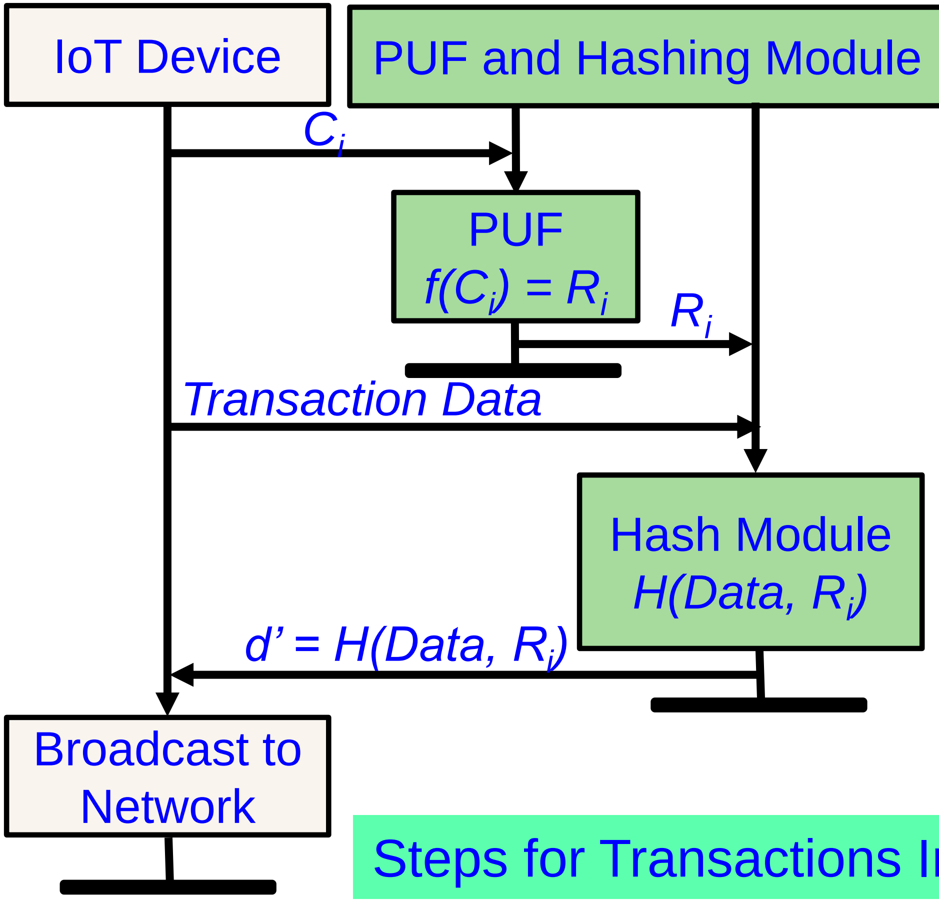
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos and D. Puthal, "PUFchain: A Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE)," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 8-16, 1 March 2020.

PUFchain: Device Enrollment Steps



Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. in Press.

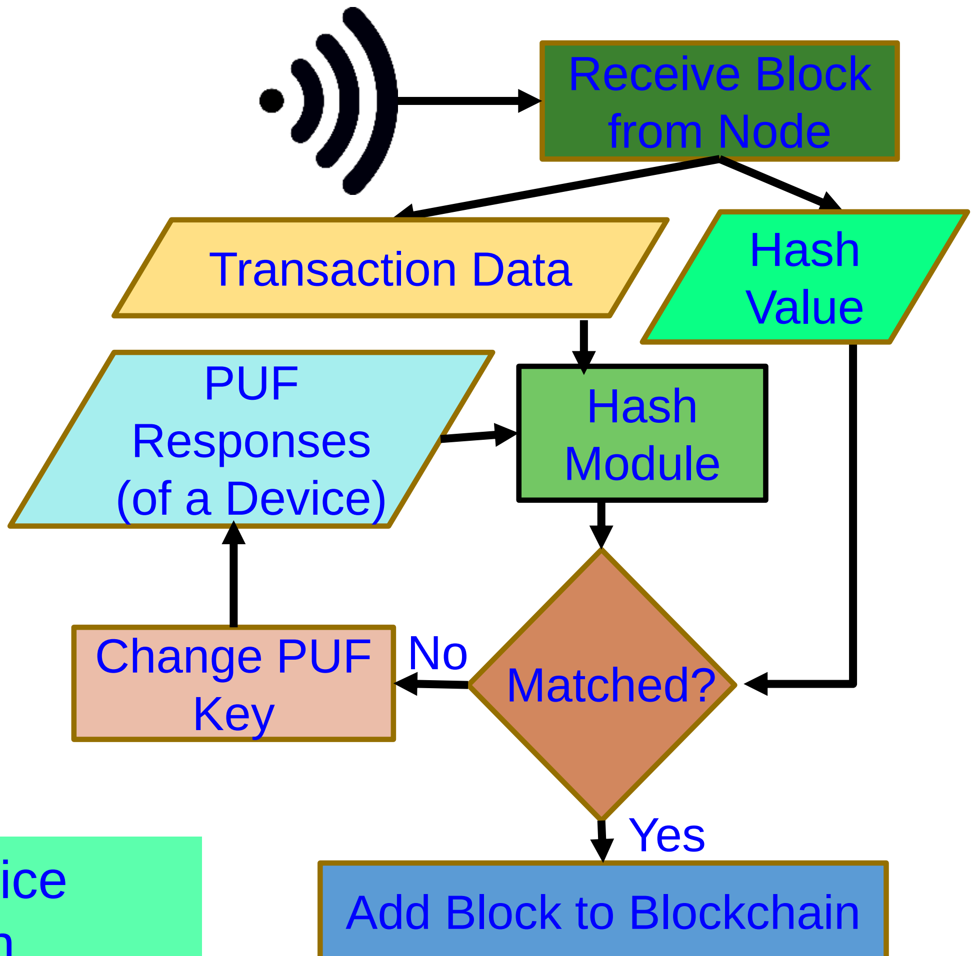
PUFchain - Transactions Initiation



Steps for Transactions Initiation

Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. in Press.

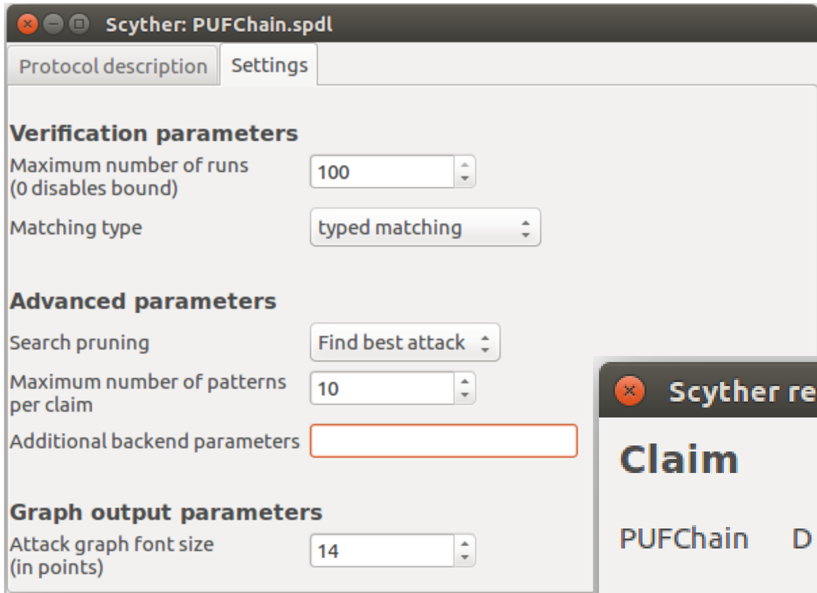
PUFchain – Device Authentication



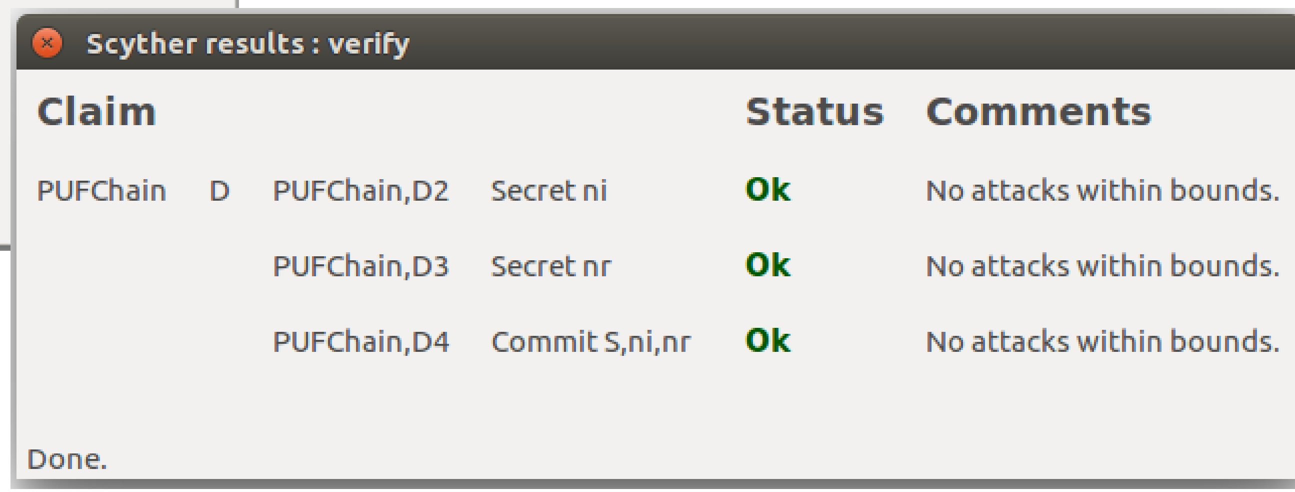
Steps for Device Authentication

Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. in Press.

PUFchain Security Validation



S - the source of the block
D - the miner or authenticator node in the networks



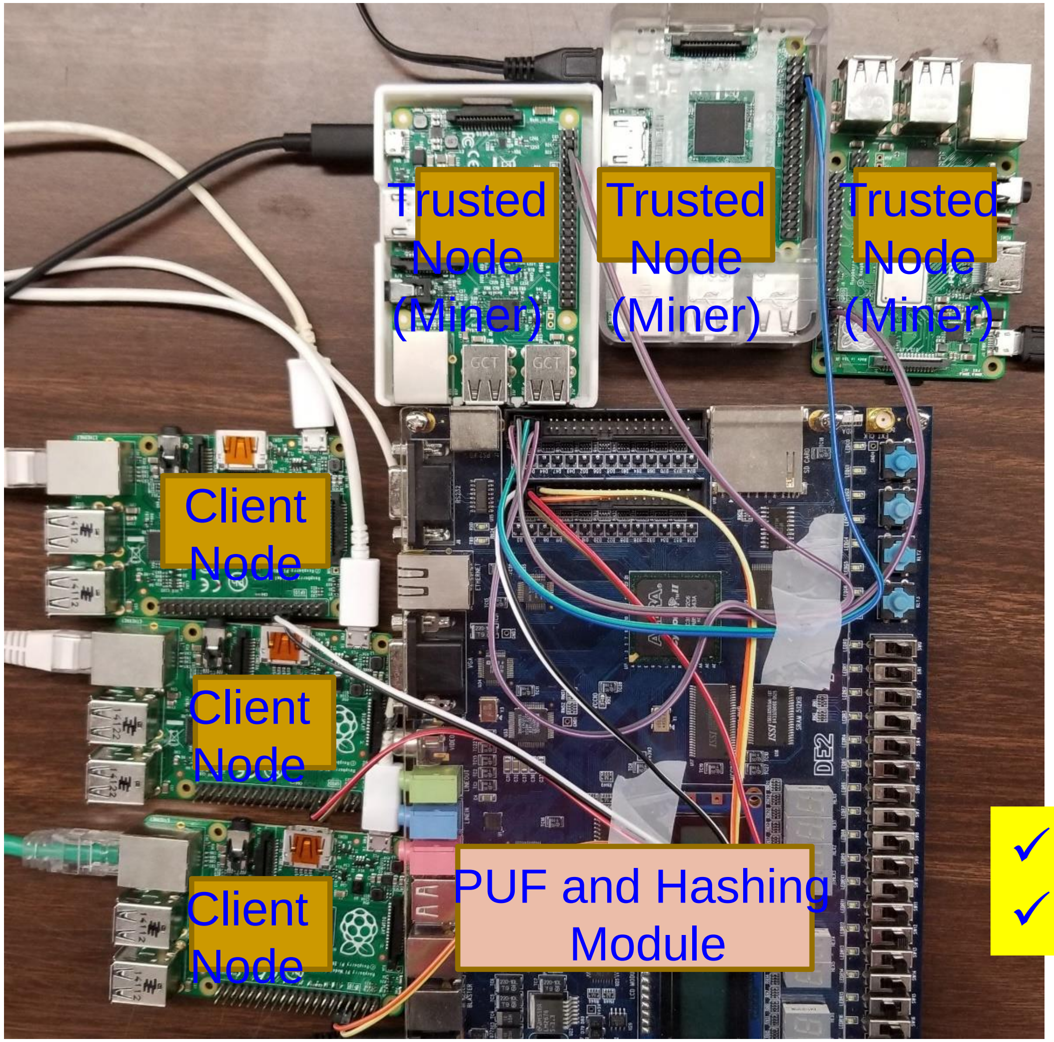
PUFchain Security Verification in Scyther simulation environment proves that PUFChain is secure against potential network threats.

Consensus Algorithms – Comparative Perspectives

Consensus Algorithm	Blockchain Type	Mining/ Consensus	Prone To Attacks	Power Consu.	Time for Consen.
Proof-of-Work (PoW)	Public	Computation Power Based	Sybil, 51%	538 KWh	10 min
Proof-of-Stake (PoS)	Public	Validation	Sybil, DoS	5.5 KWh	NA
Ripple	Permissioned	Vote Based Mining	DoS, Sybil	NA	NA
Proof-of-Vote	Consortium	Vote Based Mining	NA	NA	NA
Proof-of-Trust	Permissioned	Probability & Voting Based	DDoS Attack	NA	NA
Proof-of-Authentication (PoAh)	Private	Authentication	Not Known	3.5 W	3 sec
Proof of PUF-Enabled Authentication (PoP)	Private	Authentication	Not Known	5 W	1 sec

Source: D. Puthal, S. P. Mohanty, V. P. Yanambaka, and E. Kougianos, "PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for Large-scale IoT Frameworks", *arXiv Computer Science*, arXiv:2001.07297, January 2020, 26-pages.

Our PoP is 1000X Faster than PoW



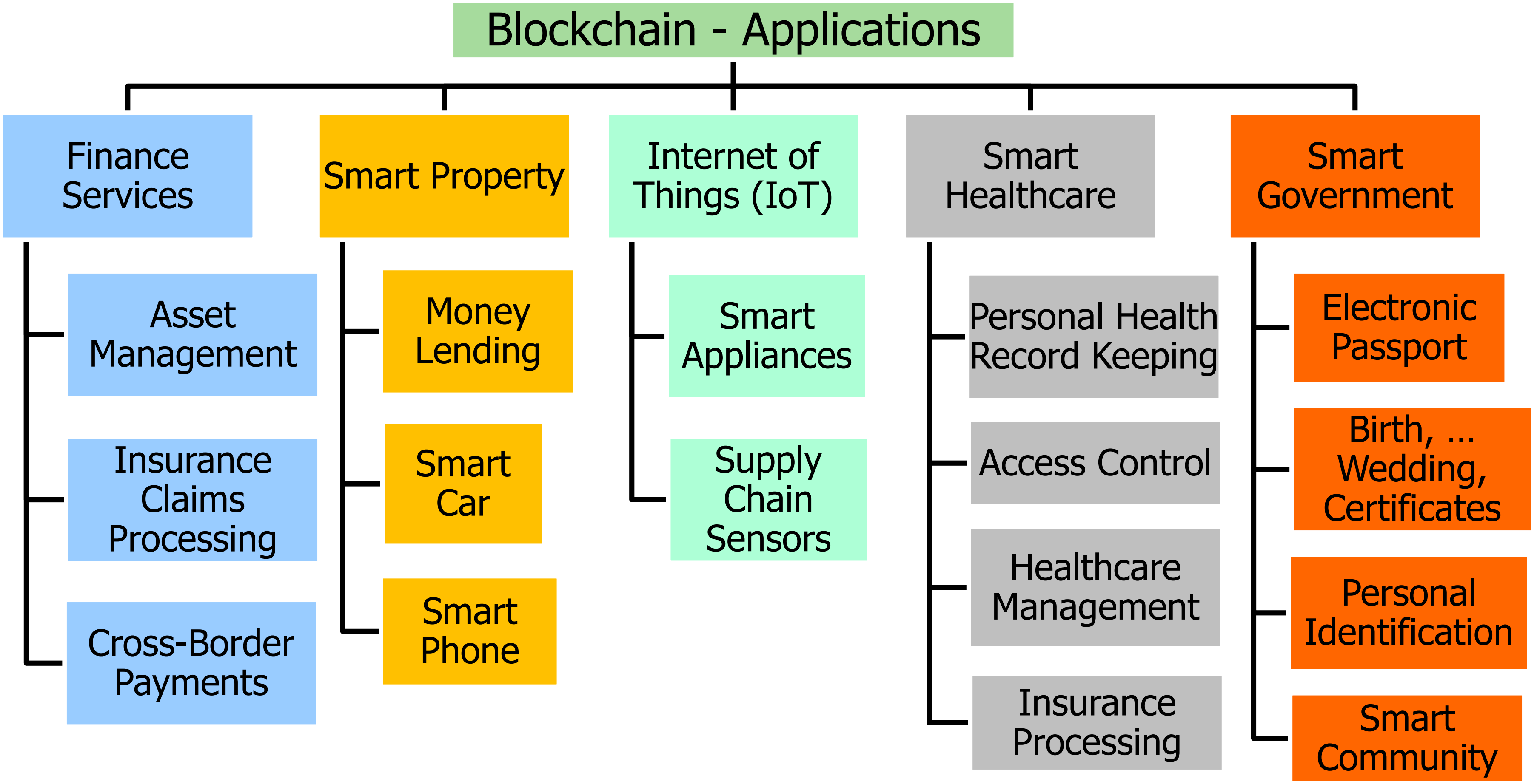
PoW - 10 min in cloud	PoAh – 950ms in Raspberry Pi	PoP - 192ms in Raspberry Pi
High Power	3 W Power	5 W Power

- ✓ PoP is 1,000X faster than PoW
- ✓ PoP is 5X faster than PoAh

Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and DataSecurity in the Internet of Everything(IoE)", arXiv Computer Science, arXiv:1909.06496, Sep 2019, 37-pages.

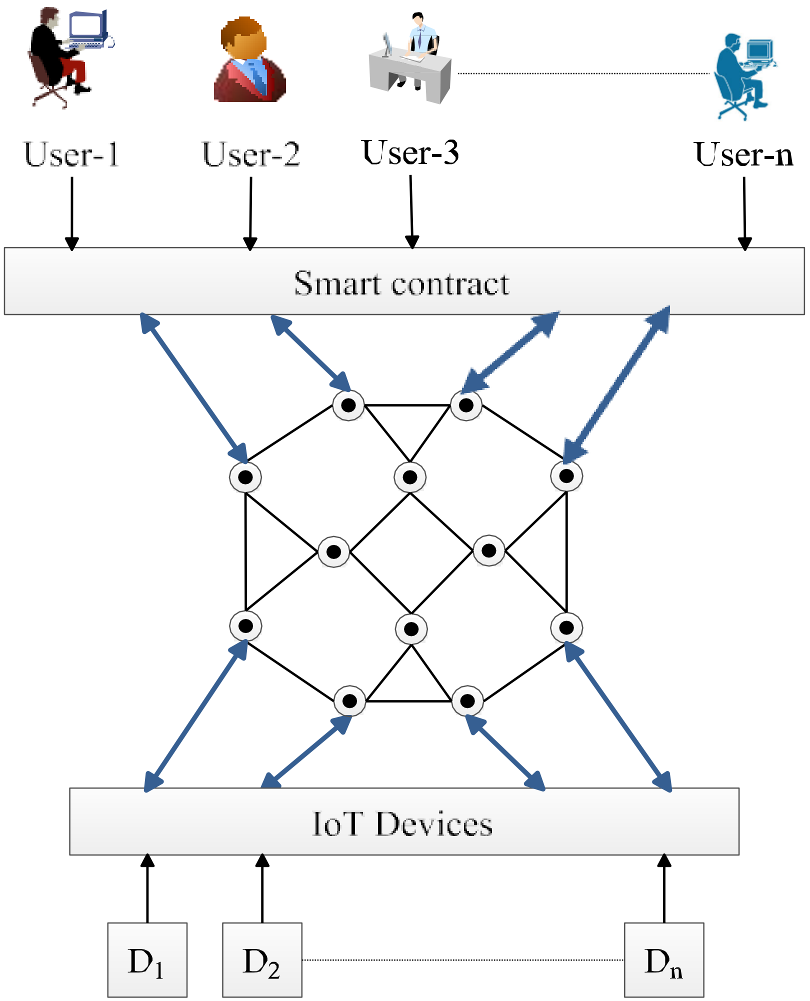
Blockchain Applications

Blockchain Applications



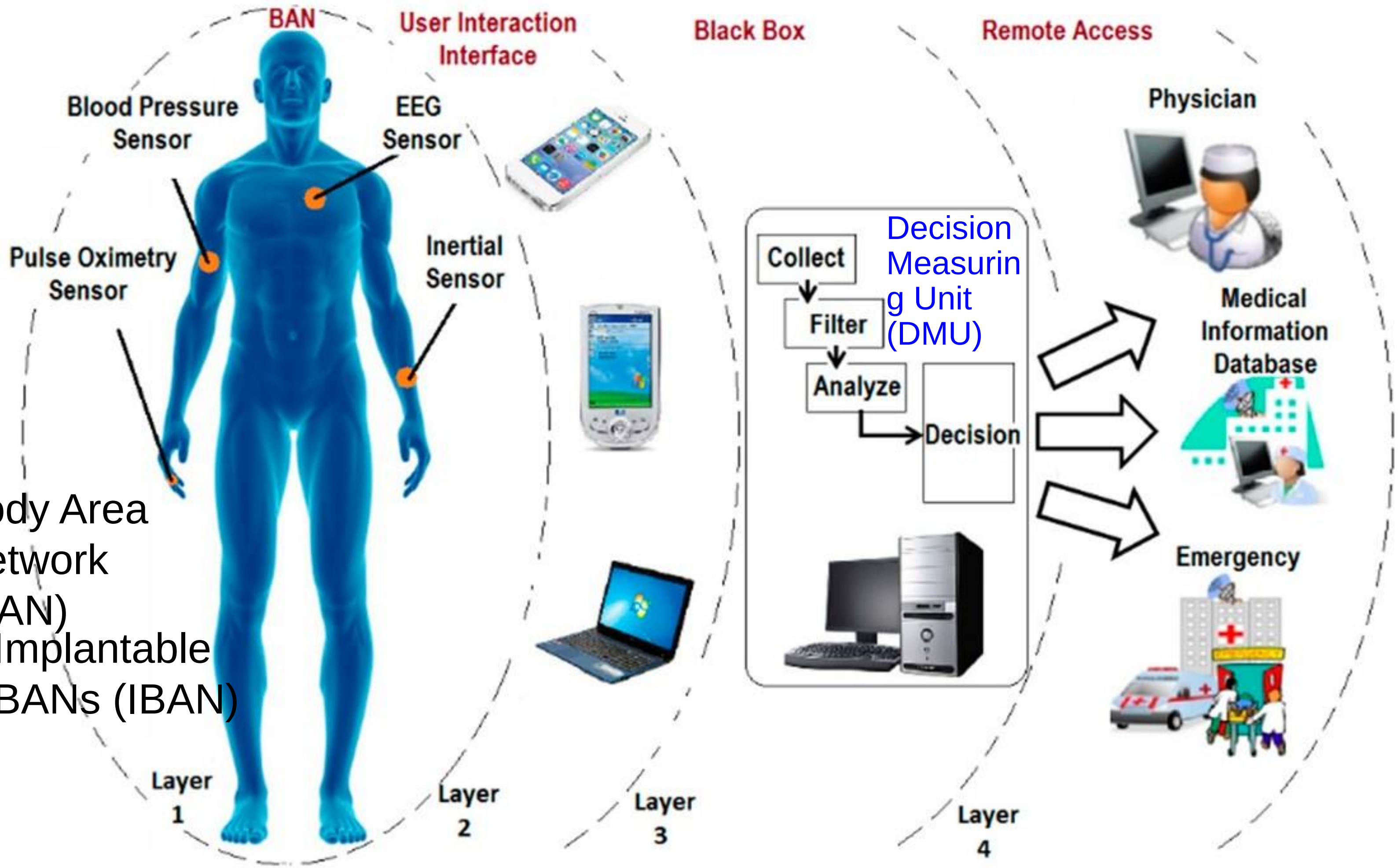
Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, “Everything you Wanted to Know about the Blockchain”, *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 4, July 2018, pp. 06--14.

Blockchain Adoption for Applications



Source: U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh and W. Hong, "A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems," in *IEEE Access*, vol. 8, pp. 54371-54401, 2020, doi: 10.1109/ACCESS.2020.2981415.

Smart Healthcare - 4-Layer Architecture



Decision Measuring Unit (DMU)

Body Area Network (BAN)

- Implantable BANs (IBAN)

Source: M. Ghamari, B. Janko, R.S. Sherratt, W. Harwin, R. Piechockic, and C. Soltanpur, "A Survey on Wireless Body Area Networks for eHealthcare Systems in Residential Environments", *Sensors*, 2016. 16(6): p. 831.

Blockchain can be a Solution for many Security Challenges in Smart Healthcare

Selected Smart Healthcare Security/Privacy Challenges

- Data Eavesdropping
- Data Confidentiality
- Data Privacy
- Location Privacy
- Identity Threats
- Access Control
- Unique Identification
- Data Integrity
- Device Security

Source: P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. Ganapathiraju, "Everything You Wanted to Know about Smart Health Care", *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 1, January 2018, pp. 18-28.

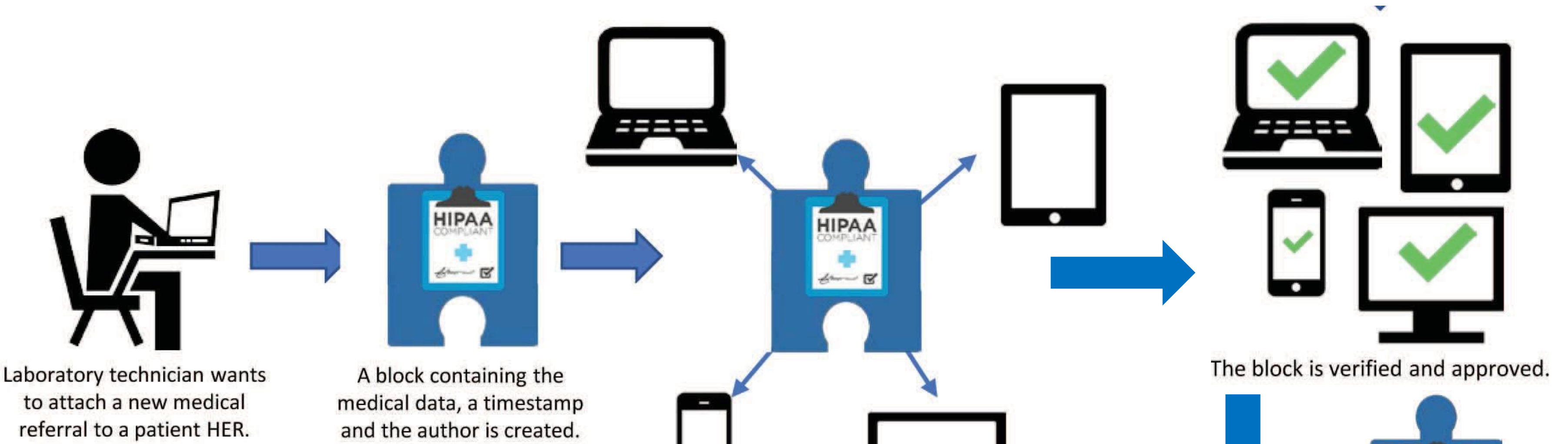
Blockchain can be a Solution for Data Quality Issue in Smart Healthcare

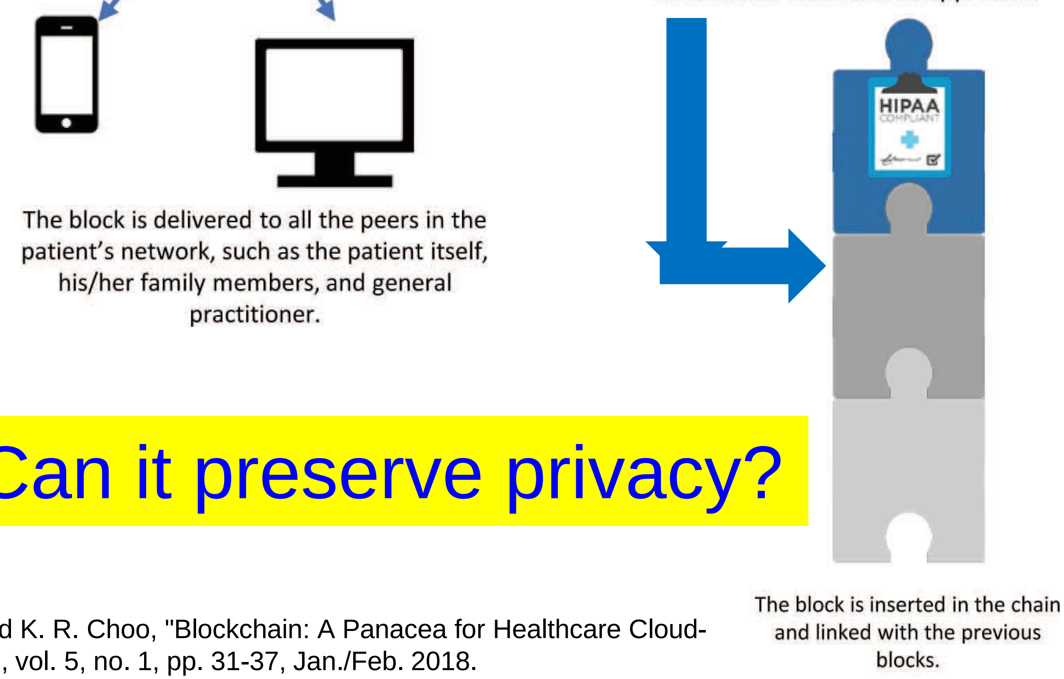
Data Quality

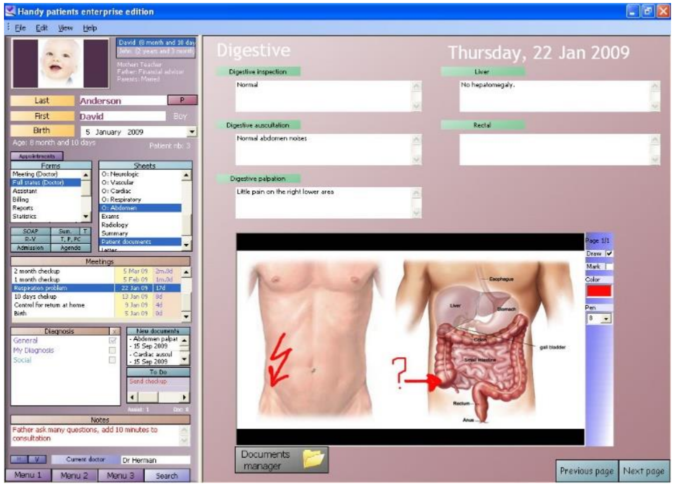
- Validity
- Reliability
- Objectivity
- Generalizability
- Utility
- Completeness
- Relevance
- Integrity

Source: H. Zhu, C. K. Wu, C. H. KOO, Y. T. Tsang, Y.Liu, H. R. Chi, and K. F. Tsang, "Smart Healthcare in the Era of Internet-of-Things", *IEEE Consumer Electronics Magazine*, vol. 8, no. 5, pp. 26-30, Sep 2019.

Blockchain in Smart Healthcare







Can it preserve privacy?

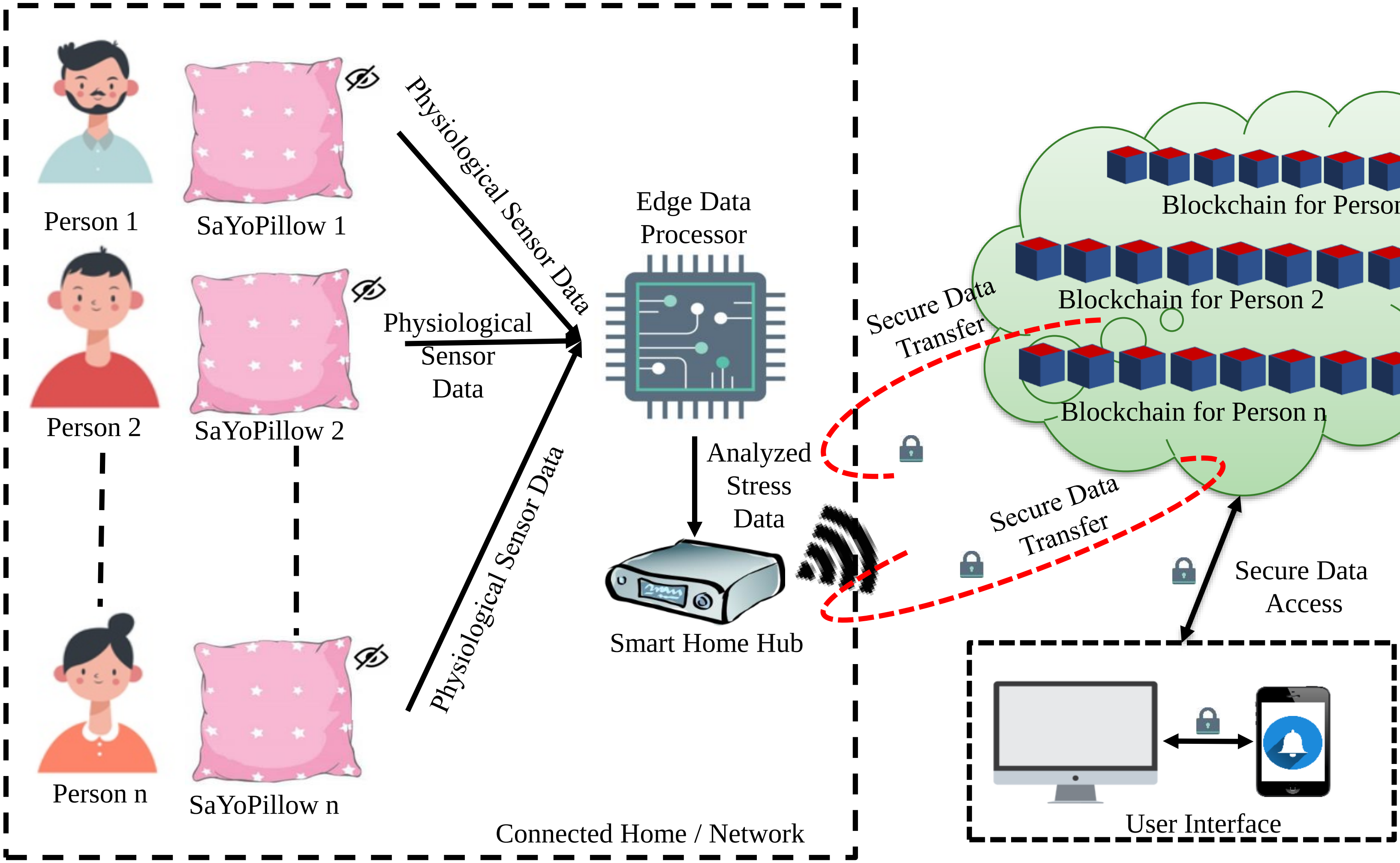
Source: C. Esposito, A. De Santis, G. Tortora, H. Chang and K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," IEEE Cloud Computing, vol. 5, no. 1, pp. 31-37, Jan./Feb. 2018.

MedRec - Overview

- Blockchain developed at MIT Media Lab.
- Permissions for ownership, viewership and is shared among private, peer-to-peer network.
- Ethereum Smart Contract is used.
- Smart contract allows automation and tracking changes.
- Cryptographic hash is used for Data integrity.
- Public key cryptography is used for patient identity.

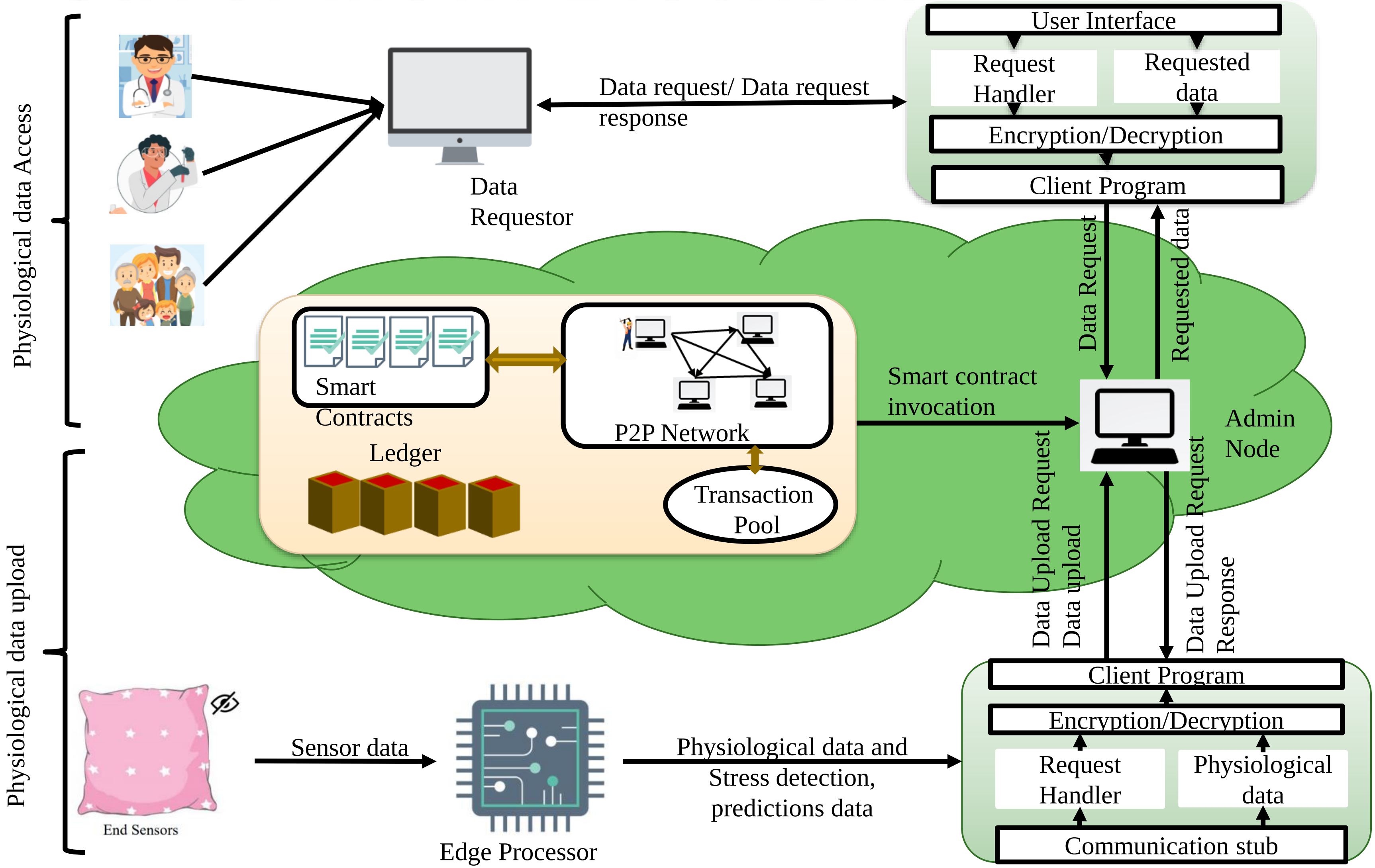
Source: A. Azaria, A. Ekblaw, Thiago Vieira and Andrew Lippman , “MedRec: Using Blockchain for Medical Data Access and Permission Management”, pp. 25--30, 2016.

Smart-Yoga Pillow (SaYoPillow) - Idea



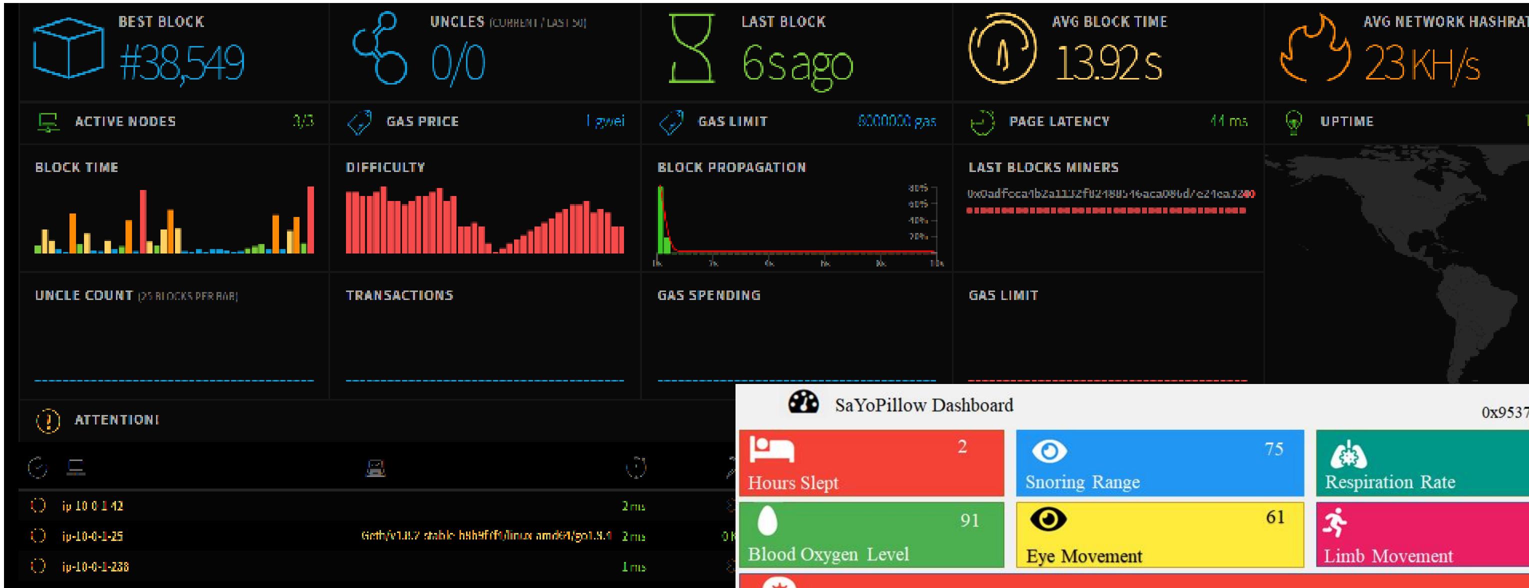
Source: L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "SaYoPillow: A Blockchain-Enabled, Privacy-Assured Framework for Stress Detection, Prediction and Control Considering Sleeping Habits in the IoMT", *arXiv Computer Science*, arXiv:2007.07377, July 2020, 38-pages.

SaYoPillow: Blockchain Details

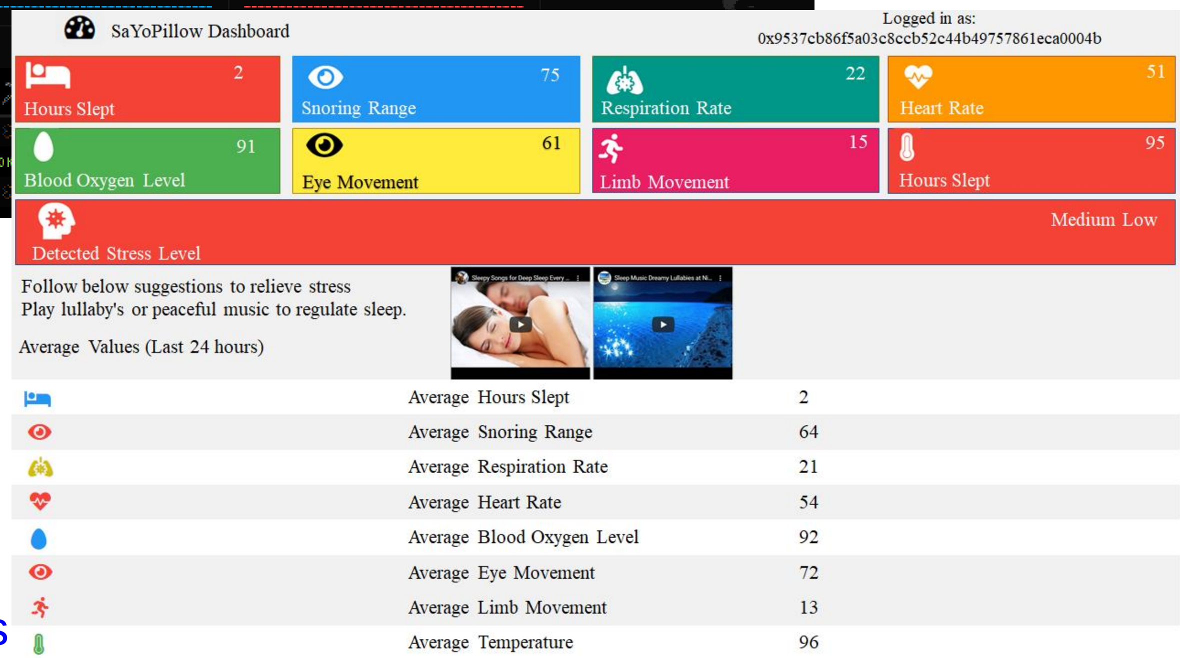


Source: L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "SaYoPillow: A Blockchain-Enabled, Privacy-Assured Framework for Stress Detection, Prediction and Control Considering Sleeping Habits in the IoMT", *arXiv Computer Science*, arXiv:2007.07377, July 2020, 38-pages.

SaYoPillow: Prototyping



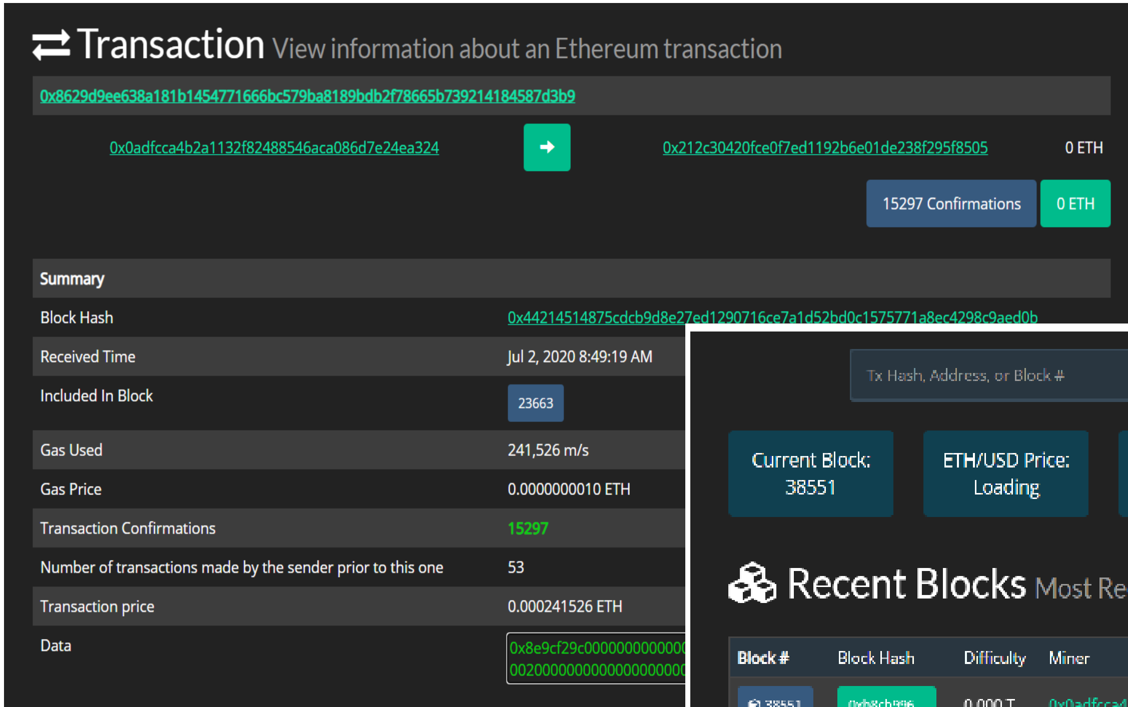
Ethereum Blockchain Status



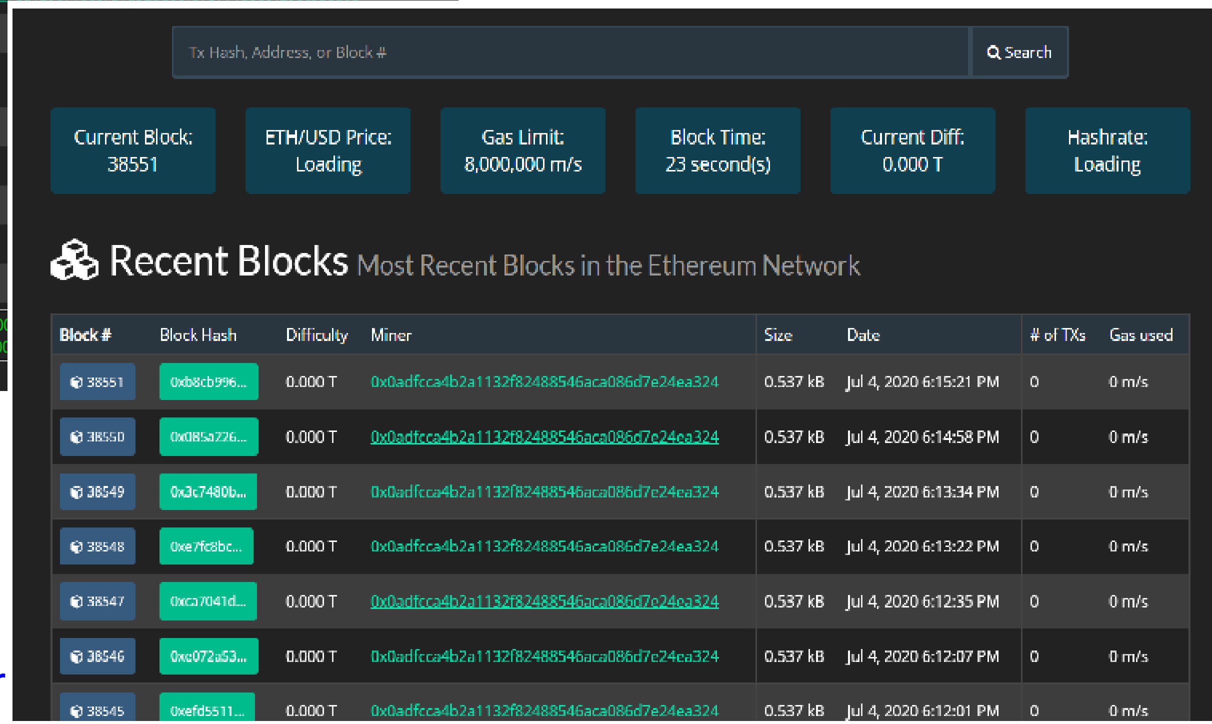
User Interface with Access

Source: L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, “SaYoPillow: A Blockchain-Enabled, Privacy-Assured Framework for Stress Detection, Prediction and Control Considering Sleeping Habits in the IoMT”, *arXiv Computer Science*, arXiv:2007.07377, July 2020, 38-pages.

SaYoPillow: Prototyping



Creating a Transaction in Ethereum



Ethereum Blockchain Explorer

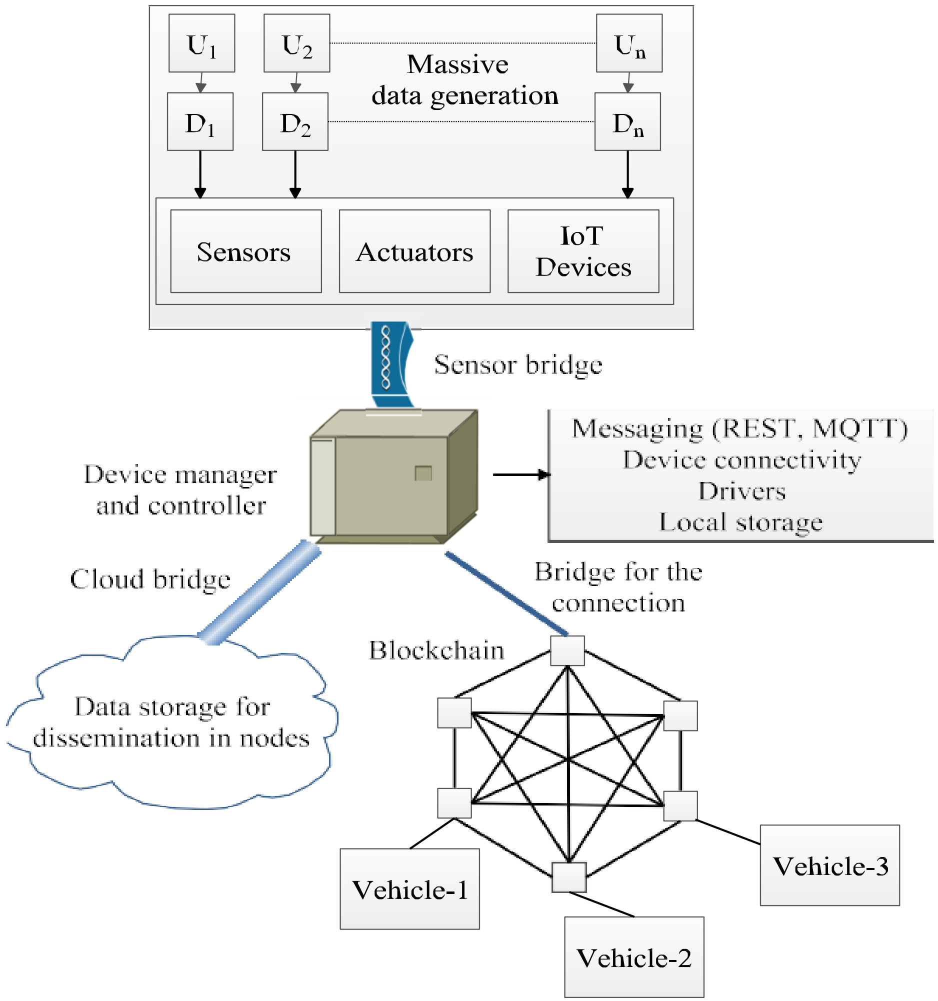
Source: L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, “SaYoPillow: A Blockchain-Enabled, Privacy-Assured Framework for Stress Detection, Prediction and Control Considering Sleeping Habits in the IoMT”, *arXiv Computer Science*, arXiv:2007.07377, July 2020, 38-pages.

Smart Transportation

- Applications meet the definition of blockchain and needs the characteristics of blockchain in smart transportation domain:
  - Car History.
  - Car locations.
  - Car Trace.
  - Car Training.
  - Car Rentals.
  - Car Ownership.
  - Blockchain could be used in the communication between cars, car – building.

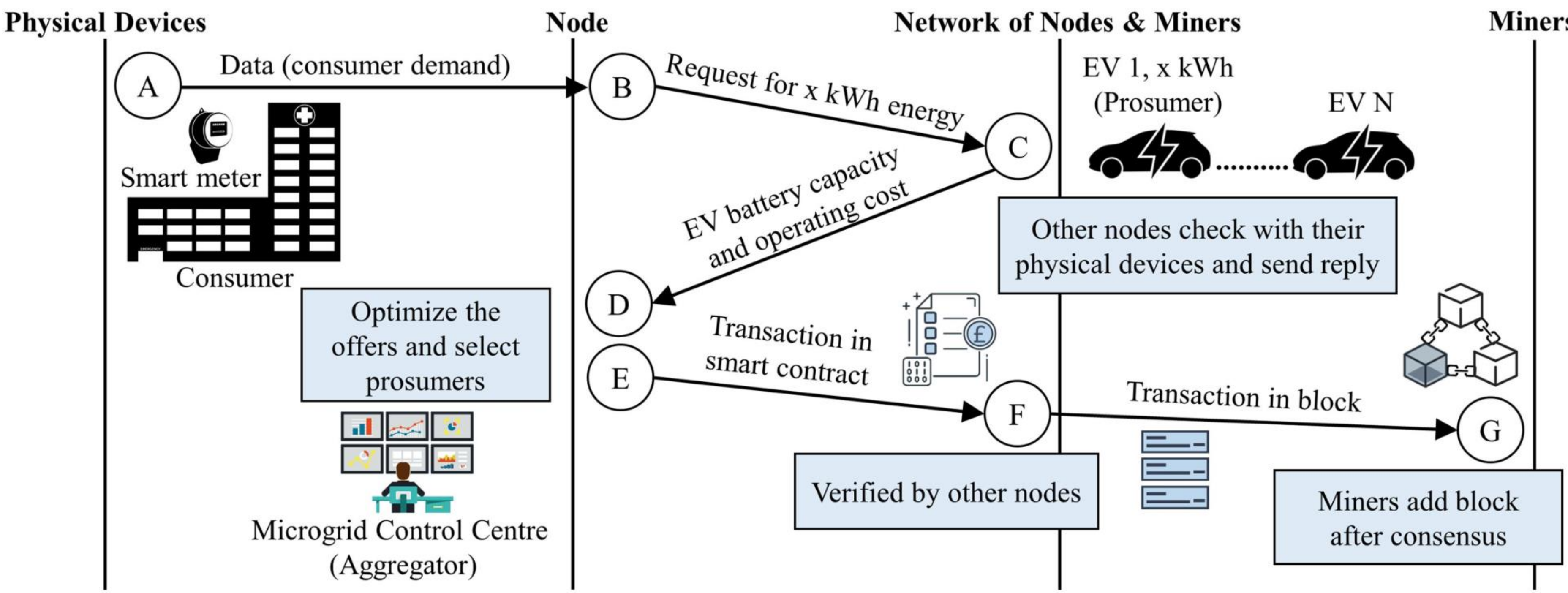
11/6/2020
259

Blockchain in Smart Transportation



Source: U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh and W. Hong, "A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems," in *IEEE Access*, vol. 8, pp. 54371-54401, 2020, doi: 10.1109/ACCESS.2020.2981415.

Blockchain based Energy Trading in Electric Vehicles



Source: I. A. Umoren, S. S. A. Jaffary, M. Z. Shakir, K. Katzis and H. Ahmadi, "Blockchain-Based Energy Trading in Electric-Vehicle-Enabled Microgrids," *IEEE Consumer Electronics Magazine*, vol. 9, no. 6, pp. 66-71, 1 Nov. 2020, doi: 10.1109/MCE.2020.2988904.

Smart Agriculture - Food Supply Chain

- Actors involved
  - Farmers
  - Shipping companies
  - Wholesalers
  - Retailers
  - Distributors
  - Grocerries

Food Supply Chain: Farm → Dinning

Source: A. M. Joshi, U. P. Shukla, and **S. P. Mohanty**, "Smart Healthcare for Diabetes: A COVID-19 Perspective", *arXiv Quantitative Biology*, arXiv:2008.11153, August 2020, 18-pages.

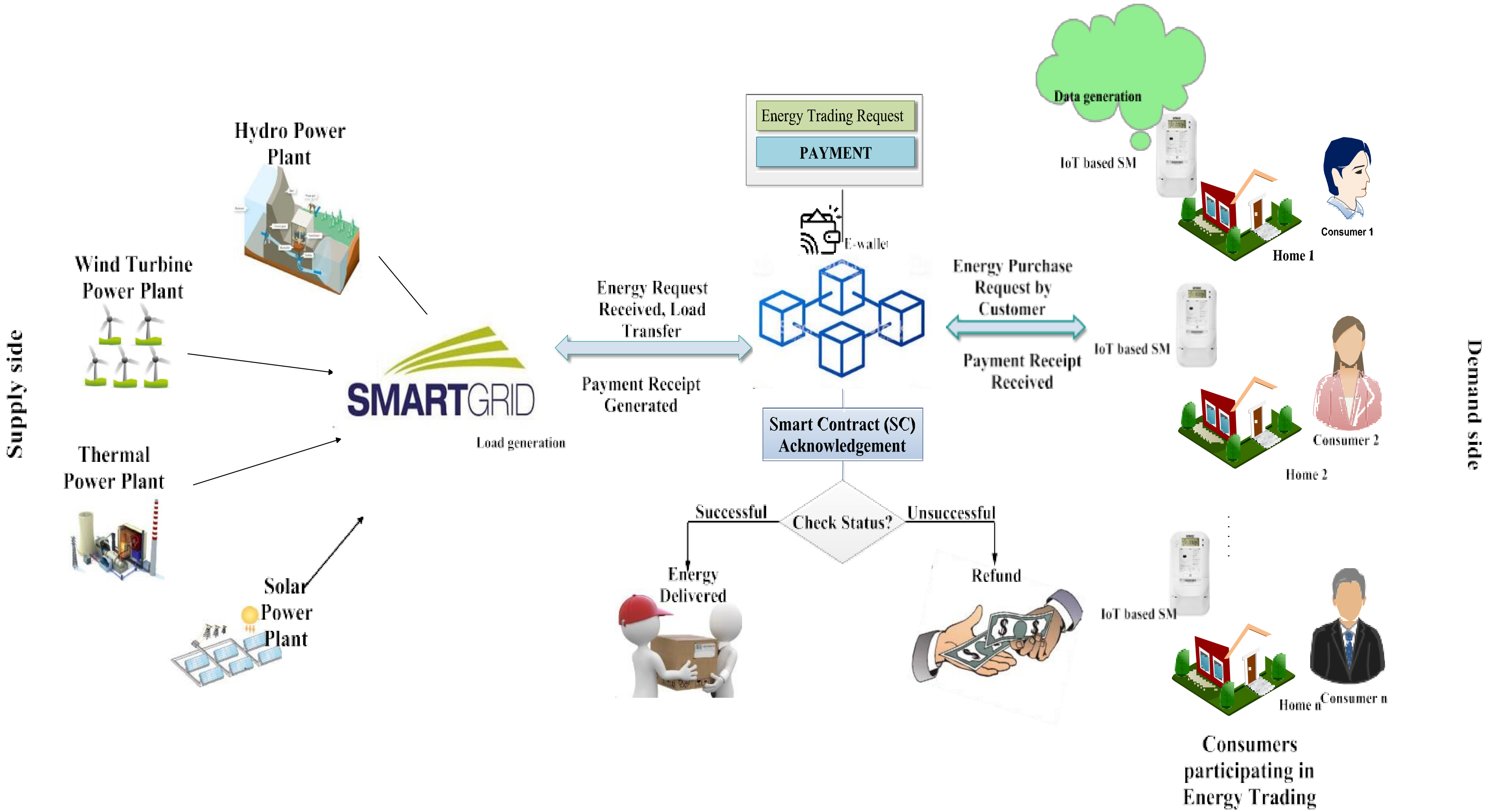
Inefficiency in Traditional Supply Chain

- High risk between buyer and seller.
- Not transparent and heavy paper based transactions
- Transactions are vulnerable to fraud
- Cost of operating supply chain will contribute to two third of the final product cost

Blockchain Potentials in Smart Agriculture

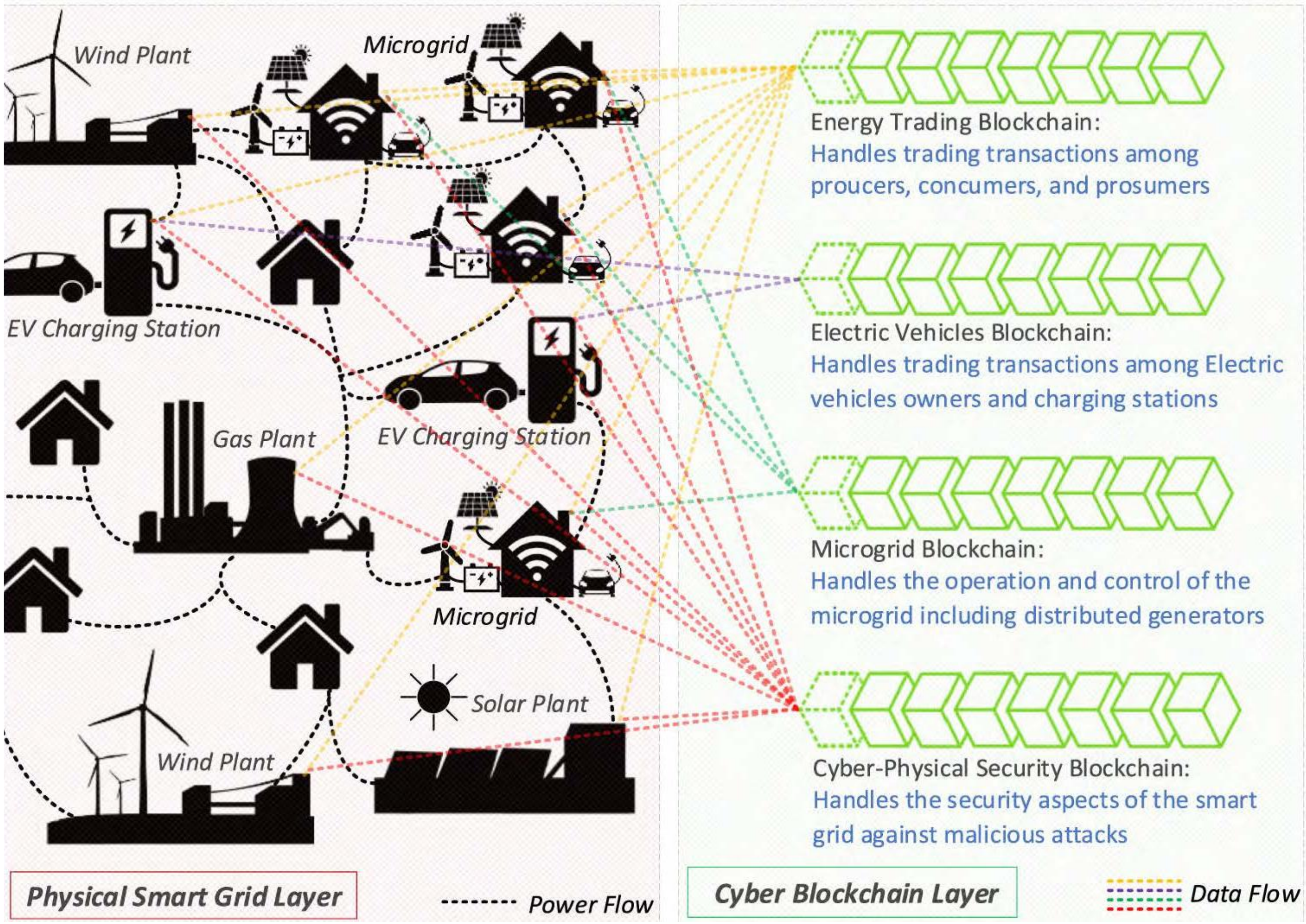
- Blockchain is expected to grow at a rate of 87% in supply chain industry
- Expected 3314.6$ million by 2023
- AgriDigital implemented settlement of 23.46 tons of grain in blockchain.
- Louis Dreyfus along with Dutch and French banks to build efficient Food stuff traders over blockchain.

Blockchain in Smart Energy



Source: U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh and W. Hong, "A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems," in *IEEE Access*, vol. 8, pp. 54371-54401, 2020, doi: 10.1109/ACCESS.2020.2981415.

Blockchain in Smart Grid



Source: A. S. Musleh, G. Yao and S. M. Muyeen, "Blockchain Applications in Smart Grid–Review and Frameworks," IEEE Access, vol. 7, pp. 86746-86757, 2019.

Hardware for Blockchain

Blockchain - Application Specific Hardware

- It is a hardware assistance to speed up the transactions process and increase the network throughput.
- The accelerator could be built using an FPGA, GPU, or ASIC processors.
- These acceleration hardware could be targeting one aspect of the blockchain or contribute in the whole network.
  - For example, an ASIC could be programmed to accelerate the trust process among nodes with lowest time and power consumption.
  - Also, increases the mining process with lowest power consumption.
- Devices in market:
- BITMAIN company has many versions of hardware mining accelerators for Blockchain applications.
- KRAMBU company provides different models of accelerators using FPGA, GPU, and ASIC.

ASIC Miner

- An application specific hardware designed for mining cryptocurrency
- ASIC's consume less power and perform better than CPU and GPU as they are application specific
- Avoids unnecessary circuitry
- Properties of miners to be considered:
  - Hash rate
  - Power efficiency
  - Price

Hardware wallets

Image source: https://www.buybitcoinworldwide.com/wallets/ledger-nano-s/

Software for Blockchain

Blockchain Platforms

1. Tezos
2. Ethereum
3. Hyperledger Fabric
4. Hyperledger Sawtooth
5. Hedera Hashgraph
6. Ripple
7. Quorum
8. Hyperledger Iroha
9. Corda
10. EOS
11. OpenChain
12. Stellar
13. Dragonchain
14. NEO

Source: https://www.leewayhertz.com/blockchain-platforms-for-top-blockchain-companies/

Blockchain Platforms

Ethereum	Hyperledger Fabric	R3 Corda	Ripple	Quorum	Hyperledger Sawtooth	EOS	Hyperledger Iroha	OpenChain	Stellar
Industry focus	Cross-Industry	Cross-Industry	Financial Services	Financial Services	Cross-Industry	Cross-Industry	Cross-Industry	Cross-Industry	Digital Asset Management
Ledger Type	Permissionless	Permissioned	Permissioned	Permissioned	Permissioned	Permissioned	Permissioned	Permissioned	Permissioned
Consensus Algorithm	Proof of Work	Pluggable Framework	Pluggable Framework	Probabilistic Voting	Majority Voting	Pluggable Framework	Delegated Proof-of-Stake	Chain-based Byzantine Fault Tolerant	Partionned Consensus
Smart Contract	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes
Governance	Ethereum Developers	Linux Foundation	R3 Consortium	Ripple Labs	Ethereum Developers and JP Morgan Chase	Linux Foundation	EOSIO Core Arbitration Forum(ECAF)	Linux Foundation	CoinPrism

Source: https://www.leewayhertz.com/blockchain-platforms-for-top-blockchain-companies/

Blockchain Development Tools

1. Geth
2. Mist
3. Solc
4. Remix
5. Testnet
6. GanacheCLI
7. Coinbase
8. EtherScripter
9. BaaS
10. Metamask
11. Ethers.js
12. Tierion
13. Embark
14. Truffle
15. MyEtherWallet

Source: https://blockgeeks.com/guides/15-best-tools-blockchain-development/

Blockchain Performance Metrics

Gas Price

- Gas is defined as the fundamental network cost unit in Ethereum networks
- It exists only inside the Ethereum computational Engine
- Gas may not be considered as proper metric because:
  - It is cost unit and used only in execution stage
  - Doesn't evaluate during other stages like block committing, validation etc.
  - Gas price is floating and may vary time to time

Transactions per Second (TPS)

- Different blockchains will have different execution times for deploying, invoking and executing of smart contracts.
- The throughput can be measured by Transactions per second
- TPS = count(Tx in (ti,tj))/(ti-tj) txns/second

where ti,tj are time in between which transactions are counted

- Throughput for n peers in the network can be calculated

$$\overline{TPS} = \frac{\sum_u TPSu}{N} \frac{txns}{sec}$$

Where TPSu = Throughput of each node and N is number of nodes

Source: Zheng, Peilin & Zheng, Zibin & Luo, Xiapu & Chen, Xiangping & Liu, Xuanzhe. (2018). A detailed and real-time performance monitoring framework for blockchain systems. 134-143. 10.1145/3183519.3183546.

Average Response Delay

- Time between the transaction being sent to the peer and transaction is confirmed is called Average Response Delay (ARD).
- Tx is number of transactions and tTxconfirmed, tTxinput are time at which the transaction is confirmed and sent respectively

$$\mathrm{ARD}_u = \frac{\sum Tx\,(t_{Tx\ confirmed} - t_{Tx\ input})}{Count\,(Tx\ in\ (t_i, t_j))}(txs/s).$$

$$\overline{ARD} = \frac{\sum_u ARD_u}{N}(txs/s).$$

Source: Zheng, Peilin & Zheng, Zibin & Luo, Xiapu & Chen, Xiangping & Liu, Xuanzhe. (2018). A detailed and real-time performance monitoring framework for blockchain systems. 134-143. 10.1145/3183519.3183546.

Transaction per CPU

- As different networks work on different CPU powers and the CPU utilization depends on business logic complexity and block validation capacity of CPU
- To quantify below Transaction per CPU will help
- F is the frequency of CPU and CPU(t)is the utilization of CPU at that time.

$$\mathrm{TPC}_u = \frac{Count\left(Tx\ in\left(t_i, t_j\right)\right)}{\int_{t_i}^{t_j} F * CPU(t)}(txs/(GHz \cdot s)),$$

$$\overline{TPC} = \frac{\sum_u TPC_u}{N}(txs/(GHz \cdot s)).$$

Source: Zheng, Peilin & Zheng, Zibin & Luo, Xiapu & Chen, Xiangping & Liu, Xuanzhe. (2018). A detailed and real-time performance monitoring framework for blockchain systems. 134-143. 10.1145/3183519.3183546.

Transaction per Memory Second

- Execution the account data is loaded into main memory.
- RMEM(t) is real memory consumed by blockchain program at time t and VMEM(t) is the virtual memory consumed.

$$TPMS_u = \frac{Count\left(Tx\ in\left(t_i, t_j\right)\right)}{\int_{t_i}^{t_j} RMEM(t) + VMEM(t)} (txs/(MB \cdot s))$$

$$\overline{TPMS} = \frac{\sum_u TPMS_u}{N} (txs/(MB \cdot s)).$$

Source: Zheng, Peilin & Zheng, Zibin & Luo, Xiapu & Chen, Xiangping & Liu, Xuanzhe. (2018). A detailed and real-time performance monitoring framework for blockchain systems. 134-143. 10.1145/3183519.3183546.

Transactions per Disk I/O

- Blockchain will have separate disk space to store data including world ledger state
- DISKR(t) is size of data read from the disk at time t and DISKW(t) is the size of data write to disk at time t

$$\mathrm{TPDIO}_u = \frac{Count\left(Tx\ in\left(t_i, t_j\right)\right)}{\int_{t_i}^{t_j} DISKR(t) + DISKW(t)}(txs/kilobytes),$$

$$\overline{TPDIO} = \frac{\sum_u TPDIO_u}{N}(txs/kilobytes).$$

Source: Zheng, Peilin & Zheng, Zibin & Luo, Xiapu & Chen, Xiangping & Liu, Xuanzhe. (2018). A detailed and real-time performance monitoring framework for blockchain systems. 134-143. 10.1145/3183519.3183546.

Transactions Per Network Data

- Bases on different consensus mechanism, the data will be shared over network to append to ledgers
- UPLOAD(t) is size of upstream and DOWNLOAD(t) is size of downstream in the network at time t

$$TPND_u = \frac{Count\left(Tx\ in\left(t_i, t_j\right)\right)}{\int_{t_i}^{t_j} UPLOAD(t) + DOWNLOAD(t)} (txs/kilobytes),$$

$$\overline{TPND} = \frac{\sum_u TPND_u}{N} (txs/kilobytes).$$

Source: Zheng, Peilin & Zheng, Zibin & Luo, Xiapu & Chen, Xiangping & Liu, Xuanzhe. (2018). A detailed and real-time performance monitoring framework for blockchain systems. 134-143. 10.1145/3183519.3183546.

Block Generation Time

- Block Time / Block creation time is defined as time taken to create a new block in the blockchain
- This depends on complexity of consensus mechanism
- Bitcoins network’s block time is nearly 10 minutes and Ethereum it is 20 seconds nearly
- Consensus determines the ordering of events and coming up on an agreement between all the nodes
- It is performed by miners

Blockchain Validation Time

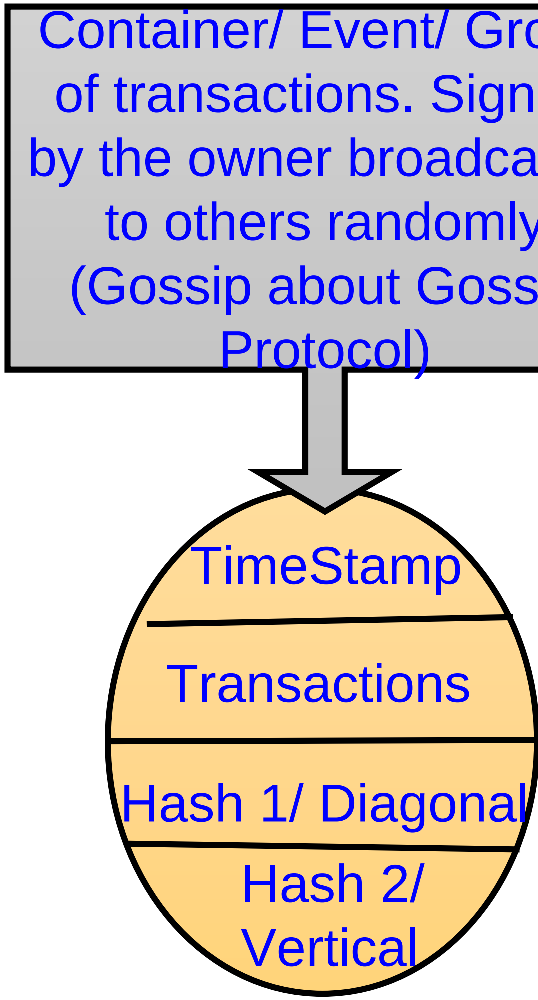
- Blockchain validation is different from blockchain consensus
- Any full-node can validate a transaction
- There is no incentive for validation, except security which is not a motivation
- Miners will be validators in most of the chains
- Validation checks the double spending maliciousness of the transactions

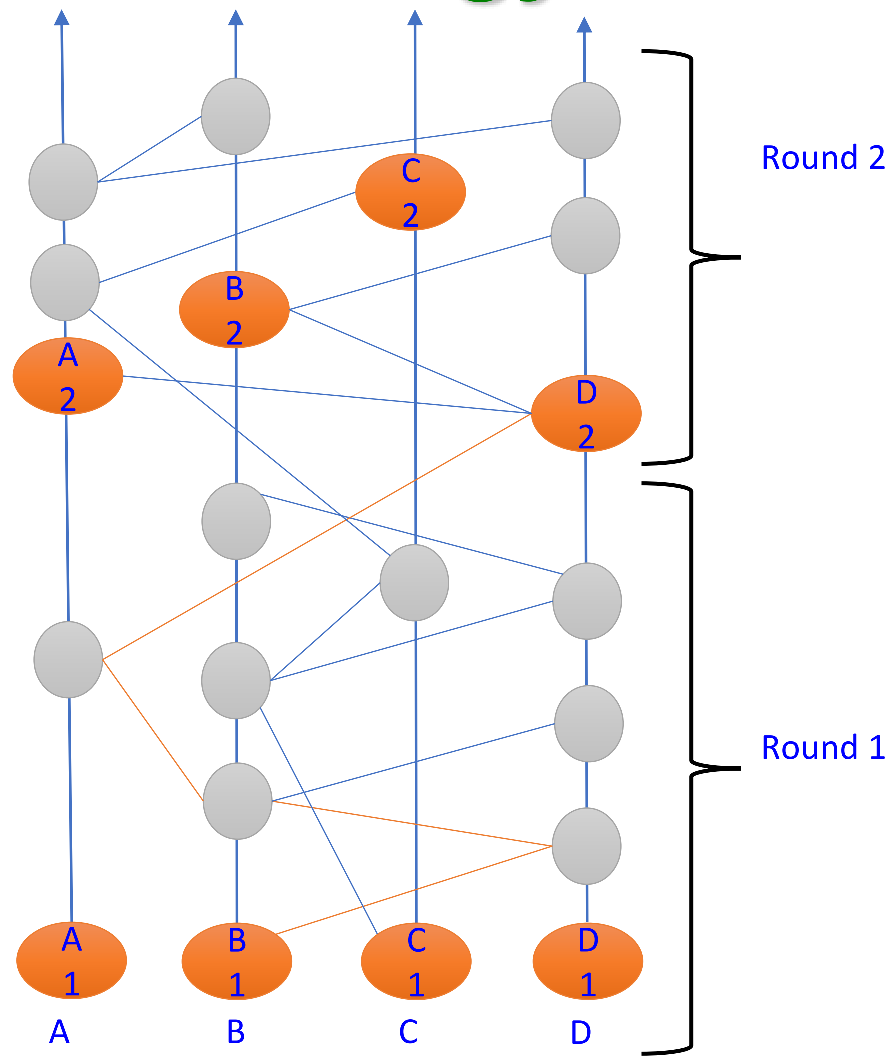
Blockchain Memory Usage

- As discussed in limitations, Memory is directly impacting the costs of operating the blockchain
- Less data to store on blockchain is desirable, hashing can help in storing such large data

Next Generation Blockchain/Ledger Solutions

Hashgraph Technology





Tangle Technology

- One disadvantage of blockchain-based cryptocurrencies like bitcoin: The concept of a transaction fee that is levied for all transactions occurring on the network irrespective of the transaction value.
- Transaction costs make the use of blockchain-based cryptocurrency impractical for such small payments.
- Tangle: A directed acyclic graph (DAG) structure stores the transactions occurring on the public ledger. It does not incorporate blockchain technology, thereby attempting to address the issue of transaction costs by using the Tangle storage system.

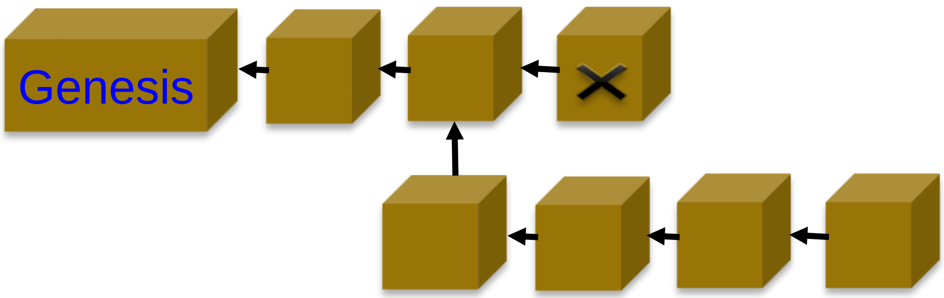
Source: https://www.investopedia.com/terms/t/tangle-cryptocurrency.asp

Tangle Technology

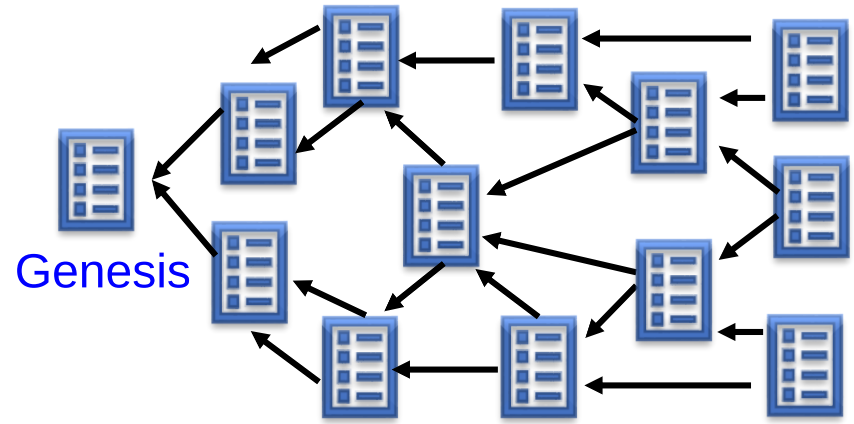
- The working mechanism of Tangle requires a new transaction to approve the previous two transactions.
- Tangle forces a transaction issuing-participant, or node, to contribute towards the agility and security of the network by making him/her approve earlier two pending transactions.
- The nodes also ensure that there are no duplicate transactions leading to double spending, and there are no conflicts among the various transactions as per the Tangle transaction history.

Source: https://www.investopedia.com/terms/t/tangle-cryptocurrency.asp

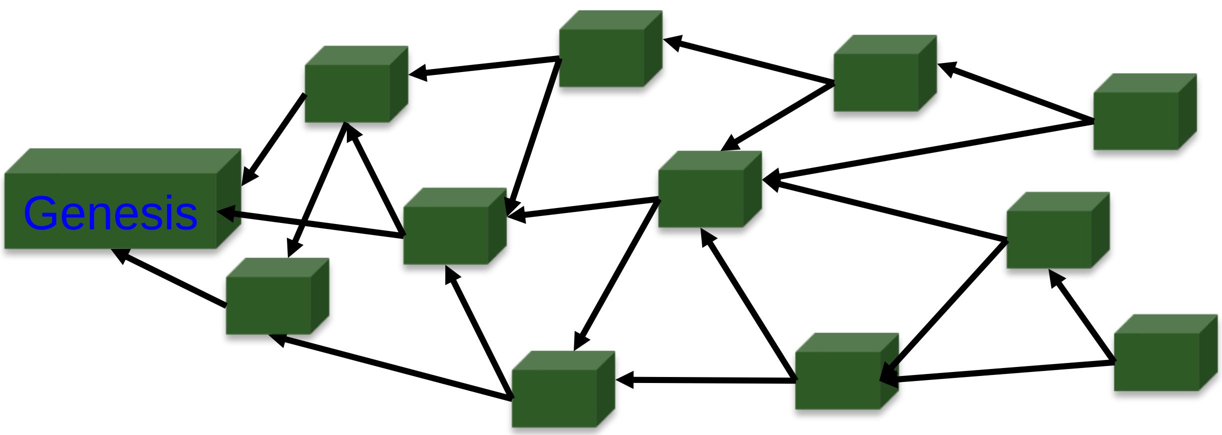
Comparative Perspective of BC, Tangle, Versus Proposed MC



(a) Blockchain Technology



(b) Tangle Technology



(c) Post-Blockchain Multichain as a Directed Acyclic Graph (DAG)

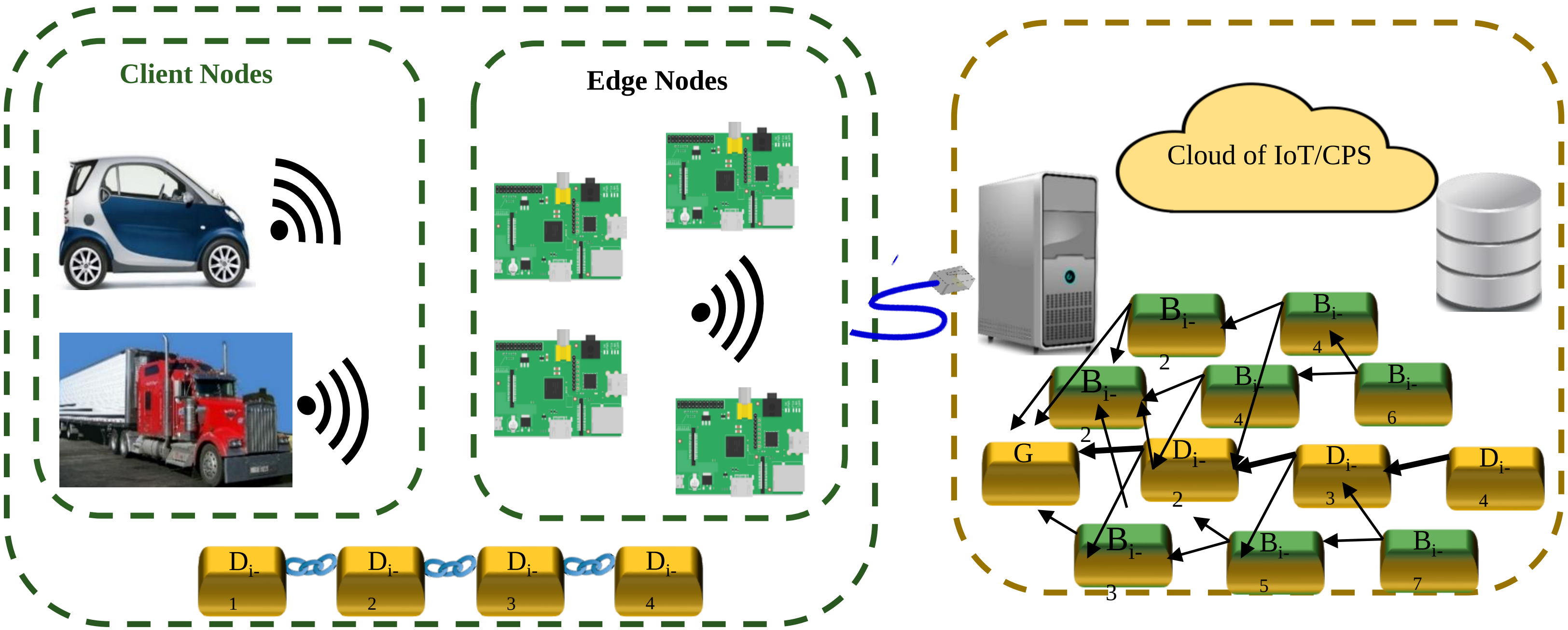
Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, “McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems”, *Proc. 9th IEEE-CS Annual Sympo. on VLSI (ISVLSI)*, 2020, pp. 446--451.

A Perspective of BC, Tangle Vs Our Multichain

Features/Technology	Blockchain (Bitcoin)	Proof of Authentication	Tangle	HashGraph	McPoRA (current Paper)
Linked Lists	• One linked list of blocks. • Block of transactions.	• One linked list of blocks. • Block of transactions.	• DAG linked list. • One transaction.	• DAG linked List. • Container of transactions hash	• DAG linked List. • Block of transactions. • Reduced block.
Validation	Mining	Authentication	Mining	Virtual Voting (witness)	Authentication
Type of validation	Miners	Trusted Nodes	Transactions	Containers	All Nodes
Ledger Requirement	Full ledger required	Full ledger required	Portion based on longest and shortest paths.	Full ledger required	Portion based on authenticators' number
Cryptography	Digital Signatures	Digital Signatures	Quantum key signature	Digital Signatures	Digital Signatures
Hash function	SHA 256	SHA 256	KECCAK-384	SHA 384	SCRYPT
Consensus	Proof of Work	Cryptographic Authentication	Proof of Work	aBFT	Predefined UID
Numeric System	Binary	Binary	Trinity	Binary	Binary
Involved Algorithms	HashCash	No	• Selection Algorithm • HashCash	No	BFP
Decentralization	Partially	Partially	Fully	Fully	Fully
Appending Requirements	Longest chain	One chain	Selection Algorithm	Full Randomness	Filtration Process
Energy Requirements	High	Low	High	Medium	Low
Node Requirements	High Resources Node	Limited Resources Node	High Resources Node	High Resources Node	Limited Resources Node
Design Purpose	Cryptocurrency	IoT applications	IoT/Cryptocurrency	Cryptocurrency	IoT/CPS applications

Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, "McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems", *Proc.19th IEEE-CS Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446--451.

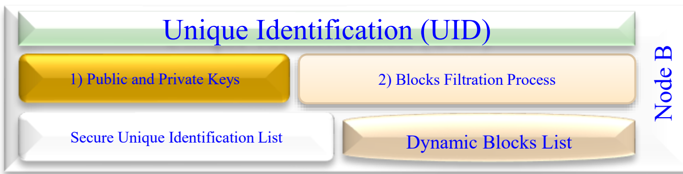
Our Multi-Chain Technology to Enhance Scalability

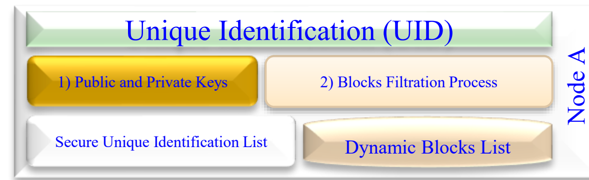


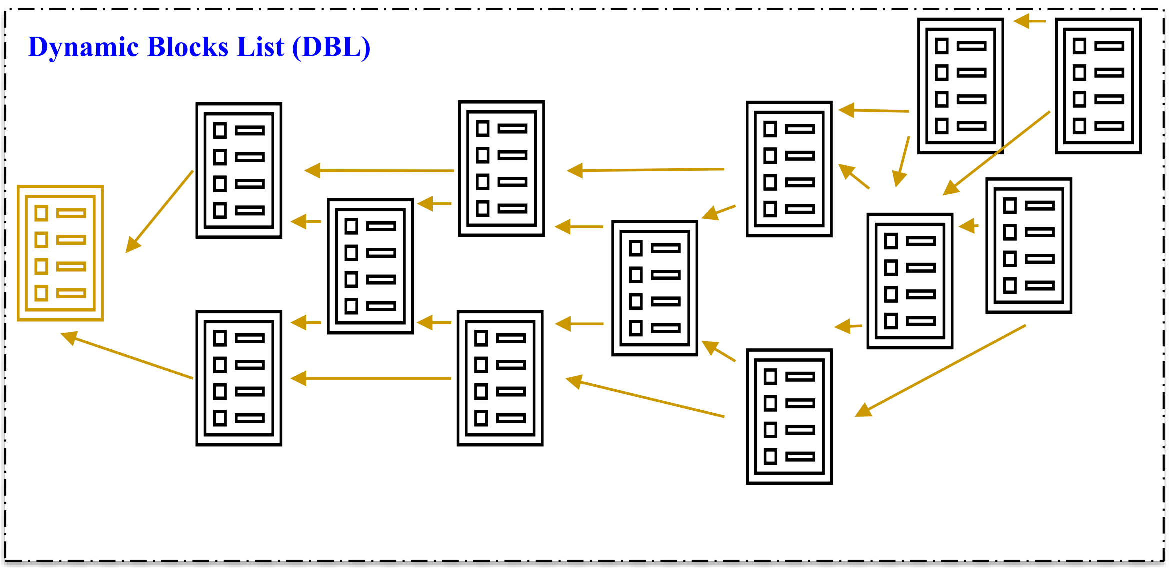
(a) Nodes-Chain (b) Multi-Blockchains

Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, "McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems", *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446--451.

McPoRA -- Components







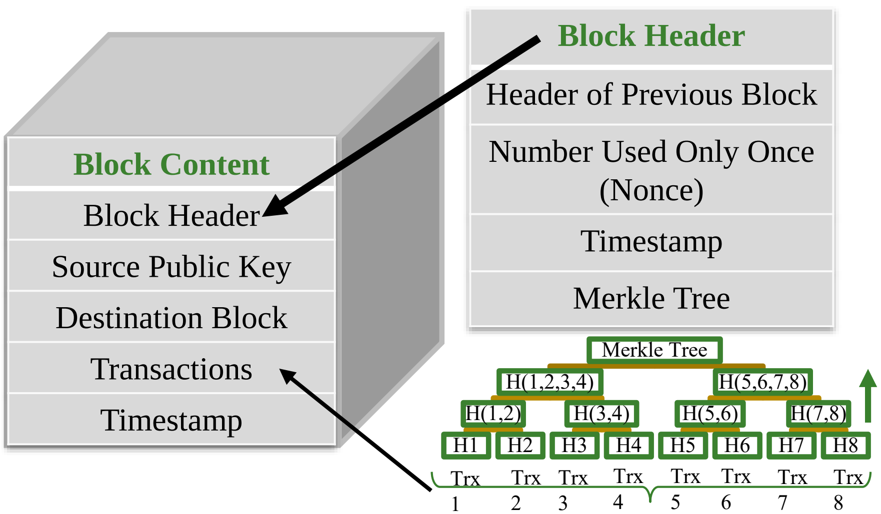
Secure Unique Identification List (SUIL)

Secure IDs' file consists of all active Nodes joined the Private network.

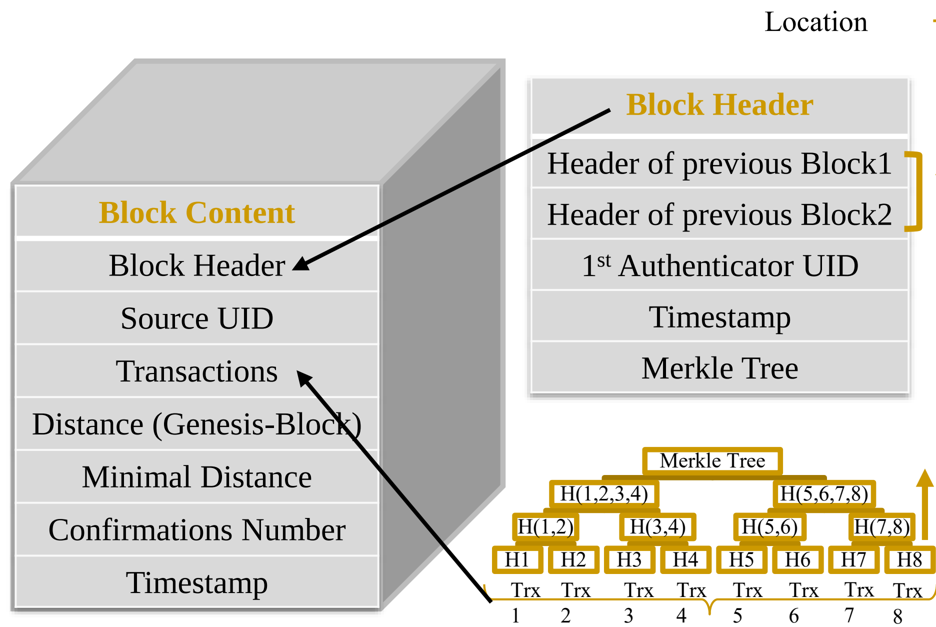
Hashed
Node A Unique Identification (UID)
Node B Unique Identification (UID)
Node C Unique Identification (UID)
Node D Unique Identification (UID)
Node E Unique Identification (UID)
Node F Unique Identification (UID)
Node G Unique Identification (UID)
Node H Unique Identification (UID)
Node I Unique Identification (UID)

Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, "McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems", *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446—451.

McPoRA - Block Structure



(a) For Traditional Blockchain

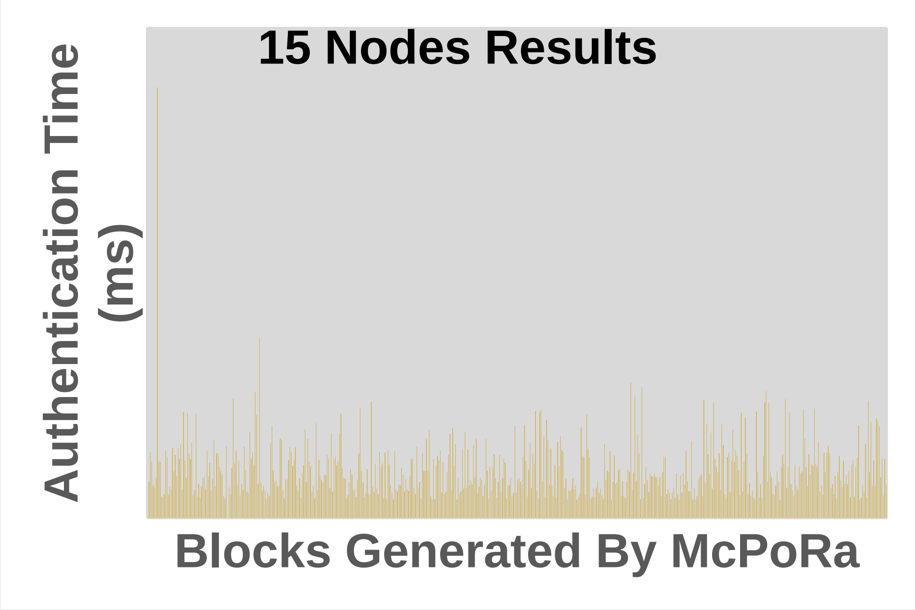


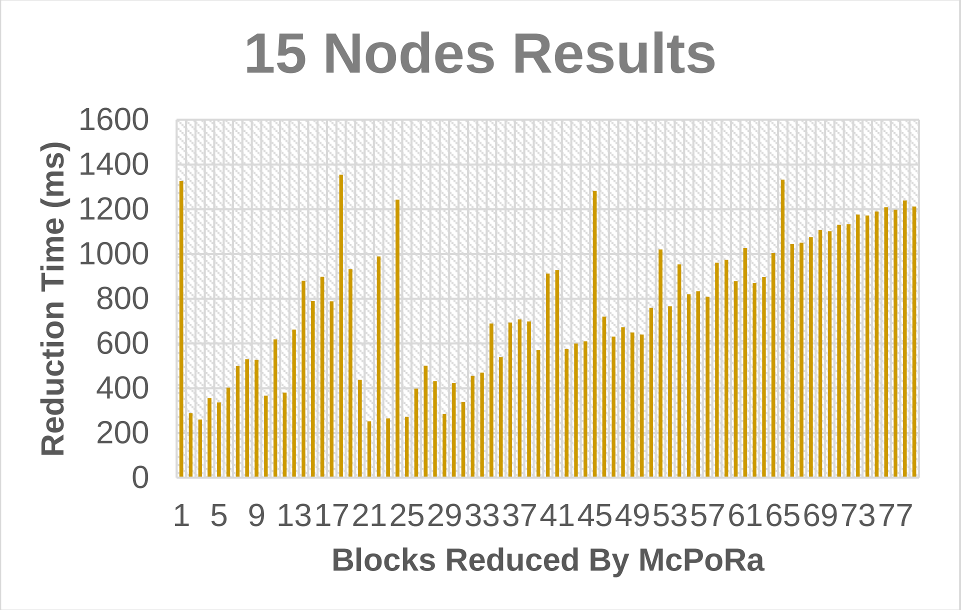
(b) For Proposed Post-Blockchain

Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, “McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems”, *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446—451.

McPoRA – Experimental Results

Time (ms)	Authentication (ms)	Reduction (ms)
Minimum	1.51	252.6
Maximum	35.14	1354.6
Average	3.97	772.53

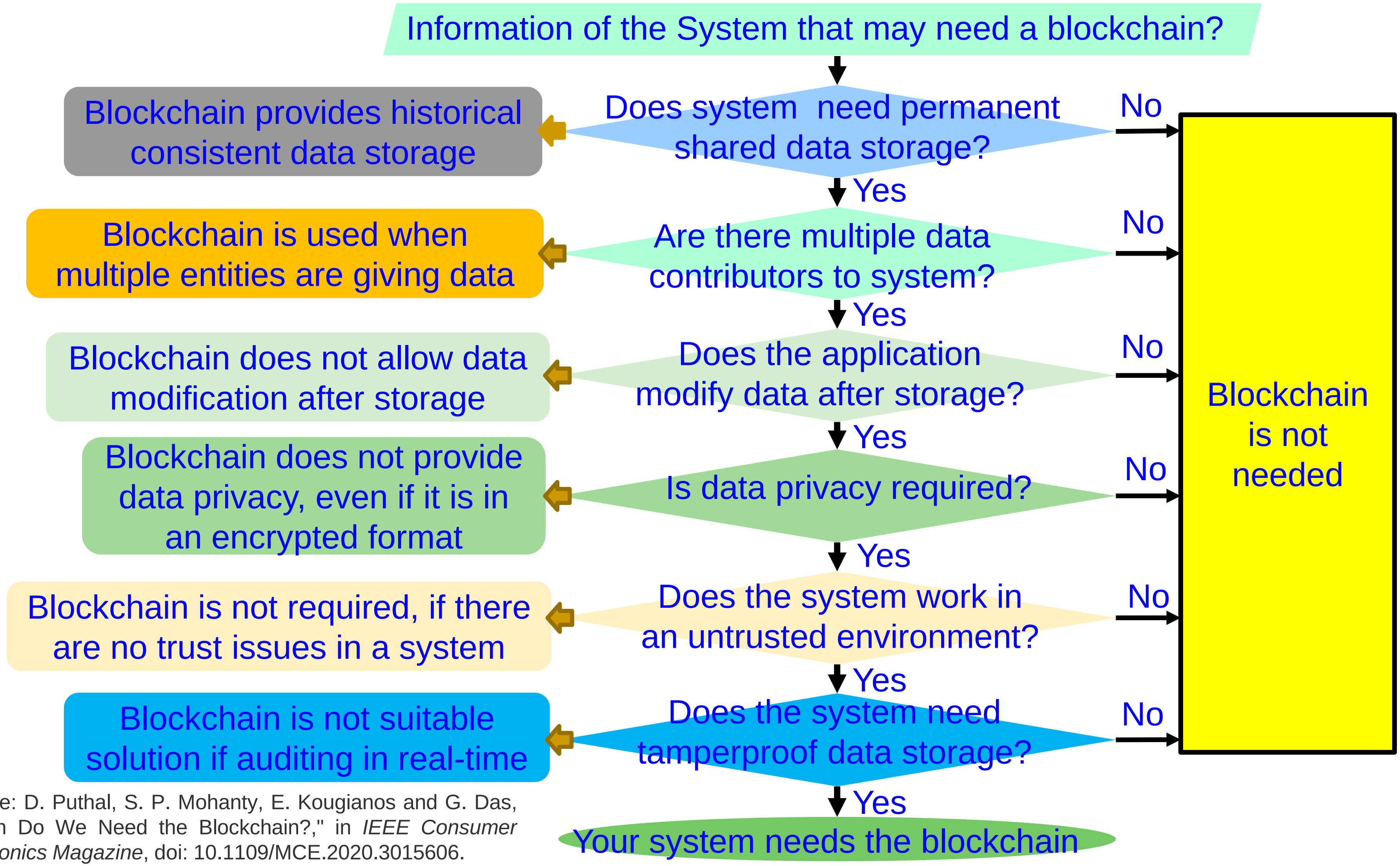




Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, "McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems", *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446—451.

Conclusions and Future Directions

When do You Need the Blockchain?



Source: D. Puthal, S. P. Mohanty, E. Kougianos and G. Das, "When Do We Need the Blockchain?," in *IEEE Consumer Electronics Magazine*, doi: 10.1109/MCE.2020.3015606.

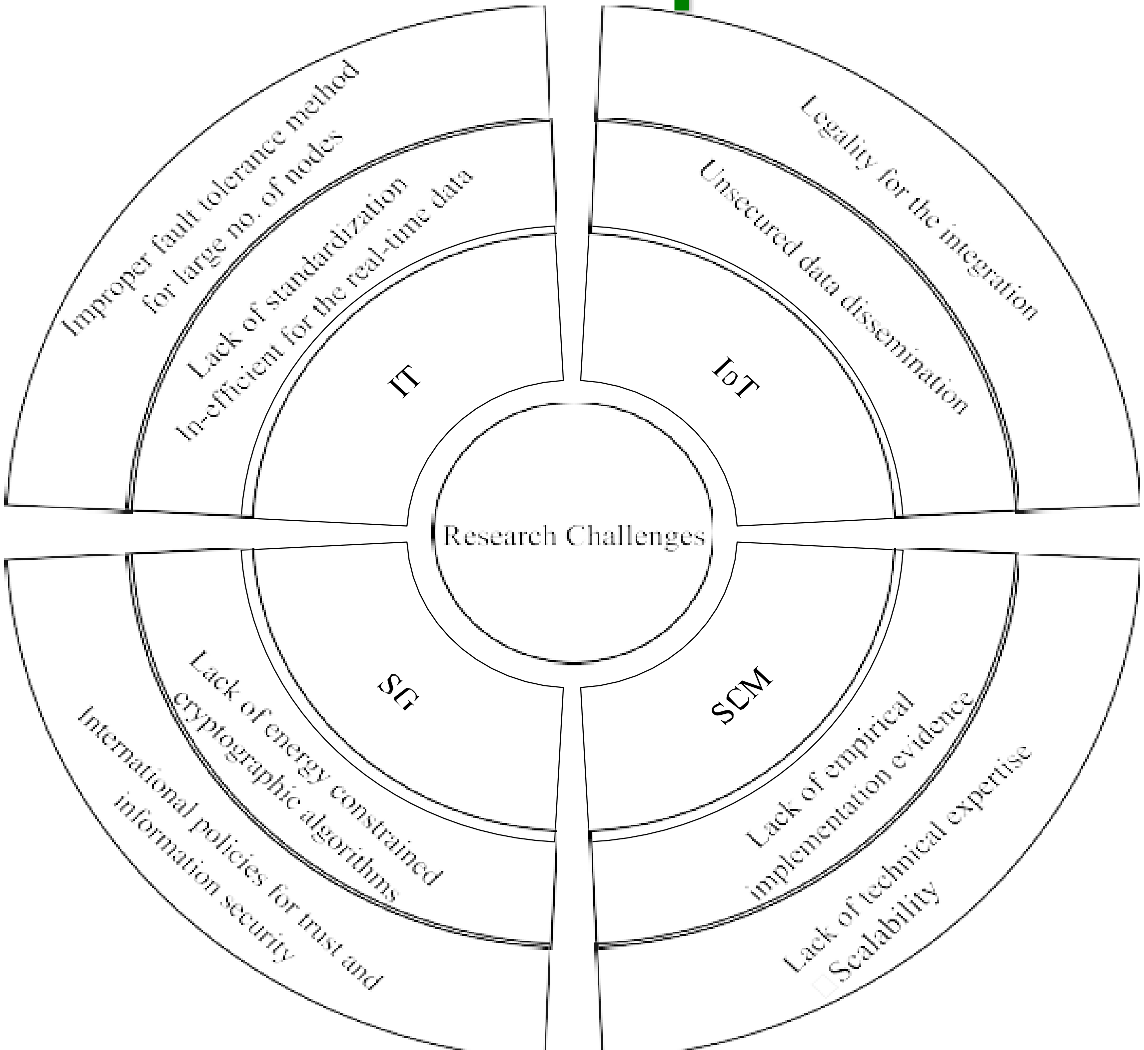
Conclusions

- Blockchain technology has many advantages and applicability in different fields.
- Blockchain is a secure platform that could contribute in smart healthcare, smart transportation, smart contract, and smart agriculture.
- Blockchain could consolidate IoT applications in smart environments.
- DAG is an alternative technique for blockchain technology and could be used of applications that require rapid responses.
- Acceleration hardware is a new hardware assistance to fasten the calculation and processes of the blockchain.

Future Directions

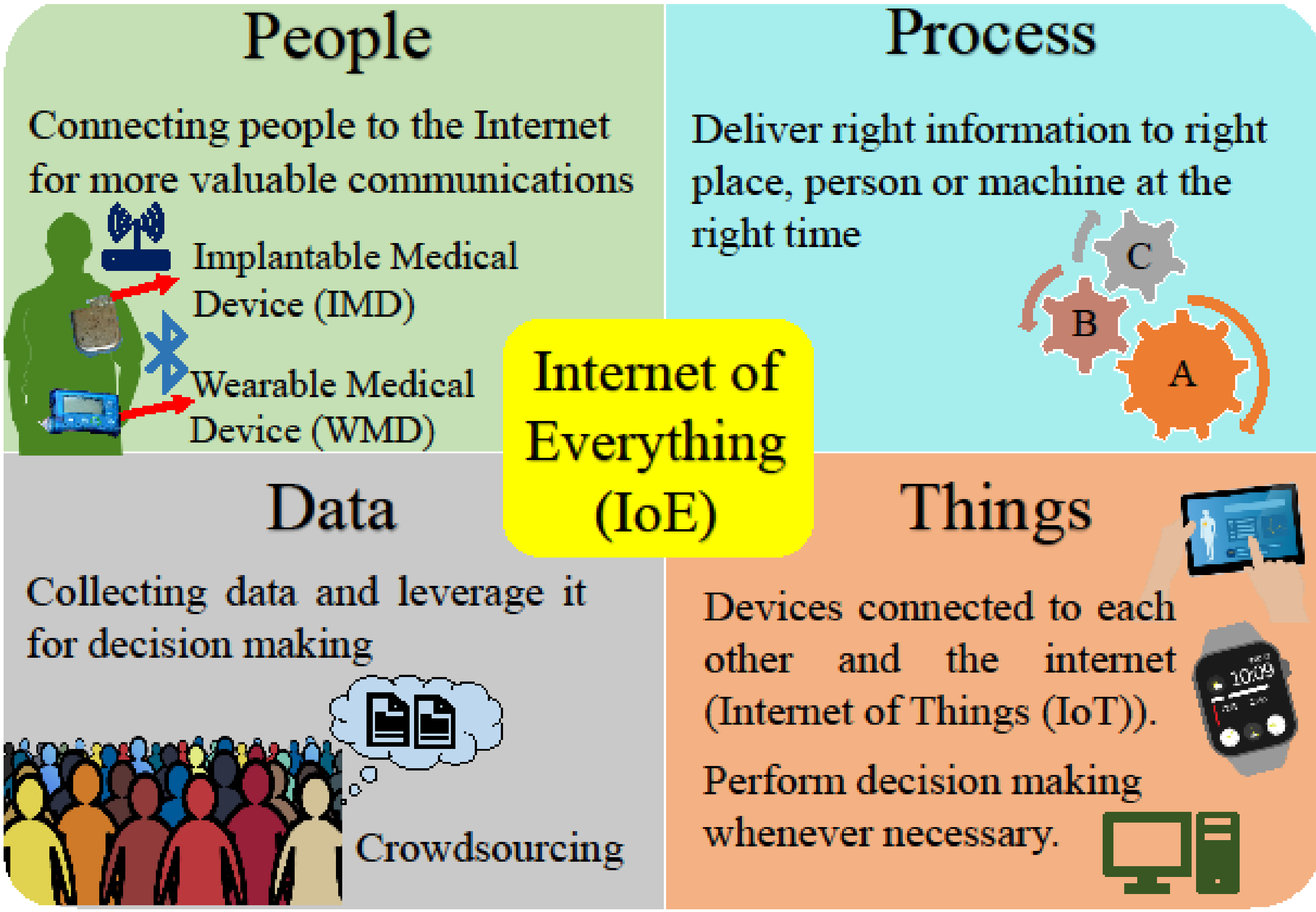
- As future directions, more efficient and low power algorithms for blockchain can be developed.
- Even though Blockchain has many advantages, it has some limitations.
- These limitations created opportunities for researchers, and companies to figure out a way to overcome it.

Blockchain - Open Issues



Source: U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh and W. Hong, "A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems," in *IEEE Access*, vol. 8, pp. 54371-54401, 2020, doi: 10.1109/ACCESS.2020.2981415.

Internet of Every Things (IoE)



Requires:
- Data, Device, and System Security
- Data, Location, and System Privacy

Need of the Hour:
- Security/Secure by Design (SbD)
- Privacy by Design (PbD)

Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE)", *arXiv Computer Science*, arXiv:1909.06496, September 2019, 37-pages.

References

- D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, “The Blockchain as A Decentralized Security Framework”, IEEE Consumer Electronics Magazine, Vol. 7, No. 2, pp. 18--21, 2018.
- D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, “Everything you Wanted to Know about the Blockchain”, IEEE Consumer Electronics Magazine, Vol. 8, No. 4, pp. 6--14, 2018.
- M. Samaniego and R. Deters, “Blockchain as a Service for IoT”, 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 433--436, 2016.
- S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system.”, https://bitcoin.org/bitcoin.pdf, Last visited 08 Oct 2018.
- A. Azaria, A. Ekblaw, T. Vieira and A. Lippman , “MedRec: Using Blockchain for Medical Data Access and Permission Management”, pp. 25--30, 2016.

References

- D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, “Everything You Wanted to Know About Blockchain,” IEEE Consum. Electron. Mag., vol. 7, no. 4, pp. 6–14, 2018.
- D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, “The blockchain as a decentralized security framework,” IEEE Consum. Electron. Mag., vol. 7, no. 2, pp. 18–21, 2018.
- D. Puthal, N. Malik, and S. P. Mohanty, “Proof of authentication: IoT-friendly blockchains,” IEEE Consum. Electron. Mag., vol. 38, no. 1, pp. 26–29, 2018.
- S. P. Mohanty, U Choppali, and E Kougianos “Everything You Wanted to Know About Smart Cities,” IEEE Consum. Electron. Mag., vol.5, no. 3, pp. 60–70, 2016.
- D. Puthal, N. Malik, and S. P. Mohanty, “Everything You Wanted to Know About Smart Healthcare,” IEEE Consum. Electron. Mag., vol.7, no. 1, pp. 18–28, 2018.
- A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, “Enabling Blockchain Innovations with Pegged Sidechains ,” Public Domain, 2014.
- Y. Ribero, D. Raissar , “DAGCOIN,” Public Domain, 2015.
- Bitmain S9 model Datasheet.