Distributed Ledger Technology (Blockchain) – Comprehensive Review

Fulbright Lecture 2023 – KL Deemed University

Guntur, India, 1-31 July 2023

Homepage

Prof./Dr. Saraju Mohanty

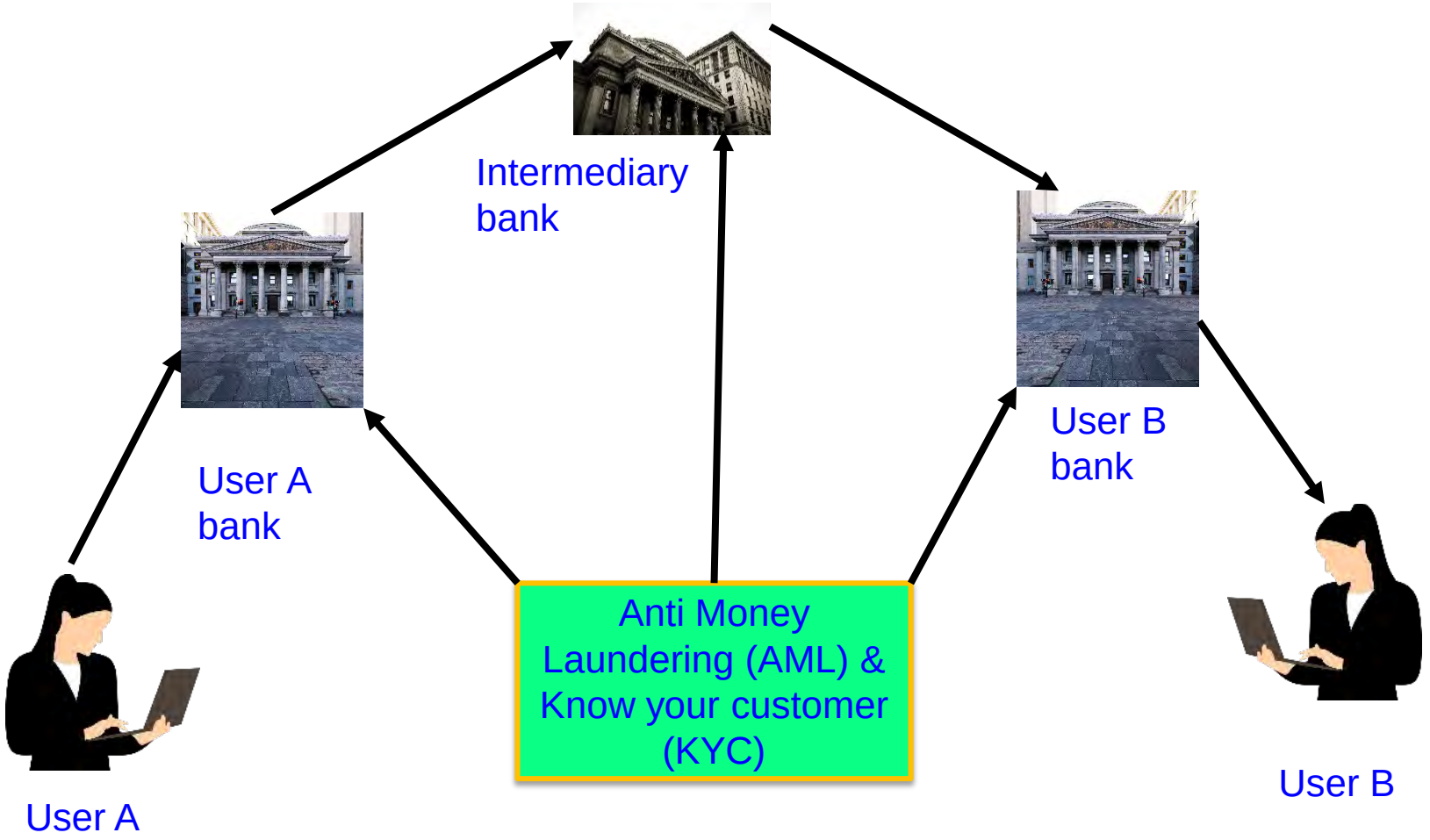
University of North Texas, USA.

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

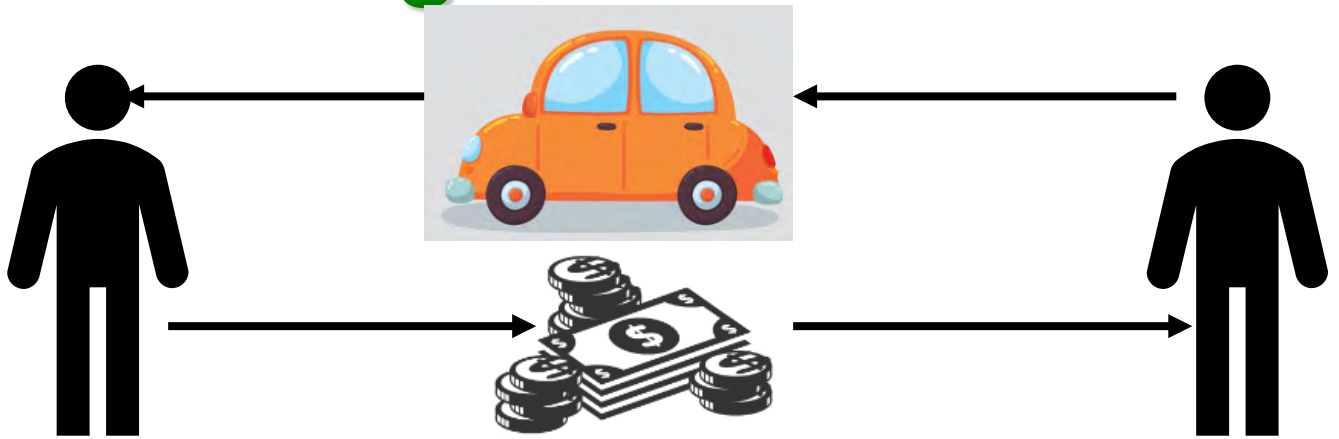
Issues in Banking system

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

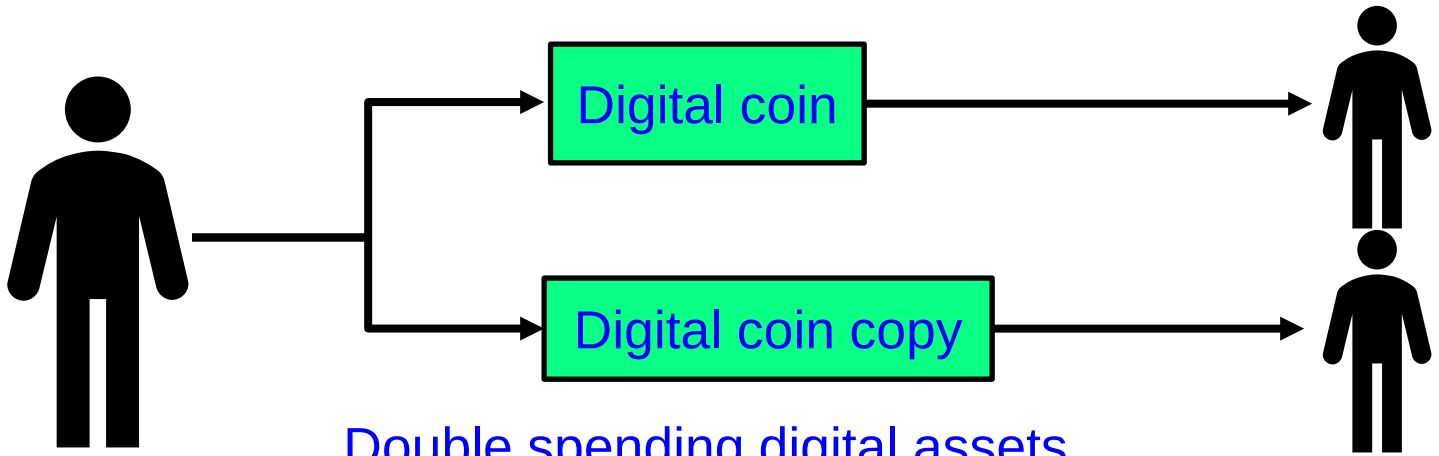
Digital Assets

- 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

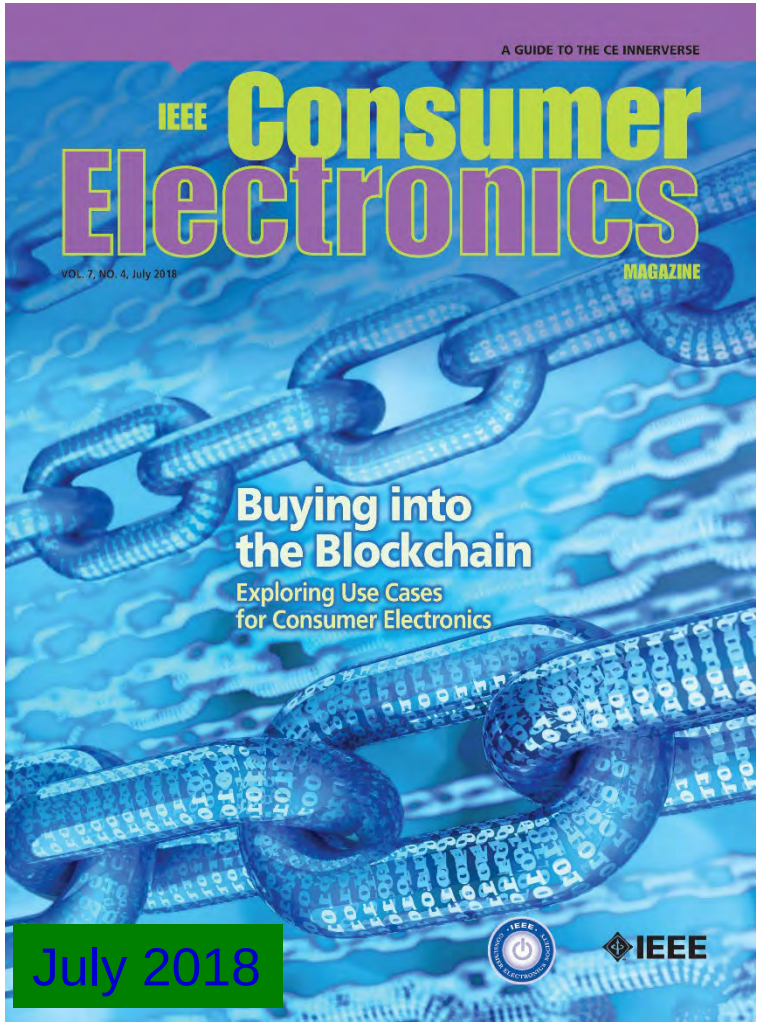


Double spending digital assets

Bitcoin

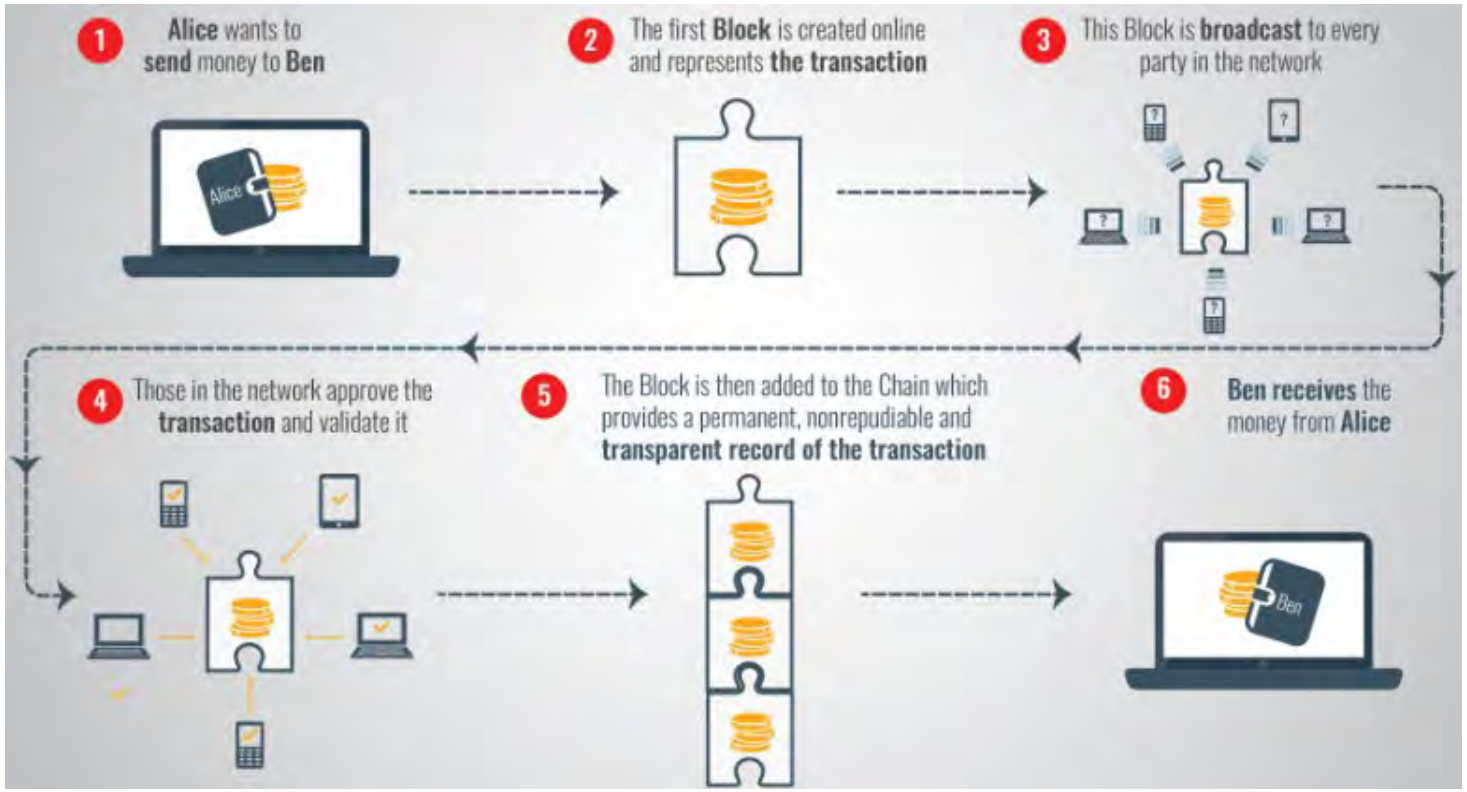
- First successful implementation of Blockchain
- Introduced by Satoshi Nakamoto
- Public distributed ledger
- Underlying architecture is Blockchain
- Problems solved
  - Double spending
  - Anonymity

Blockchain Technology



What is a Blockchain

Blockchain



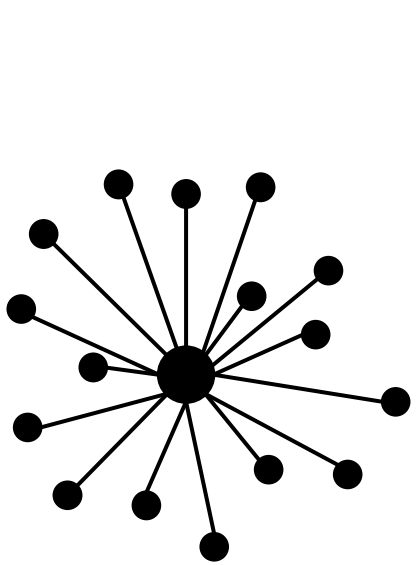
Source: https://www.linkedin.com/pulse/securing-internet-things-iot-blockchain-ahmed-banafa

"A Blockchain is a cloud based database shared by every participant in a given system, in the case of this exemplar, its currency trade. The Blockchain contains the complete transaction of the cryptocurrency or other record keeping in other applications. Think of it as cloud based peer to peer ledger."

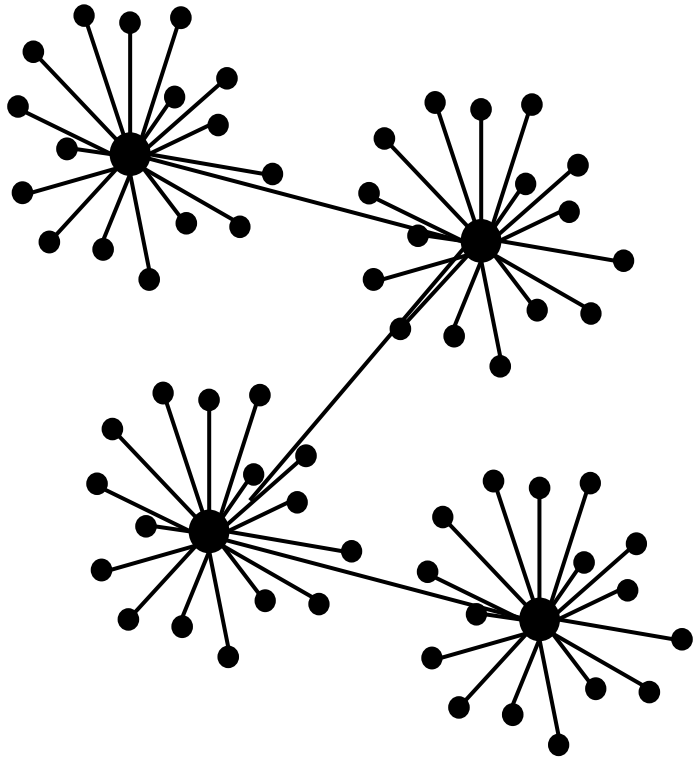
What is Blockchain?

- 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.

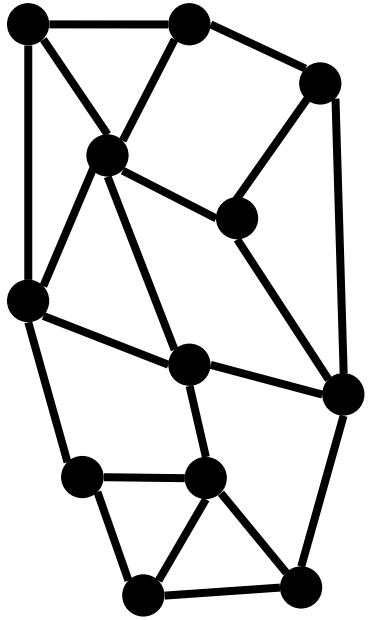
Types of Networks Based on Control



Centralized



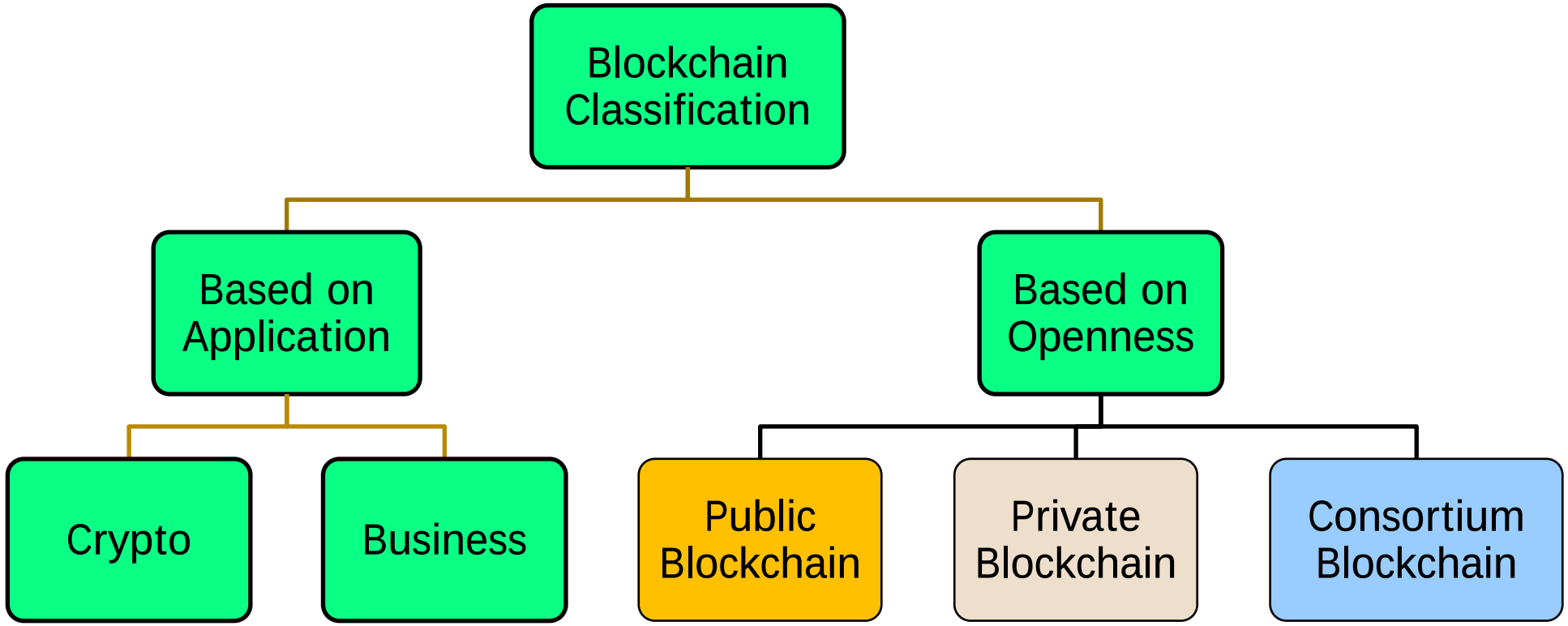
Decentralized



Distributed

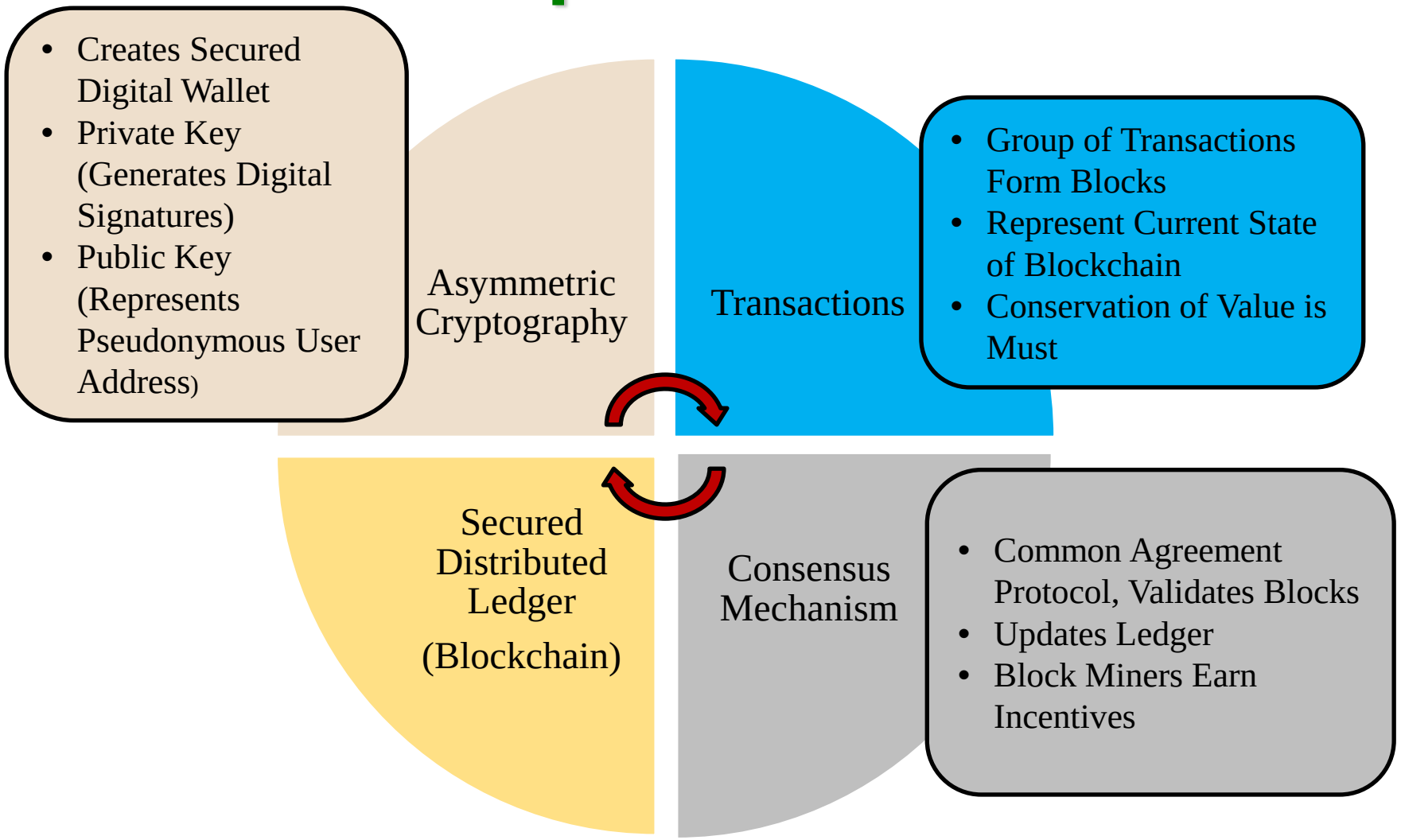
https://blog.maidsafe.net/2015/12/04/evolving-terminology/

Classification of Blockchain



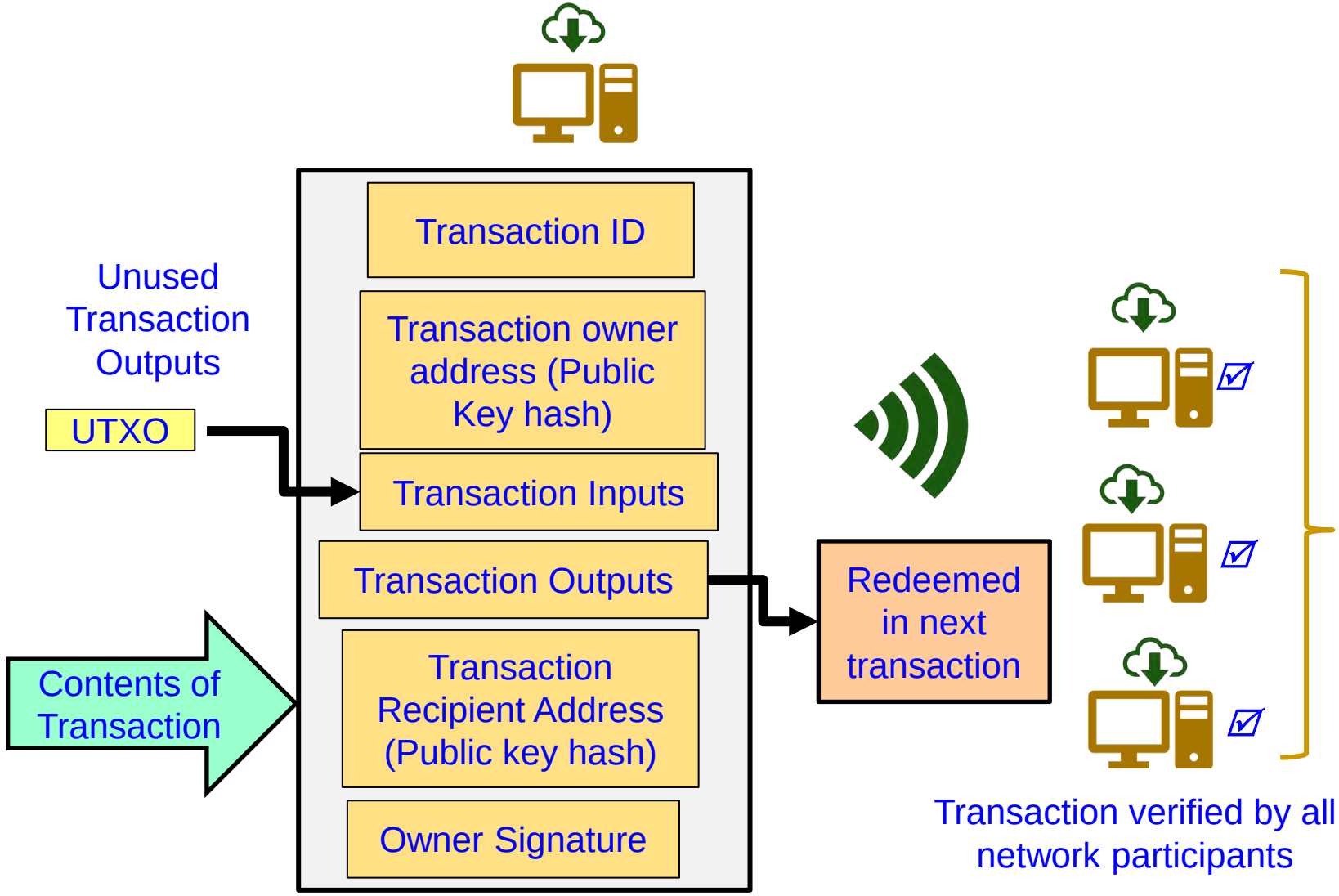
Blockchain – Architecture

Different Aspects of Blockchain

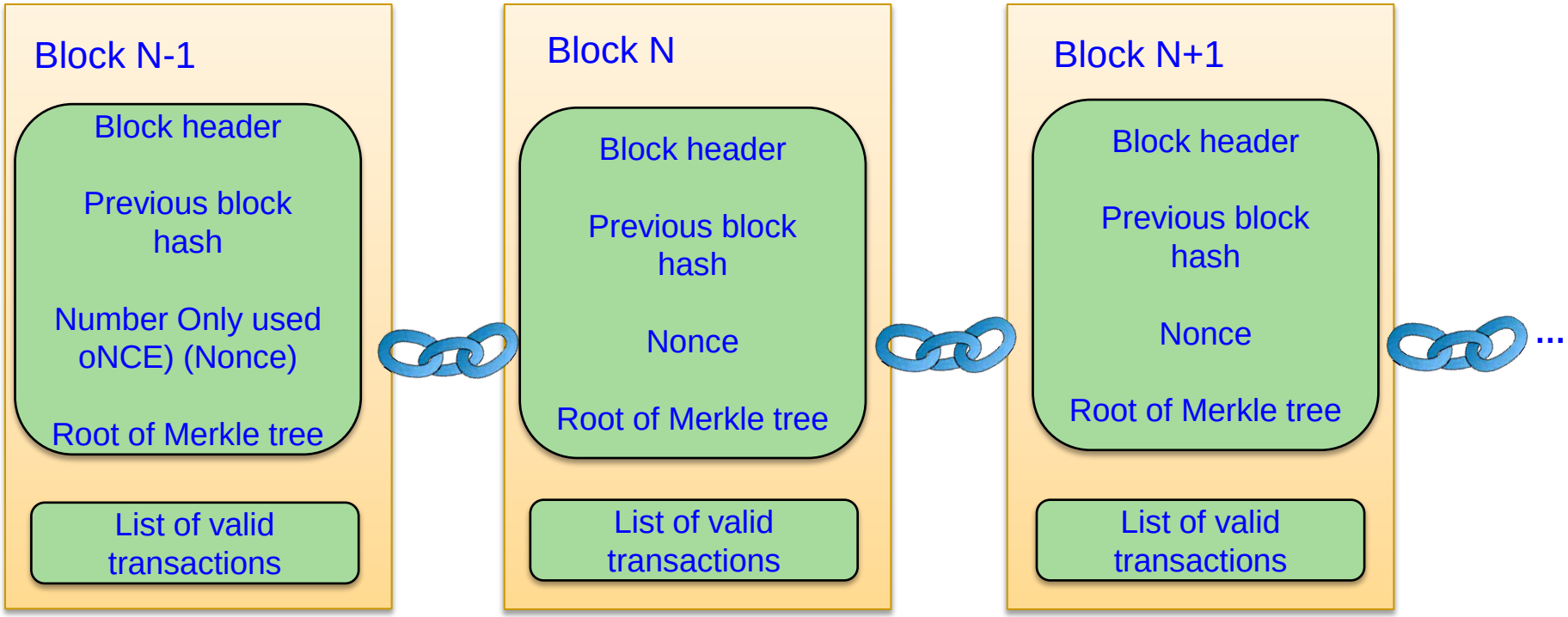


Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you Wanted to Know about the Blockchain", *IEEE Consumer Electronics Magazine*, Volume 7, Issue 4, July 2018, pp. 06--14.

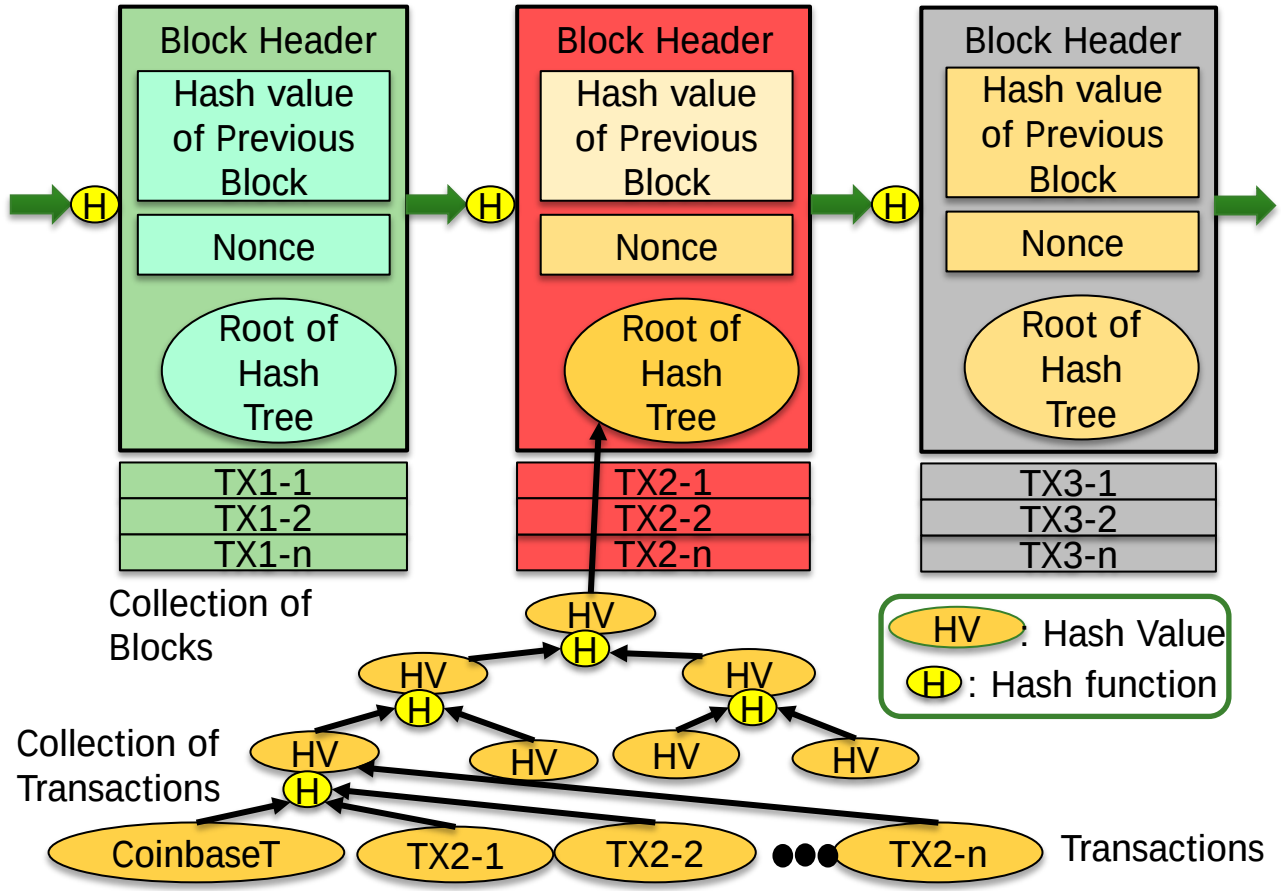
Contents of a Transaction



Blockchain Structure

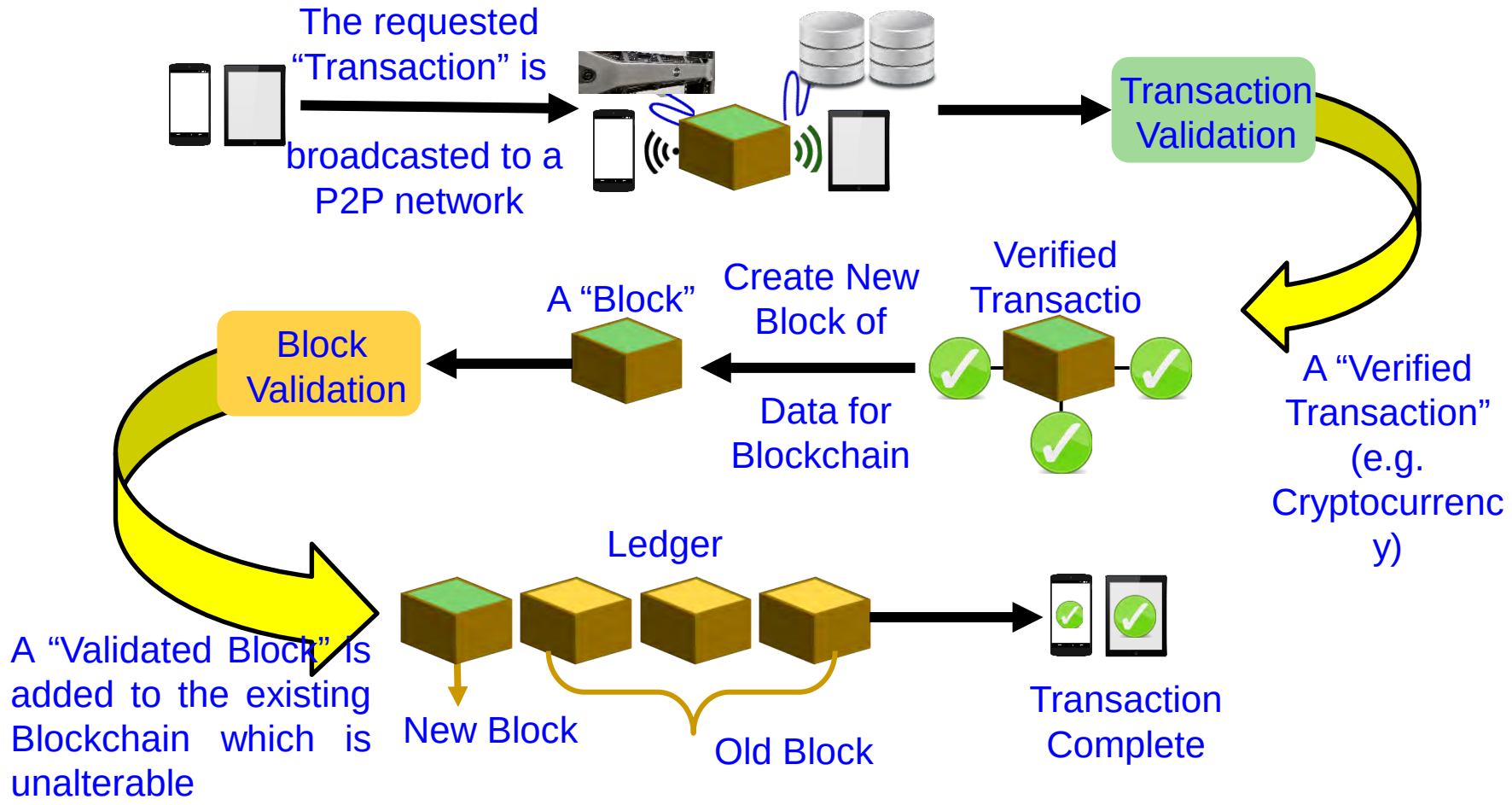


Block Structure



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.

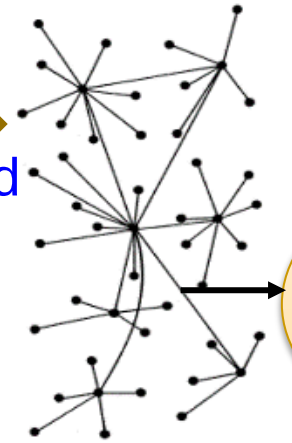
Transaction

- Electronic coin can be defined as a chain of digital signatures
- Transfer happens by signing the hash of the previous transaction and public key of next owner.
- A payee can verify signatures for chain of ownership

Transaction Generation

Transaction is requested by a node

Broadcasted to a P2P network of nodes



Users in same network know address of each other

P-2-P Network

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

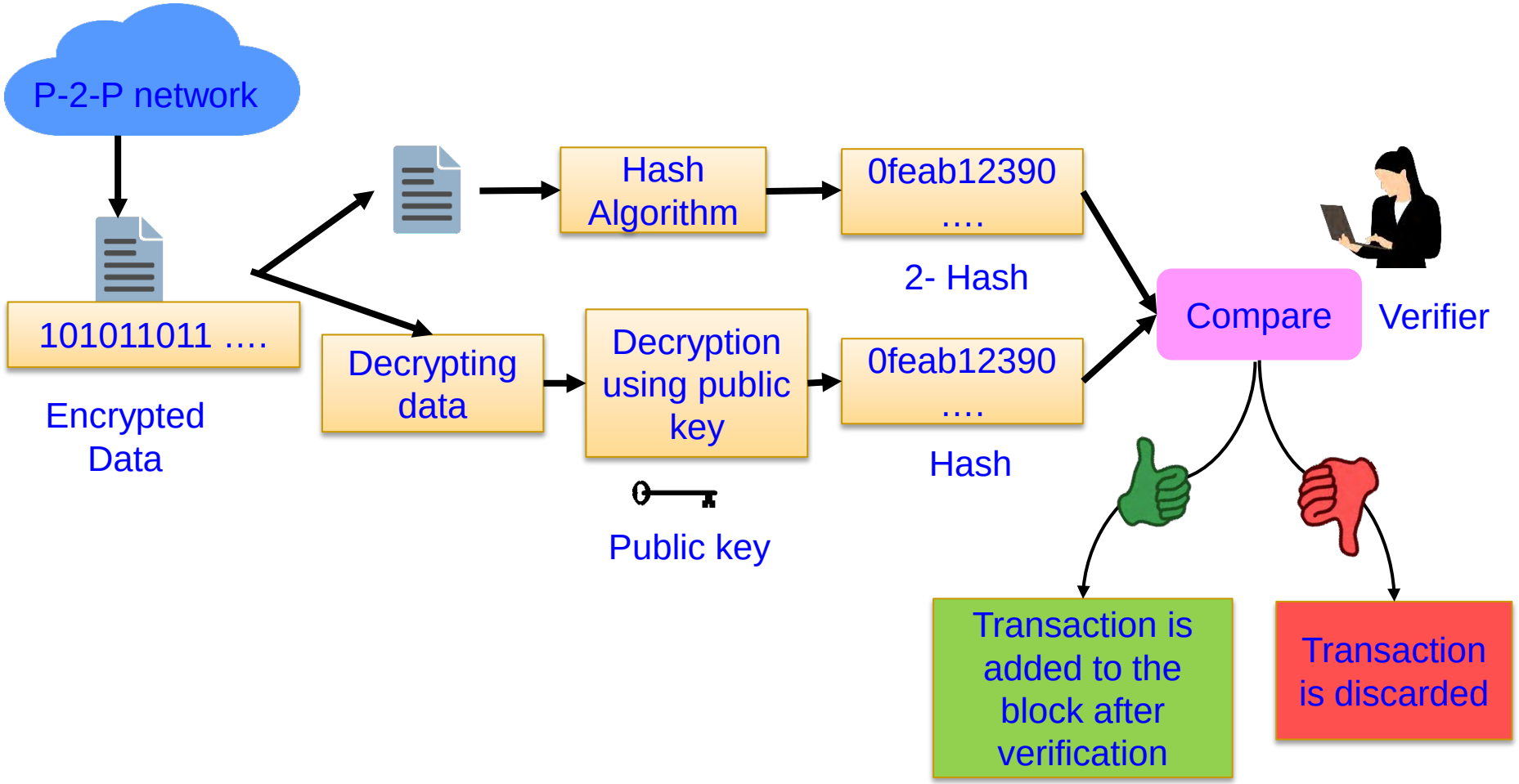
Sender's Private key

Digital Signature

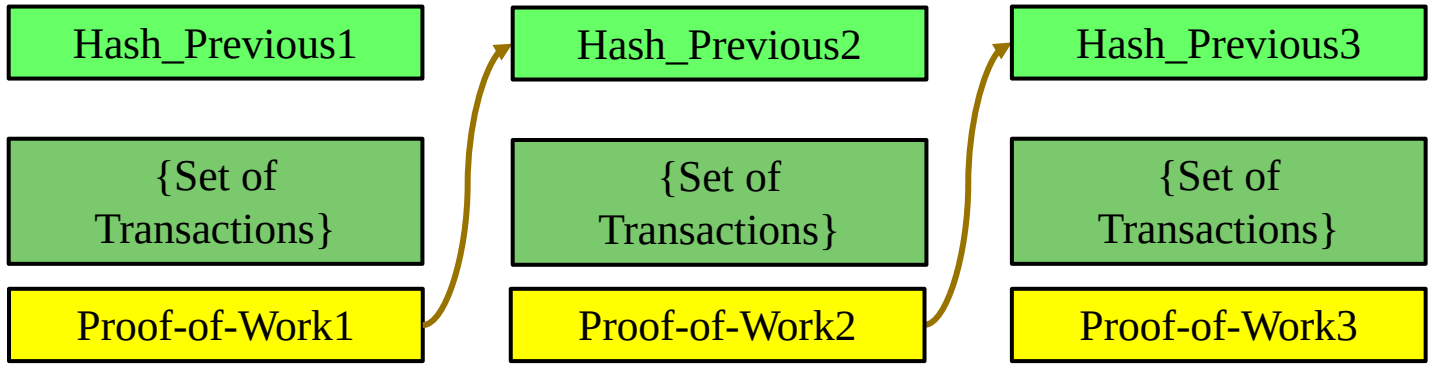
Data computation

- Block header without transactions is about 80KB
- Bitcoin is designed to generate a block for every 10 minutes
- Data generated in one year
  - 360(days) * 24(hours) * 6 (blocks per hour) * 80 bytes (Each header)= 4.2 MB per year

Transaction Validation

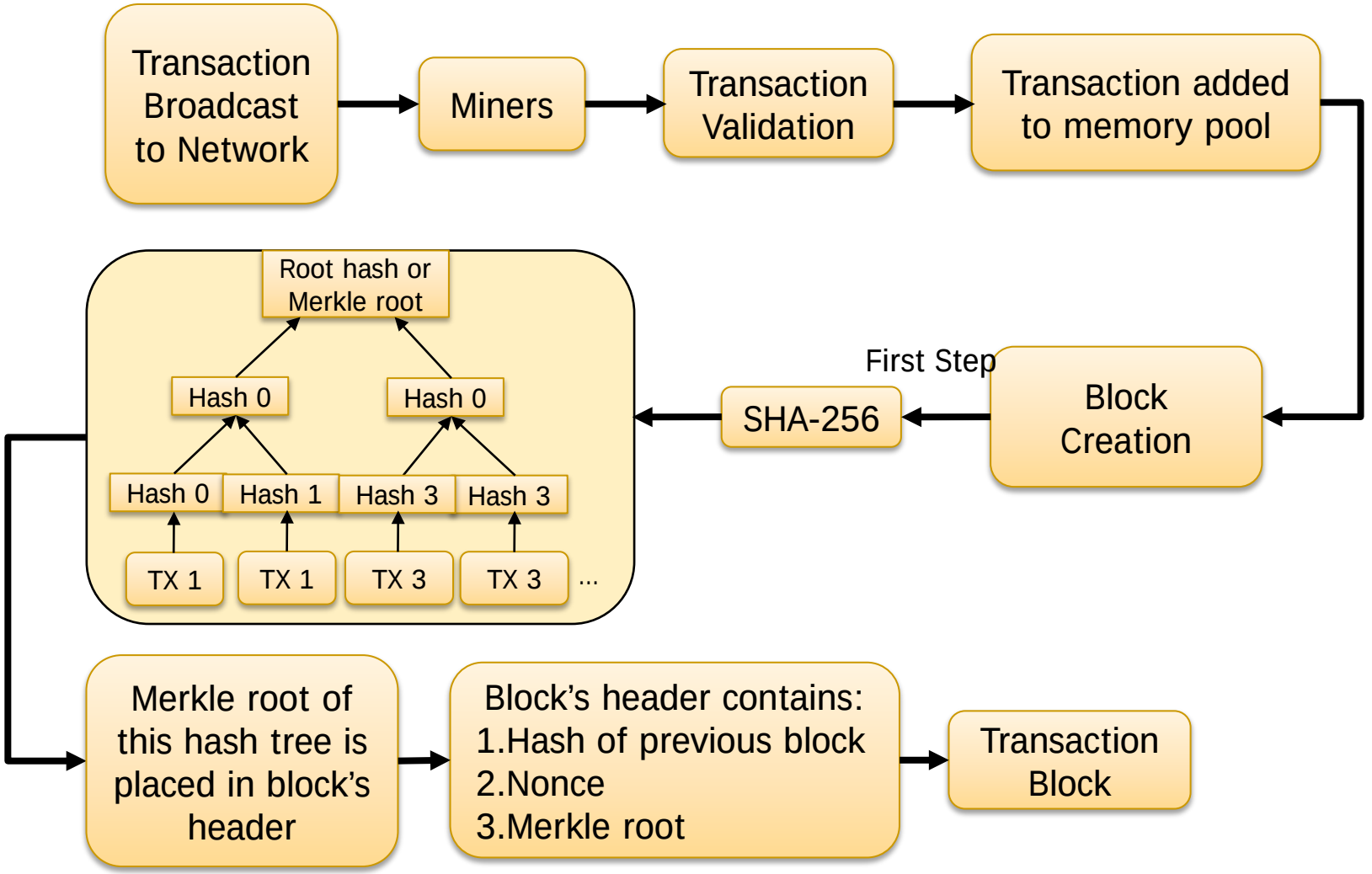


Process of Adding New Value to Blockchain



Hash_Previous2 = Proof-of-Work1
Hash_Previous3 = Proof-of-Work2
Proof-of-Work = H ({Value_Found, Set of Transactions, Hash_Previous})
H() = Cryptographic Hash Function, e.g. SHA-256

Merkle Root Generation



Block Hash Creation

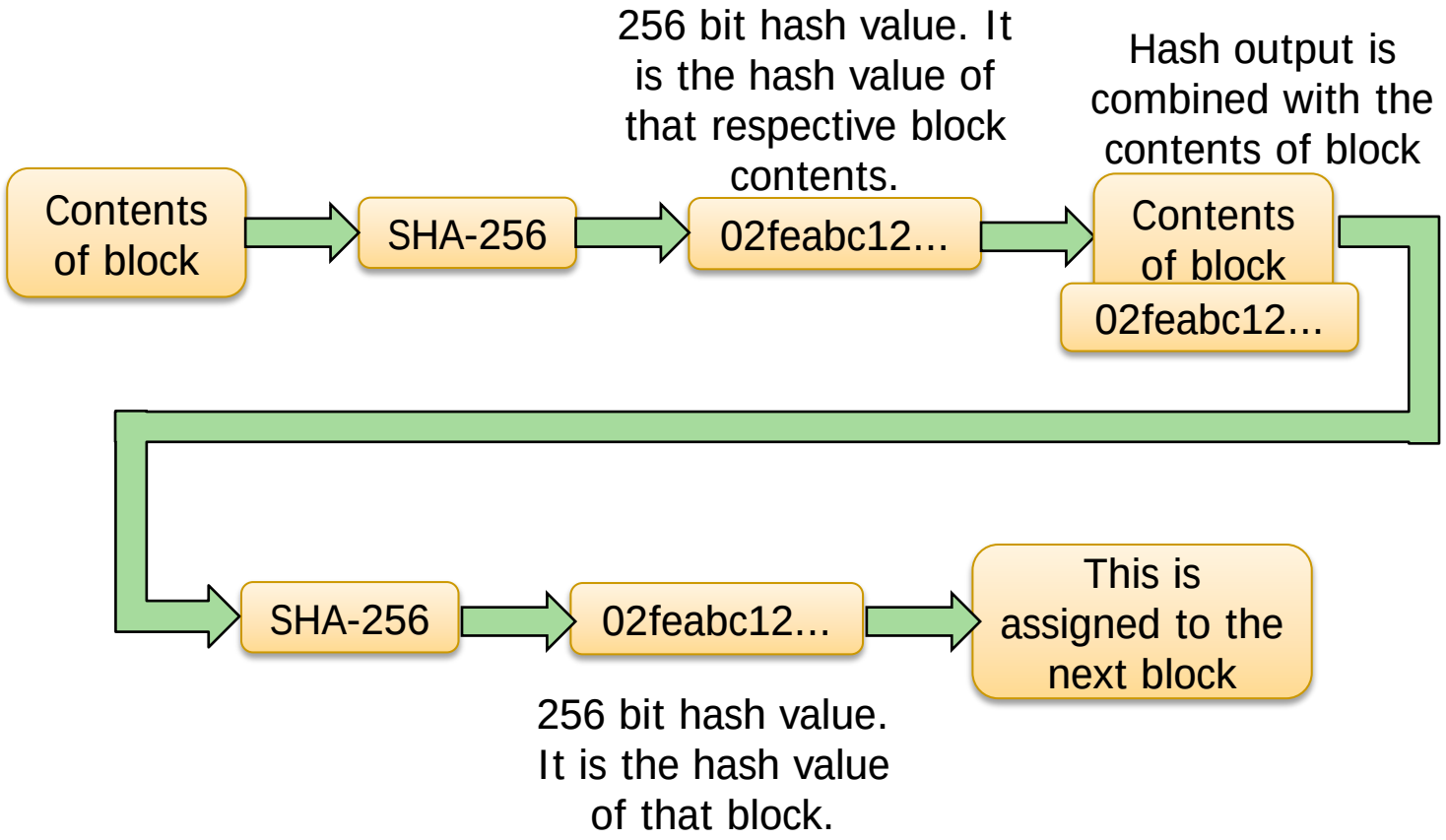
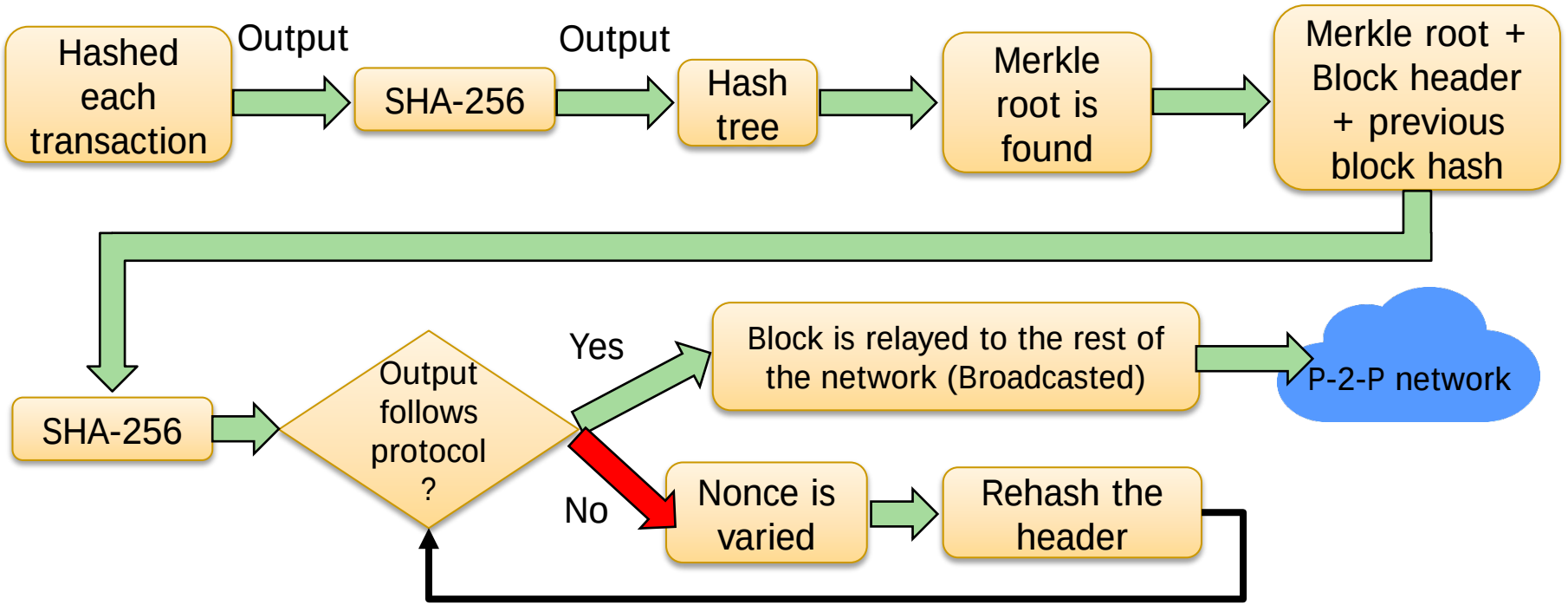


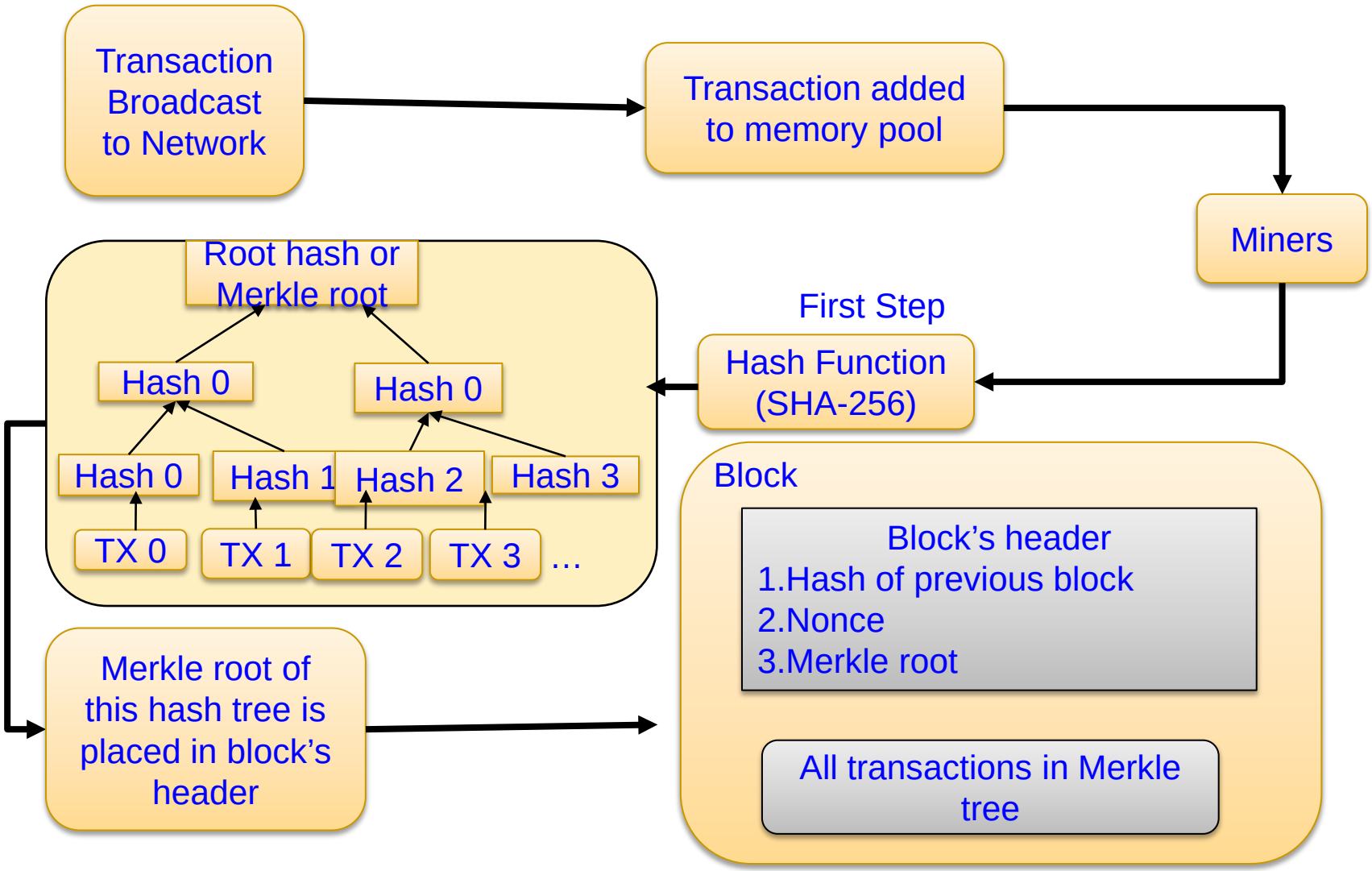
Fig: Blockchain- Nonce, Contents of Block

Nonce Calculation

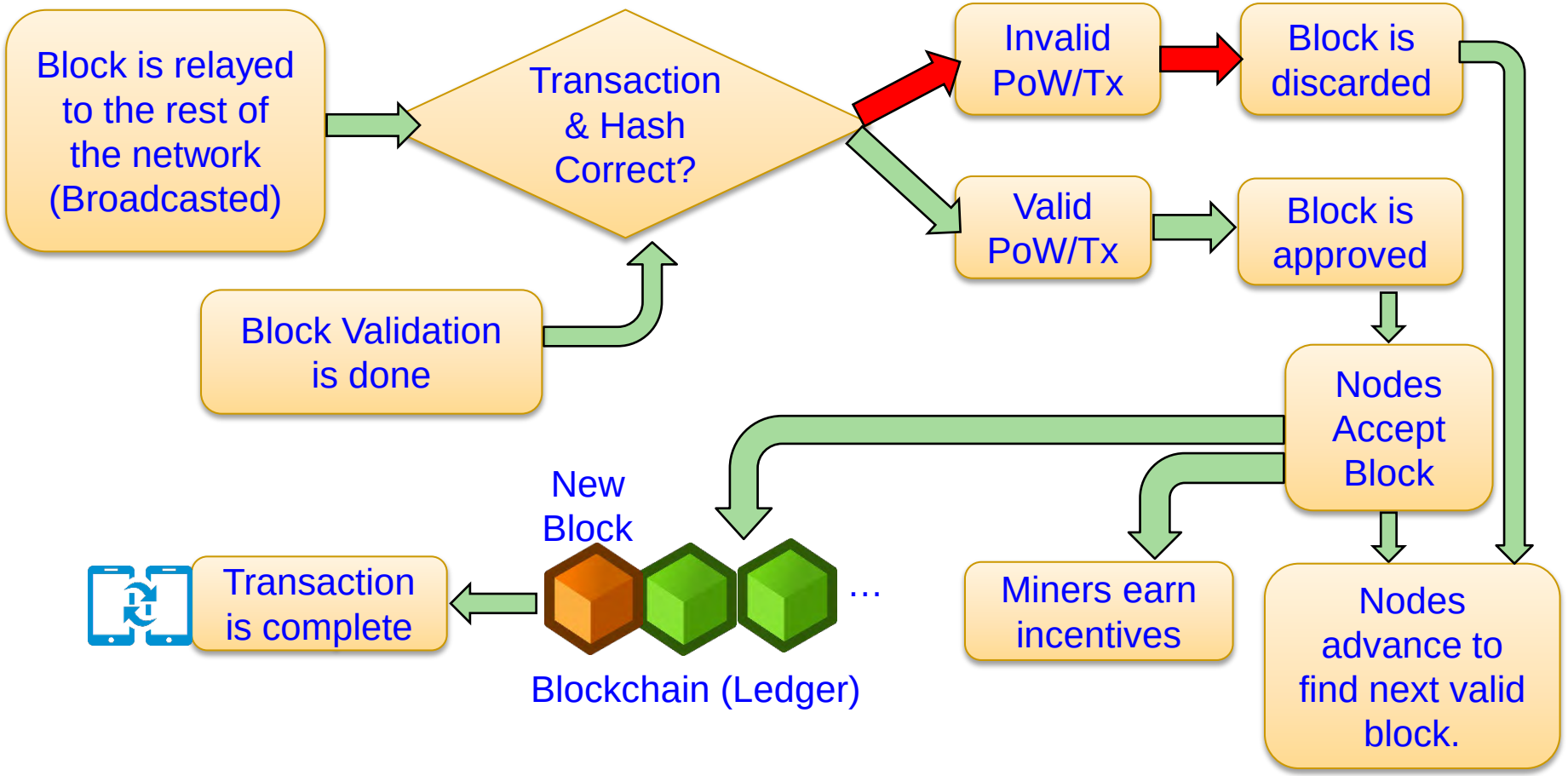
A target value is set for block header's hash, for example, the block header starts with a certain number of zeros, which is called "**Nonce.**"



Block Generation

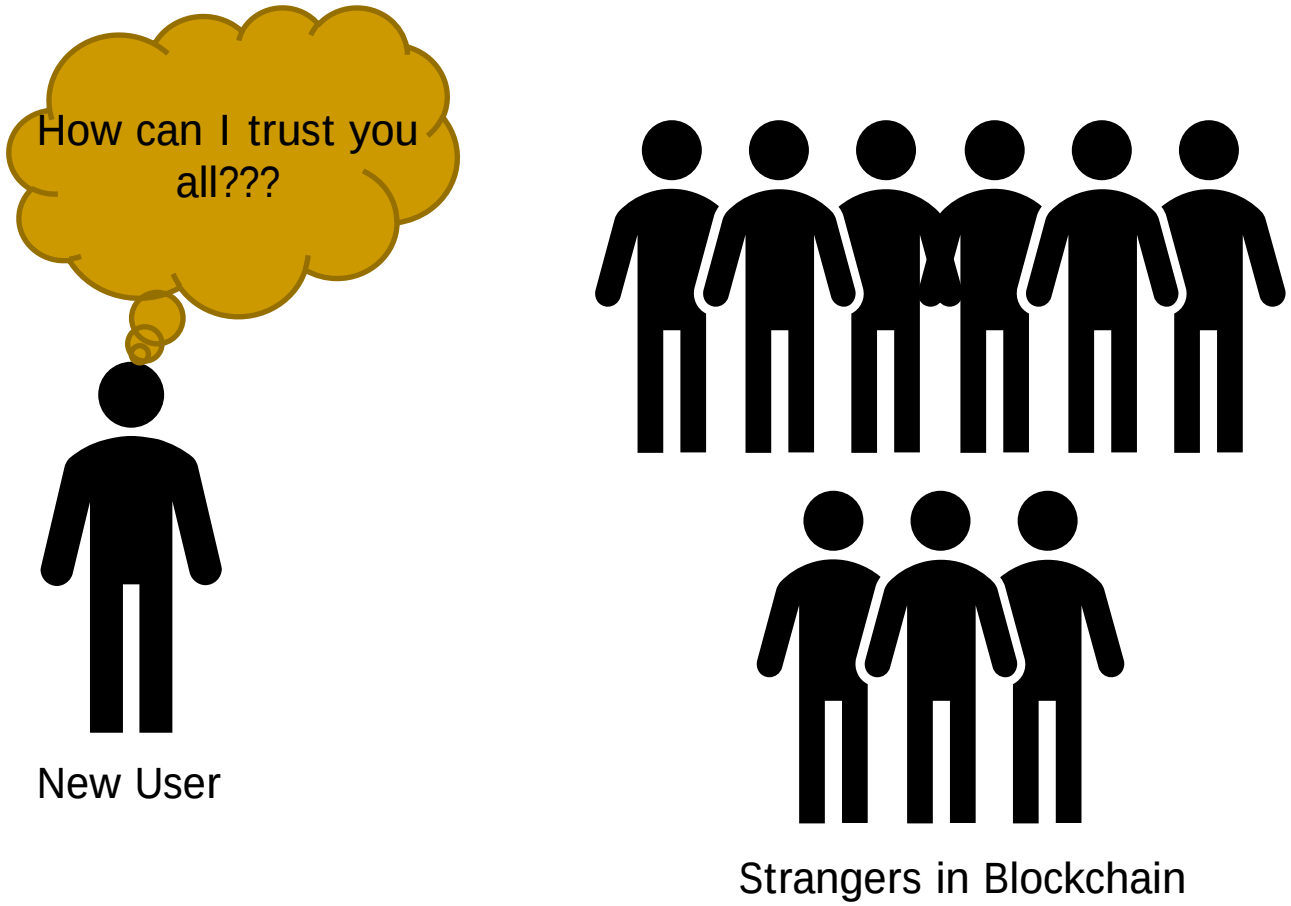


Block Validation

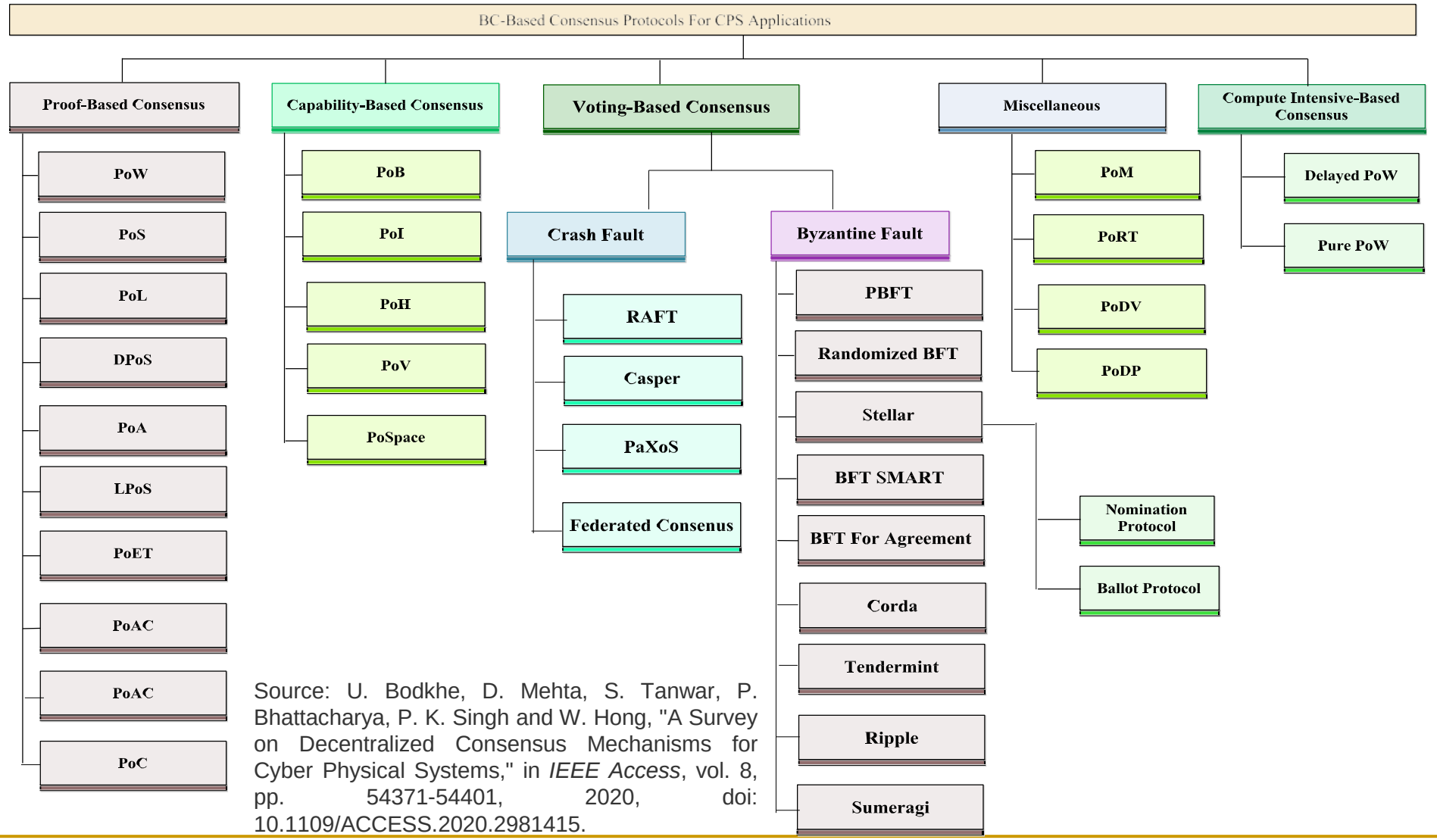


Blockchain Consensus Algorithms

Trust in Blockchain

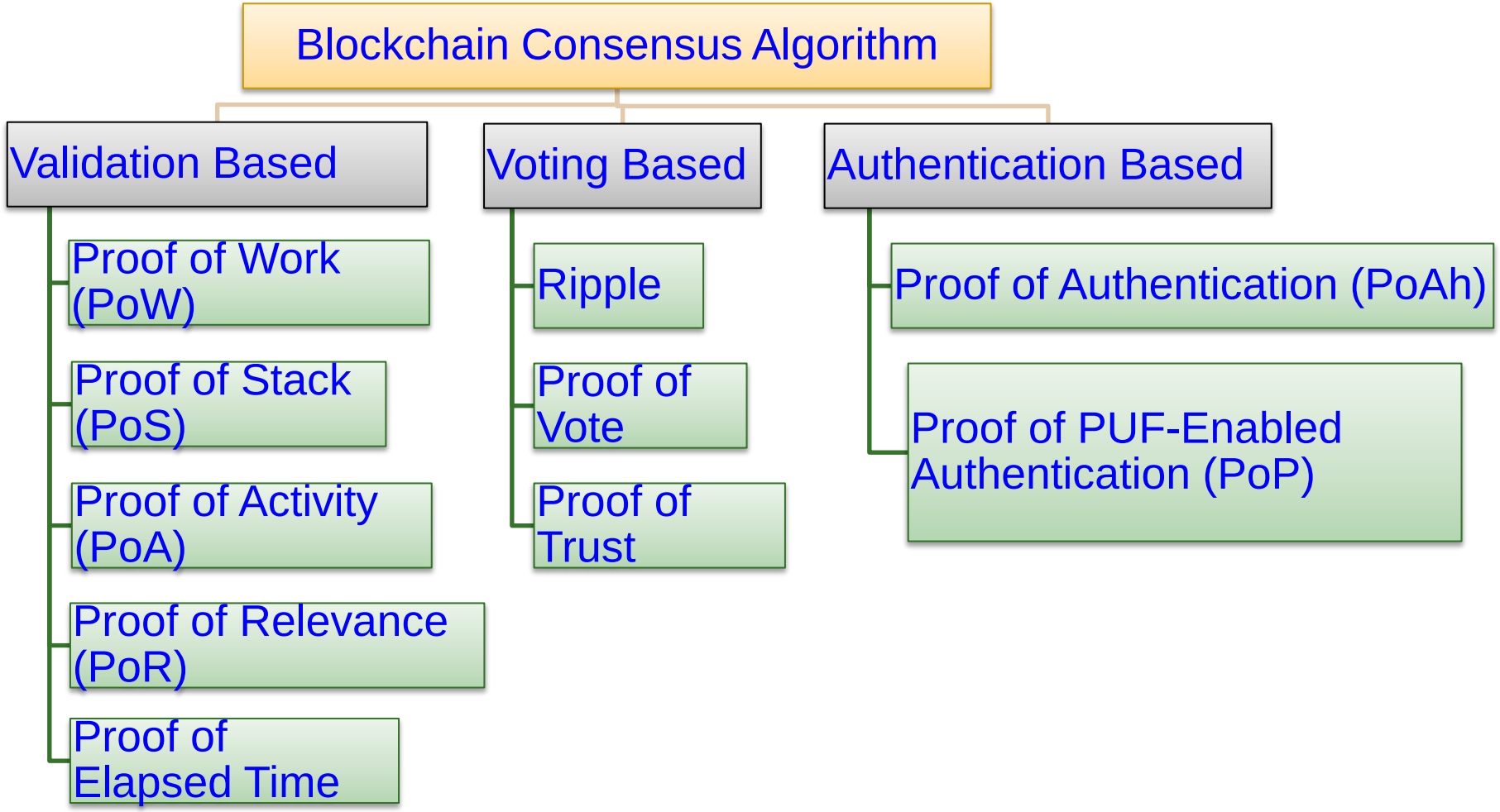


Consensus Algorithm - Taxonomy

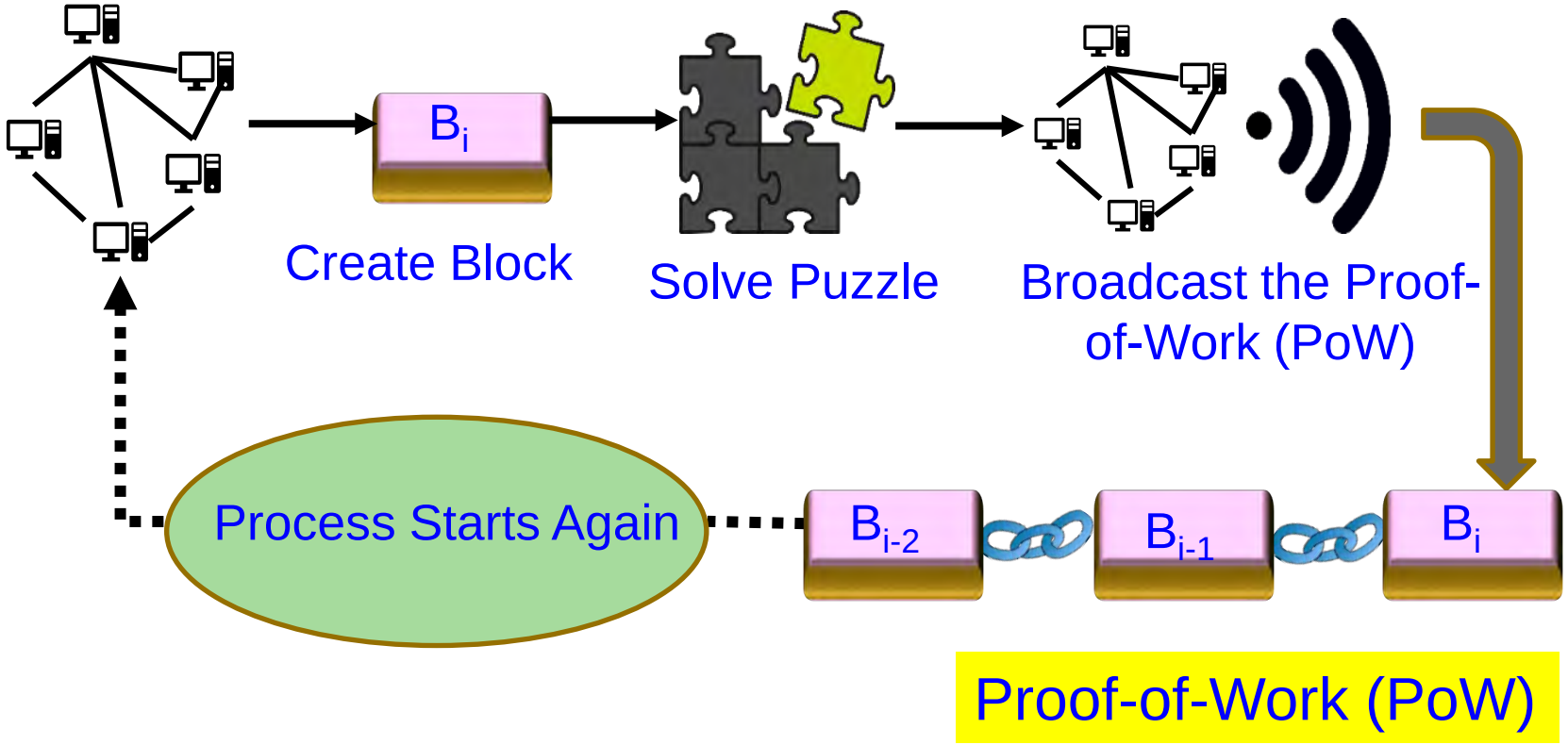


Source: U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh and W. Hong, "A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems," in *IEEE Access*, vol. 8, pp. 54371-54401, 2020, doi: 10.1109/ACCESS.2020.2981415.

Consensus Algorithm Types



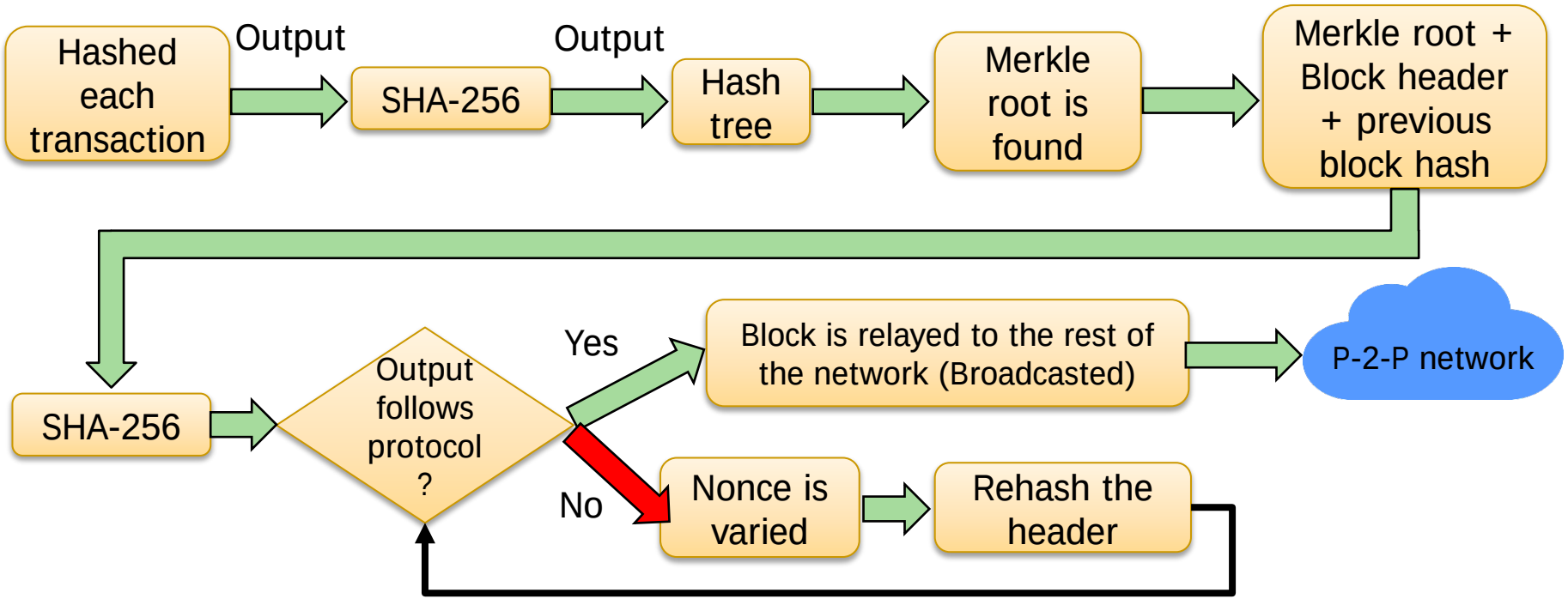
Proof-of-Work (PoW)



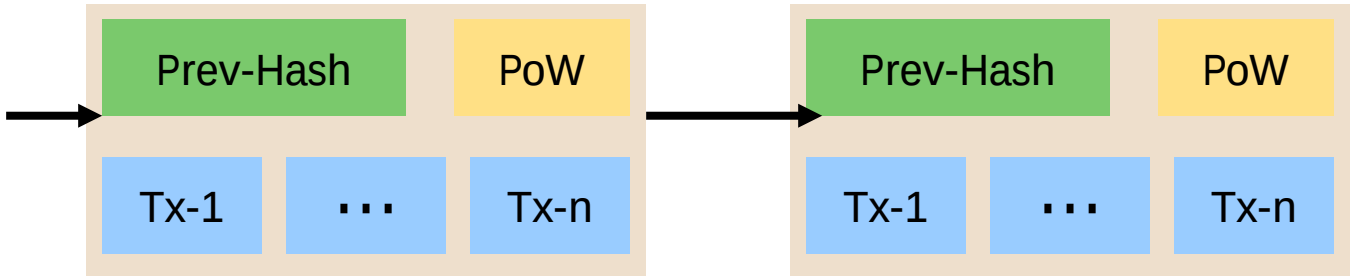
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and DataSecurity in the Internet of Everything(IoE)", arXiv Computer Science, arXiv:1909.06496, Sep 2019, 37-pages.

Nonce Calculation

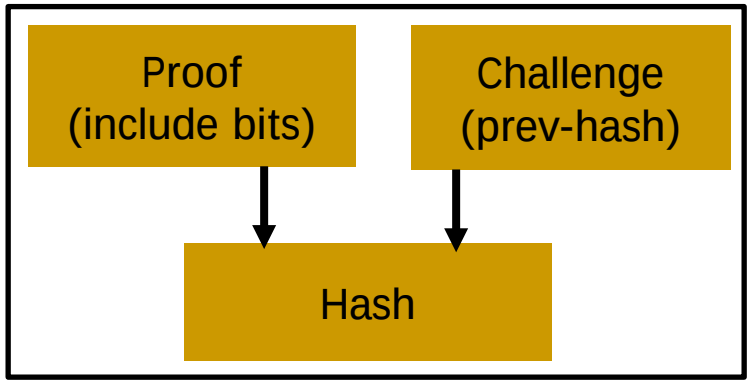
A target value is set for block header's hash, for example, the block header starts with a certain number of zeros, which is called "**Nonce.**"



Proof-of-Work (PoW)



Proof-of-Work (PoW) transactions



PoW

- Public blockchain - Untrusted nodes
- Solving cryptographic puzzle needs computational resource and consumes significant energy

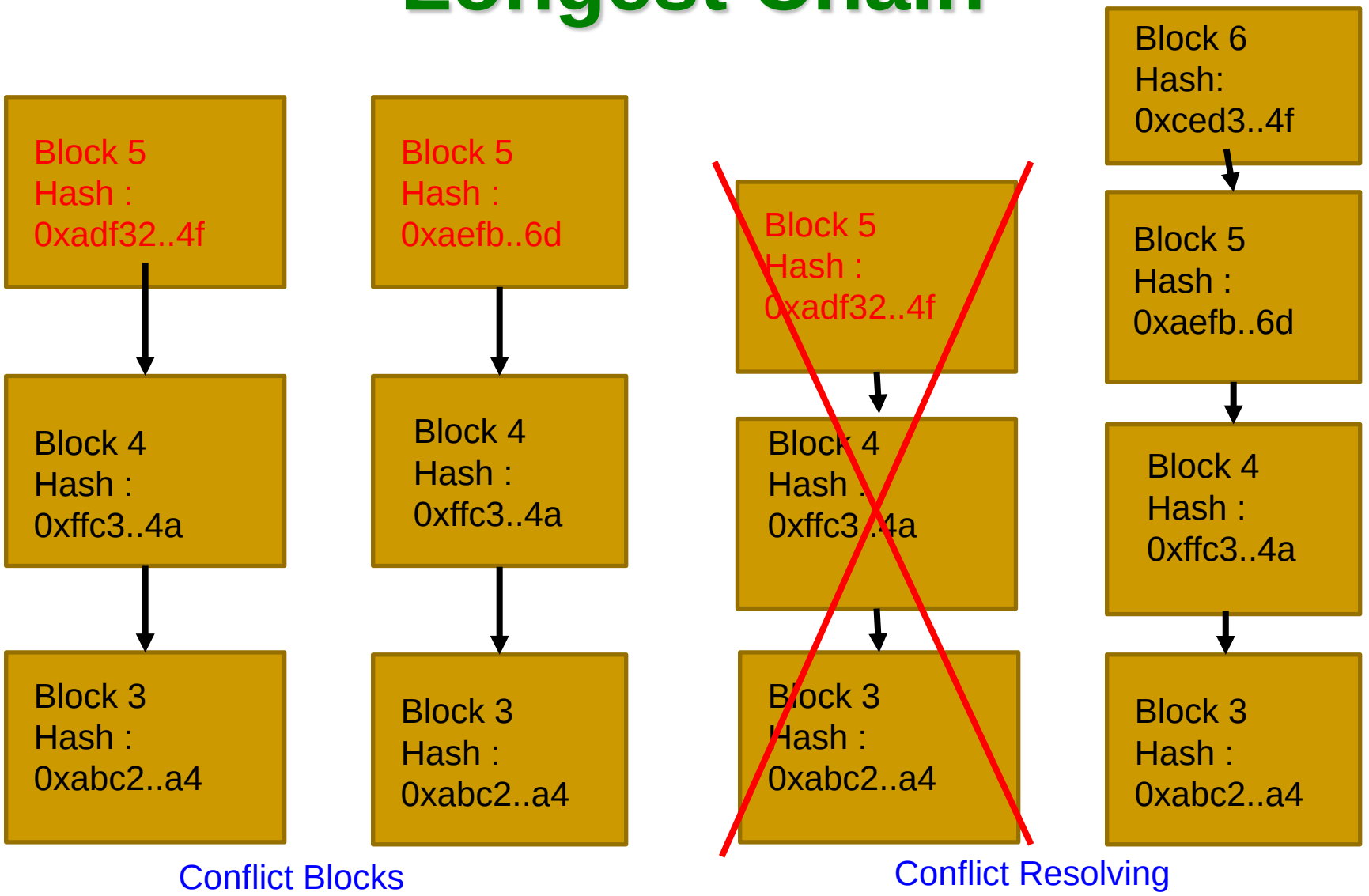
PoW - Problems

- It is slow (1 block / 10 minutes in bitcoin)
- Computational intensive
- Needs specialized hardware as complexity increases
- Not good for environment
- Chance of two miners broadcasting block at same time
  - Can be resolved using conflict mechanism

PoW - Complexity

- Problem with too complex puzzle:
  - Transactions will stuck
  - Work-flow stops
- Problem with too easy puzzle:
  - DoS attack
  - SPAM
- A moving average difficult based on the computational power and number of peers so that the network generates fixed number of blocks pe hour

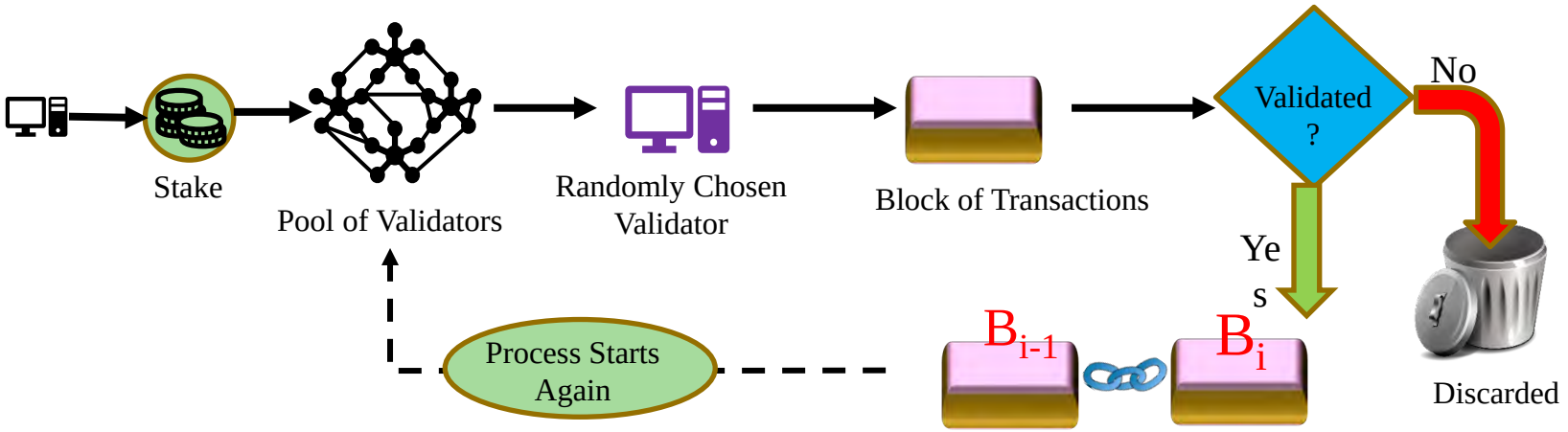
Longest Chain



Conflict Blocks

Conflict Resolving

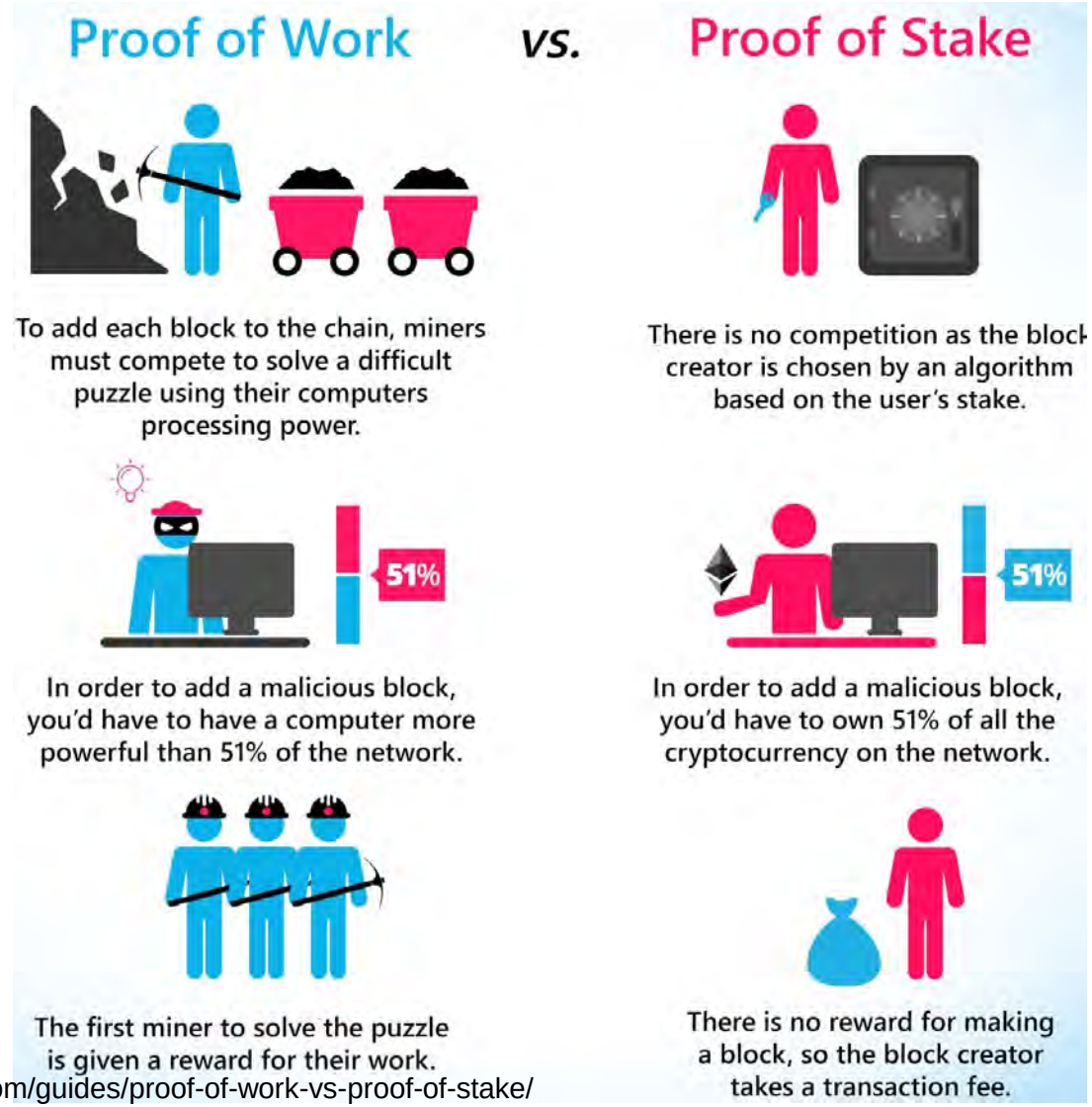
Proof-of-Stake



https://steemit.com/pow/@tunguyen.info/what-is-proof-of-brain-can-change-social-world

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.

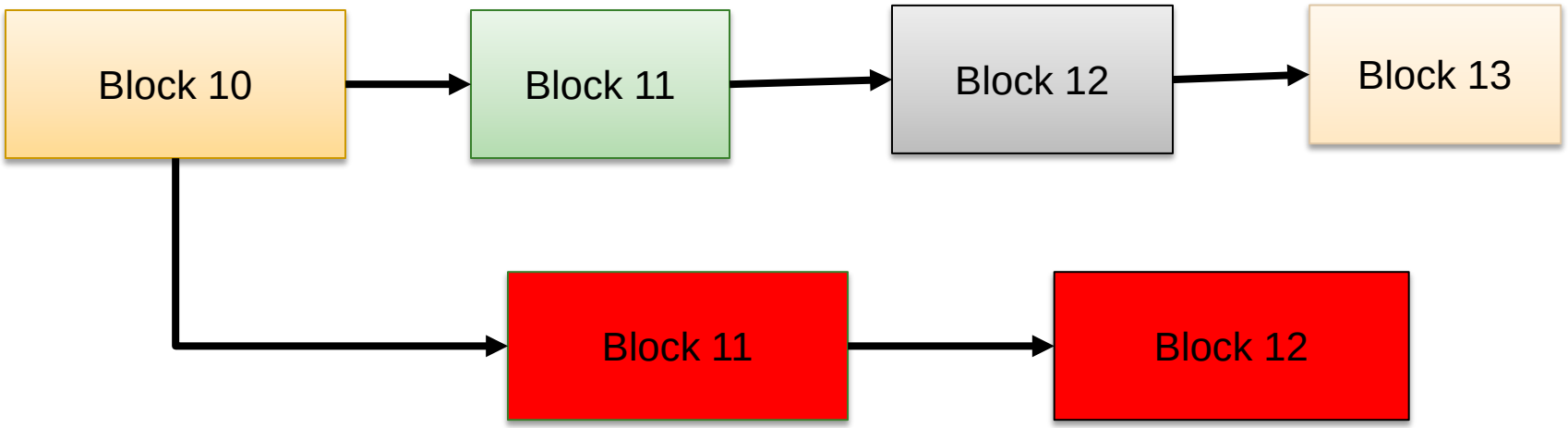
PoW Vs PoS



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

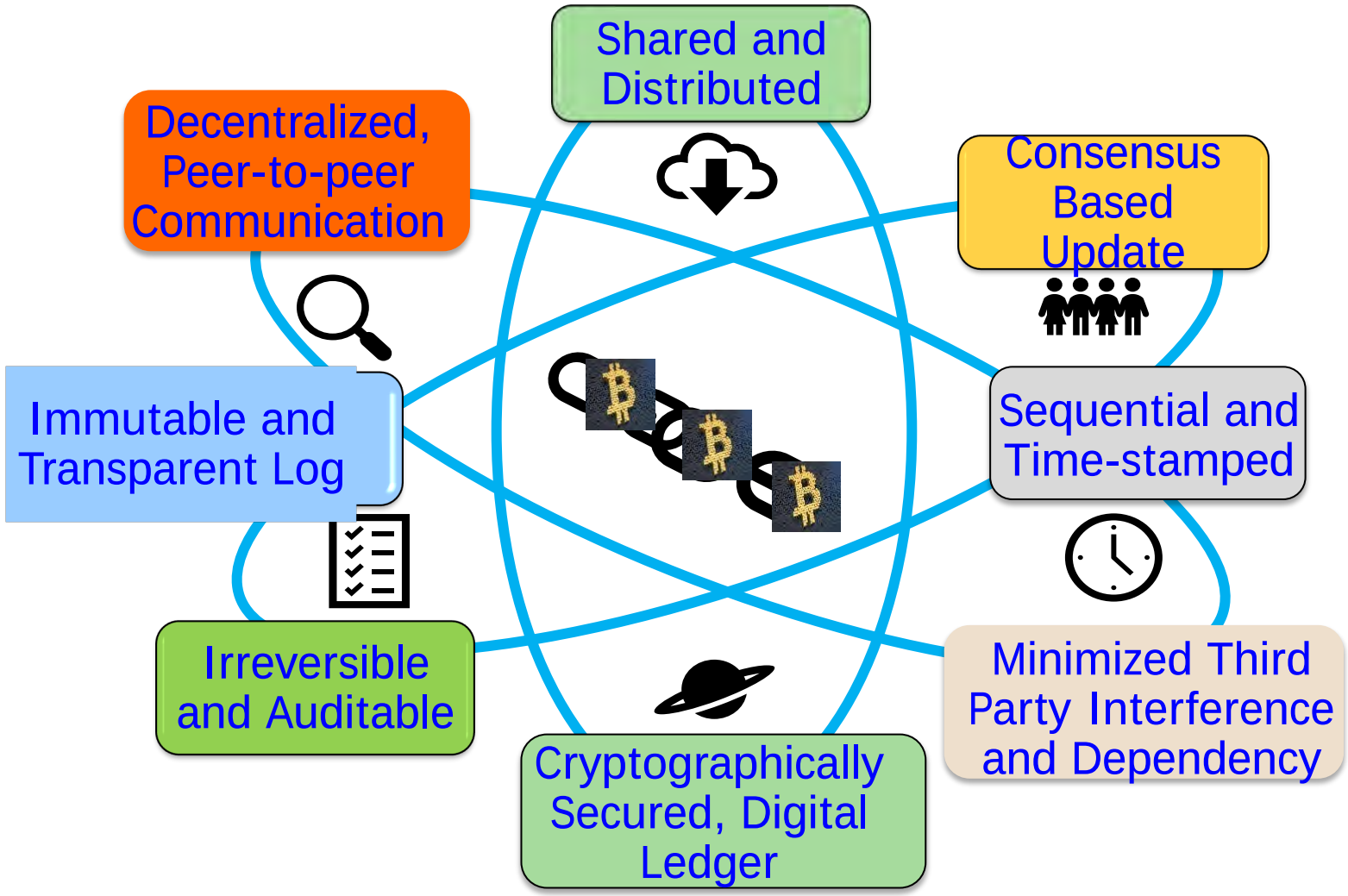
Nothing at stake problem

- PoS doesn't have any procedure as in Proof-of-Work, any malicious attempts to tamper the chain will reduce the value of coin and is profitable to play by rules.



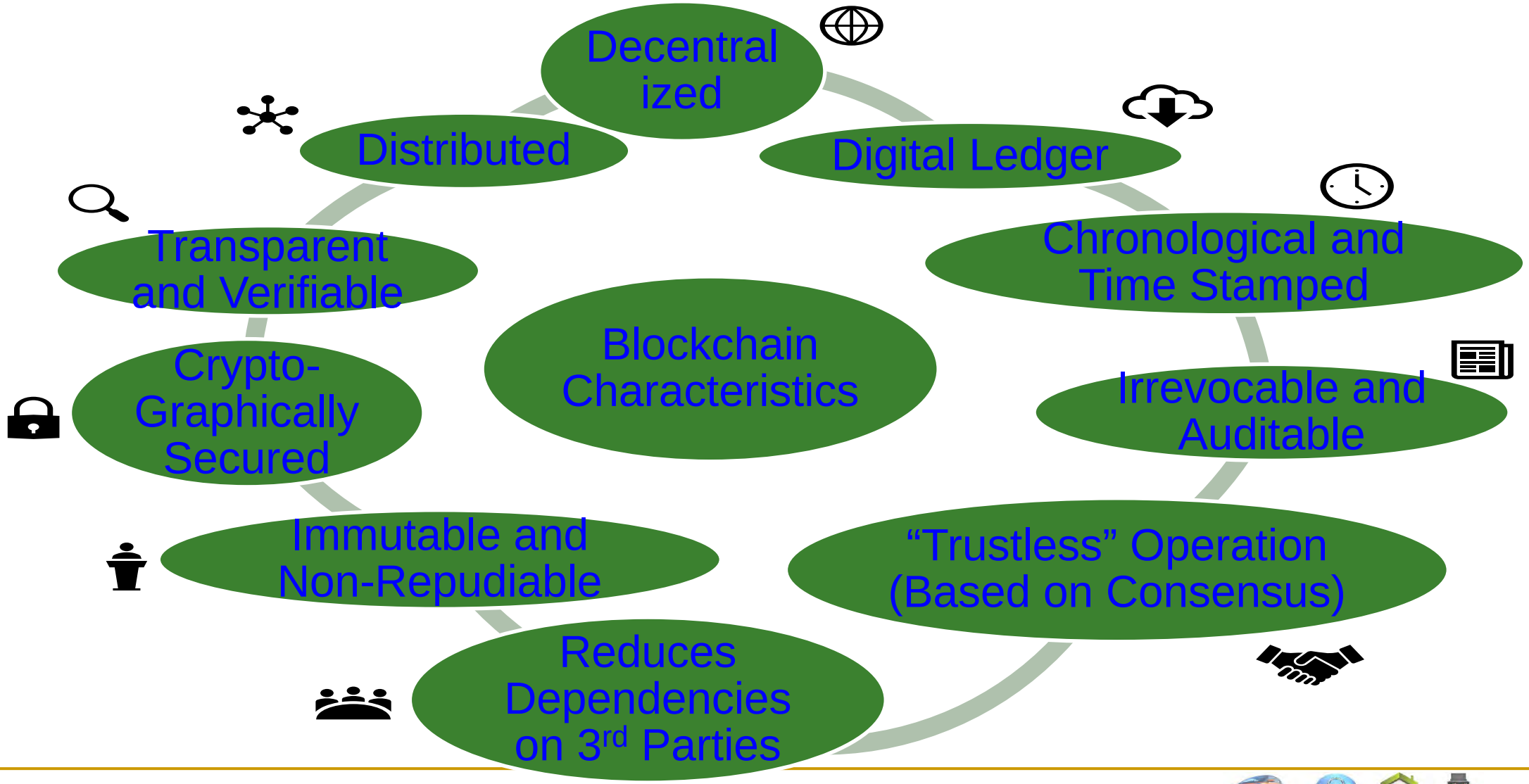
Blockchain Characteristics

Blockchain - Characteristics



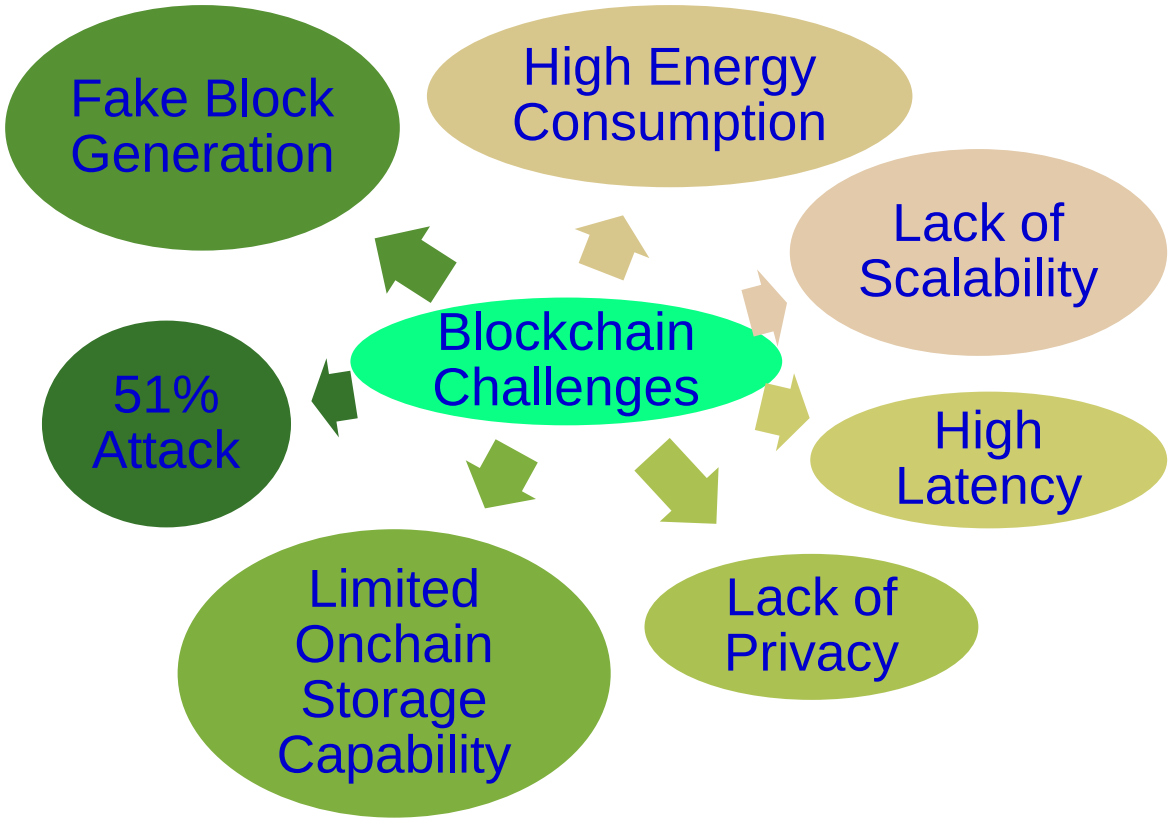
Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The Blockchain as a Decentralized Security Framework", *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 2, March 2018, pp. 18--21.

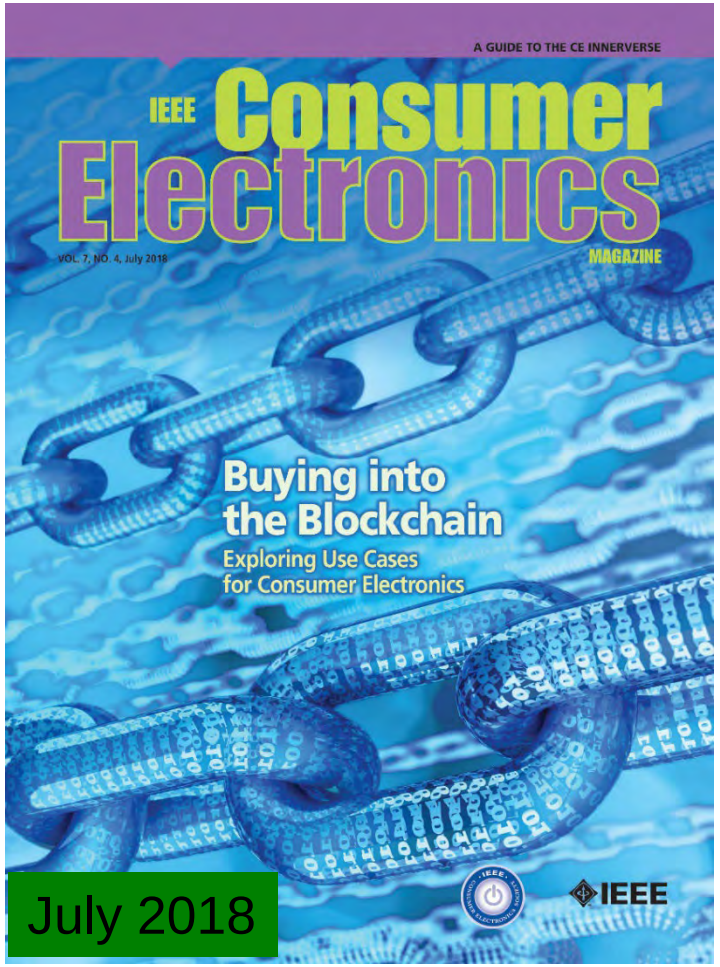
Blockchain - Characteristics



Blockchain Challenges

Blockchain has Many Challenges





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

Blockchain – Energy Issue

- Energy for mining of 1 bitcoin → 2 years consumption of a US household.
- Energy consumption for each bitcoin transaction → 80,000X of energy consumption of a credit card processing.

Blockchain – Energy Issue

We calculated Carbon Intensity of Bitcoin Compared to Other Payment Methods. Soliciting comments via

Carbon Intensity Of Bitcoin Compared to Other Payment Methods

- Per dollar of goods purchased gold is one of the most carbon intensive payment methods
- Per dollar of goods purchased paying with bitcoin can be both cleaner and more polluting than paying with cash or credit card

Payment Method	grams CO_2 per $ transaction
Gold	349.2
Bitcoin: Coal Electric Grid	37.5
Bitcoin: US Average Electric Grid	15.3
Bitcoin: California Electric Grid	8.0
Cash Payment	0.20
Credit card	0.13
Off-Grid Renewable Electricity	0.0
Bitcoin: Generator using flared gas well	0.0
Bitcoin: Generator using digester gas	-55.8
Bitcoin: Generator using unflared gas	-116.0

Source: LinkedIn posting of Steffen Mueller

Blockchain – Energy Issue

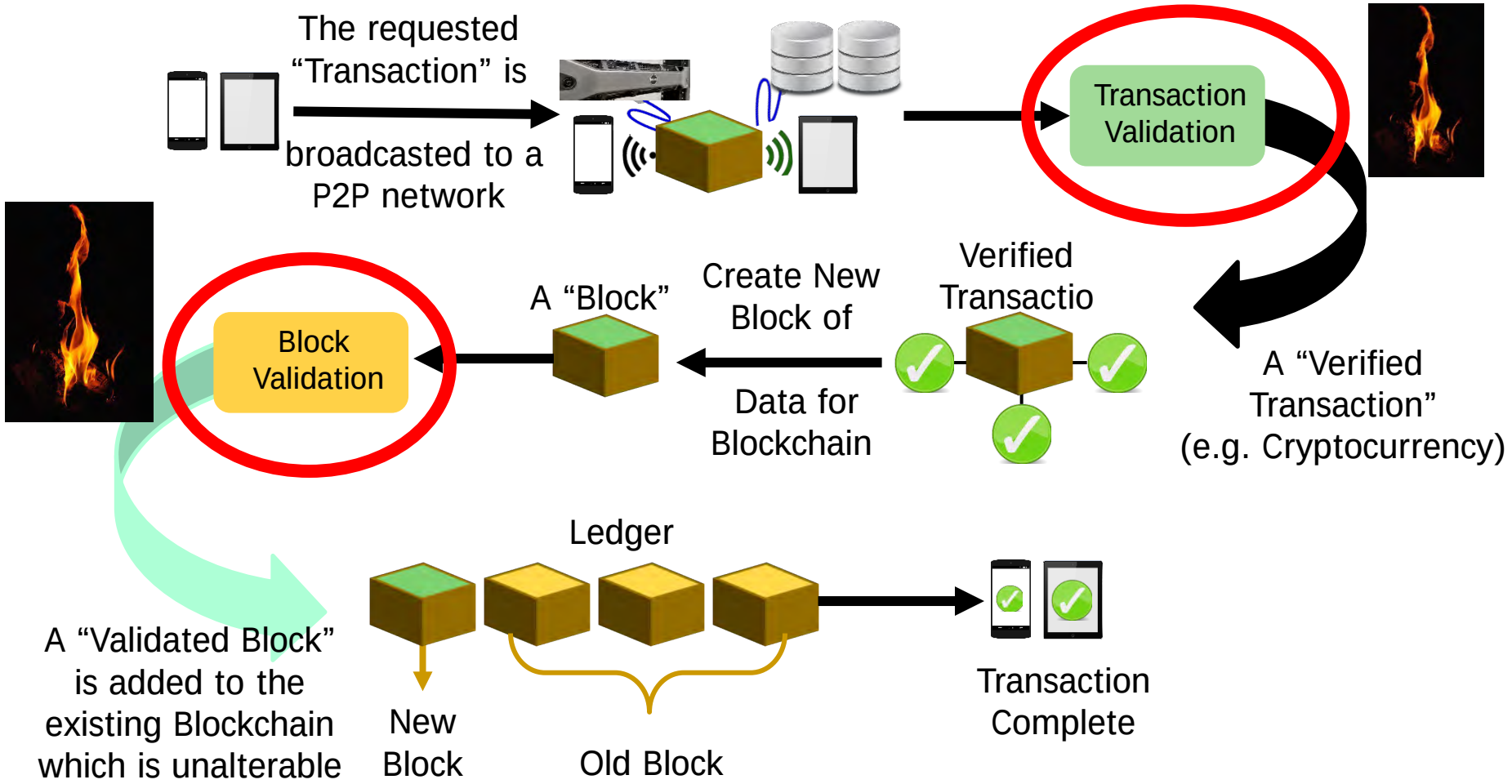
Paying with Crypto Currencies can Significantly Change a Product's Carbon Footprint

- Paying with crypto currencies can have a large carbon impact on a product and generate large carbon emissions additions or large offsets.
- For example, during the complete manufacturing process for a car about 10 tonnes of CO_2 are emitted. Paying for a car with crypto currencies produced from average US grid electricity adds 7.7% of carbon emissions to the car's manufacturing process while crypto currencies produced from unflared gas could offset up to 58% of all emissions to manufacture a car. Negative emissions crypto currencies produced with digester gas could offset 28% of all emissions to manufacture a car.
- Paying for gasoline to fuel the car could either add 0.4% of emissions or offset 3.2% of gasoline related carbon emissions which is significant.
- We have assessed this for other products as well. Paying for beef could either add 0.6% to the emissions to produce beef or subtract 4.7% from beef's carbon footprint.

	Beef	Car Manufacture	Gasoline (Refining and Use/Combustion)
Product Quantity	91 grams	1 vehicle	1 gallon
Product Emissions (gCO_2)	2,449	10,000,000	11,400
Payment Emissions (gCO_2): US Grid Electricity	15.3	765,000	47.43
Payment Emissions (gCO_2): Digester Gas	-55.8	-2,790,000	-172.98
Payment Emissions (gCO_2): Unflared Gas	-116.0	-5,800,000	-359.6
Share of Payment Emissions: US Grid Electricity	0.6%	7.7%	0.4%
Share of Payment Emissins: Digester Gas	-2.28%	-27.90%	-1.52%
Share of Payment Emissins: Unflared Gas	-4.7%	-58.0%	-3.2%

Source: LinkedIn posting of Steffen Mueller

Blockchain Challenges - Energy



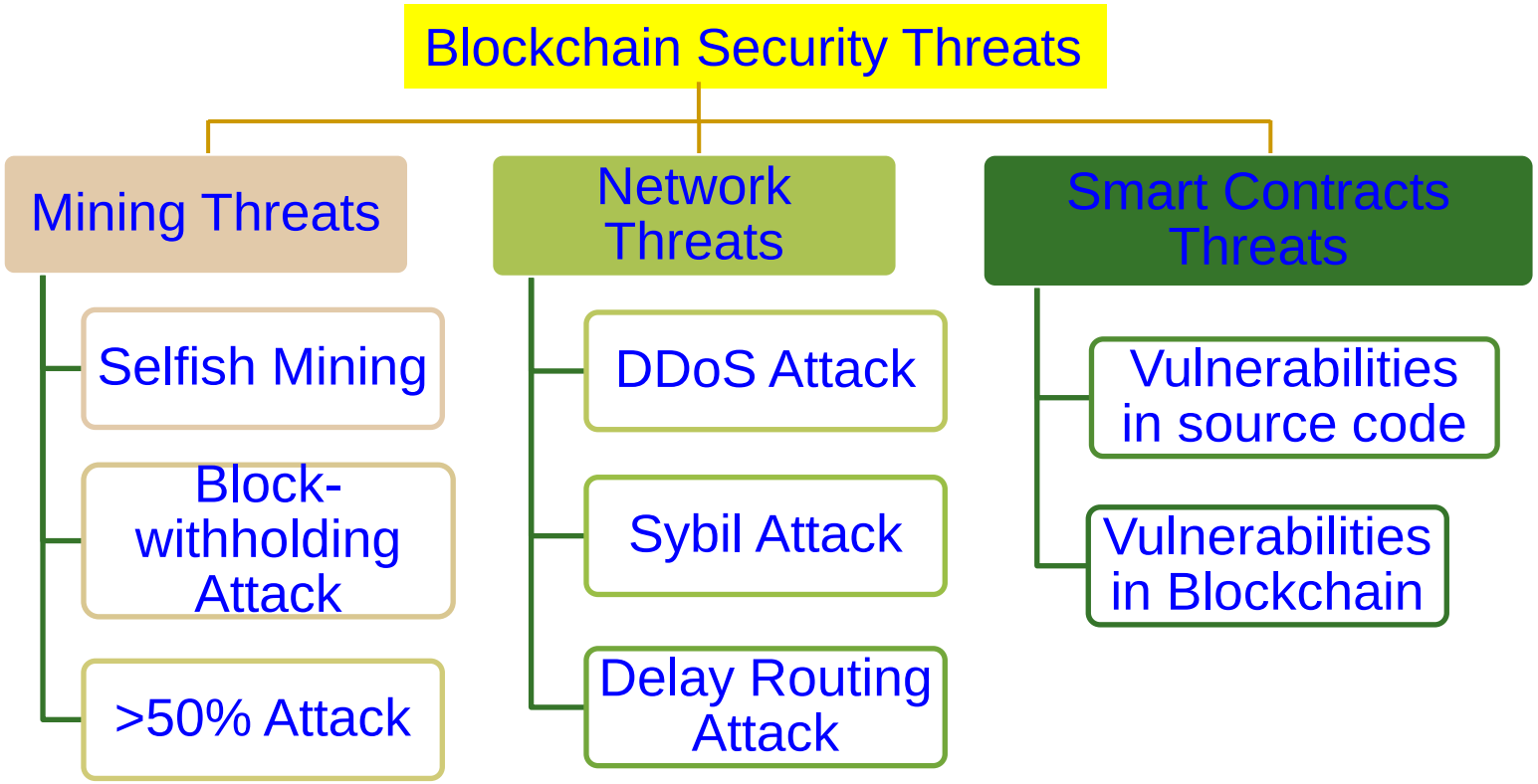
Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you Wanted to Know about the Blockchain", *IEEE Consumer Electronics Magazine*, Volume 7, Issue 4, July 2018, pp. 06--14.

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

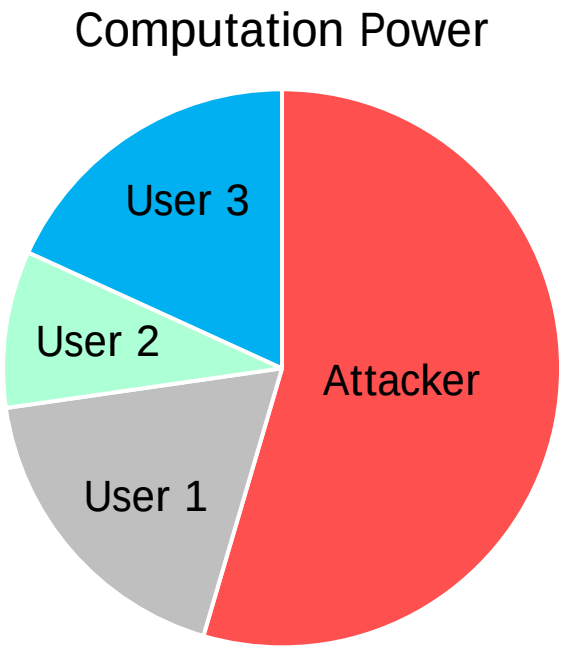
Source: J. Lee, "Rise of Anonymous Cryptocurrencies: Brief Introduction", IEEE Consumer Electronics Magazine, vol. 8, no. 5, pp. 20-25, 1 Sept. 2019.

Smart Contracts - Vulnerabilities

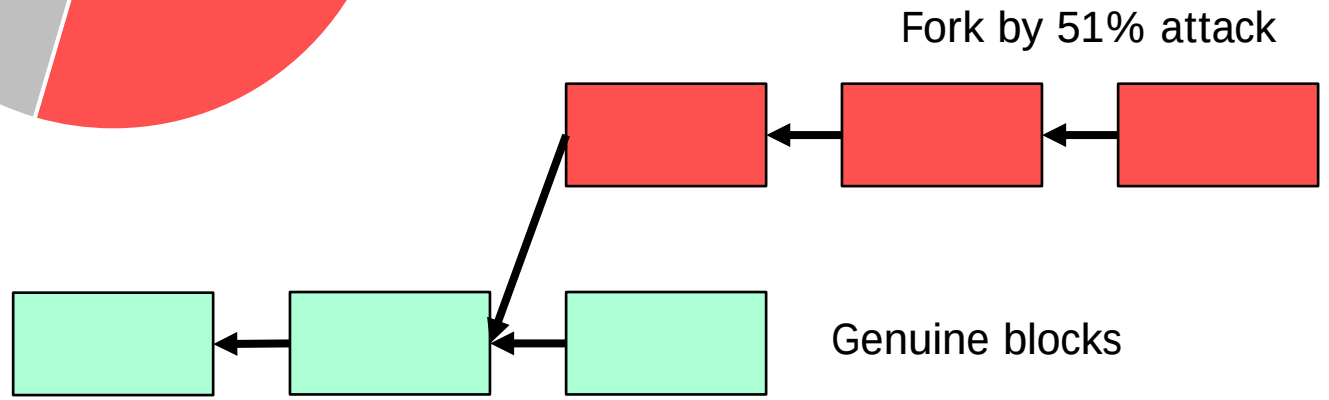
Vulnerability	Cause	Level
Call to unknown	The called function does not exist	Contract's source code
Out-of-gas send	Fallback of the callee is executed	Contract's source code
Exception disorder	Exception handling irregularity	Contract's source code
Type casts	Contract execution type-check error	Contract's source code
Reentrance flaw	Function reentered before exit	Contract's source code
Field disclosure	Private value published by miner	Contract's source code
Immutable bug	Contract altering after deployment	Ethereum virtual machine bytecode
Ether lost	Ether sent to orphan address	Ethereum virtual machine bytecode
Unpredicted state	Contract state change before call	Blockchain Mechanism
Randomness bug	Seed biased by malicious miner	Blockchain mechanism
Time-stamp failure	Malicious miner alters time stamp	Blockchain mechanism

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.

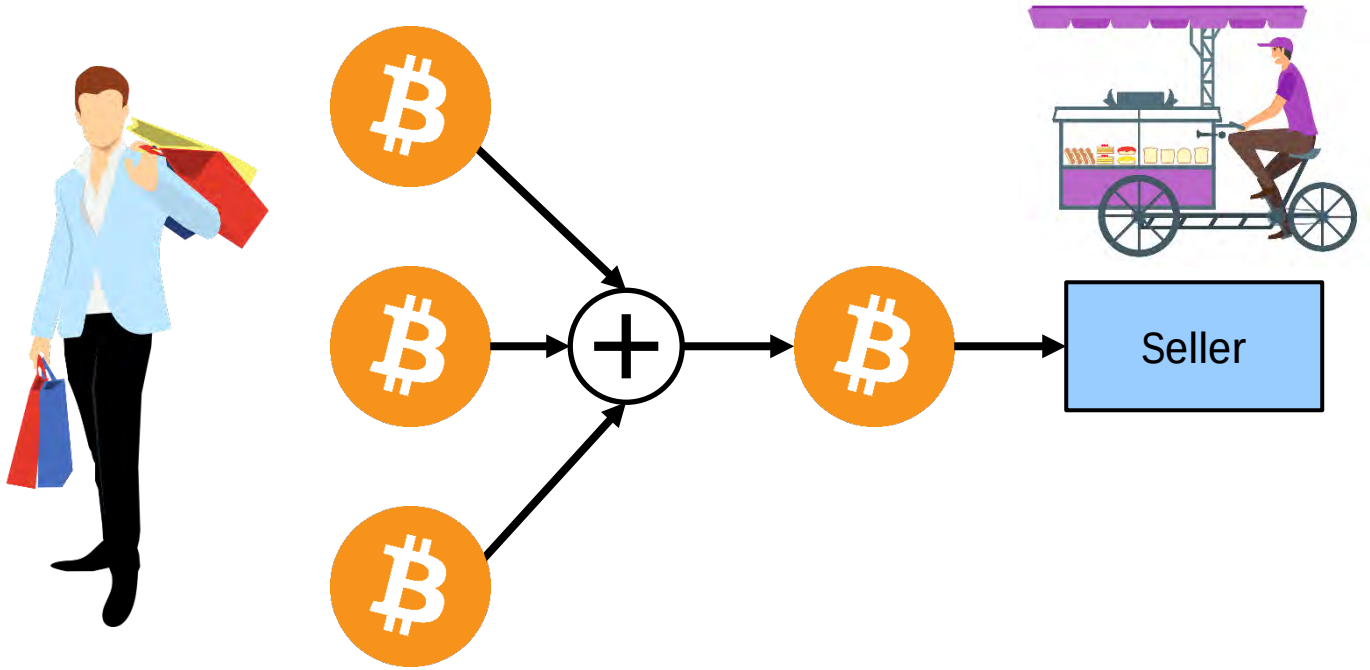
Blockchain - 51% Attack



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



Blockchain Challenges – Anonymity Can be Broken



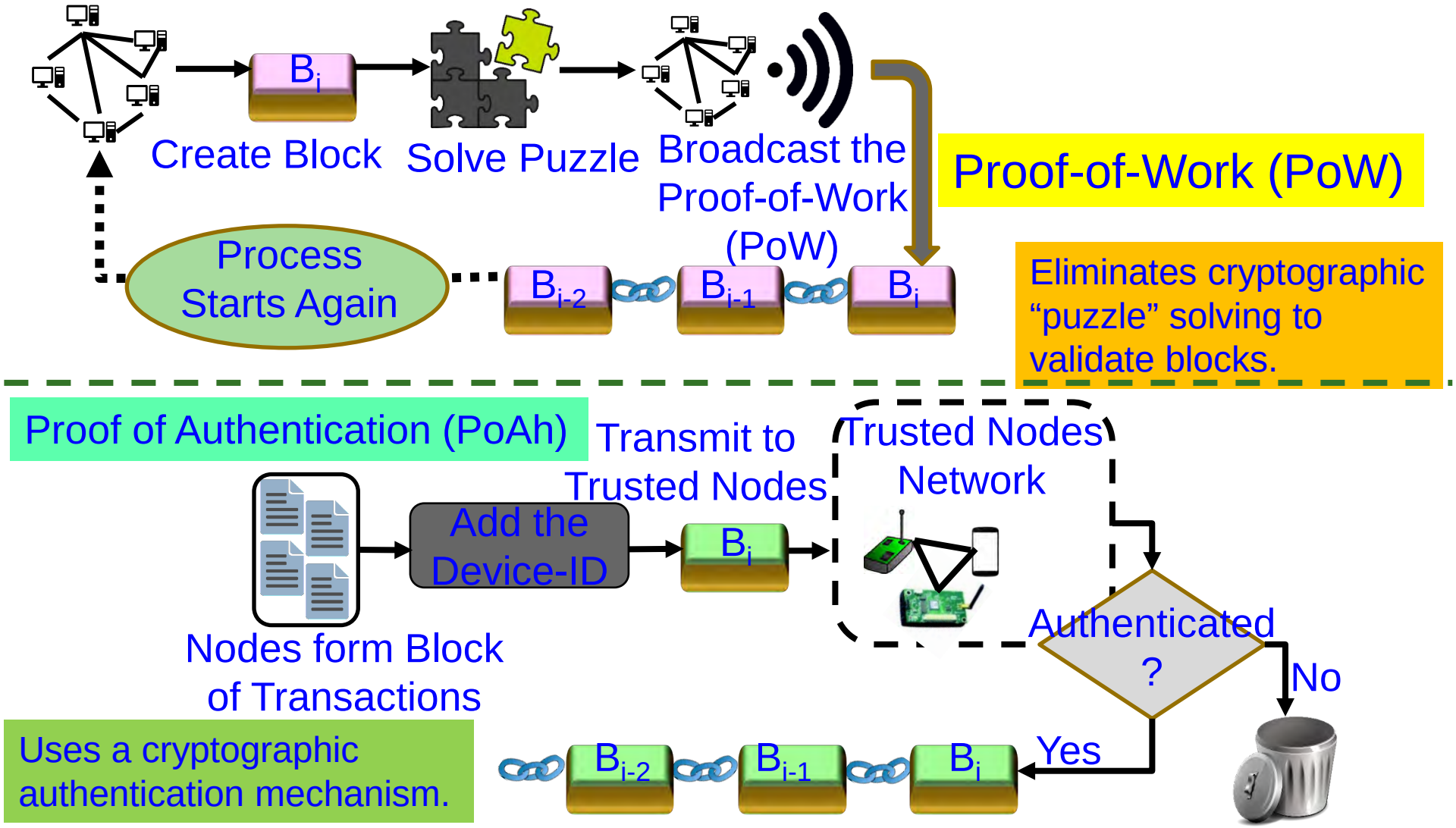
With careful analysis, anonymity can be broken

Blockchain Memory Usage

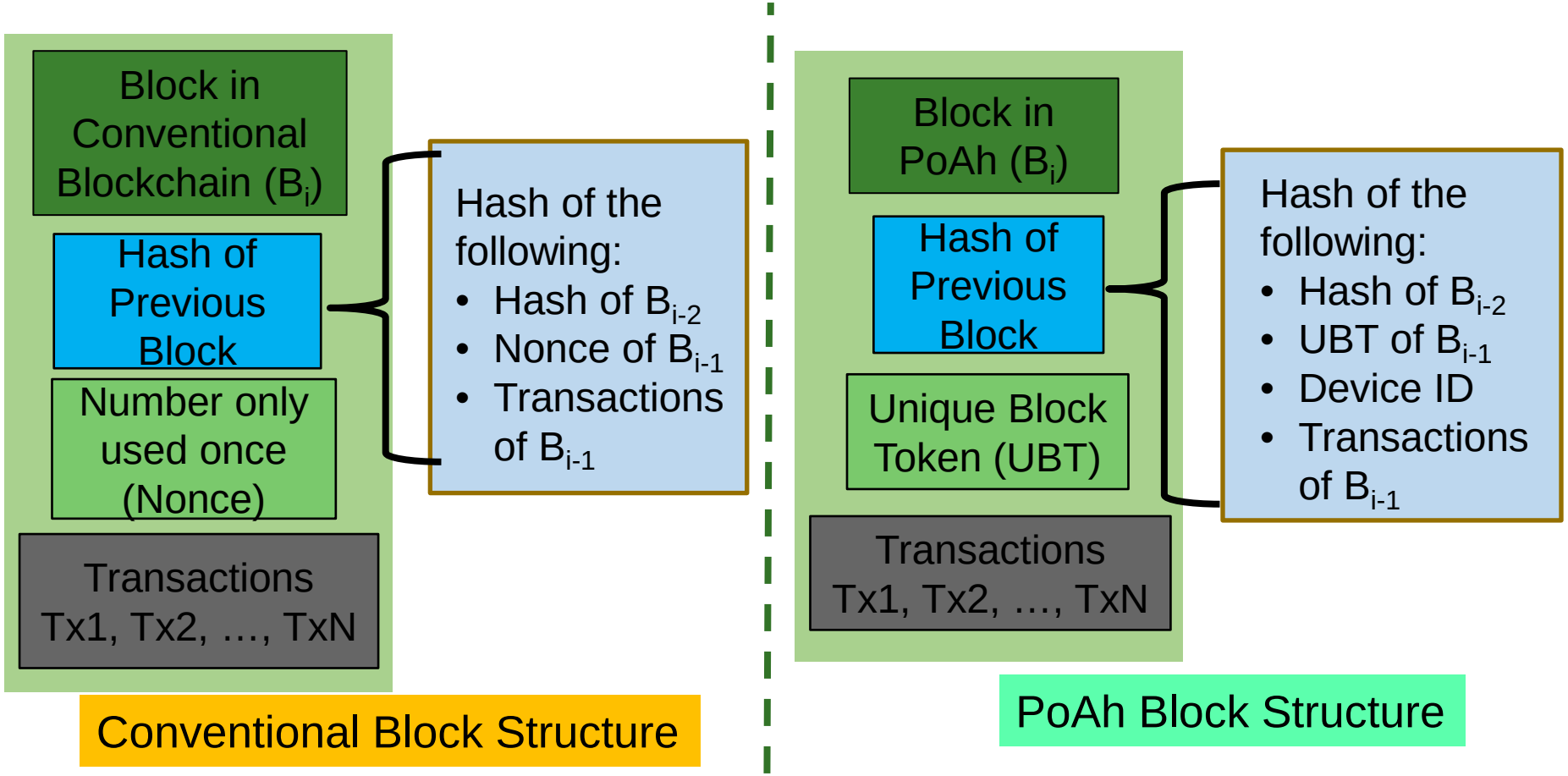
- A transaction is charged based in the amount of data
- Multiple transactions needed for larger files to break them into chunks and send multiple transactions
- This will increase cost in terms of base transaction fee, fee per byte of data
- All these factors limited amount of data to be stored on the 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/DLT Solutions

Our Proof-of-Authentication (PoAh)

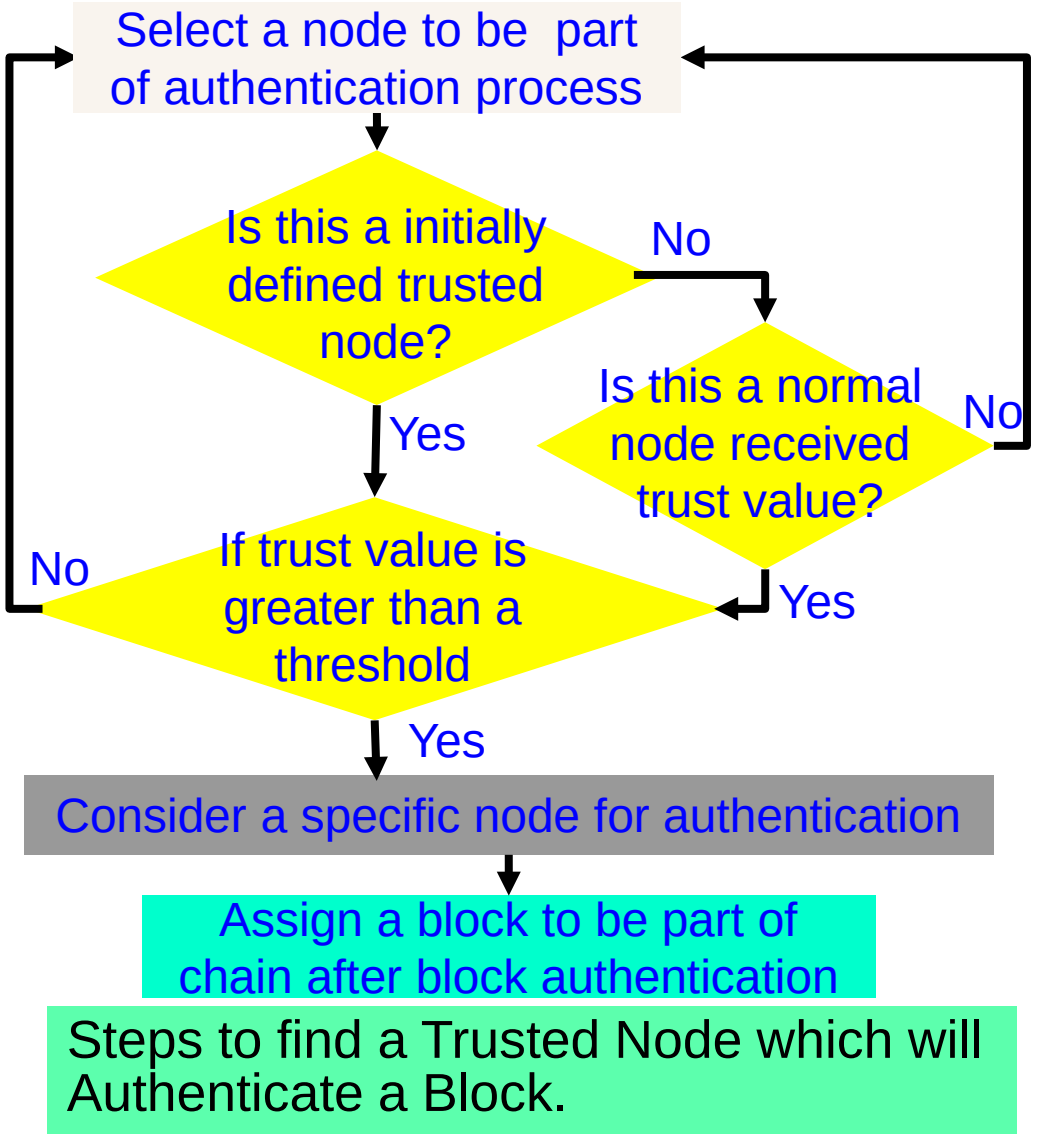


Our PoAh-Chain: Proposed New Block Structure



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) → broadcast

(3) Trusted node verifies signature with source public key

V_{PuK}(block) → MAC Checking

(4) If (Authenticated)

Block||PoAh(ID) → broadcast

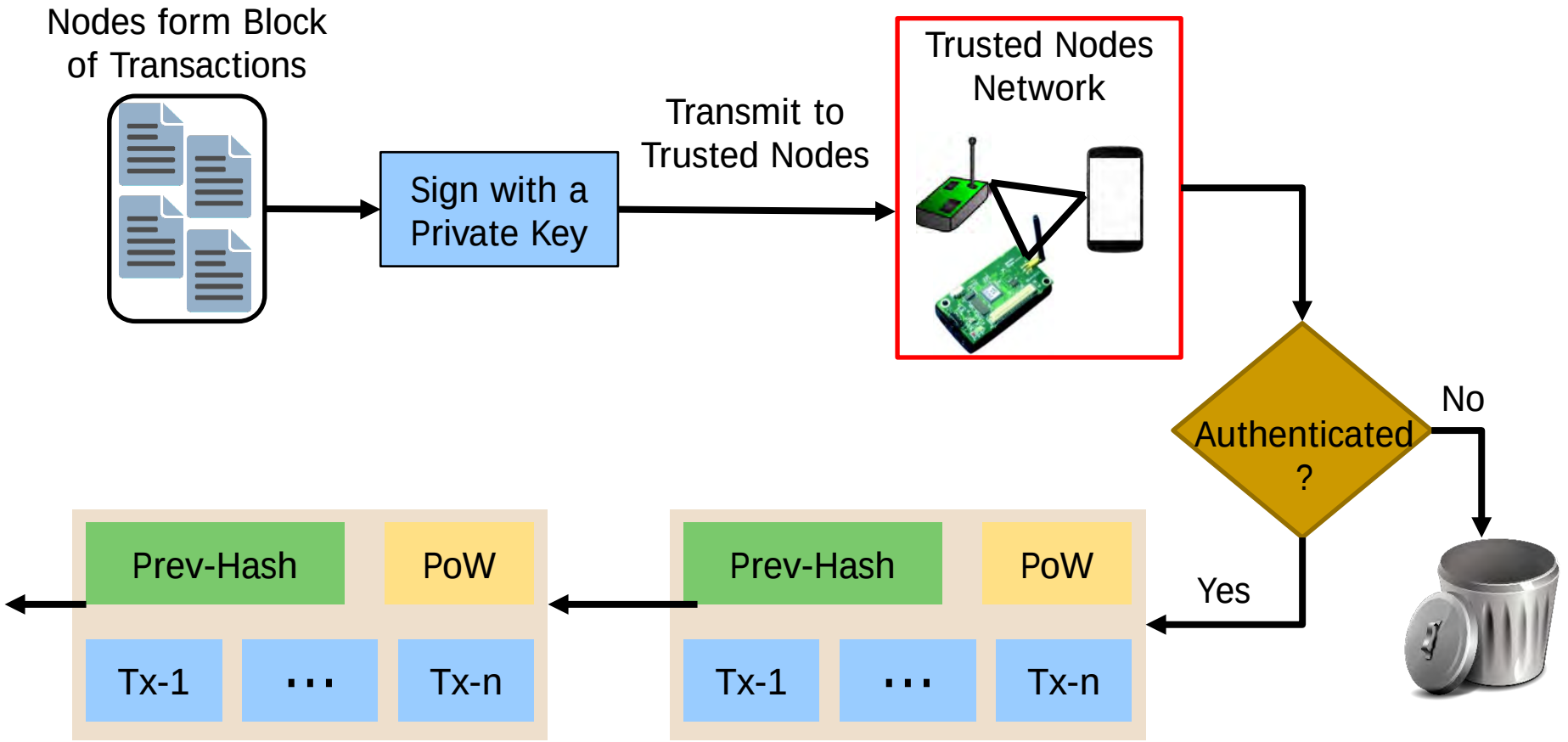
H(block) → Add blocks into chain

(5) Else

Drop blocks

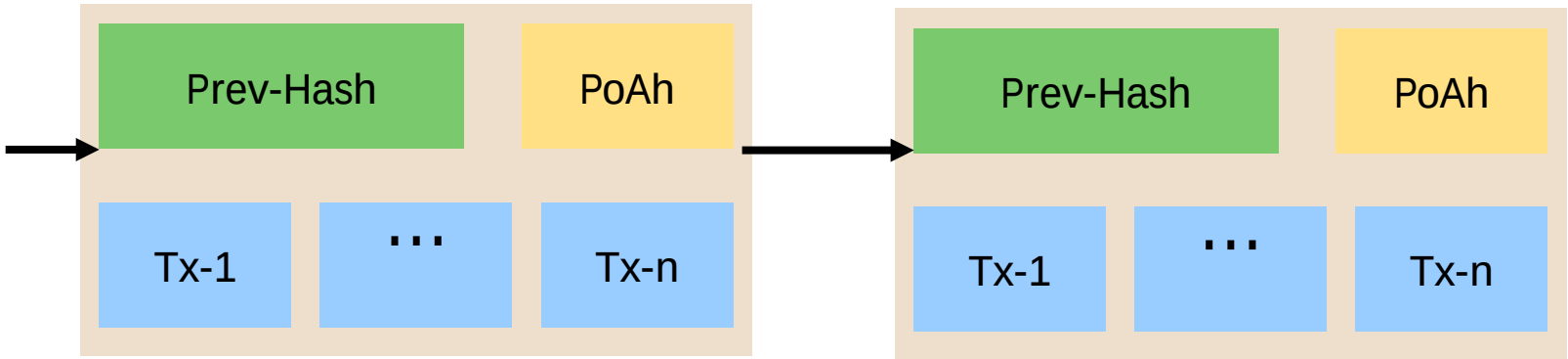
(6) GOTO (Step-1) for next block

Proof-of-Authentication (PoAh)



Source: Puthal and Mohanty 2019, IEEE Potentials Jan 2019 and ICCE 2019

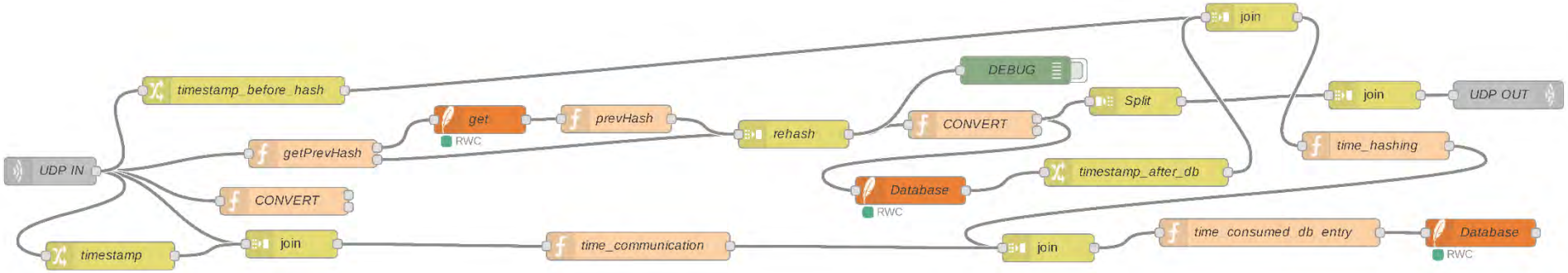
Proof-of-Authentication (PoAh)

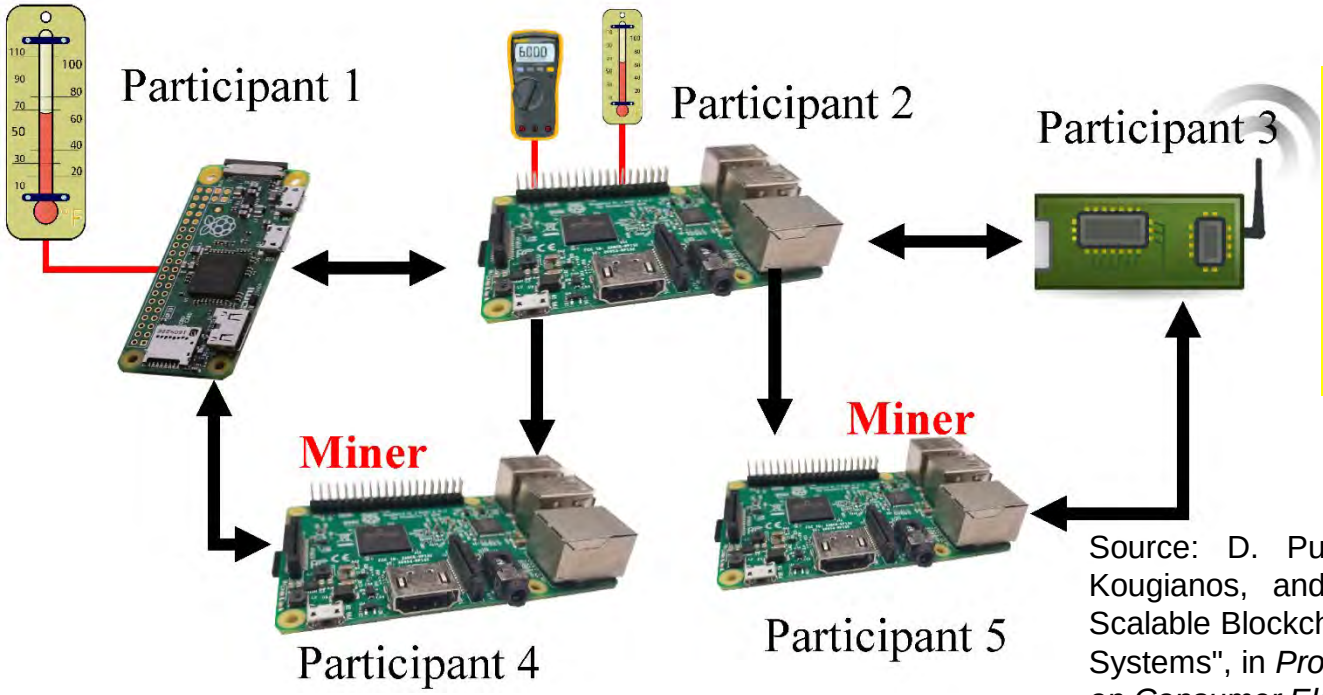


PoW - 10 min in cloud	**PoAh - 3 sec in Rasperry Pi**	**PoAh - 200X faster than PoW**

Source: Puthal and Mohanty 2019, IEEE Potentials Jan 2019 and ICCE 2019

IoT Simulators - Node-RED - Example

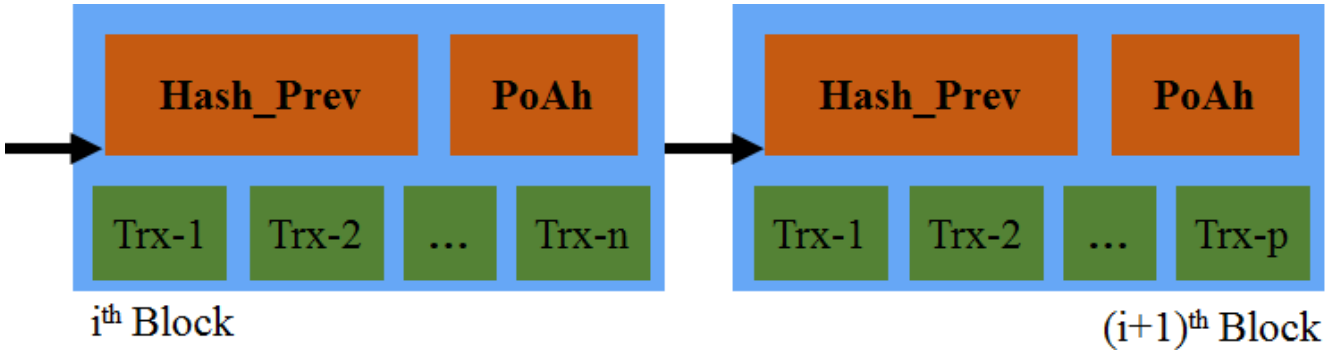




Simulation: Proof-of-Authentication (PoAh) based IoT Friendly Blockchain

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 is 200X Faster than PoW



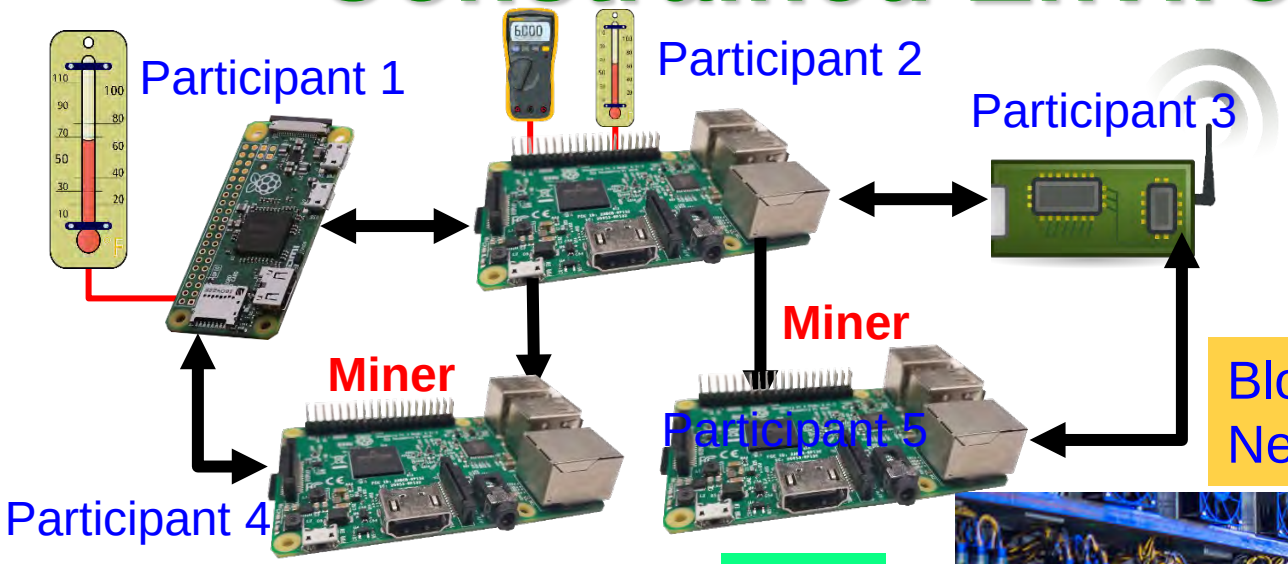
Eliminates cryptographic "puzzle" solving to validate blocks.

	Proof-of-Work (PoW)	Proof-of-Stake (PoS)	Proof-of-Activity (PoA)	Proof-of-Authentication (PoAh)
Energy consumption	High	High	High	Low
Computation requirements	High	High	High	Low
Latency	High	High	High	Low
Search space	High	Low	NA	NA

PoW - 10 min in cloud	**PoAh - 3 sec in Rasperry Pi**	**PoAh - 200X faster than PoW**

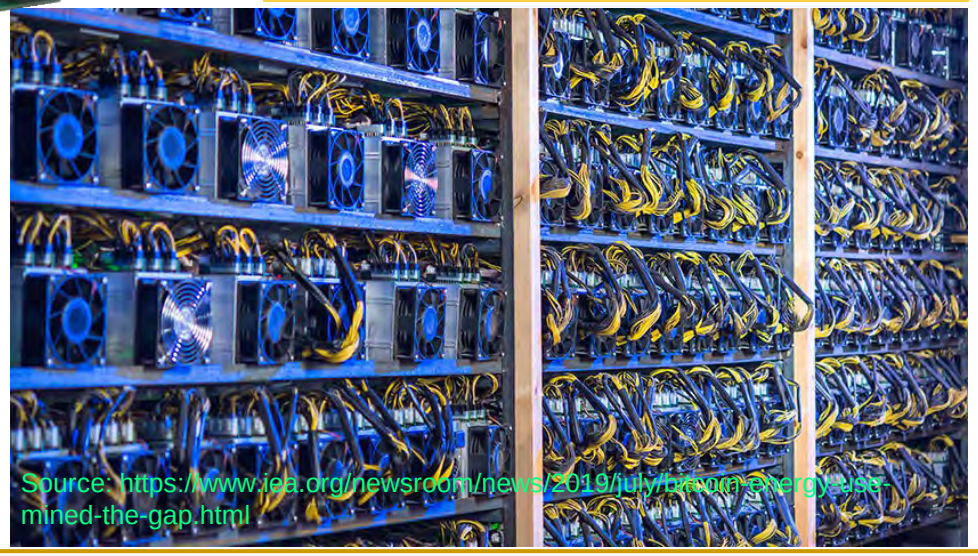
Source: D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems", in *Proc. 37th IEEE International Conference on Consumer Electronics (ICCE*), 2019.

Our PoAh-Chain Runs in Resource Constrained Environment



Our PoAh-Chain Runs here 5 W

Blockchain using PoW
Needs Significant Resource

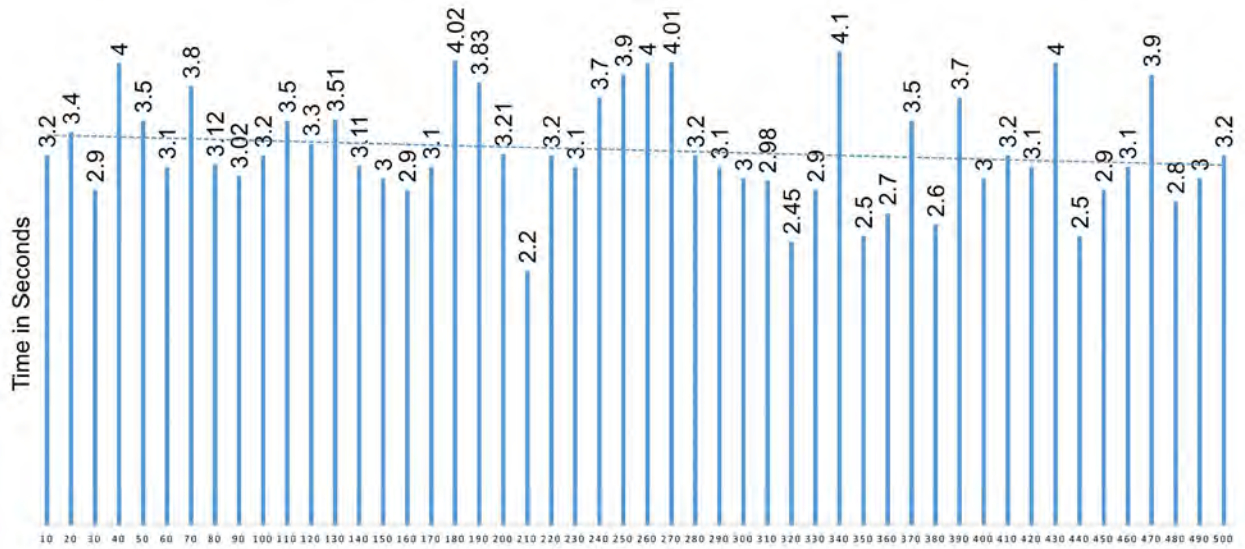


Source: https://www.iea.org/newsroom/news/2019/july/bitcoin-energy-use-mined-the-gap.html

500,0000 W

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

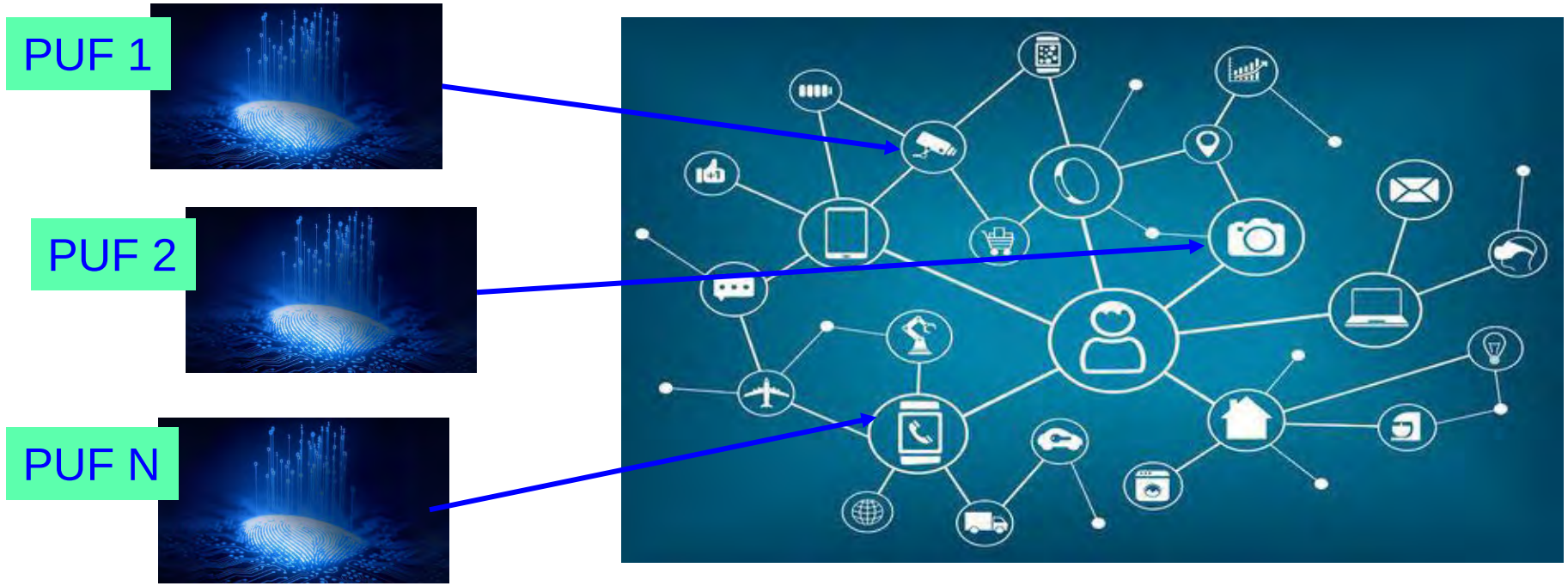
Consensus Algorithm	Blockchain Type	Prone To Attacks	Power Consumption	Time for Consensus
Proof-of-Work (PoW)	Public	Sybil, 51%	538 KWh	10 min
Proof-of-Stake (PoS)	Public	Sybil, Dos	5.5 KWh	
Proof-of-Authentication (PoAh)	Private	Not Known	3.5 W	3 sec



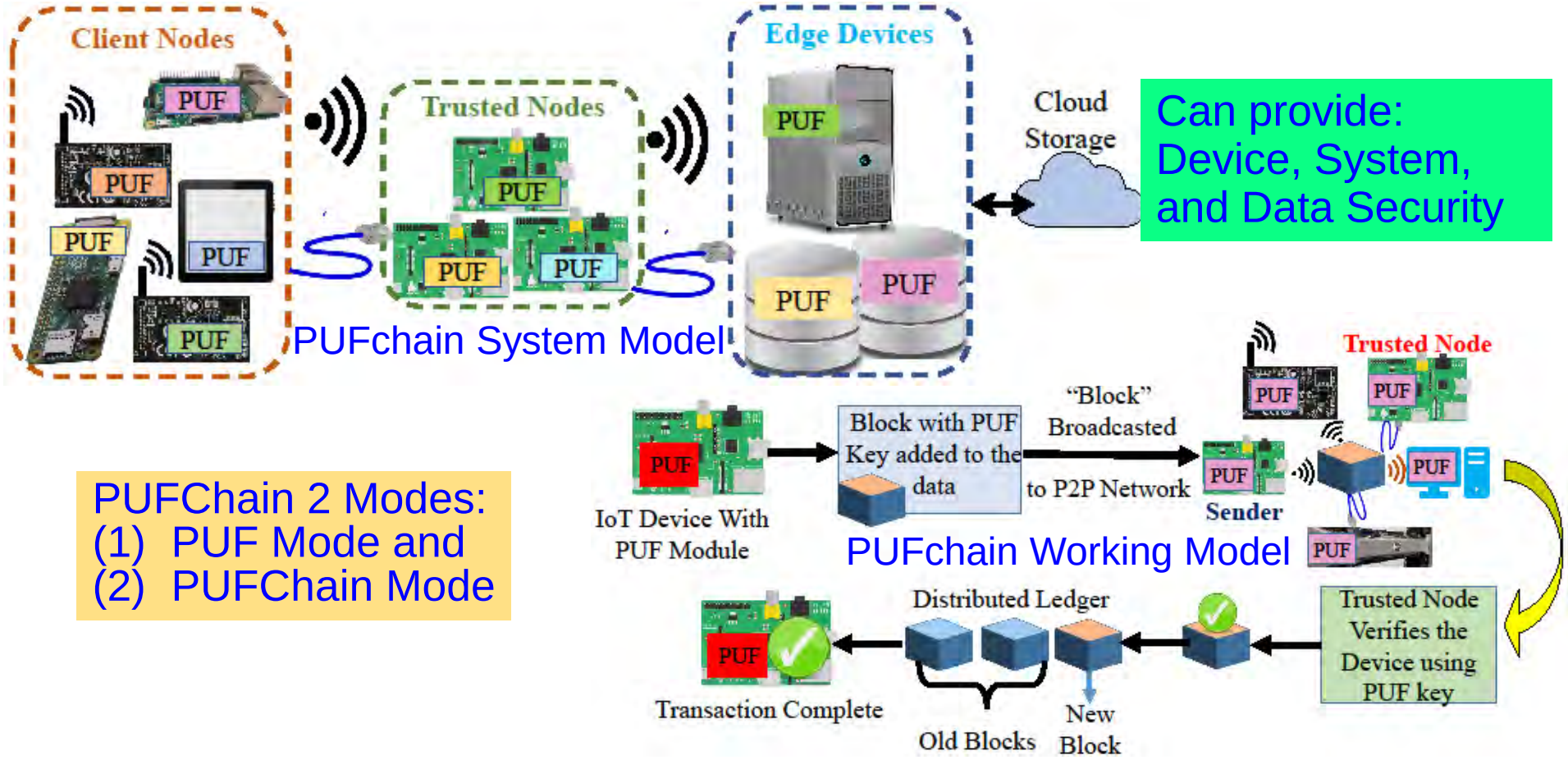
PoAh Execution for 100s of Nodes

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.

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

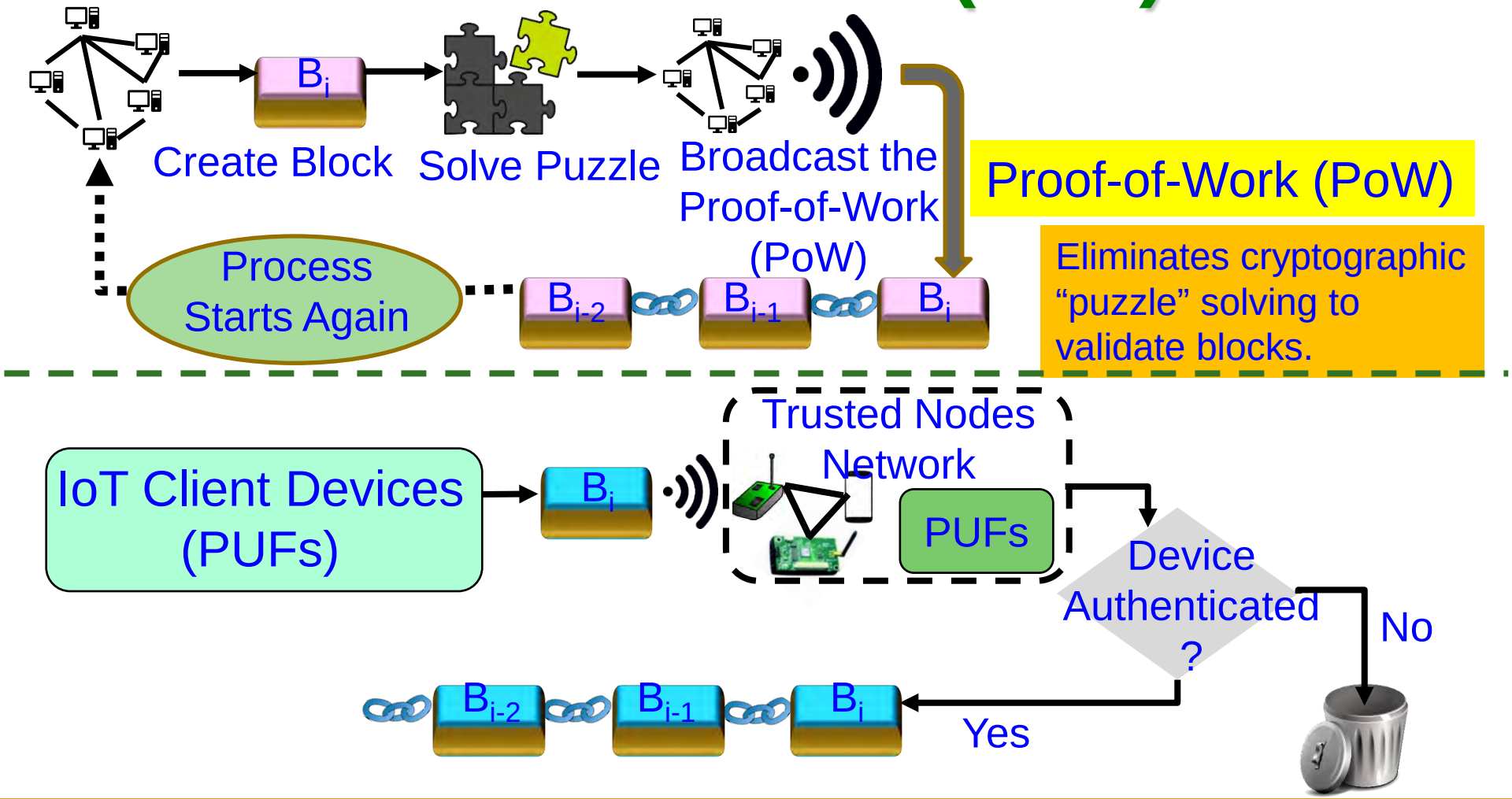


PUFchain: The Hardware-Assisted Scalable Blockchain

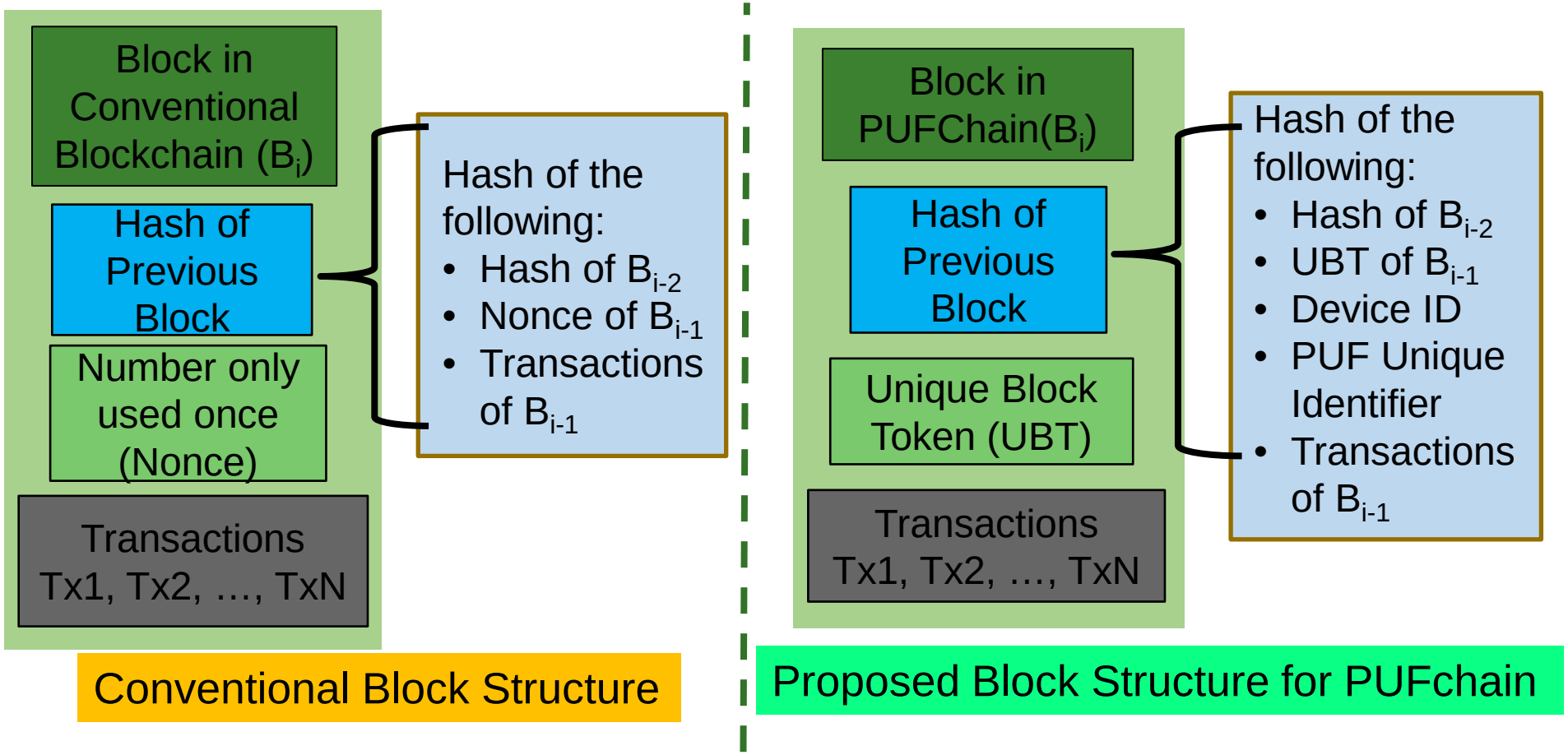


Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. in Press.

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

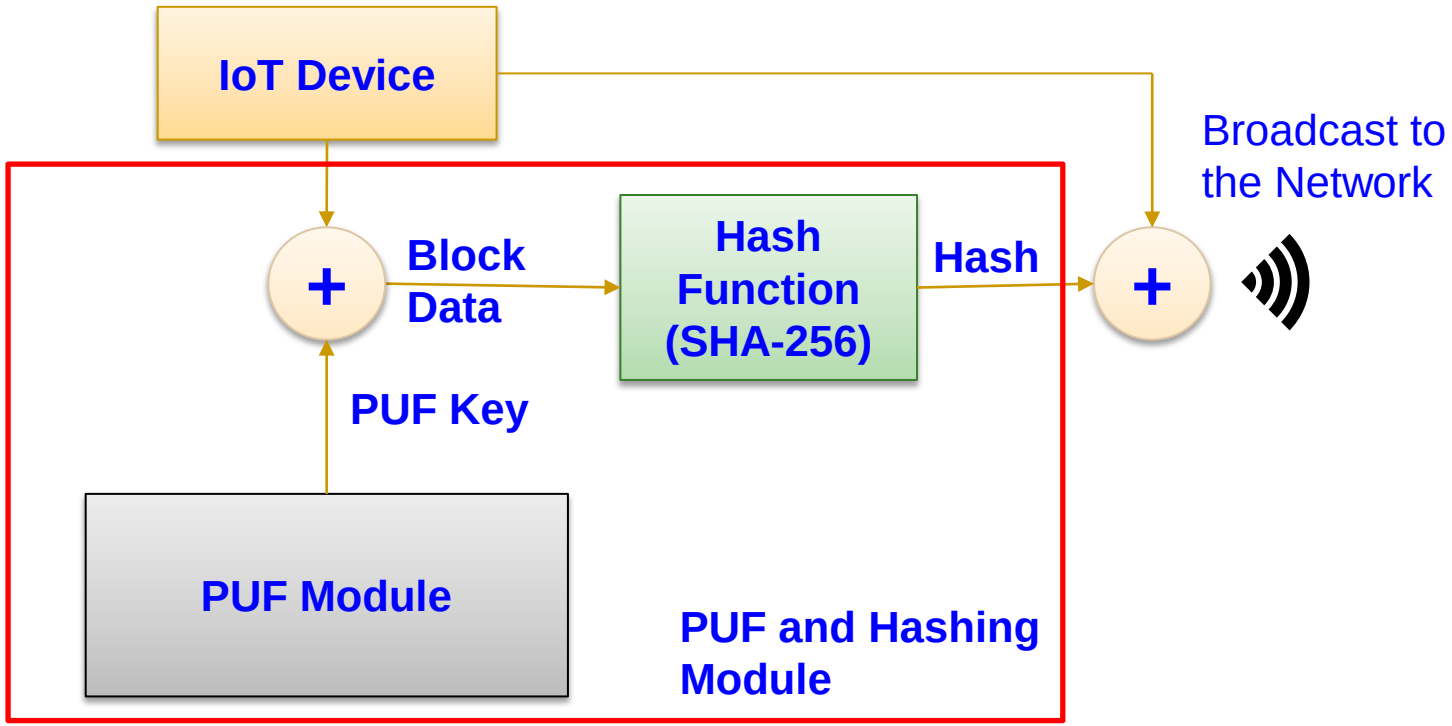


PUFchain: Proposed New Block Structure



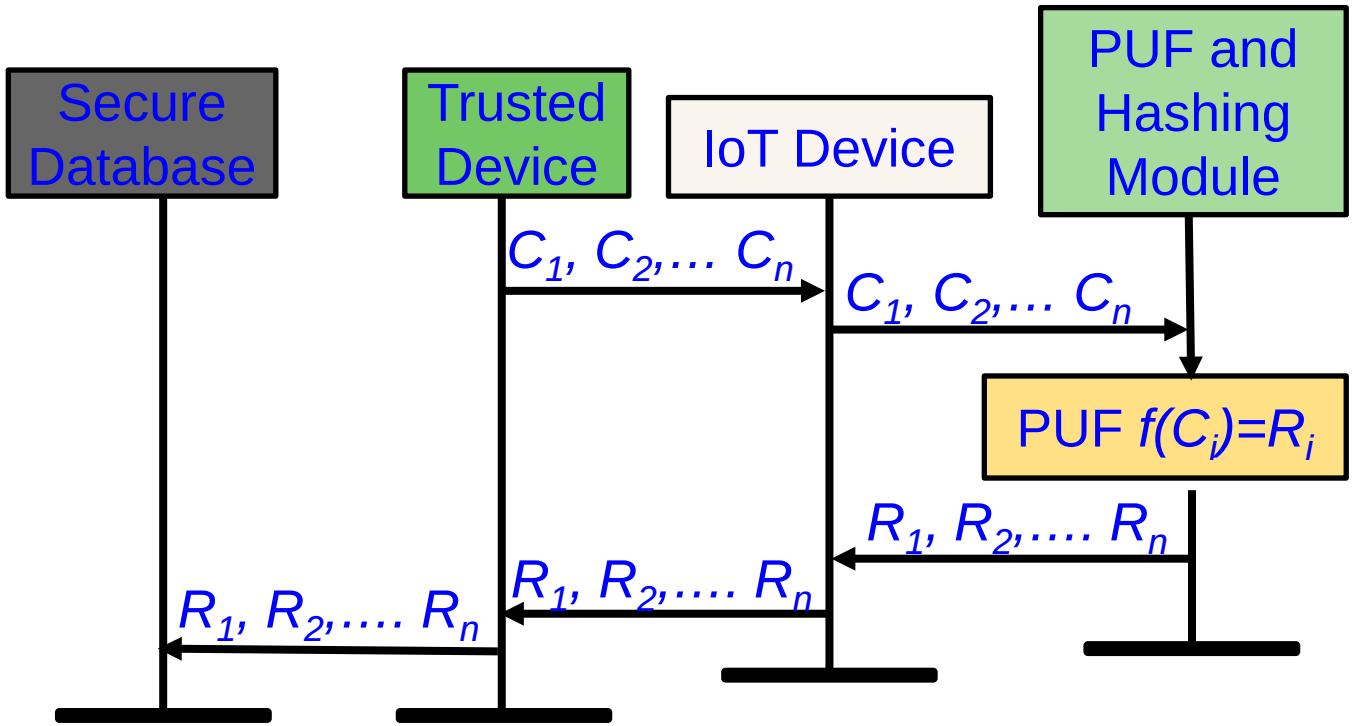
PUFchain – A Typical Node

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.

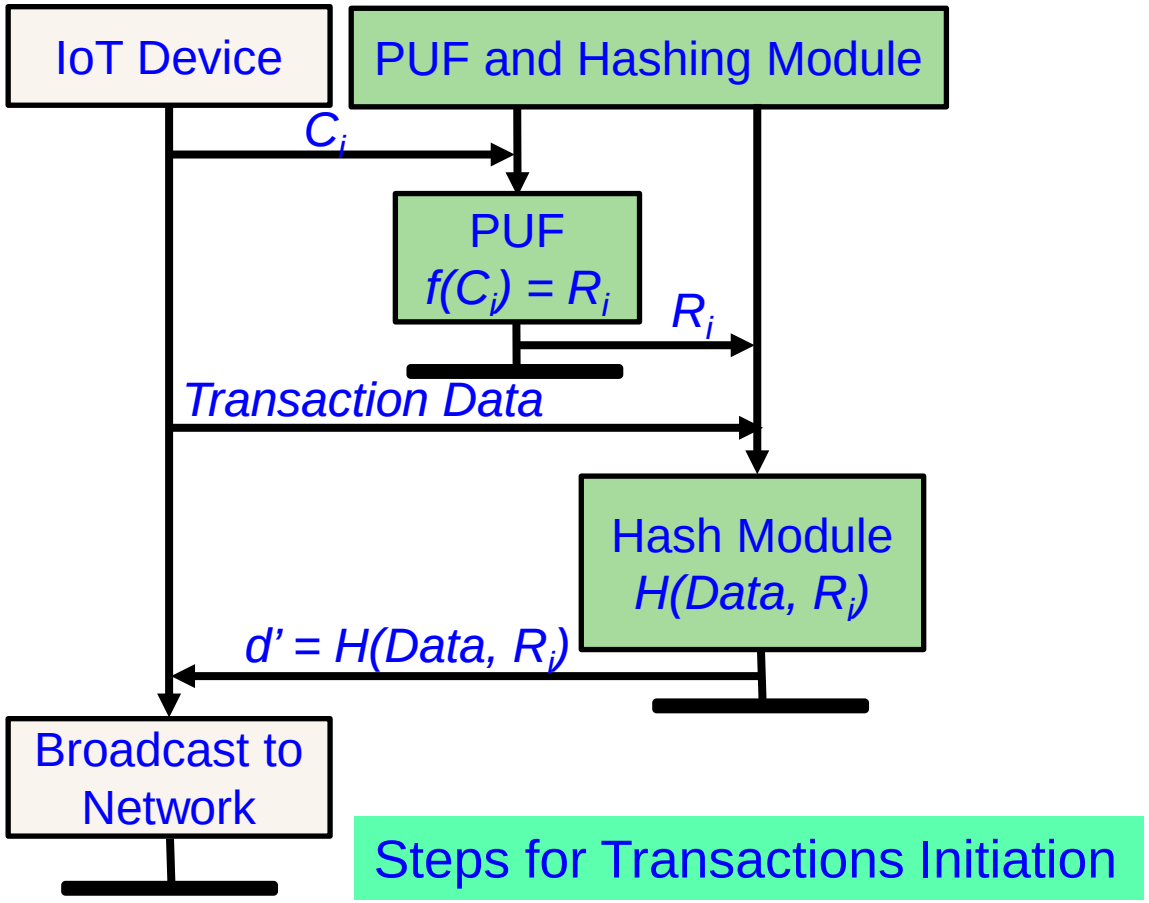
PUFchain: Device Enrollment Steps



Device Enrollment Steps

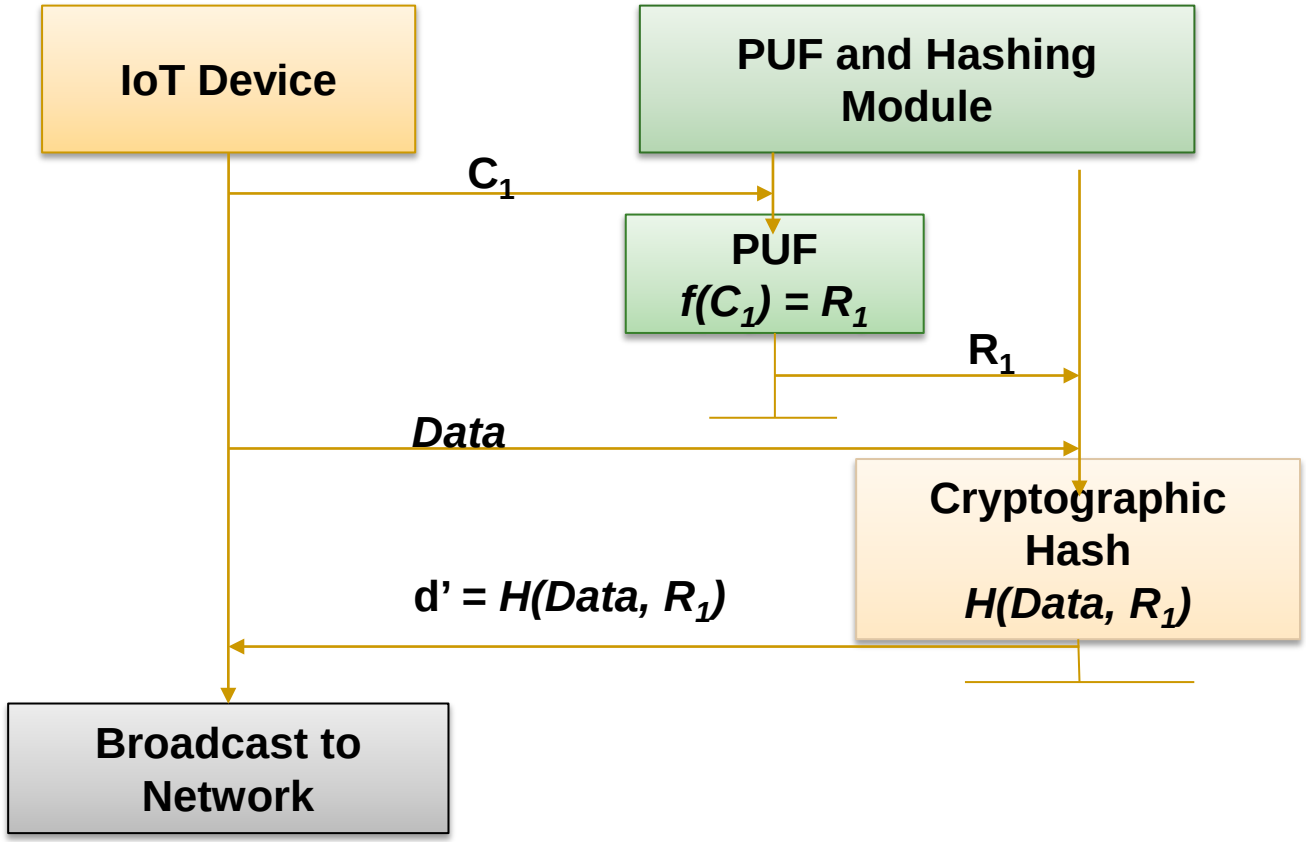
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. in Press.

PUFchain - Transactions Initiation



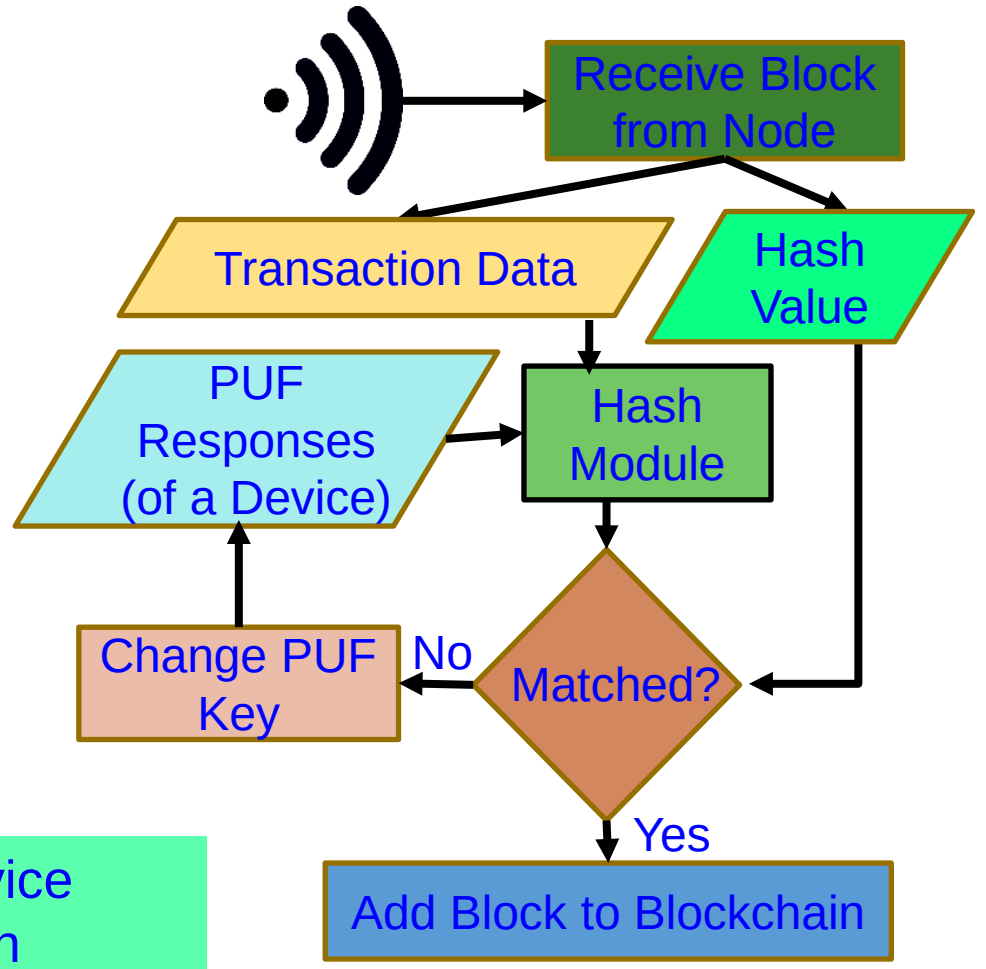
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. in Press.

Transactions Initiations Steps



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.

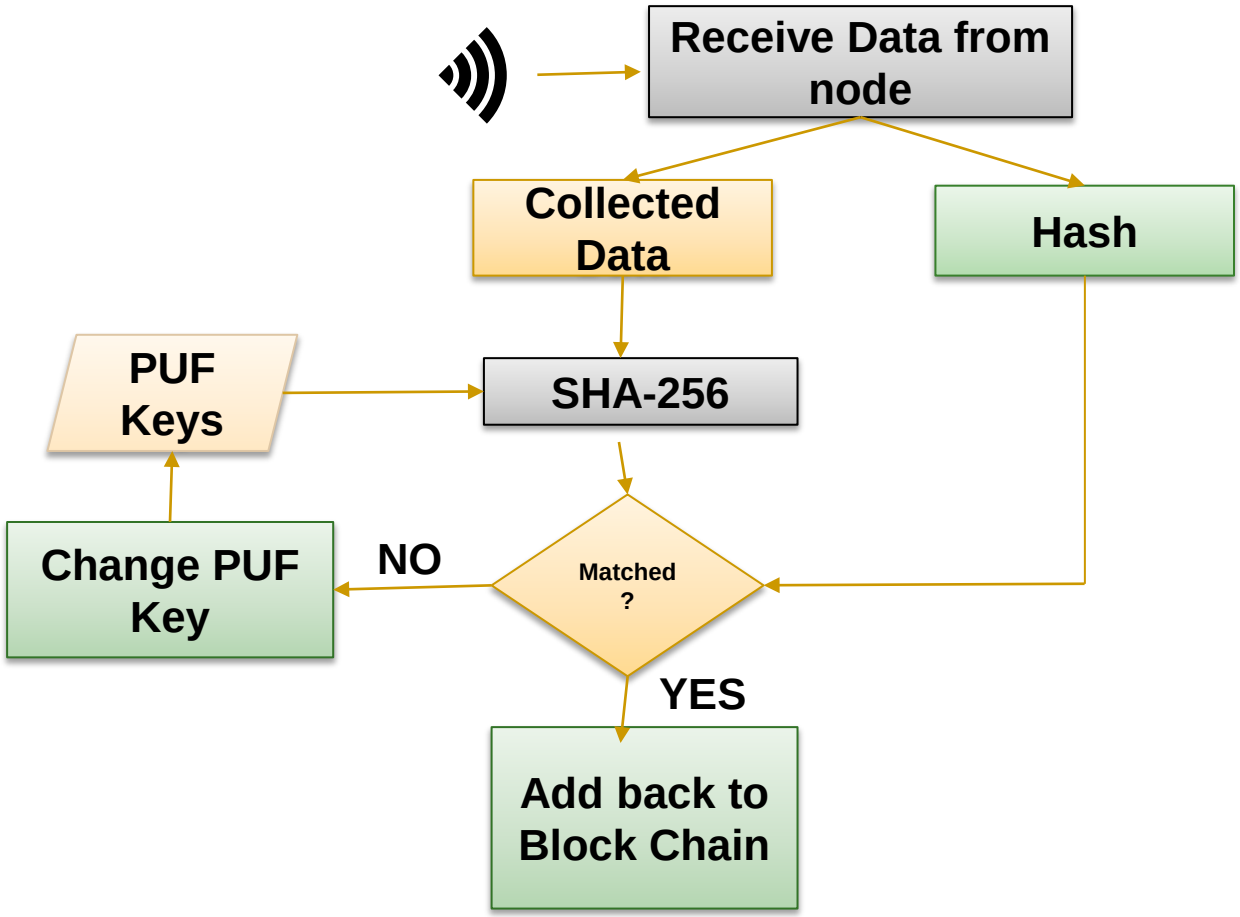
PUFchain – Device Authentication



Steps for Device Authentication

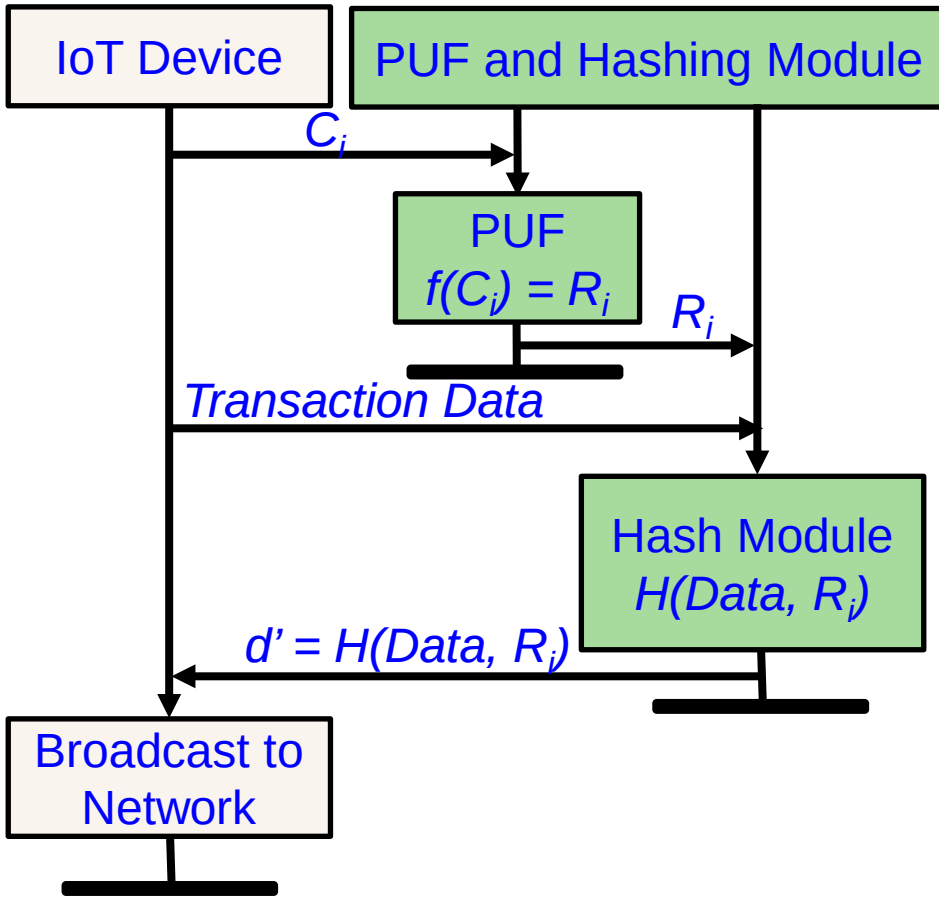
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. in Press.

Device Authentication Steps

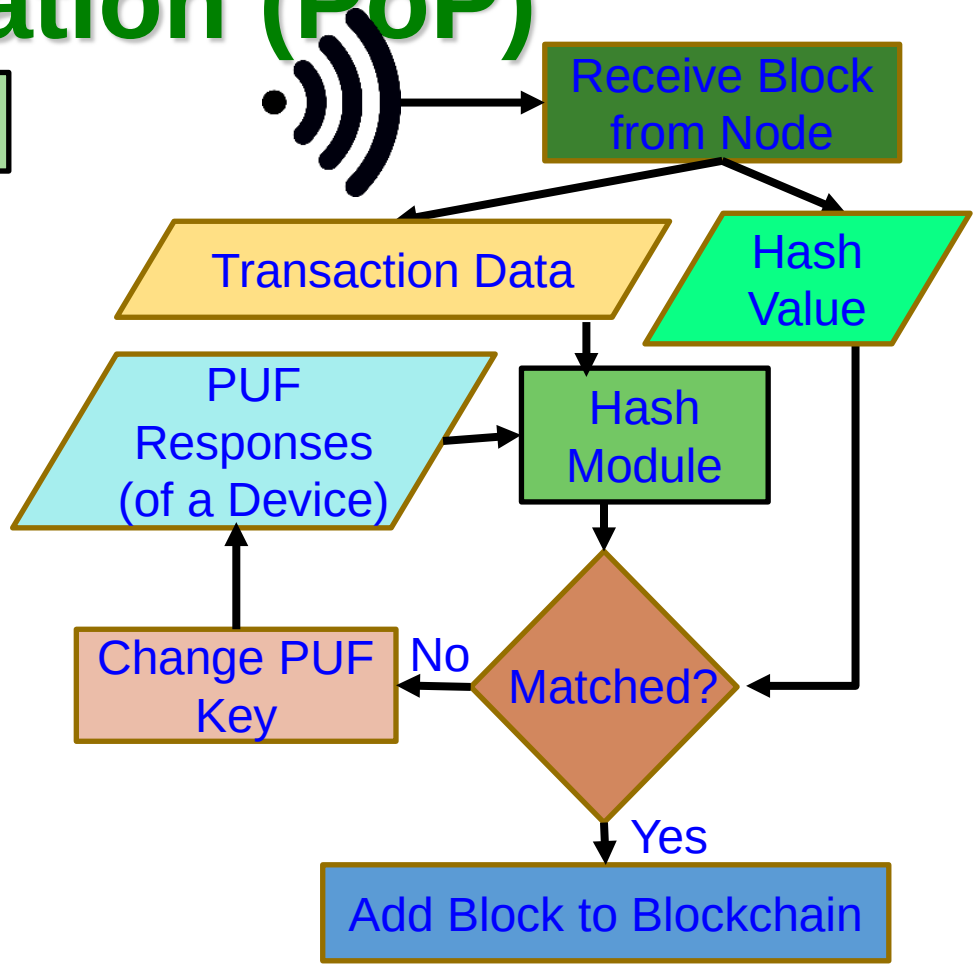


Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos and D. Puthal, "PUFchain: A Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE)," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 8-16, 1 March 2020.

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

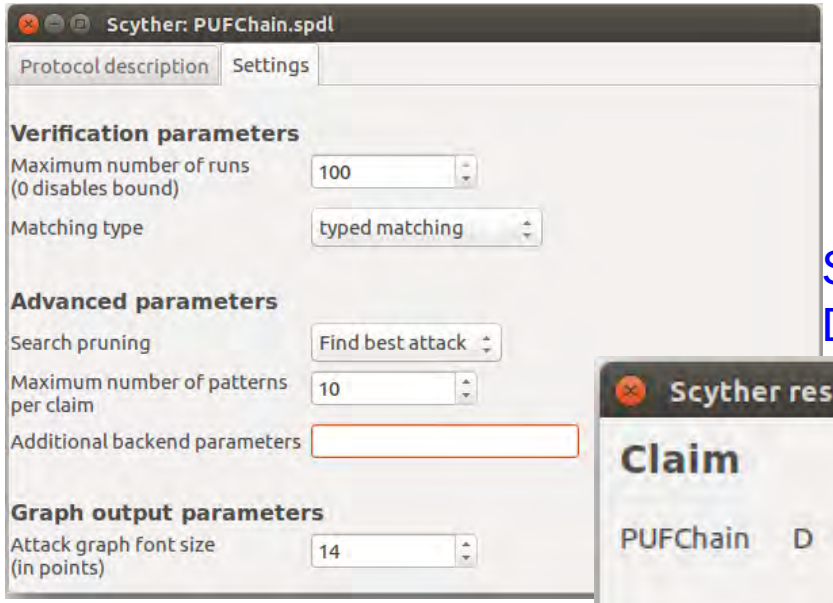


Steps for Transactions Initiation



Steps for Device Authentication

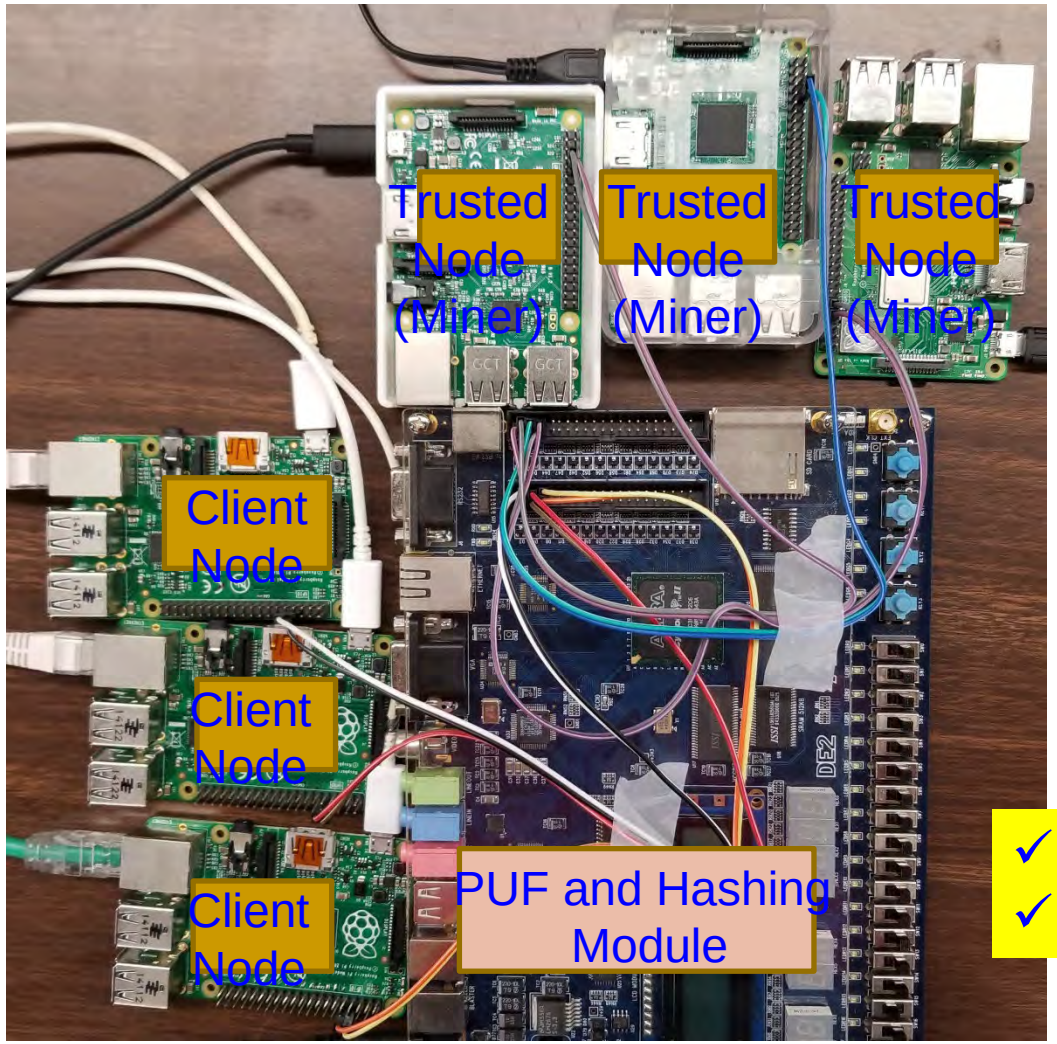
PUFchain Security Validation



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.

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.

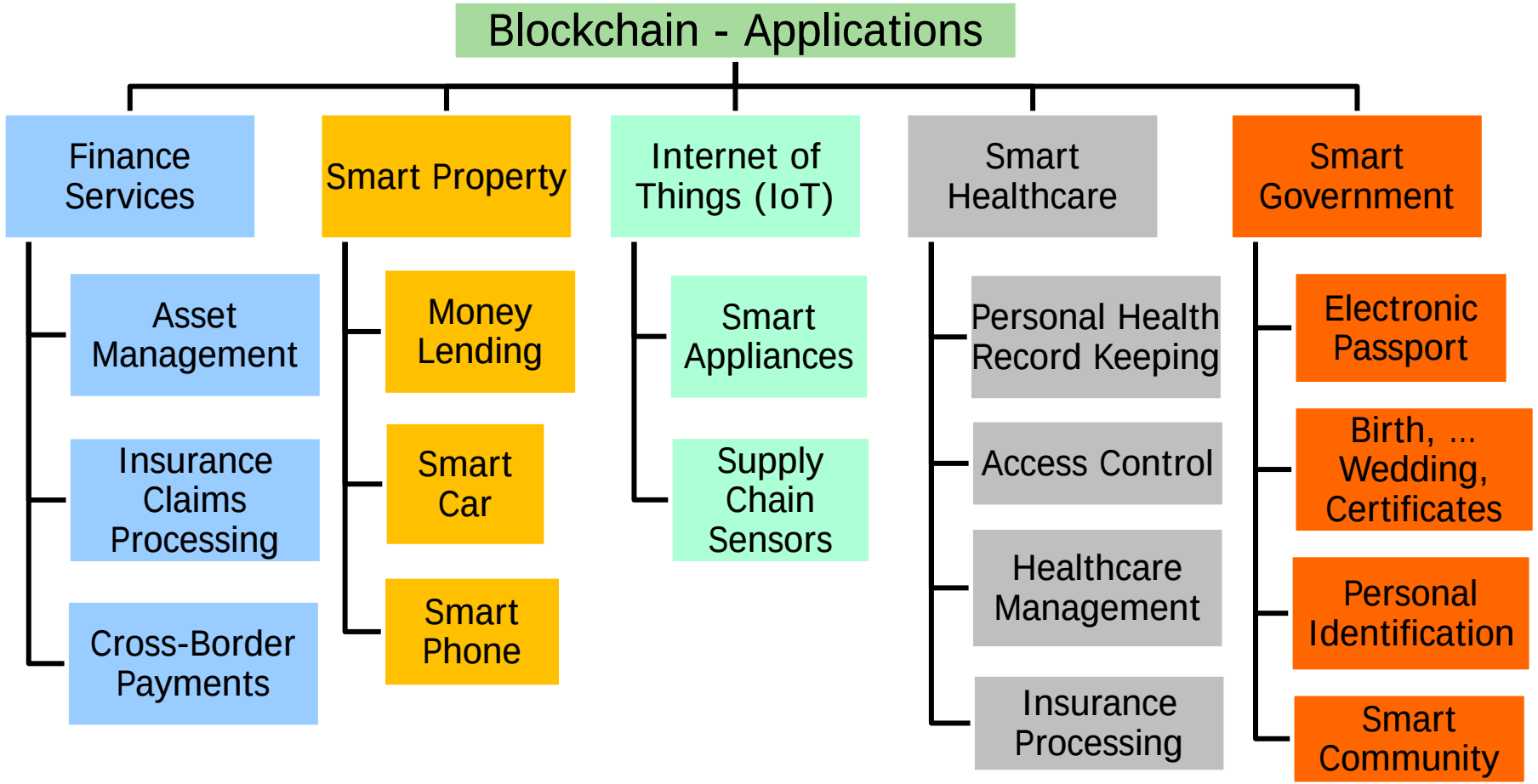
Consensus Algorithms – Comparative Perspectives

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 Block and Trade (PoBT)					
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.

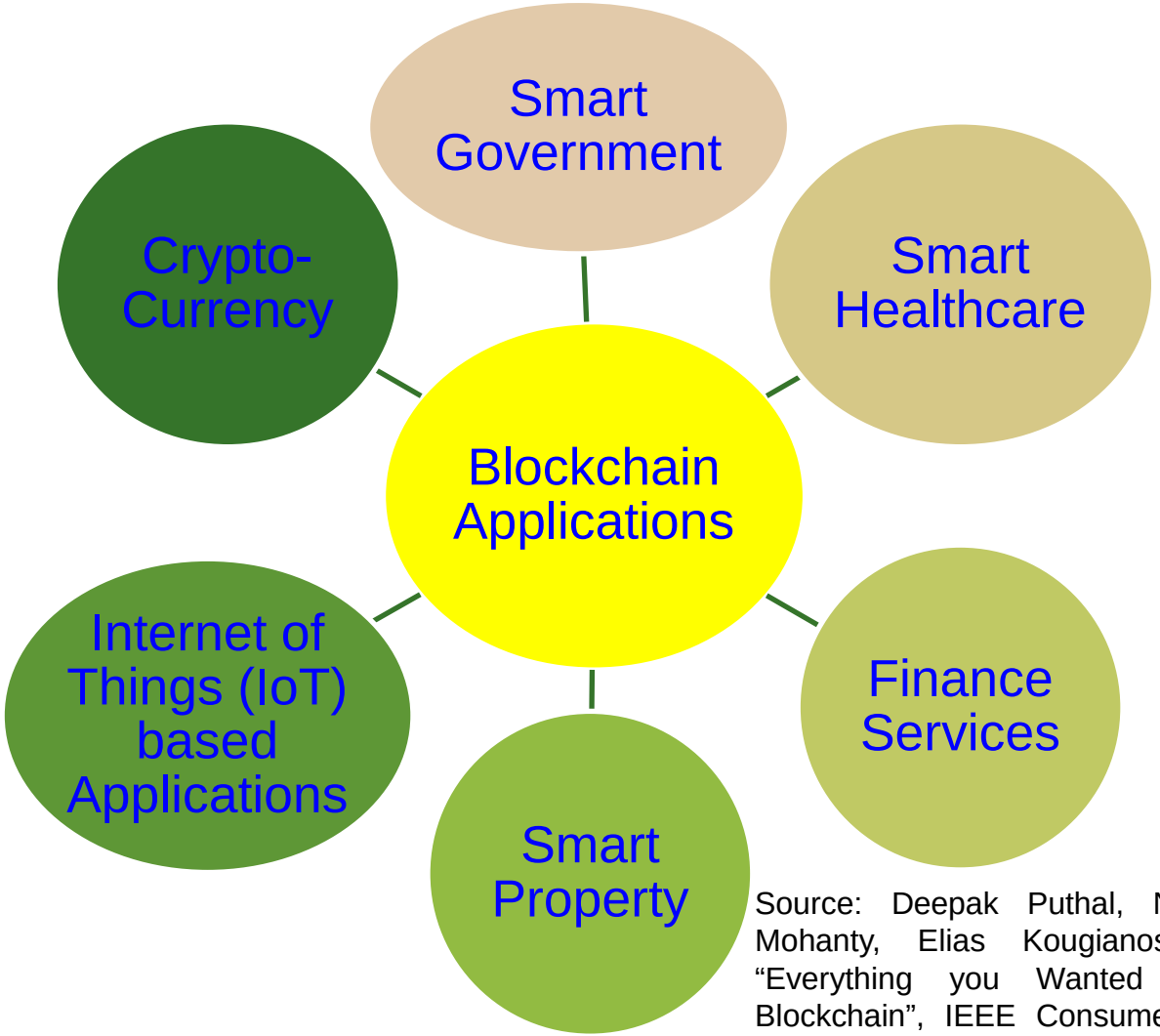
Blockchain Applications

Blockchain Applications



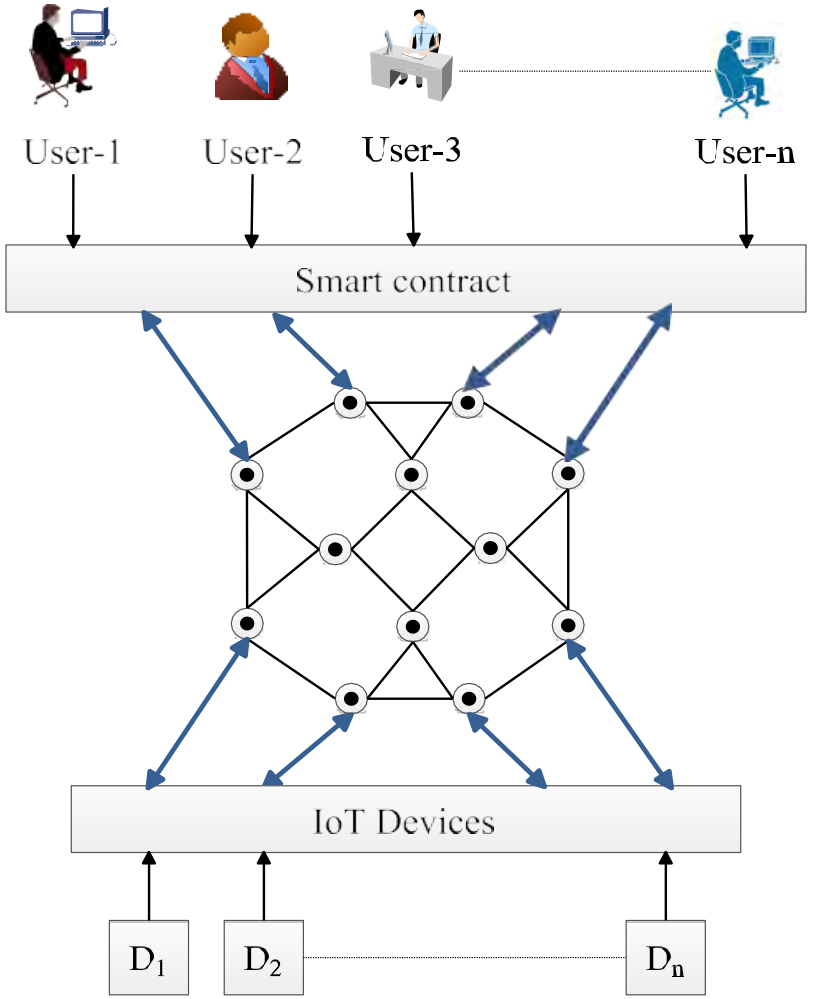
Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you Wanted to Know about the Blockchain", *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 4, July 2018, pp. 06--14.

Blockchain Applications



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.

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.

Blockchain in IoT

Blockchain in IoT:

- Blockchain could be a platform for IoT infrastructure as well as IoT applications.
- Blockchain could replace the cloud and provide secure and transparent database for all users.

Blockchain in IoT applications:

- All the traditional services nowadays are transforming to a smart applications with the advancement of technologies.
- Part of being a smart application is being a secure one. Blockchain could be part of several applications in IoT environment as the technology behind recording the data.

Other Applications

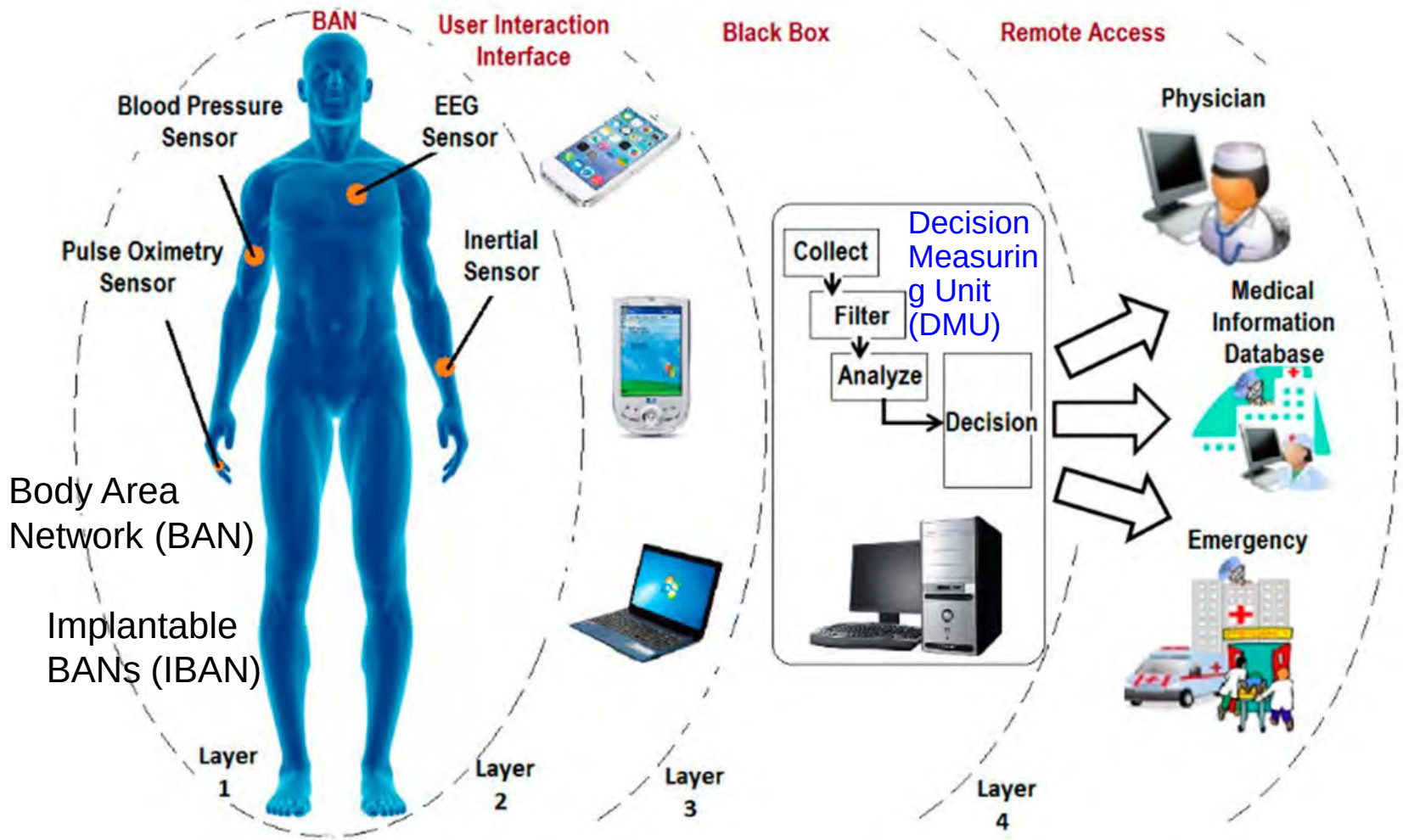
- Banking: Prevents Double Spending and Hacking, and reduce crises to large extent.
- Law enforcement: Secure Criminal Database.
- Voting: Authentication of Voter ID and secure counting of votes.
- Internet of Things: Data integrity and secure transfer among devices.

Applications

- Cryptocurrency and Financial transactions
- Health
- Gambling
- Insurance
- Agriculture

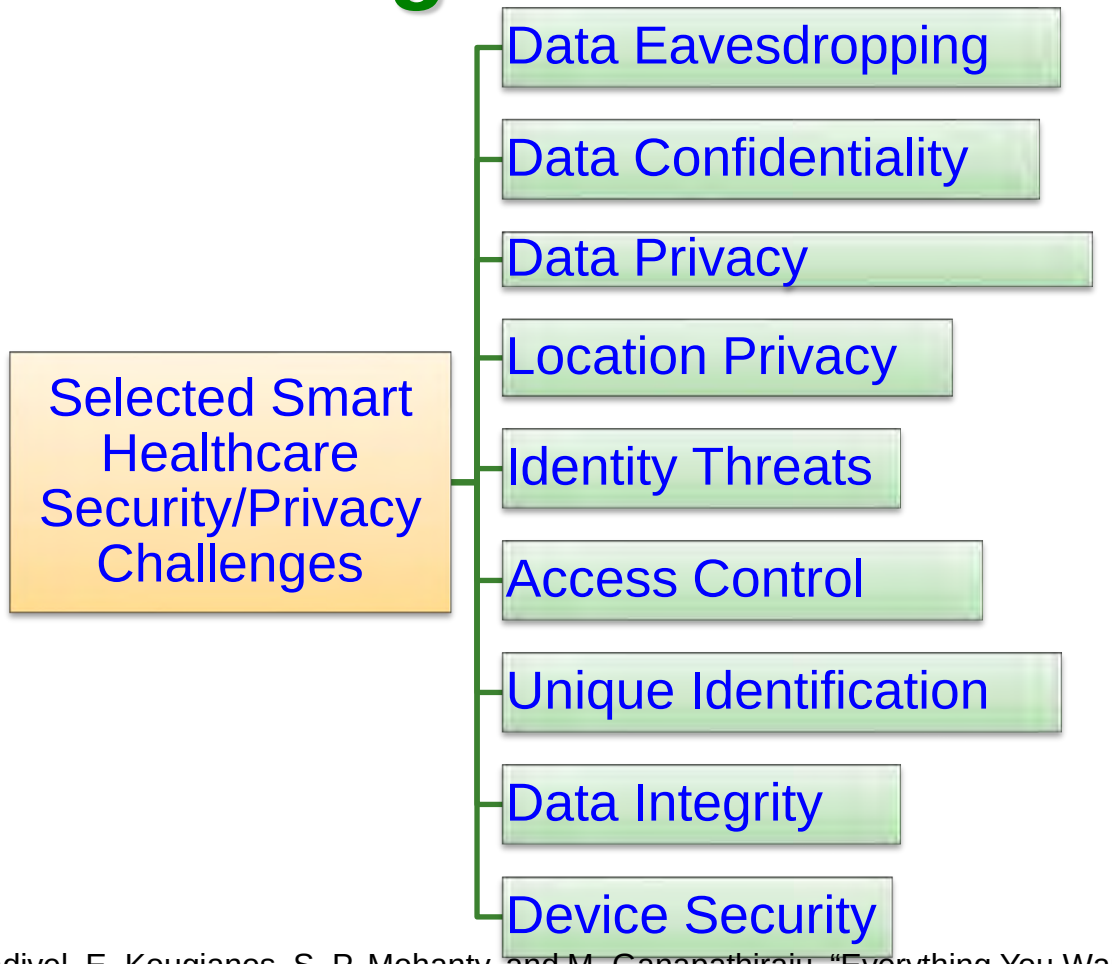
Blockchain in Smart Healthcare

Smart Healthcare - 4-Layer Architecture



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



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.

Traditional Versus Blockchain EHR

Health Information Exchange (HIE) Pain Points	Blockchain Opportunities
Establishing a Trust Network depends on the HIE as an intermediary to establish point-to-point sharing and "book-keeping" of what data was exchanged.	**Disintermediation of Trust** likely would not require an HIE operator because all participants would have access to the distributed ledger to maintain a secure exchange without complex brokered trust.
Cost Per Transaction, given low transaction volumes, reduces the business case for central systems or new edge networks for participating groups.	**Reduced Transaction Costs** due to disintermediation, as well as near-real time processing, would make the system more efficient.
Master Patient Index (MPI) challenges arise from the need to synchronize multiple patient identifiers between systems while securing patient privacy.	**Distributed framework for patient digital identities,** which uses private and public identifiers secured through cryptography, creates a singular, more secure method of protecting patient identity.
Varying Data Standards reduce interoperability because records are not compatible between systems.	**Shared data** enables near real-time updates across the network to all parties.
Limited Access to Population Health Data, as HIE is one of the few sources of integrated records.	**Distributed, secure access** to patient longitudinal health data across the distributed ledger.
Inconsistent Rules and Permissions inhibit the right health organization from accessing the right patient data at the right time.	**Smart Contracts** create a consistent, rule-based method for accessing patient data that can be permissioned to selected health organizations.

Source: Exploring the Use of Blockchain for EHRs, Healthcare Big Data, https://healthitanalytics.com/features/exploring-the-use-of-blockchain-for-ehrs-healthcare-big-data

EHR in Blockchain

Doctor

EHR smart contract

Insurance Provider

Patient

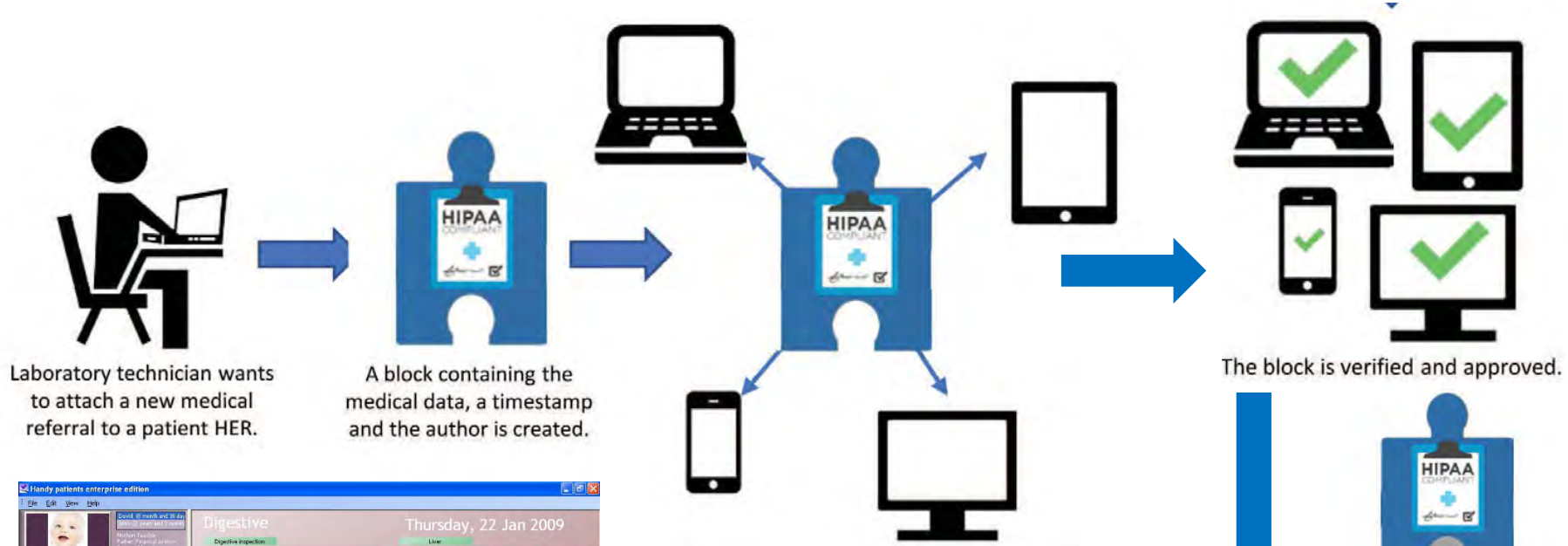
Ganache

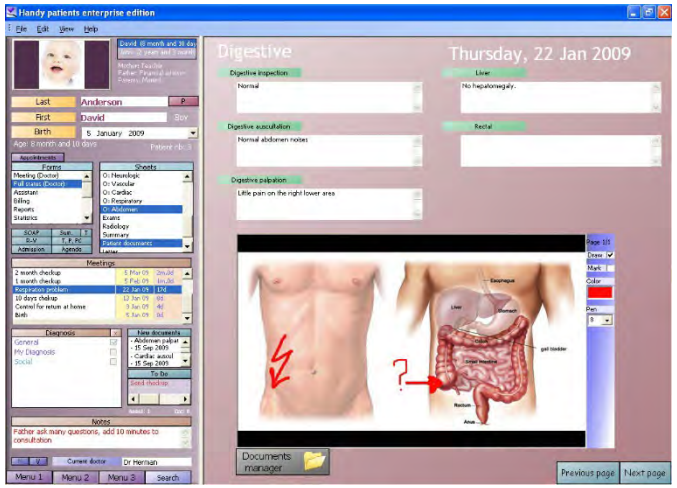
Pharmacy

Regular EH Vs Blockchain Based Secure EHR

Personal Health Record (Synthetic Data)	Valid Block Structure
Name: AAA DOB: BBB Address: TTT	Hash of current block 36024568b514589c65478d9875abc656fcd895de
Height: CCC Weight: DDD Body Temperature: XXX	Hash of previous block 15489dfc2578451bdce18d9875abc656fcd895de
Heart Rate: AAA Glucose Level: KKK	Encrypted Data
---	Nonce (Hashcash process)
Other Data	Root of hash tree

Blockchain in Smart Healthcare

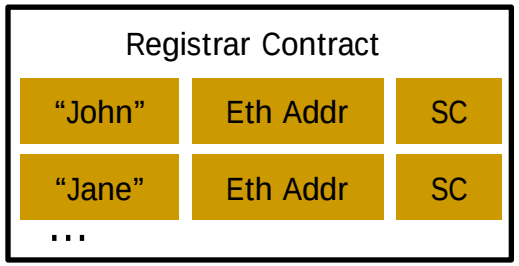


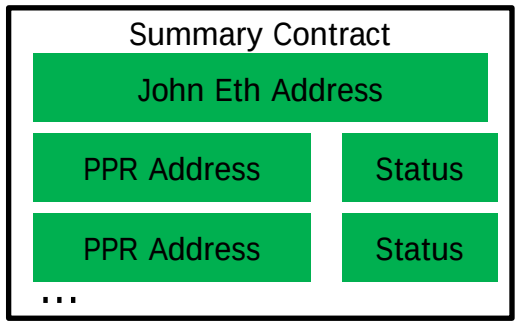


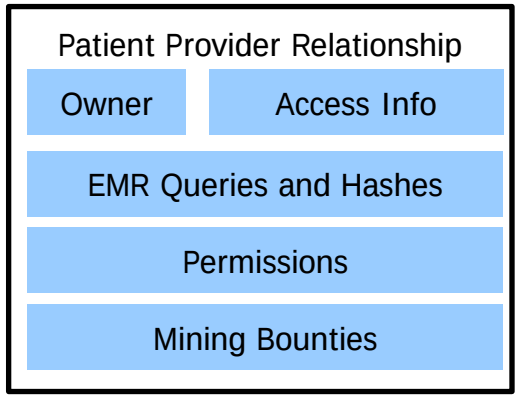
Can it preserve privacy?

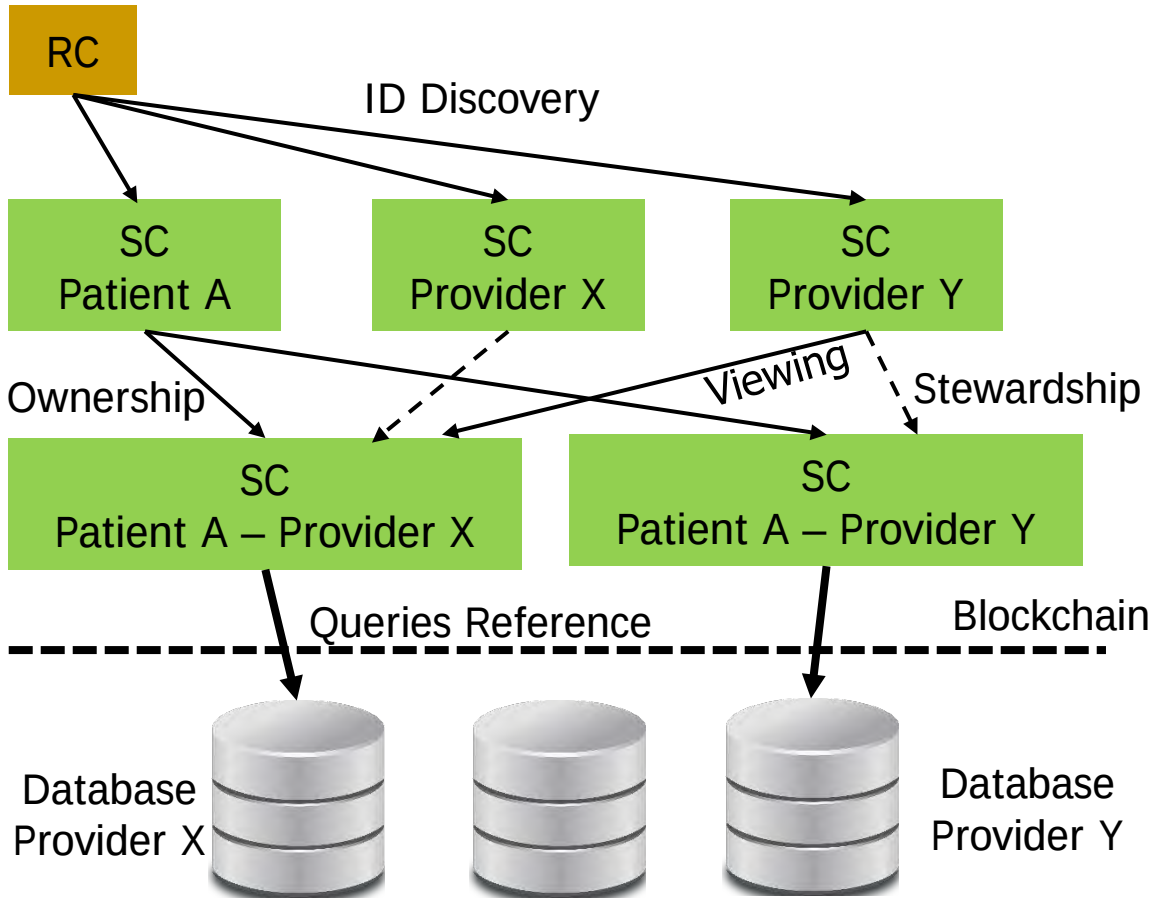
Source: C. Esposito, A. De Santis, G. Tortora, H. Chang and K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," IEEE Cloud Computing, vol. 5, no. 1, pp. 31-37, Jan./Feb. 2018.

MedRec -- Smart Contract



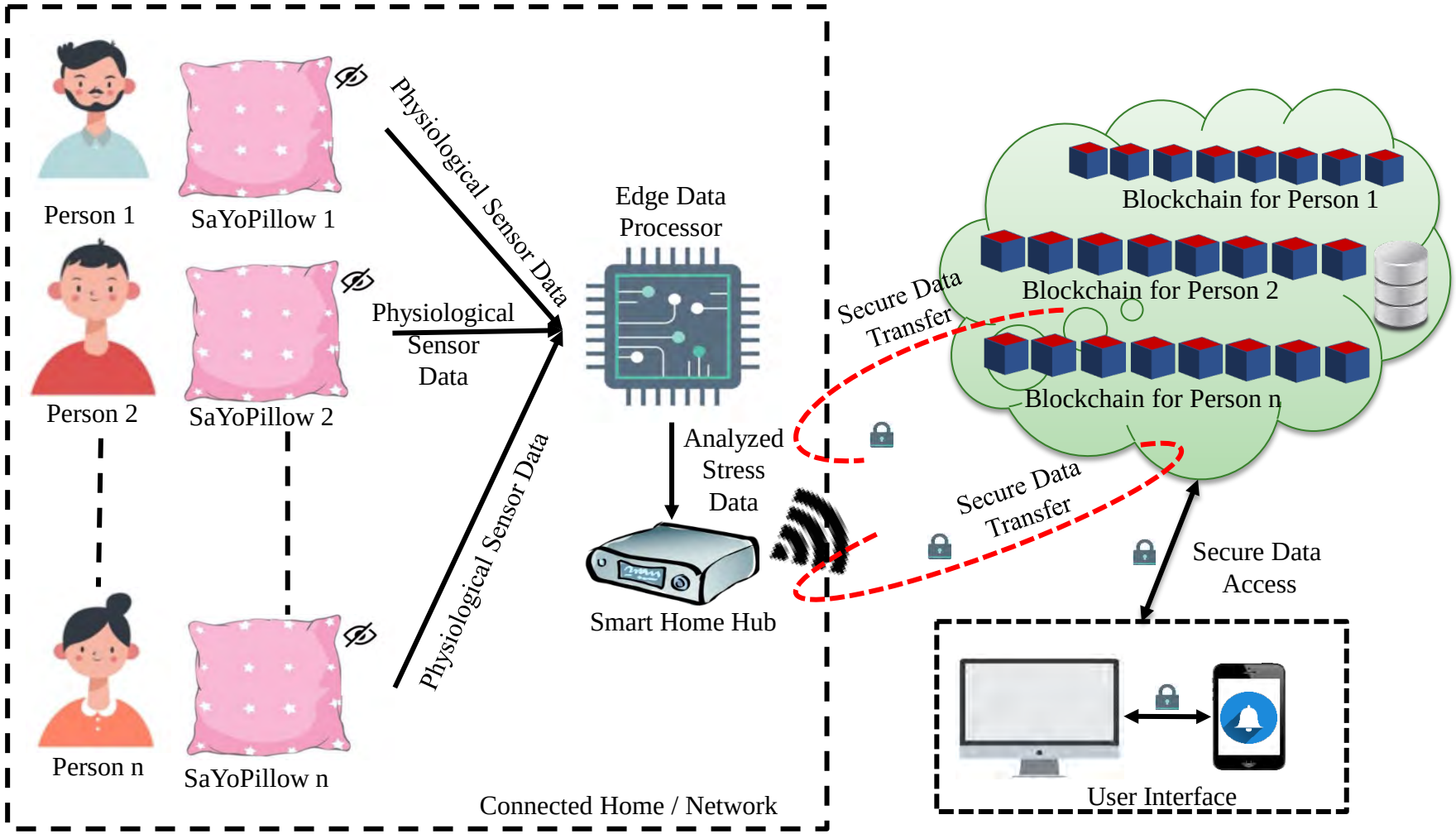






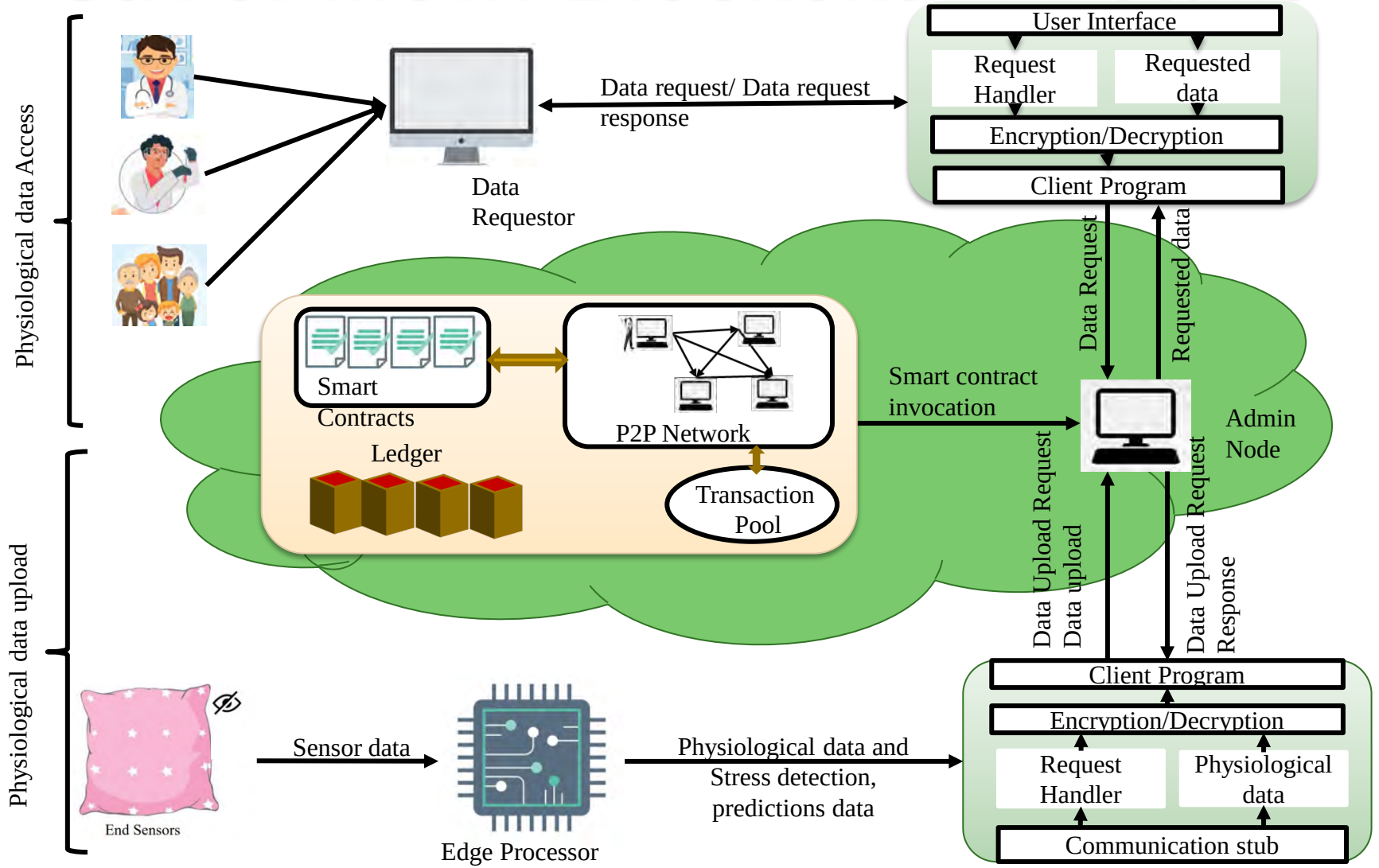
Source: A. Azaria, A. Ekblaw, Thiago Vieira and Andrew Lippman , “MedRec: Using Blockchain for Medical Data Access and Permission Management”, pp. 25--30, 2016.

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.

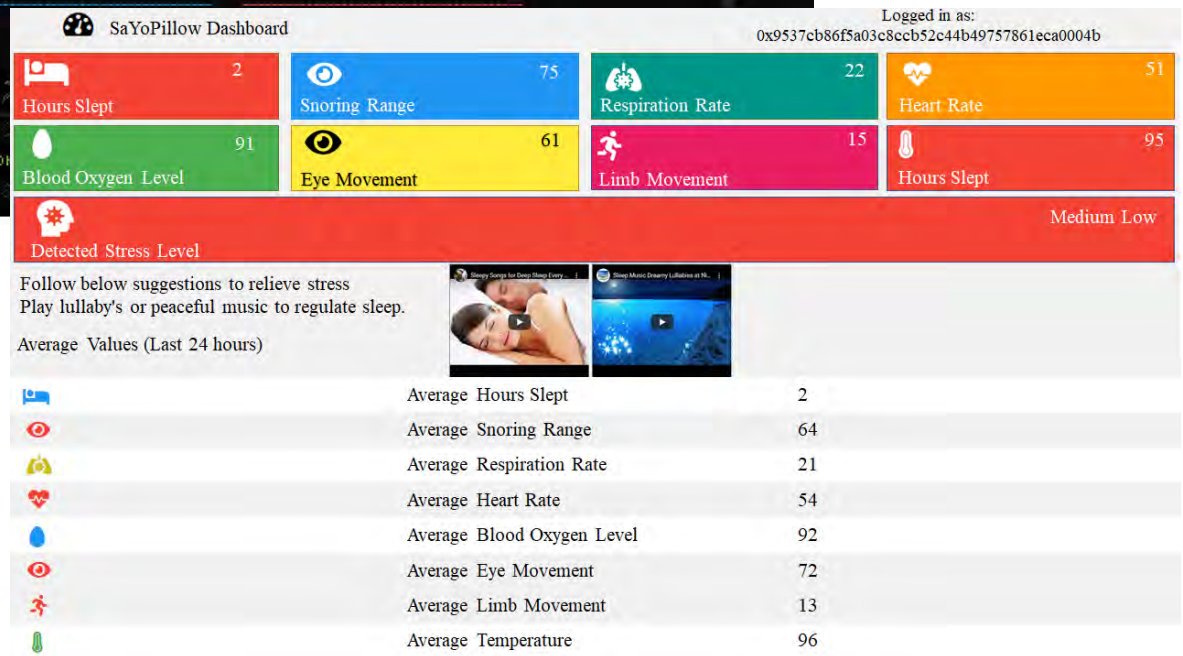
SaYoPillow: Blockchain Details



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

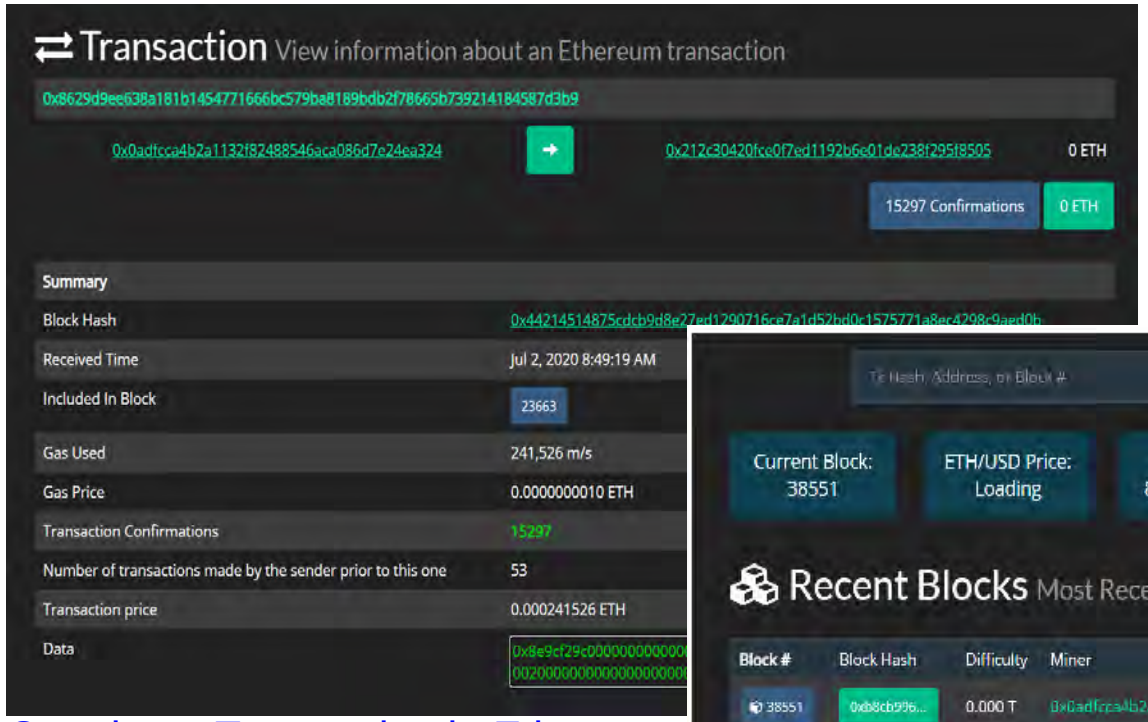
Ethereum Blockchain Status



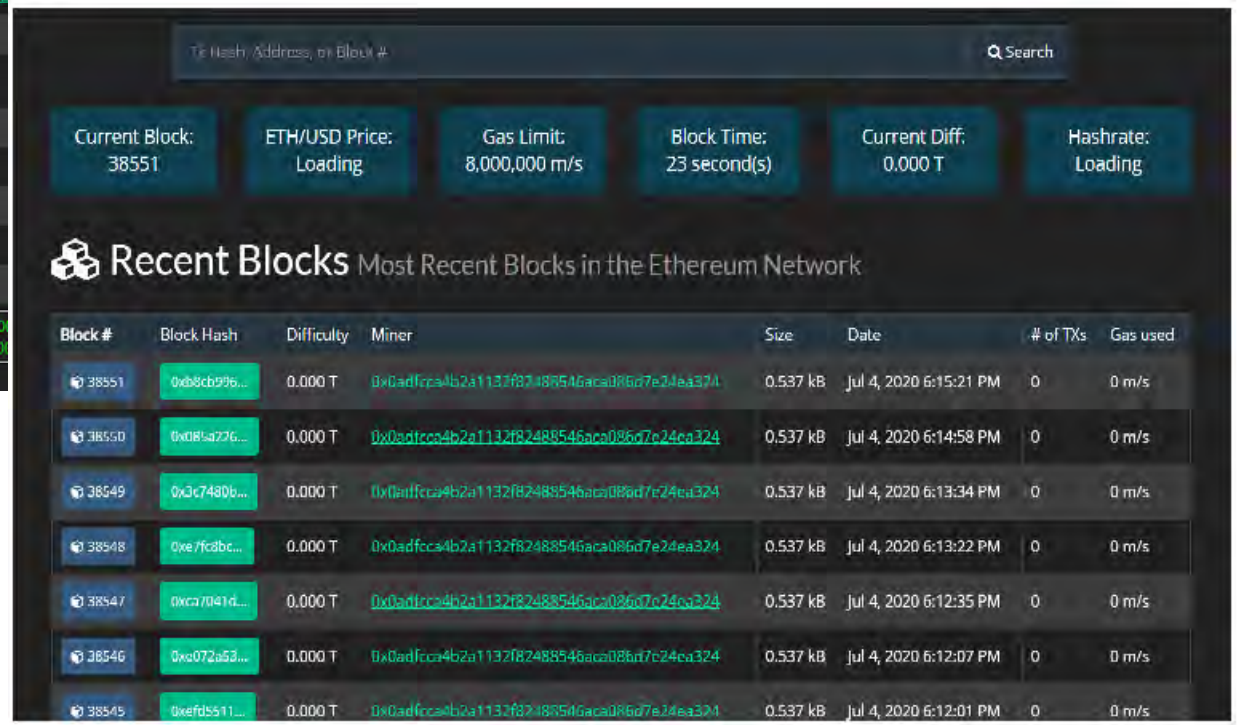
User Interface with Access

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

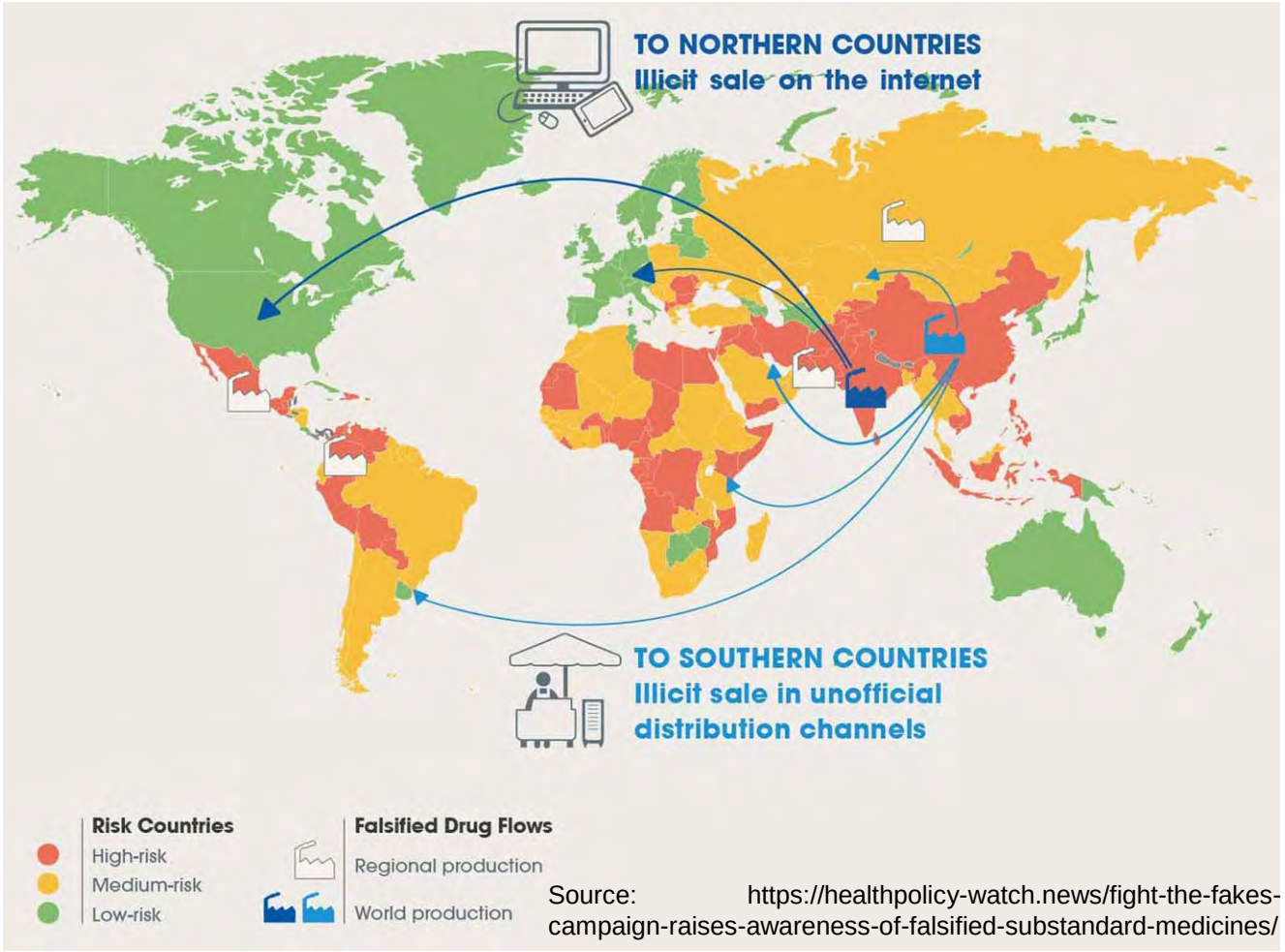
Source: L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, “SaYoPillow: A Blockchain-Enabled, Privacy-Assured Framework for Stress Detection, Prediction and Control Considering Sleeping Habits in the IoMT”, *arXiv Computer Science*, arXiv:2007.07377, July 2020, 38-pages.

Fake Medicine - Serious Global Issue

- It is estimated that close to $83 billion worth of counterfeit drugs are sold annually.
- One in 10 medical products circulating in developing countries are substandard or fake.
- In Africa: Counterfeit antimalarial drugs results in more than 120,000 deaths each year.
- USA has a closed drug distribution system intended to prevent counterfeits from entering U.S. markets, but it isn't foolproof due to many reason including illegal online pharmacy.

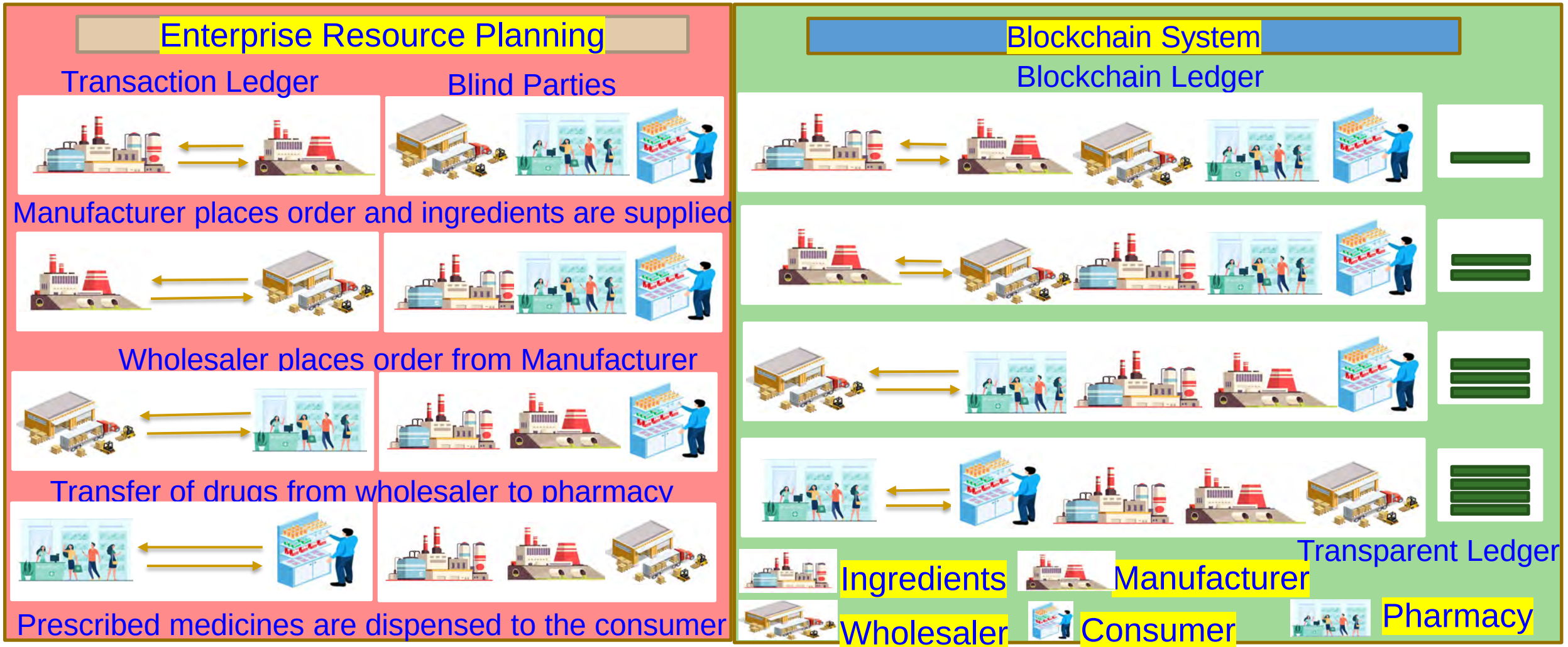
Source: https://fraud.org/fakerx/fake-drugs-and-their-risks/counterfeit-drugs-are-a-global-problem/

Source: https://allaboutpharmacovigilance.org/be-aware-of-counterfeit-medicine/



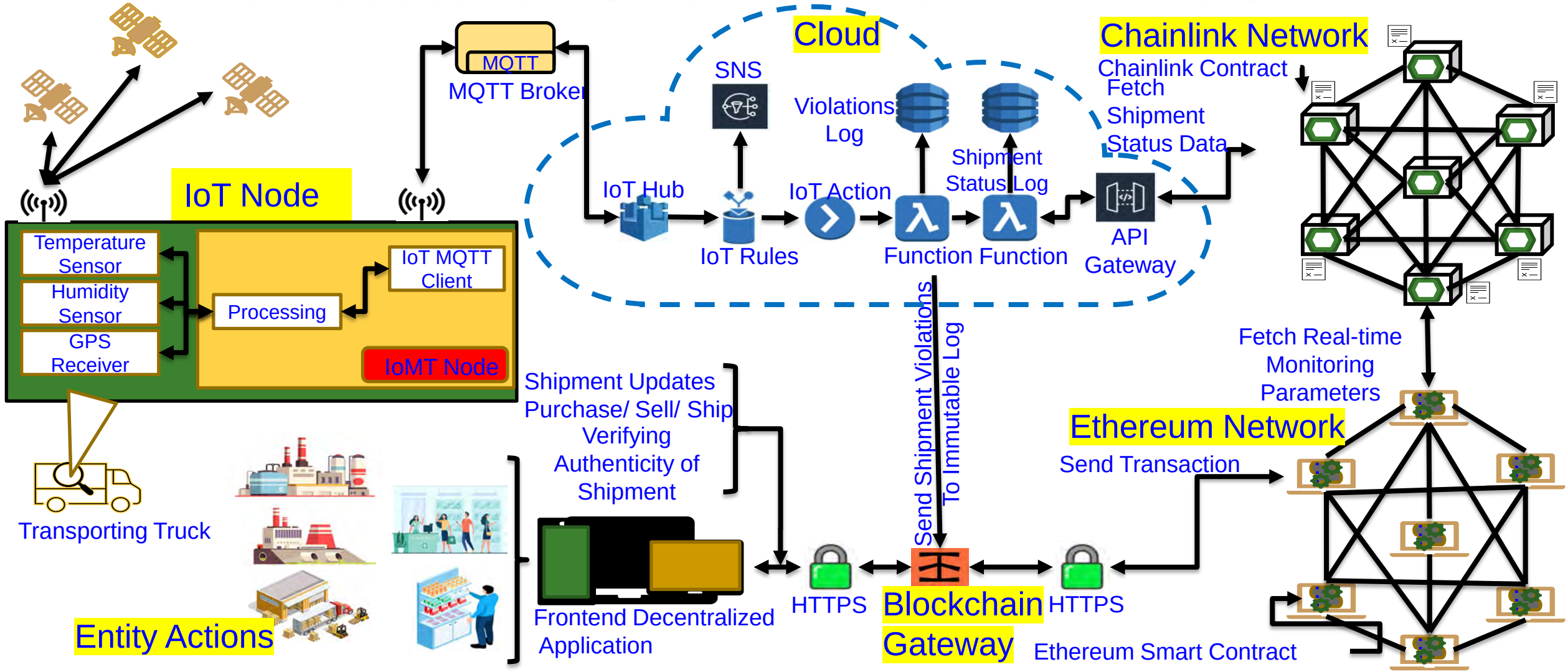
Source: https://healthpolicy-watch.news/fight-the-fakes-campaign-raises-awareness-of-falsified-substandard-medicines/

PharmaChain - Counterfeit Free Pharmaceutical



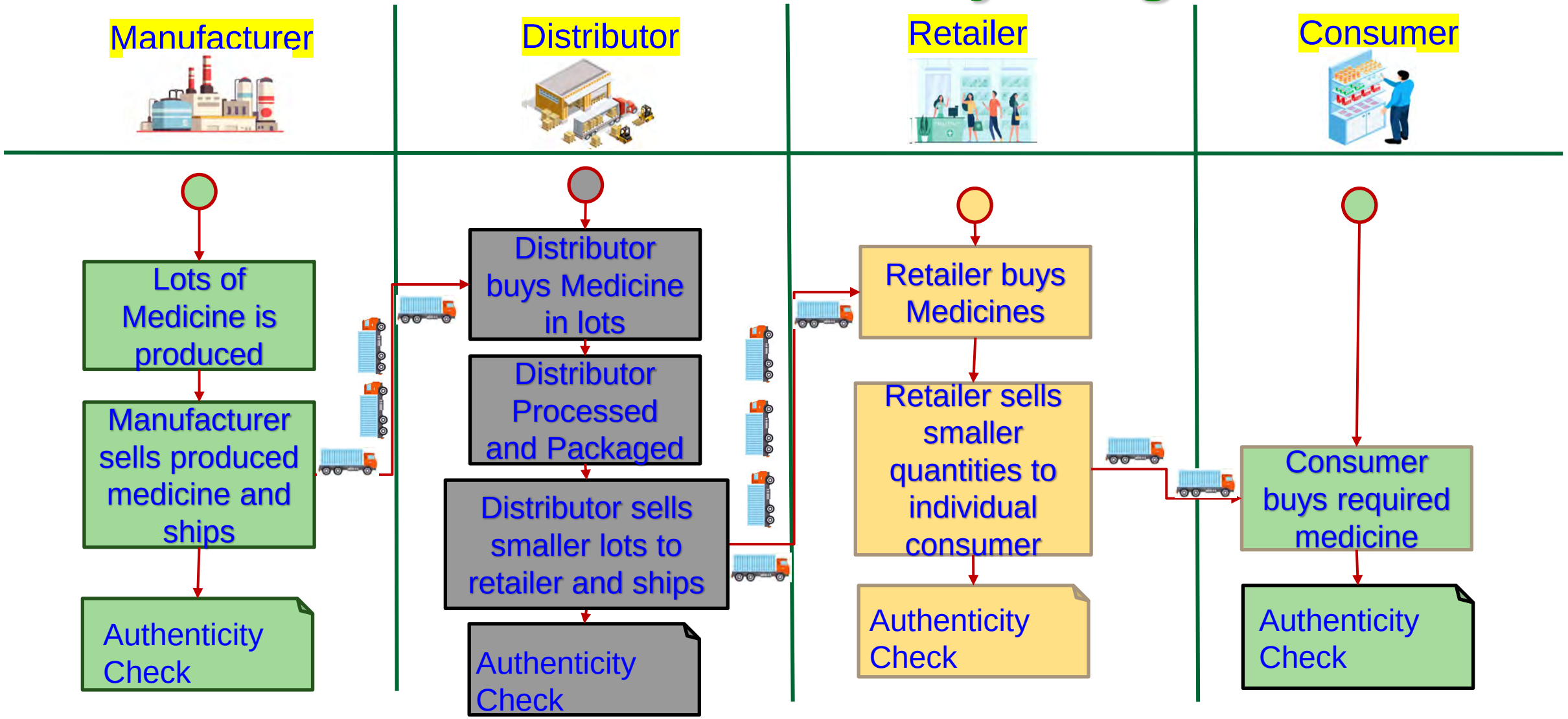
Source: A. K. Bapatla, **S. P. Mohanty**, E. Kougianos, D. Puthal, and A. Bapatla, "PharmaChain: A Blockchain to Ensure Counterfeit-Free Pharmaceutical Supply Chain", *IET Networks*, Vol. XX, No. YY, ZZ 2022, pp. Accepted on 24 June 2022, DOI: https://doi.org/10.1049/ntw2.12041. (Dataset for Research: GitHub)

Architectural Overview of PharmaChain



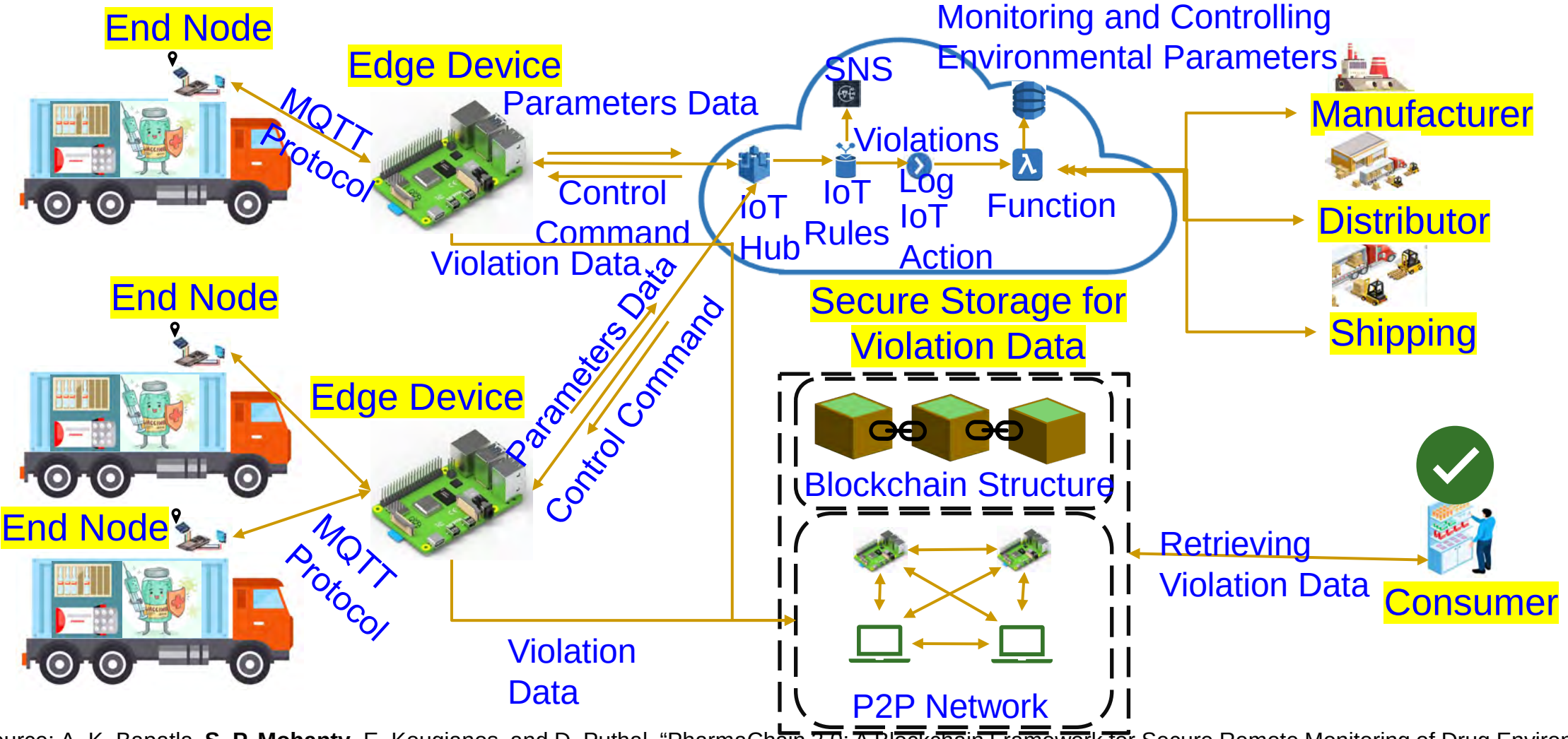
Source: A. K. Bapatla, **S. P. Mohanty**, E. Kougianos, D. Puthal, and A. Bapatla, "PharmaChain: A Blockchain to Ensure Counterfeit-Free Pharmaceutical Supply Chain", *IET Networks*, Vol. XX, No. YY, ZZ 2022, pp. Accepted on 24 June 2022, DOI: https://doi.org/10.1049/ntw2.12041. (Dataset for Research: GitHub)

PharmaChain Entity Diagram



Source: Bapatla, A.K., et al.: PharmaChain: a blockchain to ensure counterfeit-free pharmaceutical supply chain. IET Netw. 1– 24 (2022). https://doi.org/10.1049/ntw2.12041

PharmaChain 2.0 - Architecture Overview

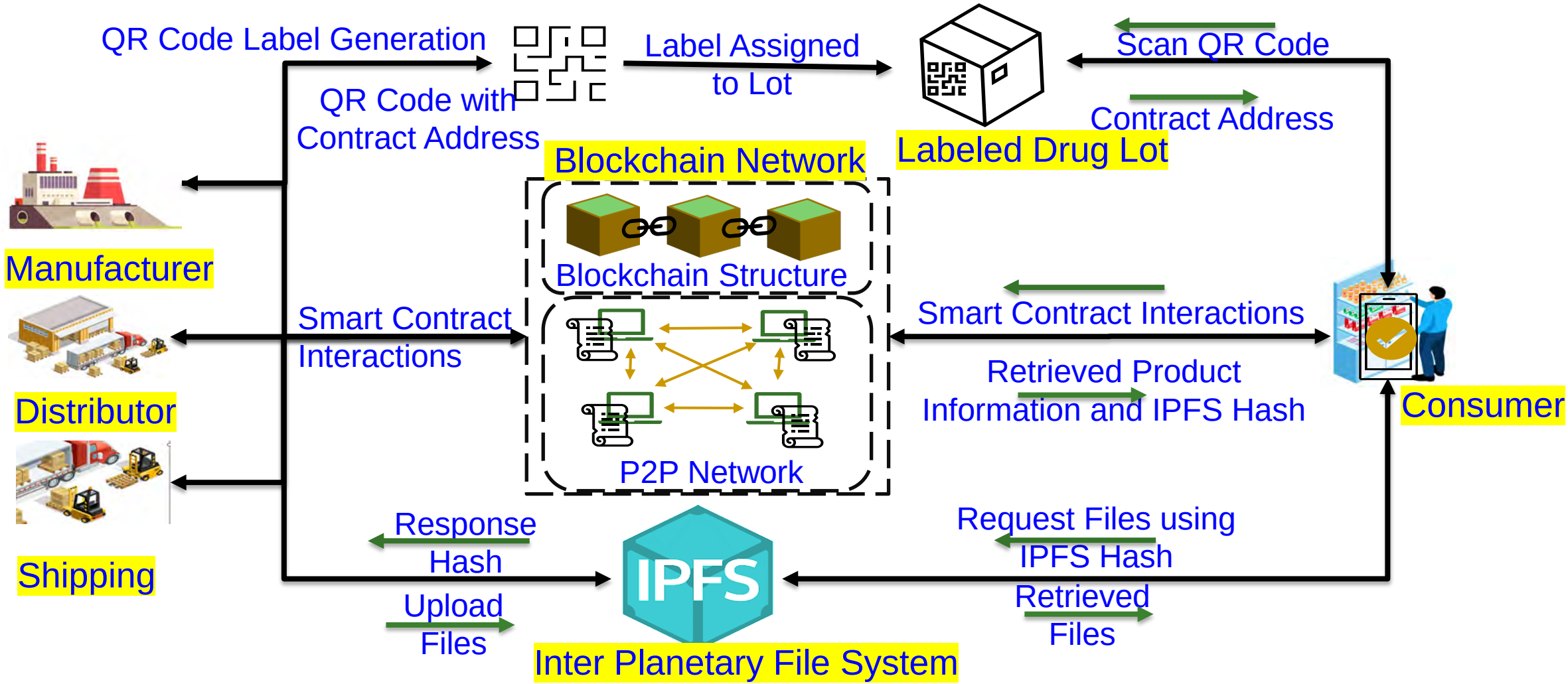


Source: A. K. Bapatla, **S. P. Mohanty**, E. Kougianos, and D. Puthal, "PharmaChain 2.0: A Blockchain Framework for Secure Remote Monitoring of Drug Environmental Parameters in Pharmaceutical Cold Supply Chain", in *Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES)*, 2022, pp. Accepted.

PharmaChain Versus PharmaChain 2.0

PharmaChain	PharmaChain 2.0
Tracking and Tracing in Pharmaceutical Supply Chain	Both Tracking & Tracing along with Monitoring and Controlling Temperature Excursions
Ethereum Blockchain	PoAh Consensus Based Blockchain (our EasyChain)
Proof-of-Authority (PoA) with less throughput compared to PoAh	Proof-of-Authentication (PoAh) with higher throughput
Private Blockchain with only nodes participating from Entities	Private Blockchain with only nodes participating from Entities
Not IoT friendly Consensus	IoT Friendly Consensus with less power and computations
Average transaction processing time is 5.6 sec.	Average transaction time has been improved significantly to 322.28 ms

PharmaChain 3.0 - Architectural Overview



Source: A. K. Bapatla, **S. P. Mohanty**, E. Kougianos, and D. Puthal, "PharmaChain 3.0: Blockchain Integrated Efficient QR Code Mechanism for Pharmaceutical Supply Chain", in *Proceedings of the OITS International Conference on Information Technology (OCIT)*, 2022, pp. Accepted.

PharmaChain 2.0 Versus PharmaChain 3.0

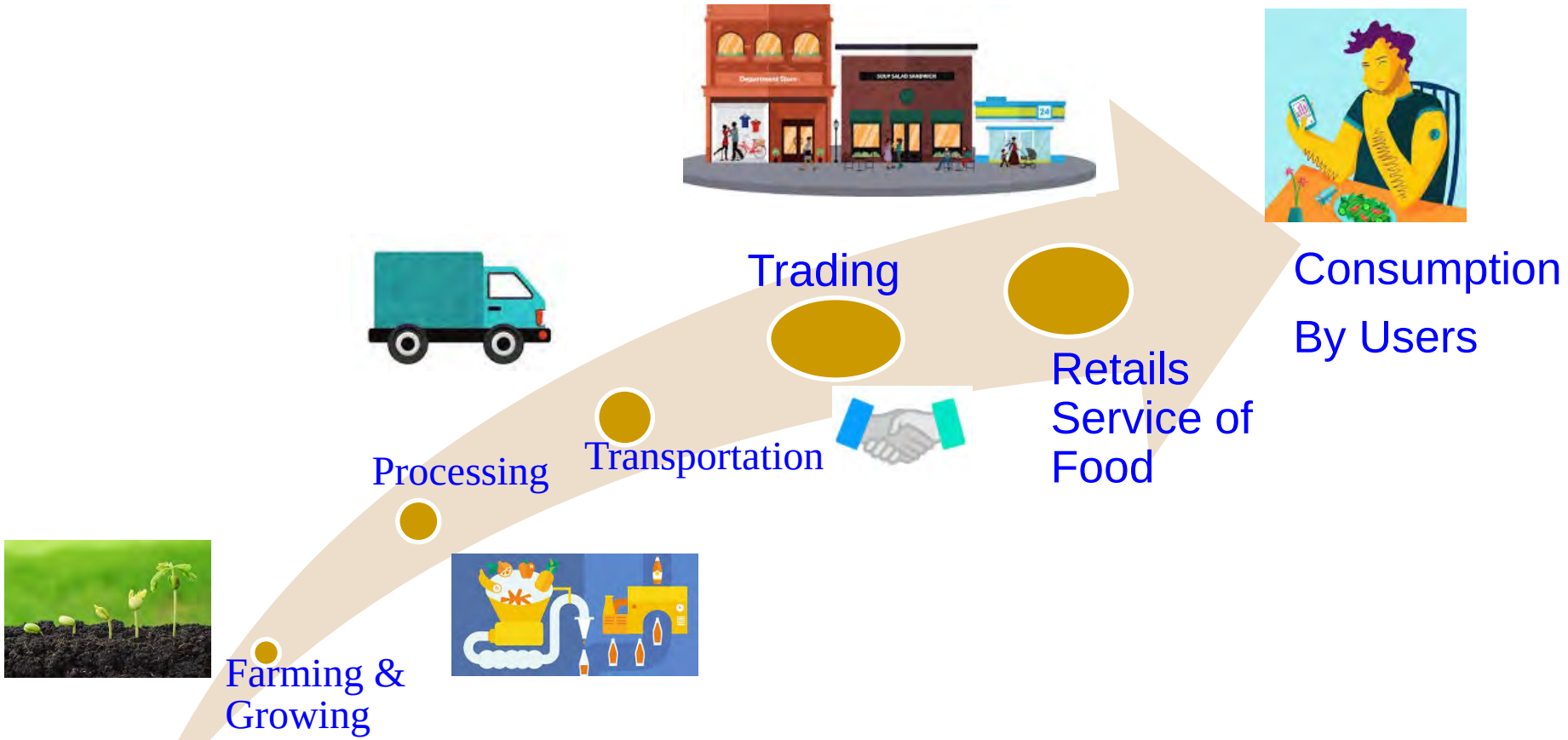
PharmaChain 2.0	PharmaChain 3.0
Both Tracking & Tracing along with Monitoring and Controlling Temperature Excursions	Integrating QR Code Mechanism for easy Tracking and Tracing and Drug Information
PoAh Consensus Based Blockchain (Our EasyChain)	Ethereum Blockchain into the CPS
Proof-of-Authentication (PoAh) with higher throughput	Proof-of-Stake (PoS) Consensus mechanism is used with lesser throughput than PoAh
Private Blockchain with only nodes participating from Entities	Private Blockchain with only nodes participating from Entities
IoT Friendly Consensus with less power and computations. Doesn't support smart Contracts.	P2P nodes are maintained by the entities and are computationally capable. No need for IoT-Friendly Consensus
The average transaction time is 322.28ms	The average Transaction time is 16.2 Sec
Less information storage capabilities	More information can be stored

PharmaChain 3.0 - Comparative Analysis

Works	Blockchain	Consensus Mechanism	Computational Needs	Openness	QR Code Integrated	Storage	Handling Large data
Crypto Cargo [11]	Ethereum	Proof-of-Work (PoW)	High	Public	No	On-Chain and Cloud	No
Kumar et.al. [9]	NA	NA	NA	NA	Yes	On-chain	No
PharmaChain [12]	Ethereum	Proof-of-Authority (PoA)	Low	Private	No	On-Chain and Cloud	No
PharmaChain 2.0	Our EasyChain	Proof-of-Authentication (PoAh)	Low	Private	No	On-Chain and Cloud	No
Current Solution (PharmaChain 3.0)	Ethereum	Proof-of-Stake (PoS)	Low	Private	Yes	On-Chain and off-Chain	Yes

Blockchain in Smart Agriculture

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.

Smart Agriculture - Food Supply Chain

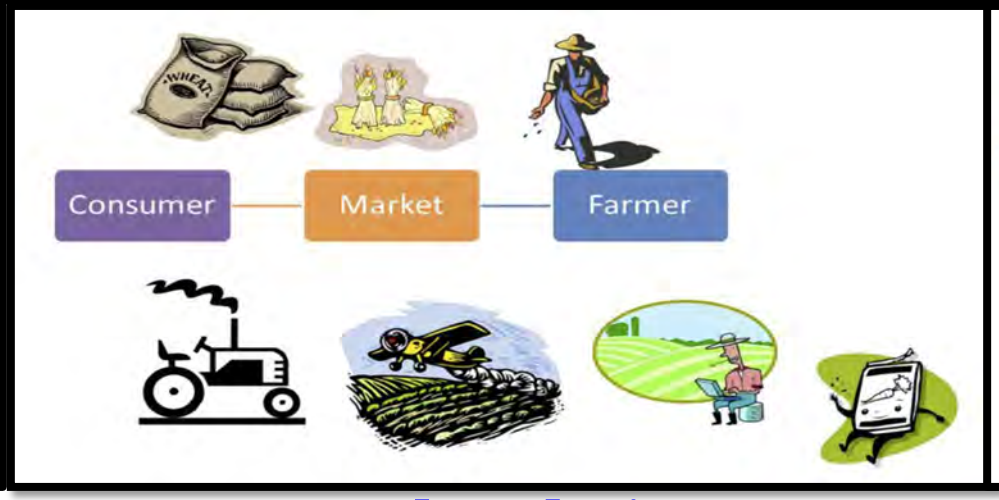
- Actors involved
  - Farmers
  - Shipping companies
  - Wholesalers
  - Retailers
  - Distributors
  - Grocerries

Roles of Blockchain in A-CPS

Visibility **Food Safety** **Provenance** **Traceability** **Farm Supervision**



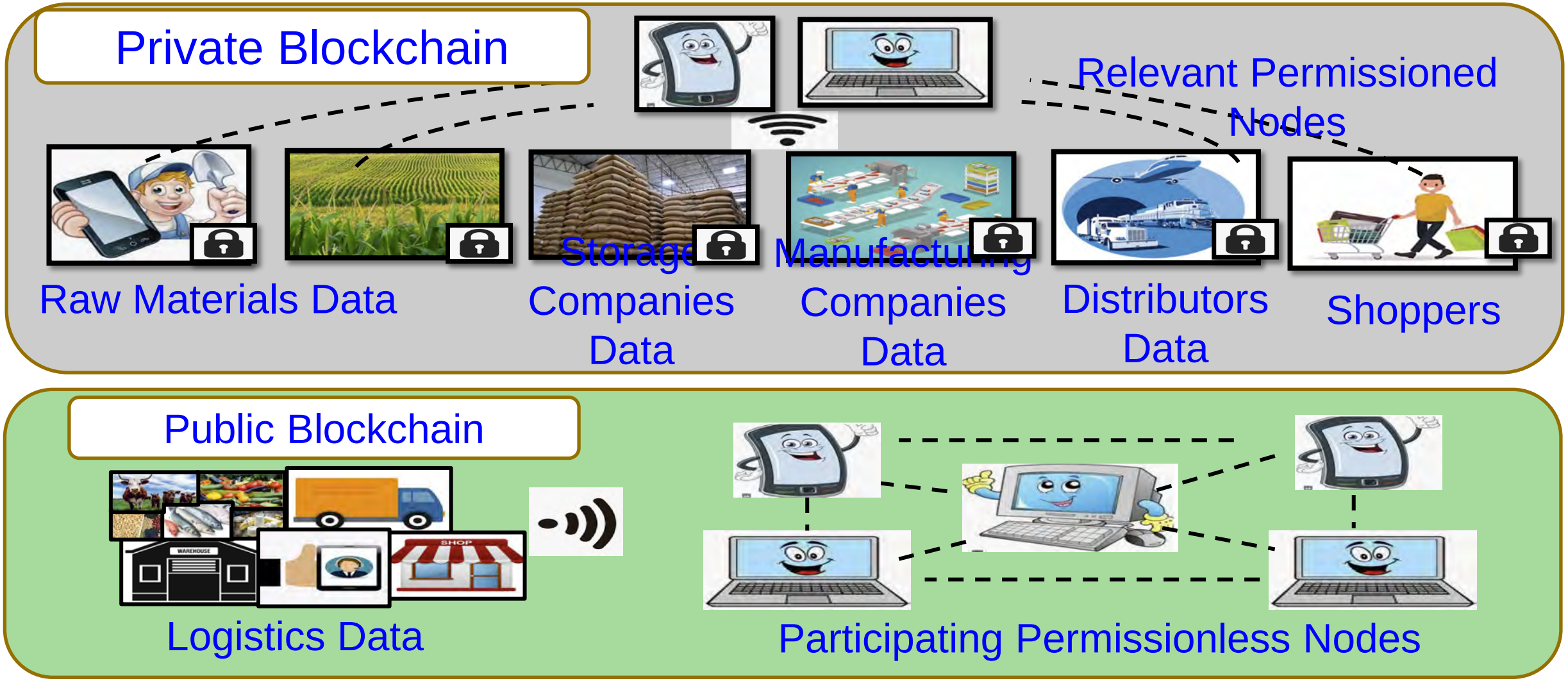


Land Registration **Supply Chain** **Farmer Incentives**

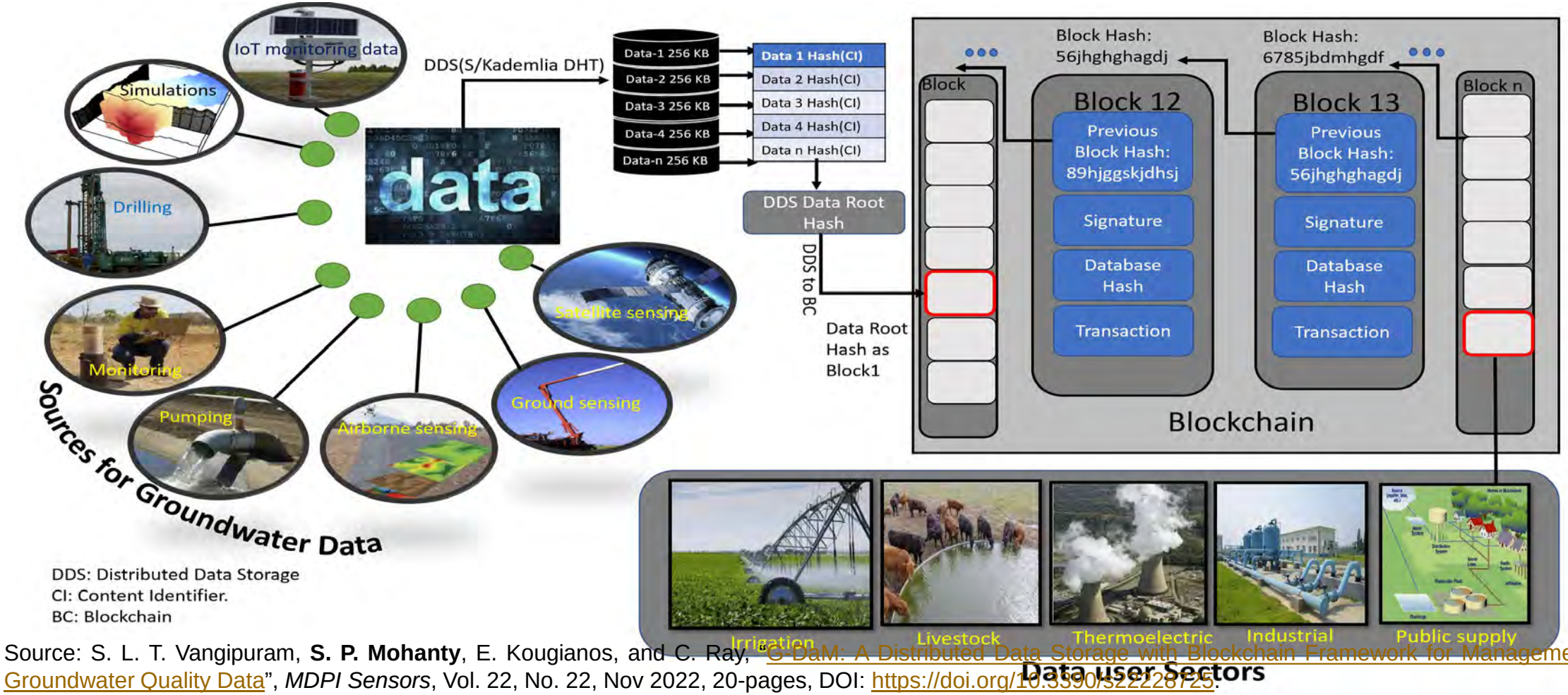
Source: S. L. T. Vangipuram, **S. P. Mohanty**, E. Kougianos, and C. Ray, "agroString: Visibility and Provenance through a Private Blockchain Platform for Agricultural Dispense towards Consumers", *MDPI Sensors*, Vol. 22, No. 21, Oct 2022, 20-pages, DOI: https://doi.org/10.3390/s22218227.

Roles of Blockchain in A-CPS - Private Vs Public



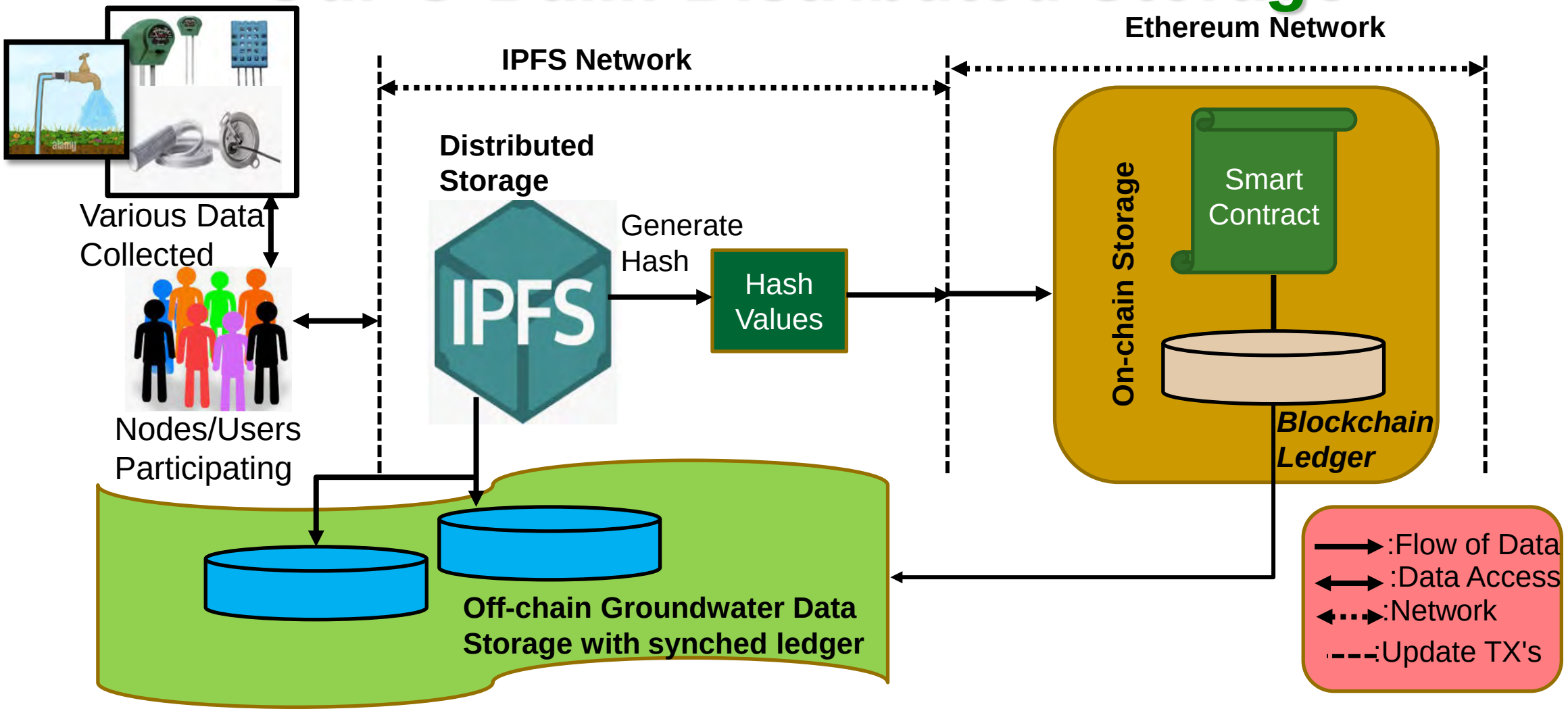
Source: S. L. T. Vangipuram, **S. P. Mohanty**, E. Kougianos, and C. Ray, "agroString: Visibility and Provenance through a Private Blockchain Platform for Agricultural Dispense towards Consumers", *MDPI Sensors*, Vol. 22, No. 21, Oct 2022, 20-pages, DOI: https://doi.org/10.3390/s22218227.

Our G-DaM: A Blockchain Framework for Management of Groundwater Quality Data



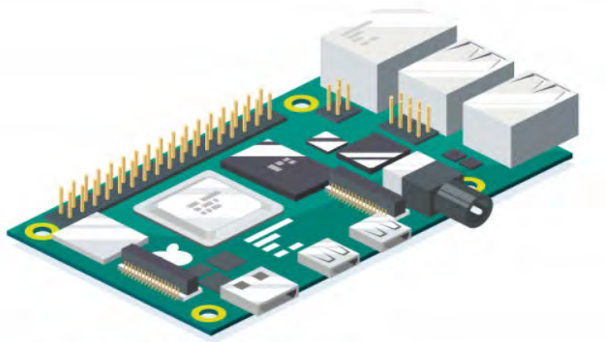
Source: S. L. T. Vangipuram, **S. P. Mohanty**, E. Kougianos, and C. Ray, "G-DaM: A Distributed Data Storage with Blockchain Framework for Management of Groundwater Quality Data", *MDPI Sensors*, Vol. 22, No. 22, Nov 2022, 20-pages, DOI: https://doi.org/10.3390/s22228725.

Our G-DaM: Distributed Storage

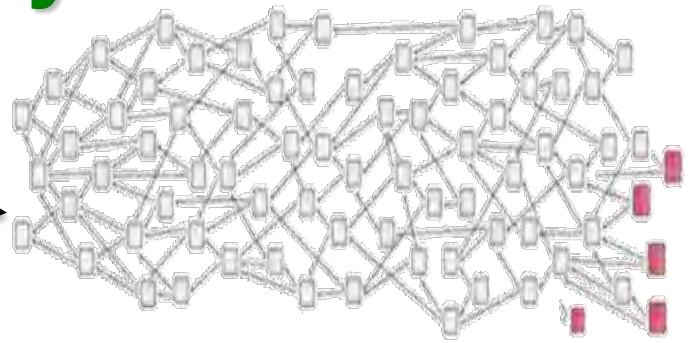


Source: S. L. T. Vangipuram, **S. P. Mohanty**, E. Kougianos, and C. Ray, "G-DaM: A Distributed Data Storage with Blockchain Framework for Management of Groundwater Quality Data", *MDPI Sensors*, Vol. 22, No. 22, Nov 2022, 20-pages, DOI: https://doi.org/10.3390/s22228725.

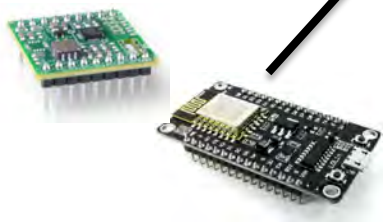
Our sFarm: A Distributed Ledger based Remote Crop Monitoring System



Transaction generation



Raspberry Pi 4
Model B



DHT11 and Node MCU

Dielectric Soil moisture sensor and Node MCU

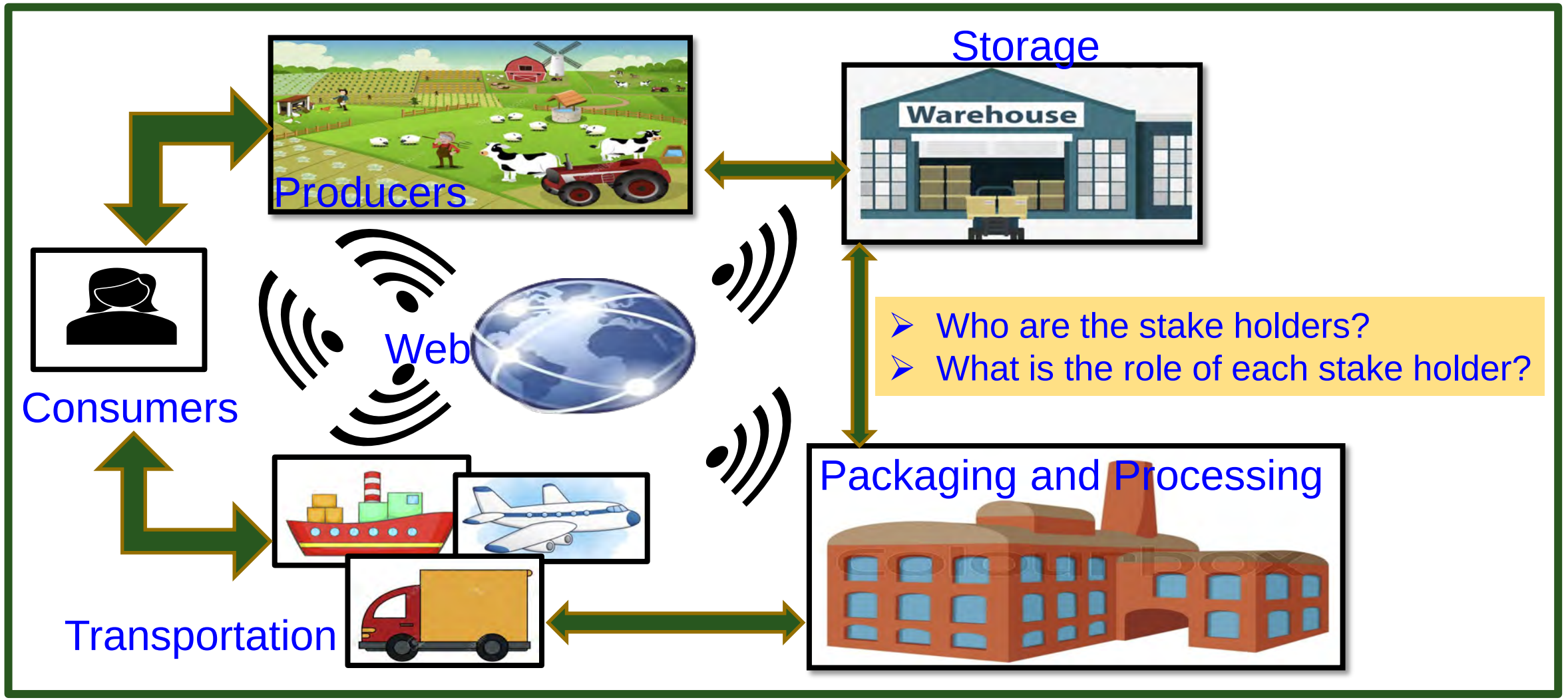
Monitoring Dashboard

Farmers

pH Sensor and Node MCU

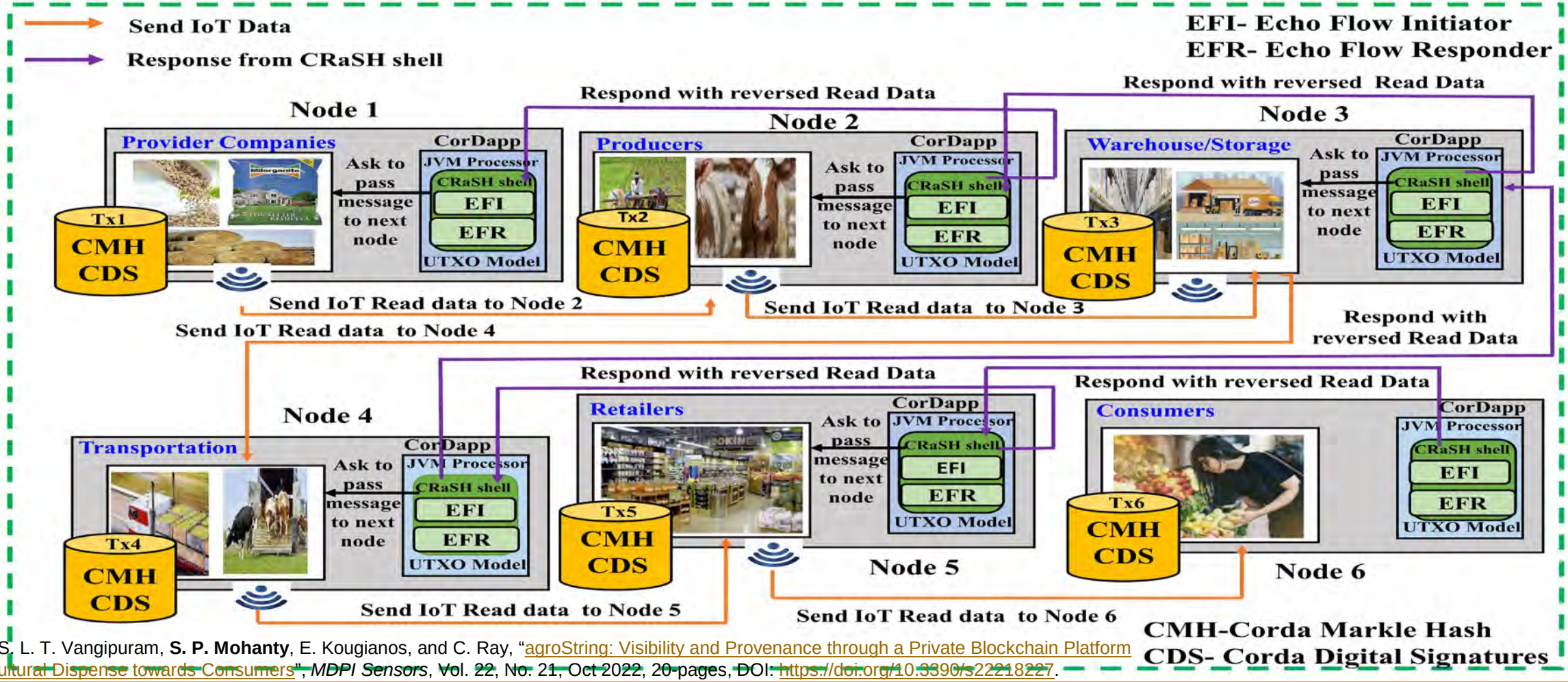
Source: A. K. Bapatla, **S. P. Mohanty**, and E. Kougianos, "sFarm: A Distributed Ledger based Remote Crop Monitoring System for Smart Farming", in *Proceedings of the 4th IFIP International Internet of Things Conference (IFIP-IoT)*, 2021, pp. 13—31, DOI: https://doi.org/10.1007/978-3-030-96466-5_2

Agriculture Supply Chain



Source: A. Mitra, S. L. T. Vangipuram, A. K. Bapatla, V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, and C. Ray, "Everything You wanted to Know about Smart Agriculture", *arXiv Computer Science*, arXiv:2201.04754, Jan 2022, 45-pages.

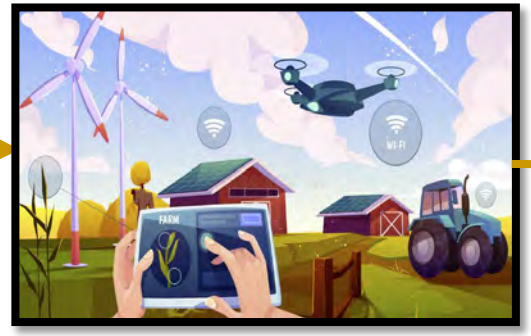
Our agroString: Visibility and Provenance in Agriculture through a Private Blockchain



Source: S. L. T. Vangipuram, **S. P. Mohanty**, E. Kougianos, and C. Ray, "agroString: Visibility and Provenance through a Private Blockchain Platform for Agricultural Dispense towards Consumers", *MDPI Sensors*, Vol. 22, No. 21, Oct 2022, 20-pages, DOI: https://doi.org/10.3390/s22218227.

Impact of Agriculture Finance on Farm Yield

Value Chain Financing



- Use of New Technology
- Improved access to banking services
- Adopting new technology easily

- Increased crop production
- Income is Increased

Agricultural Finance

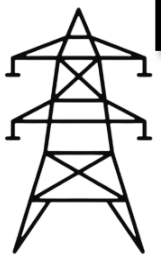
Direct Financing

- Use of Traditional Tools
- Separation from the financial Services
- Isolation from financing

- Decreased crop production
- Low Yield
- Reduced Income

Source: S. L. T. Vangipuram, **S. P. Mohanty**, E. Kougianos, and C. Ray, "agroString: Visibility and Provenance through a Private Blockchain Platform for Agricultural Dispense towards Consumers", *MDPI Sensors*, Vol. 22, No. 21, Oct 2022, 20-pages, DOI: https://doi.org/10.3390/s22218227.

Our IncentiveChain: Blockchain Crypto-Incentive for Effective Usage of Power and Water in Smart Farming



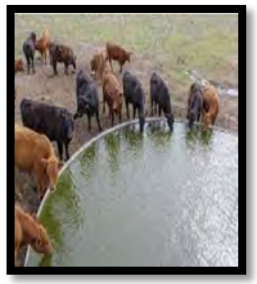
Electricity

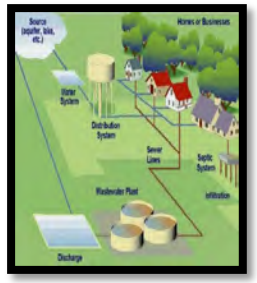
Water

Wastage reasons

Climate Change

Overpopulation

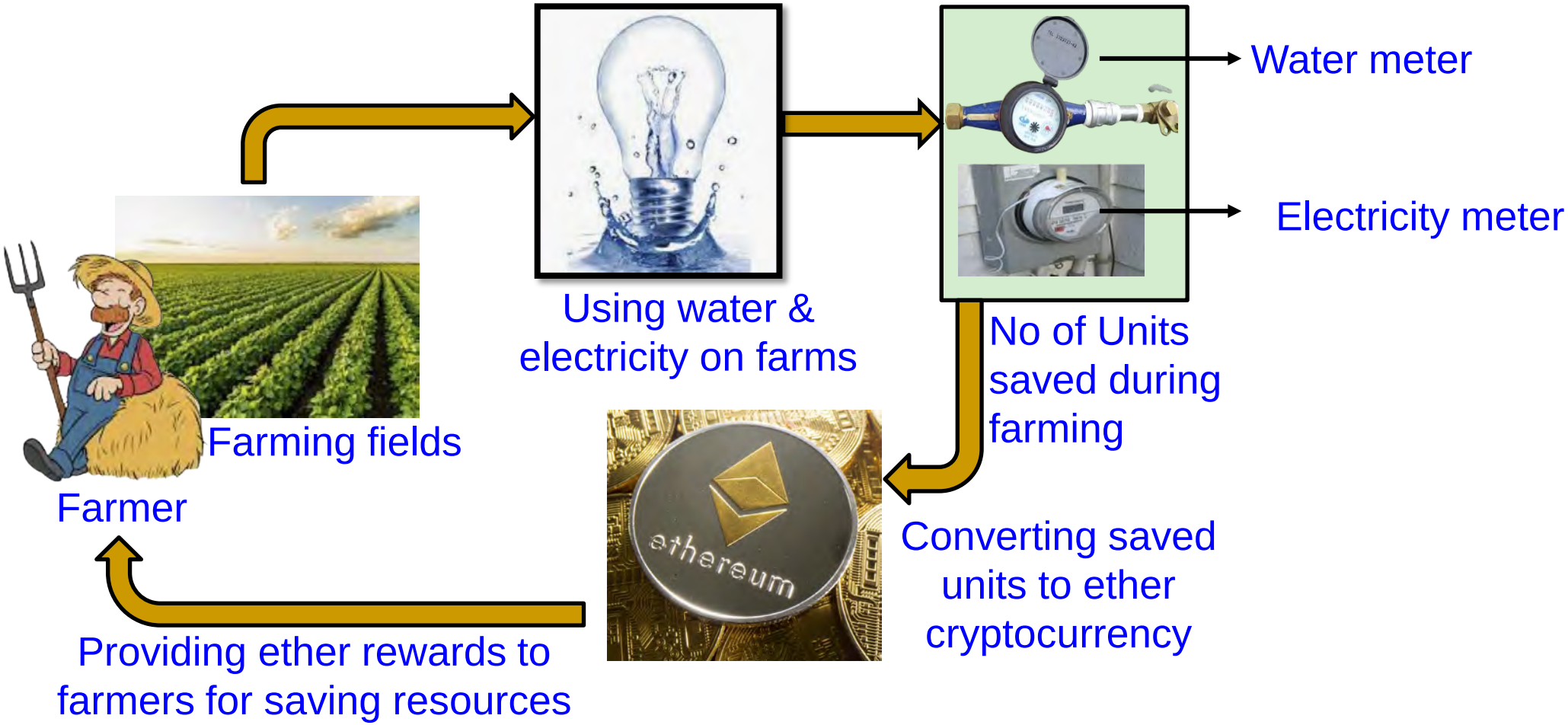




- Water & energy use in different domains.
- Present Scenario: Electricity & water wastage
- Farming as main source for water and energy wastage.
- Recognizing farmers as main entity in farming.

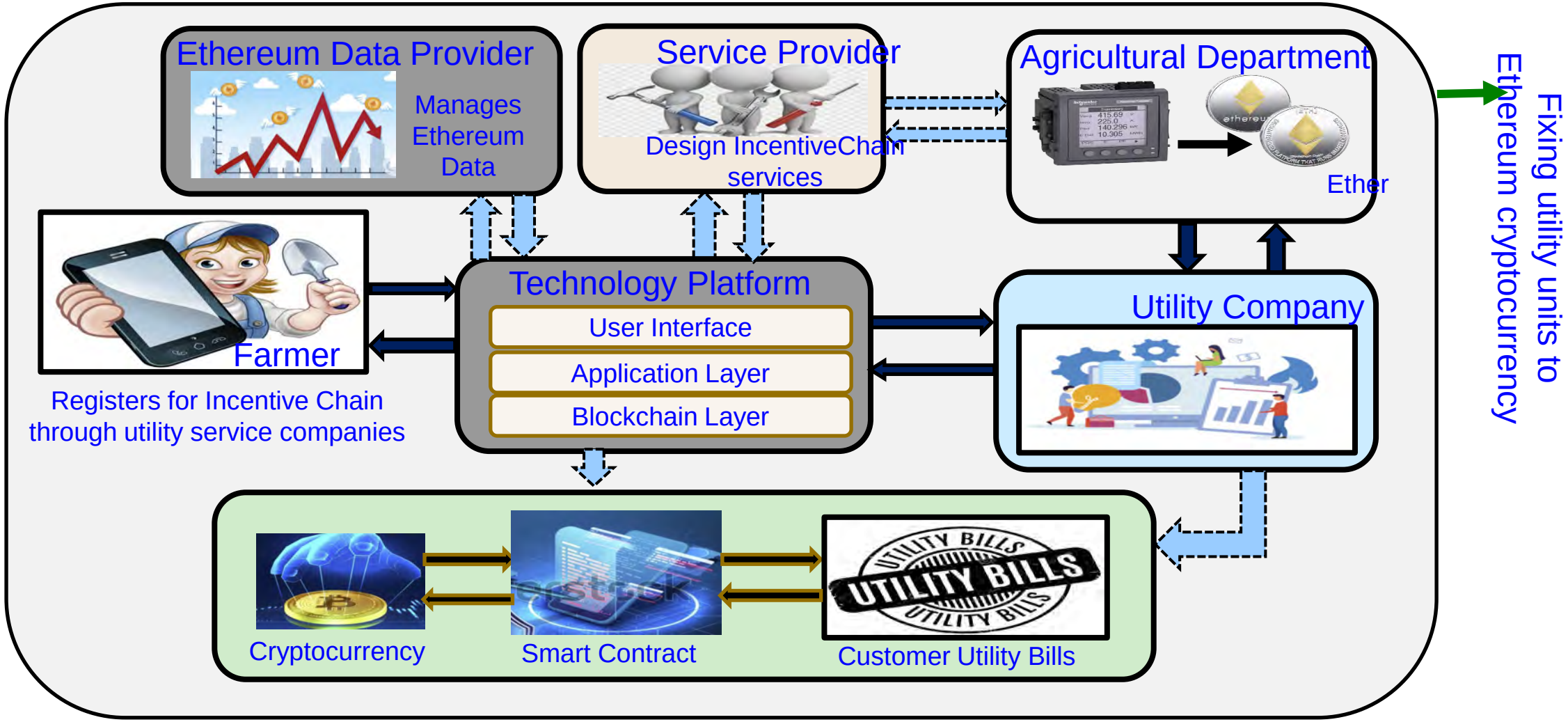
Source: S. L. T. Vangipuram, **S. P. Mohanty**, and E. Kougianos, "IncentiveChain: Blockchain Crypto-Incentive for Effective Usage of Power and Water in Smart Farming", in *Proceedings of the OITS International Conference on Information Technology (OCIT)*, 2022, pp. Accepted.

Our IncentiveChain: The Idea



Source: S. L. T. Vangipuram, **S. P. Mohanty**, and E. Kougianos, "IncentiveChain: Blockchain Crypto-Incentive for Effective Usage of Power and Water in Smart Farming", in *Proceedings of the OITS International Conference on Information Technology (OCIT)*, 2022, pp. Accepted.

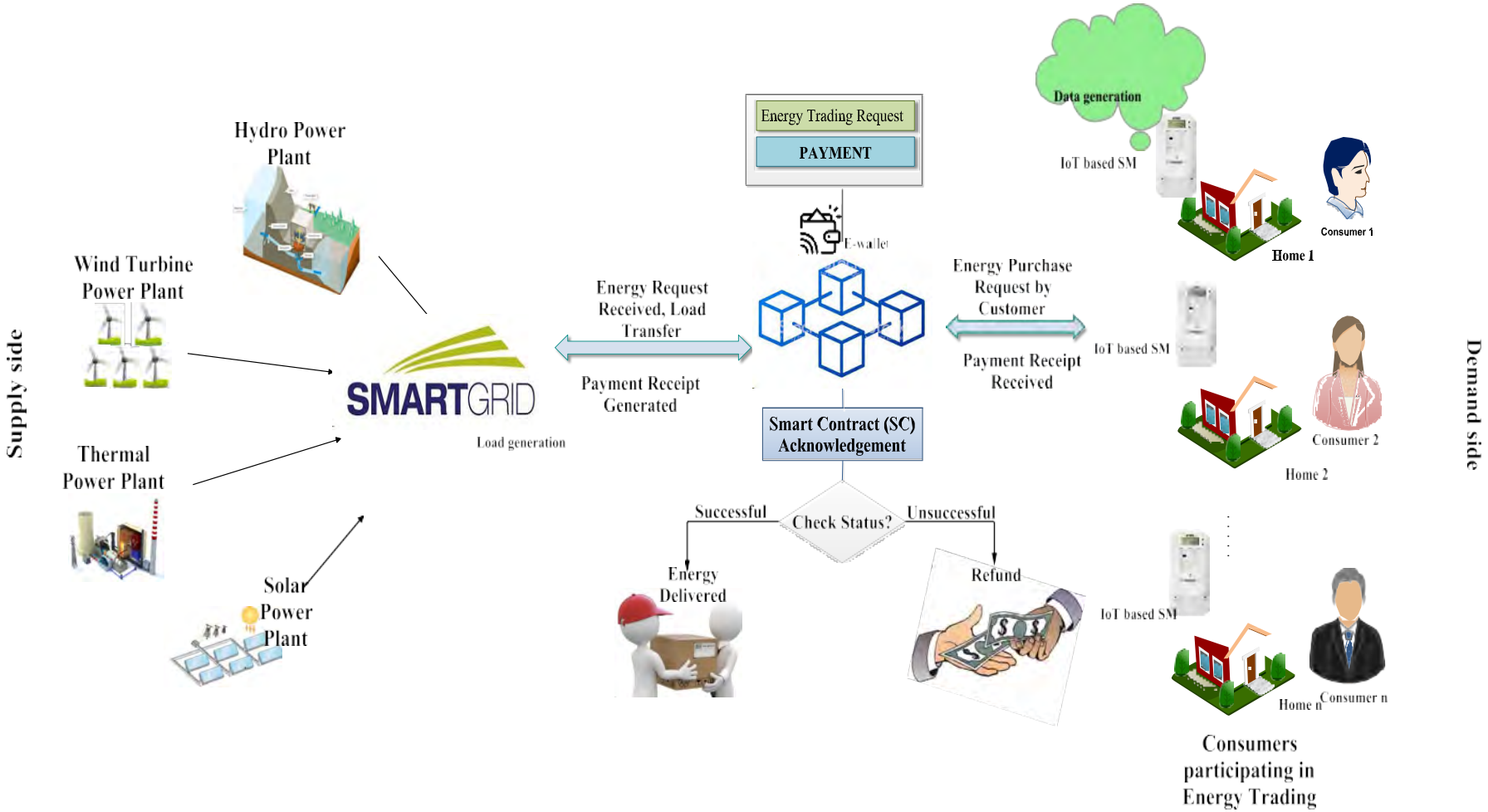
Our IncentiveChain: Architecture



Source: S. L. T. Vangipuram, **S. P. Mohanty**, and E. Kougianos, "IncentiveChain: Blockchain Crypto-Incentive for Effective Usage of Power and Water in Smart Farming", in *Proceedings of the OITS International Conference on Information Technology (OCIT)*, 2022, pp. Accepted.

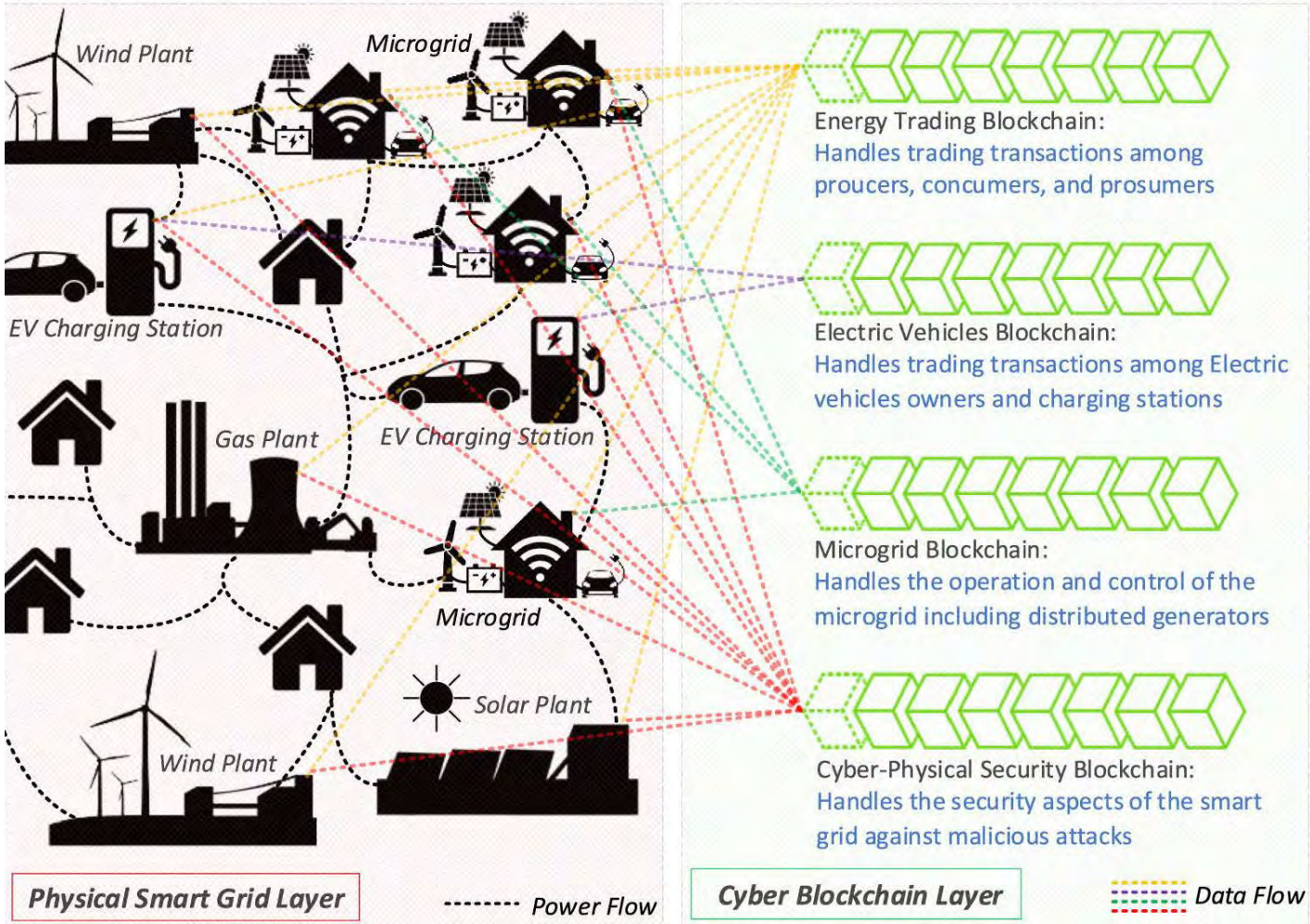
Blockchain for Smart Energy

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.

Blockchain in Smart Transportations

Source : greencarreports.com

Smart Transportation

2014: 1.2 Billion vehicles on the worlds' Roads.

2035: 2 Billion vehicles on the worlds' Roads.

Observing the figures above, we will recognize that there will be a problem in the future.

Smart transportation emerged with the advancement of technology.

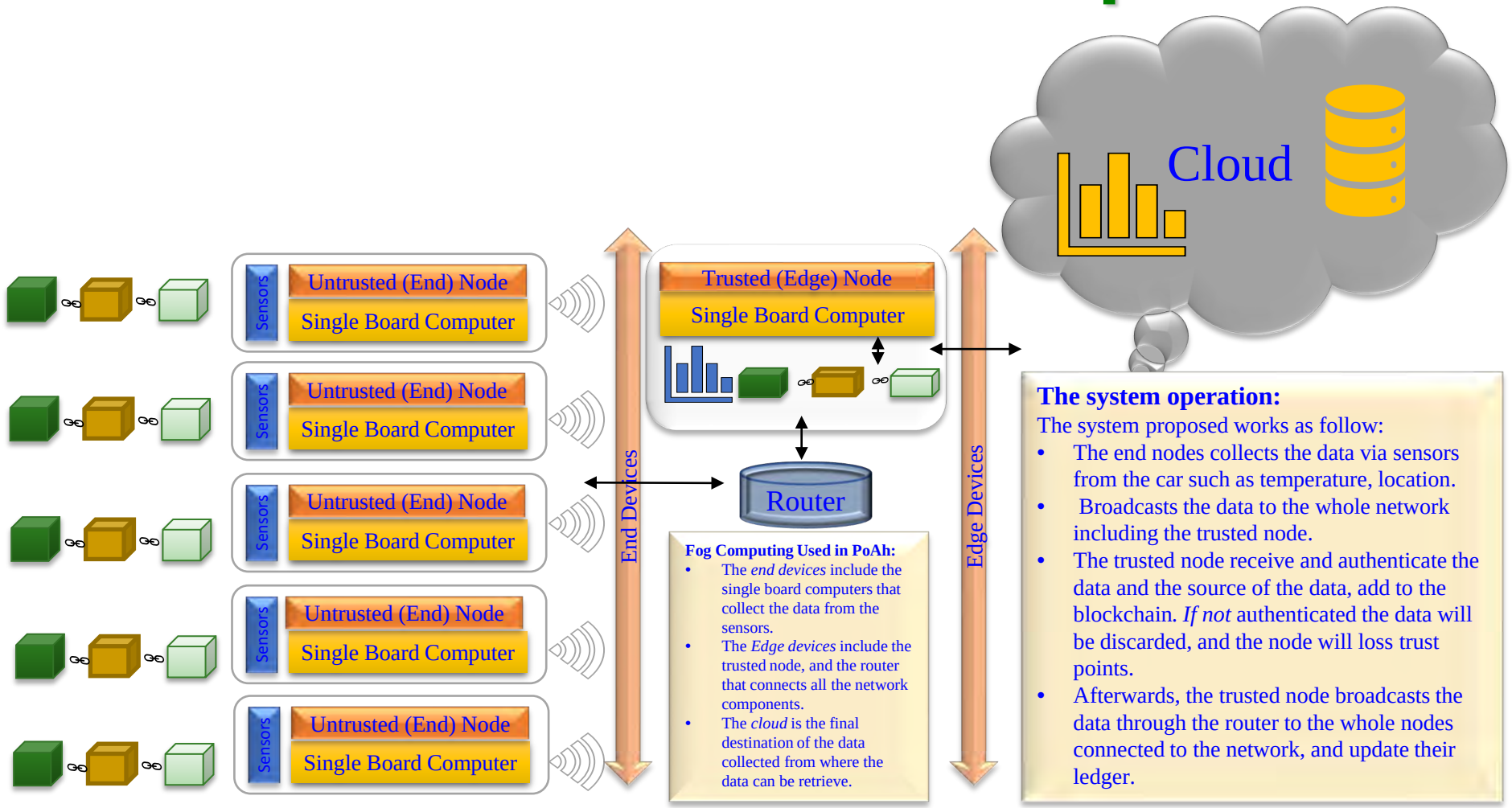
Blockchain could be used as a platform for smart transportations.

Smart Transportation

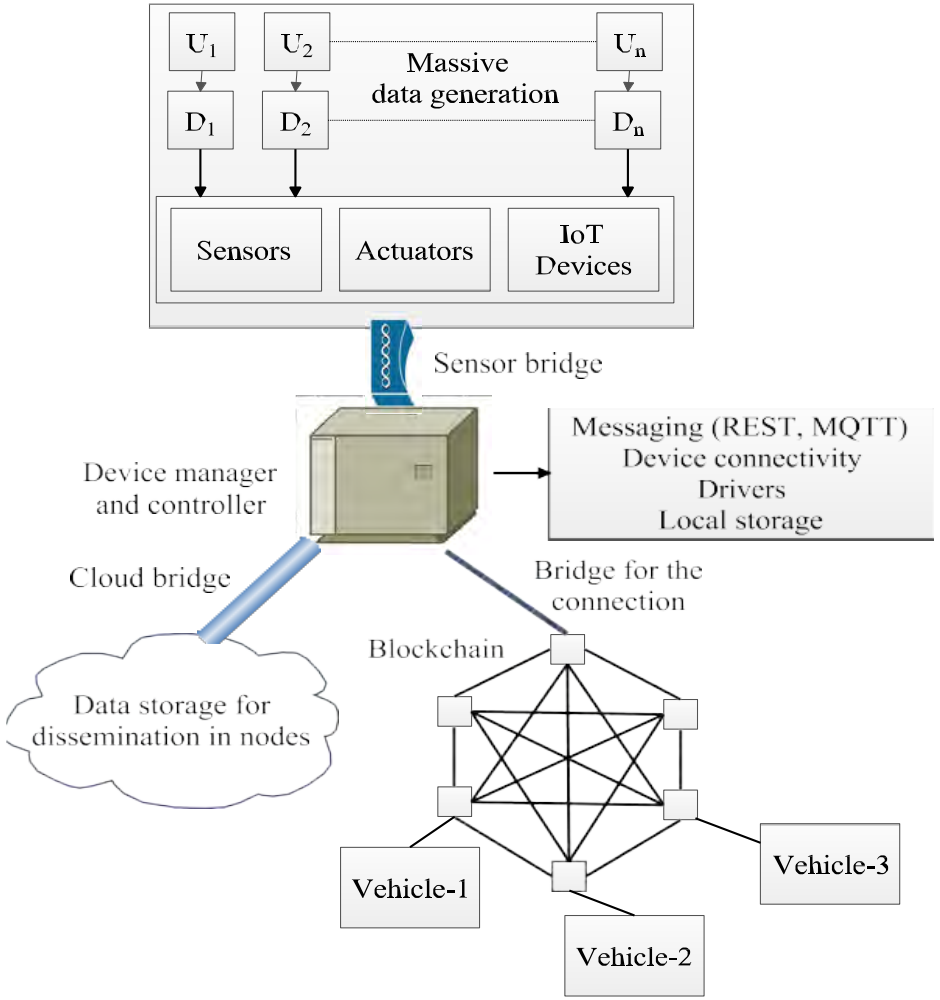
- Applications meet the definition of blockchain and needs the characteristics of blockchain in smart transportation domain:
  - Car History.
  - Car locations.
  - Car Trace.
  - Car Training.
  - Car Rentals.
  - Car Ownership.
  - Blockchain could be used in the communication between cars, car – building.

7/10/2023 310

Blockchain in Smart Transportation

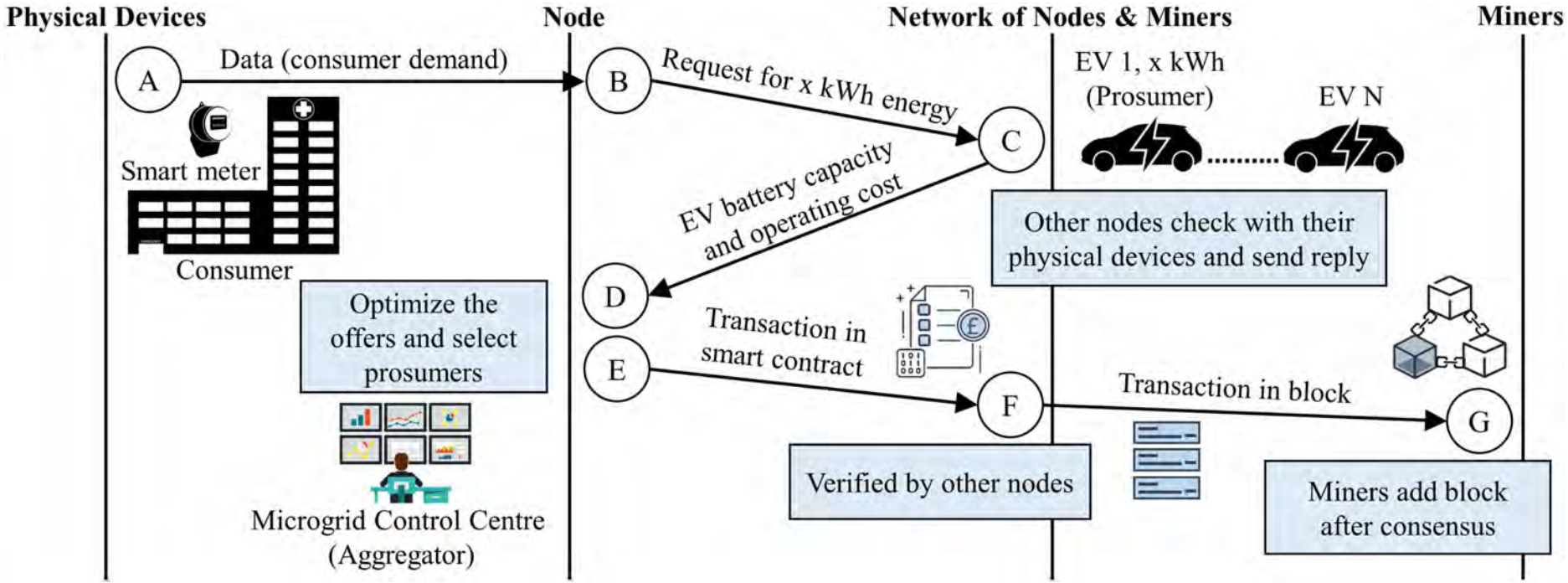


Blockchain in Smart Transportation



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.

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

ASIC Miner

Image source: https://www.bitdegree.org/tutorials/what-is-bitcoin-mining/

Hardware wallets

- This stores users private key
  - Private keys are stored in protected area of microcontroller
  - Immune to computer viruses like in software wallets
- Can work with multiple blockchains simultaneously like Ethereum, bitcoin, and other alt coins and recovered with only one single phrase
- A pin or phrase is used to extract keys
- Small and portable device giving access to Dapps
- Provides wallet to wallet transfers without exchange accounts

Hardware wallets

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

Security risks in Hardware wallets

- Relies on hardware random number generator which may not provide sufficient randomness
- Security due to firmware bugs
- Hardware backdoors during manufacturing
- Examples:
  - Trezor One
  - Keepkey
  - Opendime
  - Coldcard
  - CoolWallet
  - BlochsTech card etc.

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

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

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

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

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

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

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

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

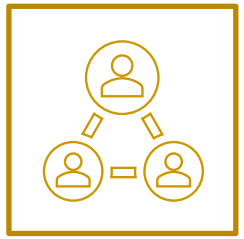
- Blockchain validation is different from blockchain consensus
- Any full-node can validate a transaction
- There is no incentive for validation, except security which is not a motivation
- Miners will be validators in most of the chains
- Validation checks the double spending maliciousness of the transactions

Blockchain Memory Usage

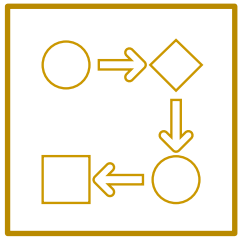
- As discussed in limitations, Memory is directly impacting the costs of operating the blockchain
- Less data to store on blockchain is desirable, hashing can help in storing such large data

Next Generation Blockchain or Ledger Technology

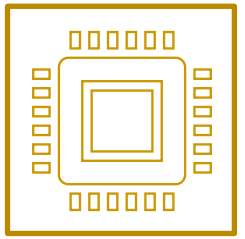
Blockchain – Next Generation Ledgers or Post-Blockchain



Hashgraph

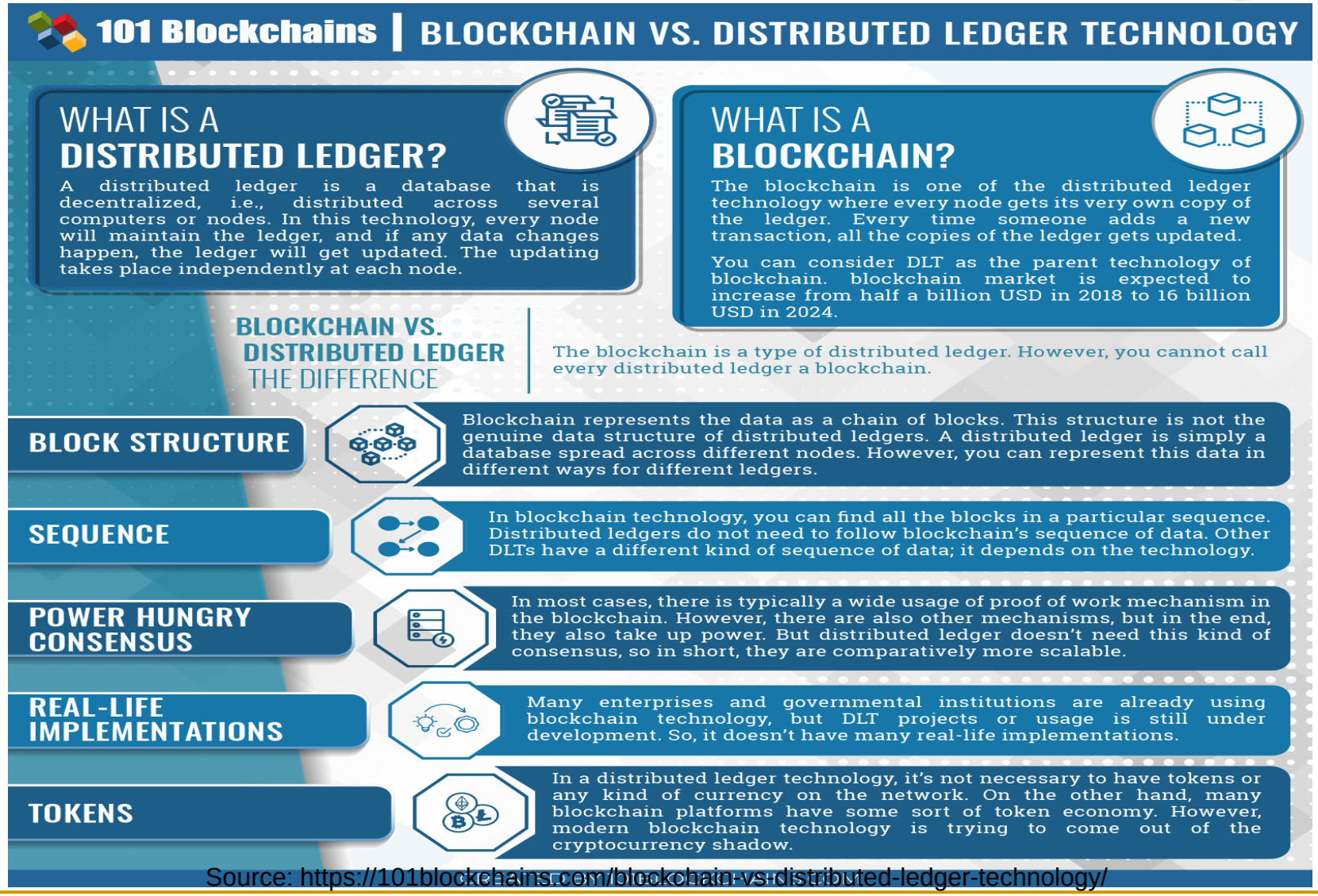


Tangle



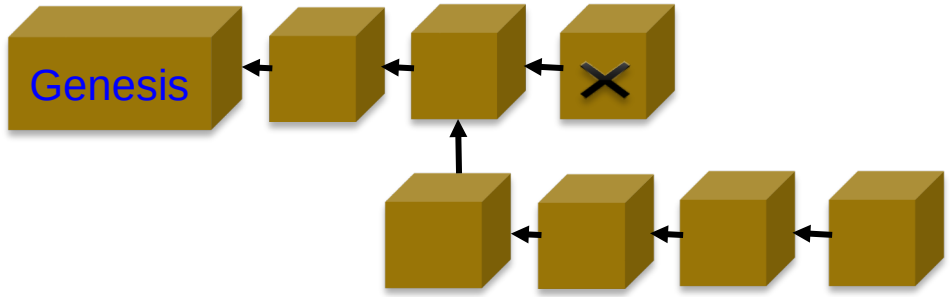
Current Paper
(McPoRa for CPS)

Blockchain vs. Distributed Ledger

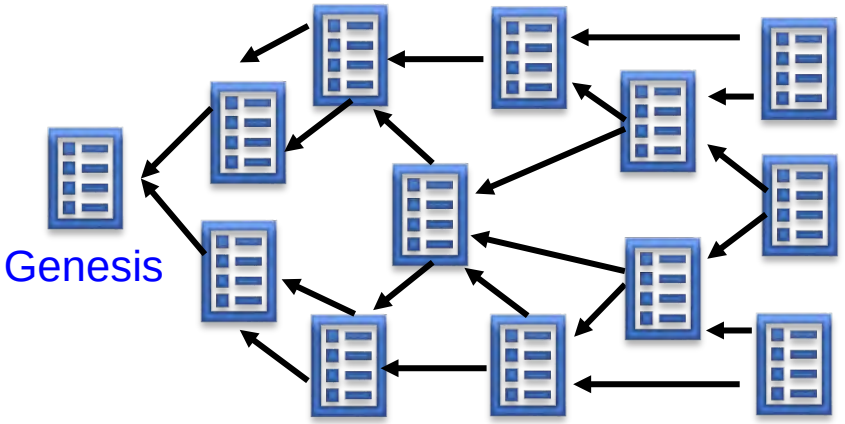


Source: https://101blockchains.com/blockchain-vs-distributed-ledger-technology/

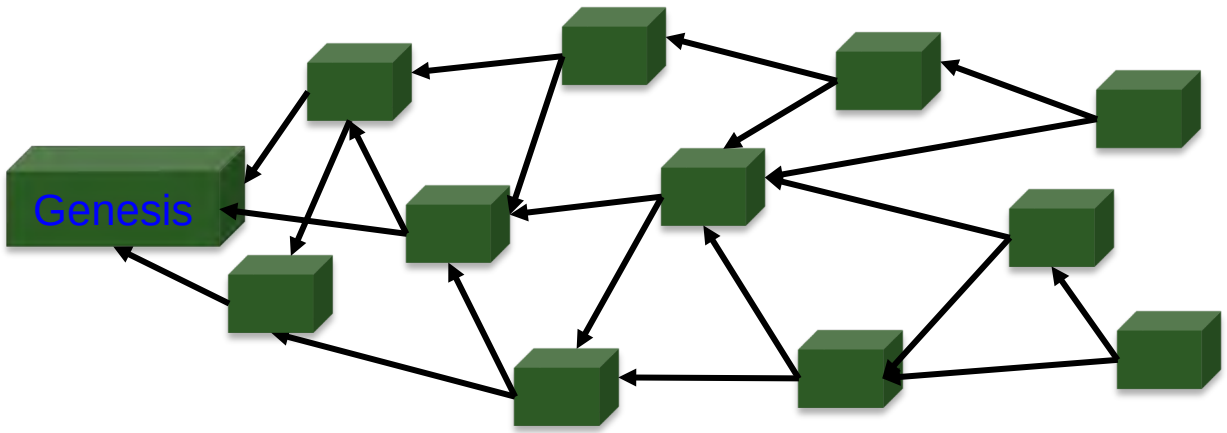
Comparative Perspective of BC, Tangle, Versus Proposed MC



(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.

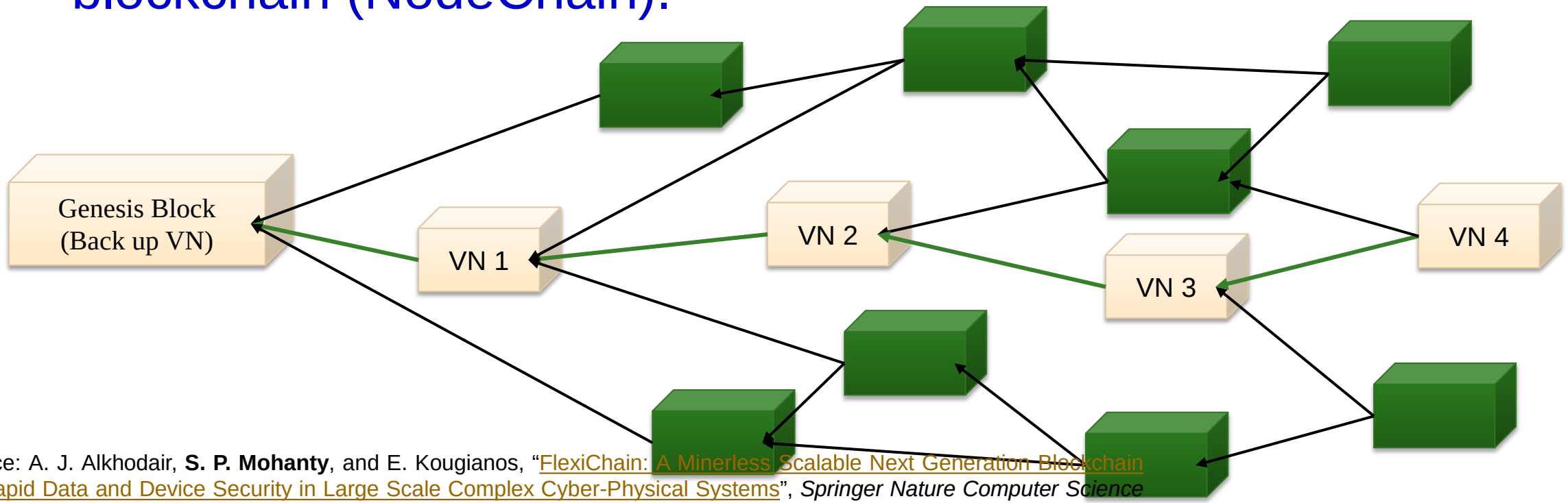
A Perspective of BC, Tangle Vs Our Multichain

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.

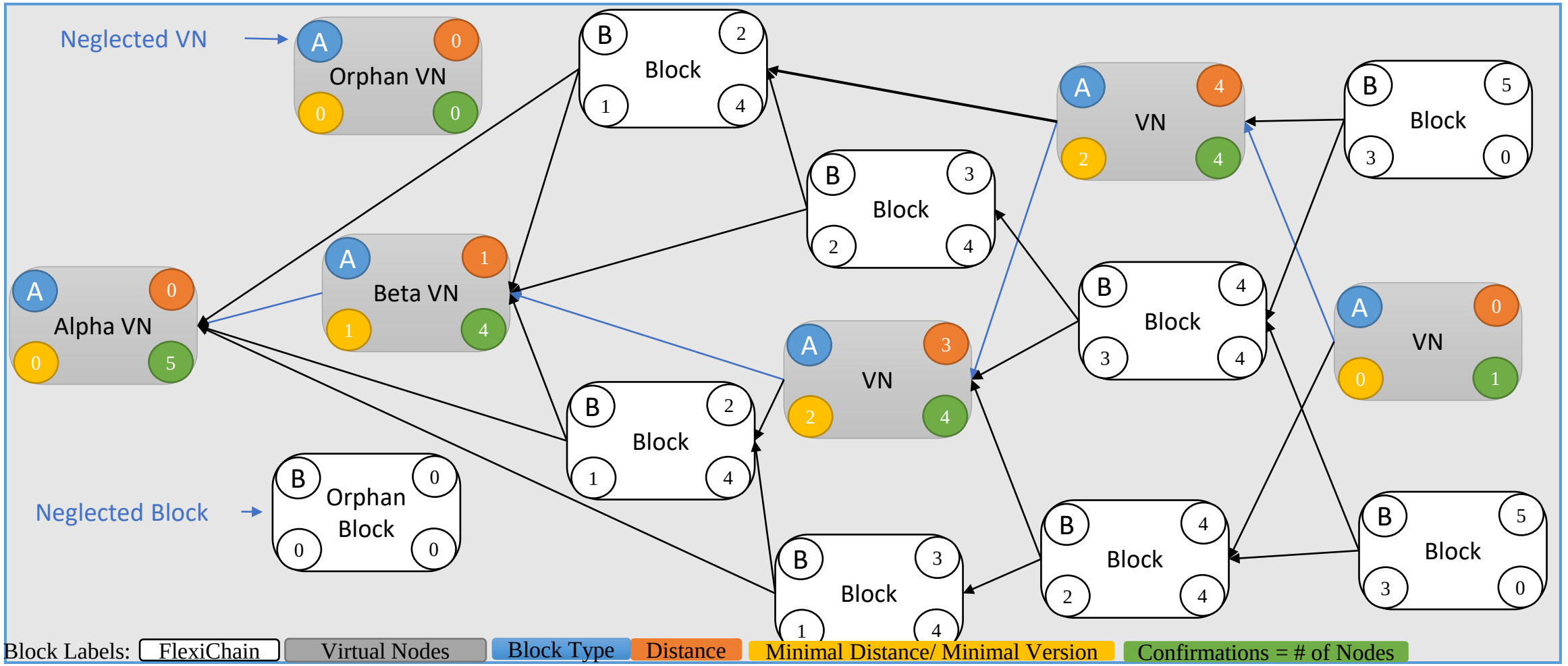
FlexiChain

- MultiChain [1] & ASID [2] combined.
- Strong connected blocks built over a genesis Integrated blockchain (NodeChain).



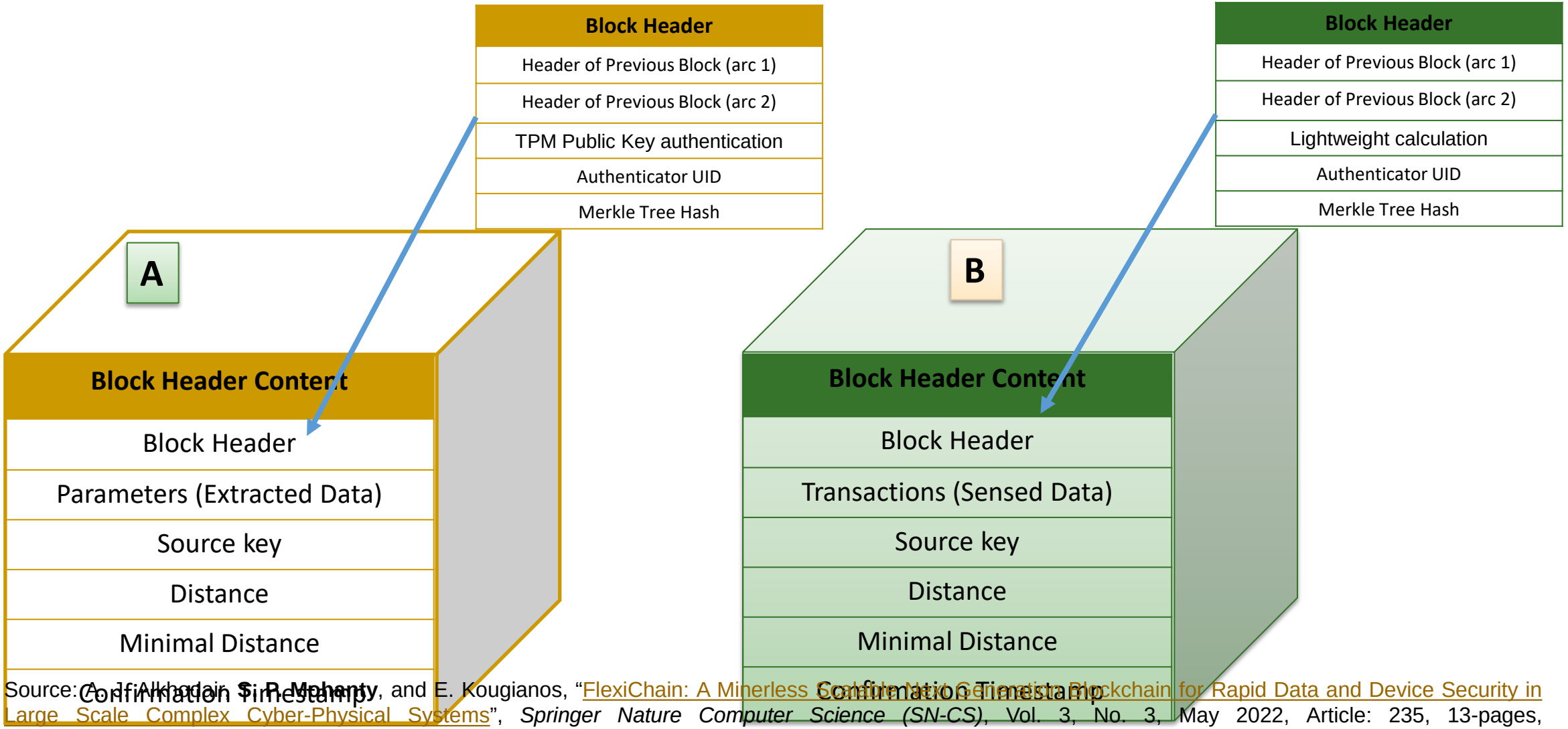
Source: A. J. Alkhodair, **S. P. Mohanty**, and E. Kougianos, "FlexiChain: A Minerless Scalable Next Generation Blockchain for Rapid Data and Device Security in Large Scale Complex Cyber-Physical Systems", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 3, May 2022, Article: 235, 13-pages, DOI: https://doi.org/10.1007/s42979-022-01139-4.

FlexiChain Characteristics



Source: A. J. Alkhodair, **S. P. Mohanty**, and E. Kougianos, "FlexiChain: A Minerless Scalable Next Generation Blockchain for Rapid Data and Device Security in Large Scale Complex Cyber-Physical Systems", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 3, May 2022, Article: 235, 13-pages, DOI: https://doi.org/10.1007/s42979-022-01139-4.

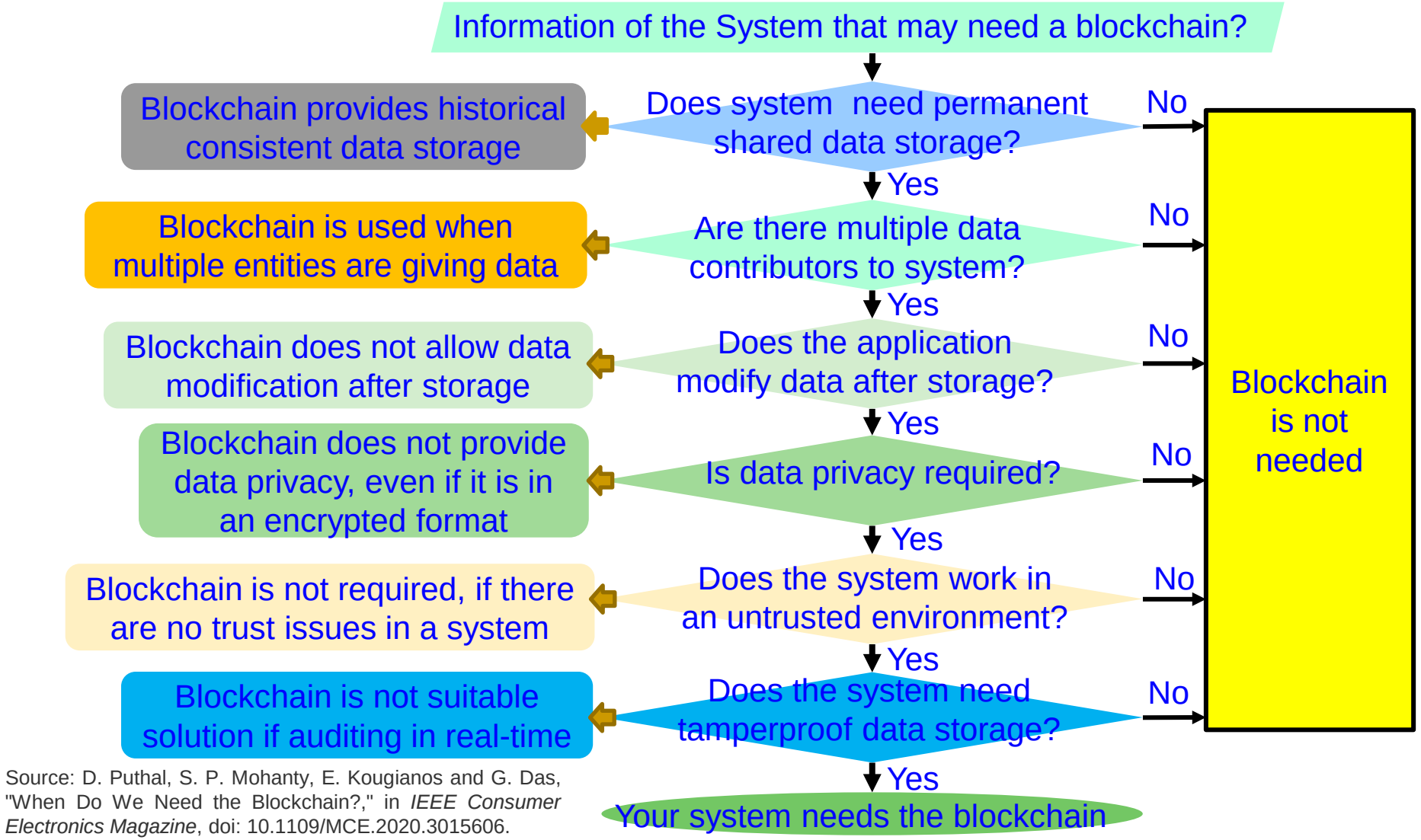
FlexiChain Block Types



Source: A. Al-Khashan, **S. P. Mohanty**, and E. Kougianos, "FlexiChain: A Minerless Scalable Next Generation Blockchain for Rapid Data and Device Security in Large Scale Complex Cyber-Physical Systems", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 3, May 2022, Article: 235, 13-pages, DOI: https://doi.org/10.1007/s42979-022-01139-4.

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.

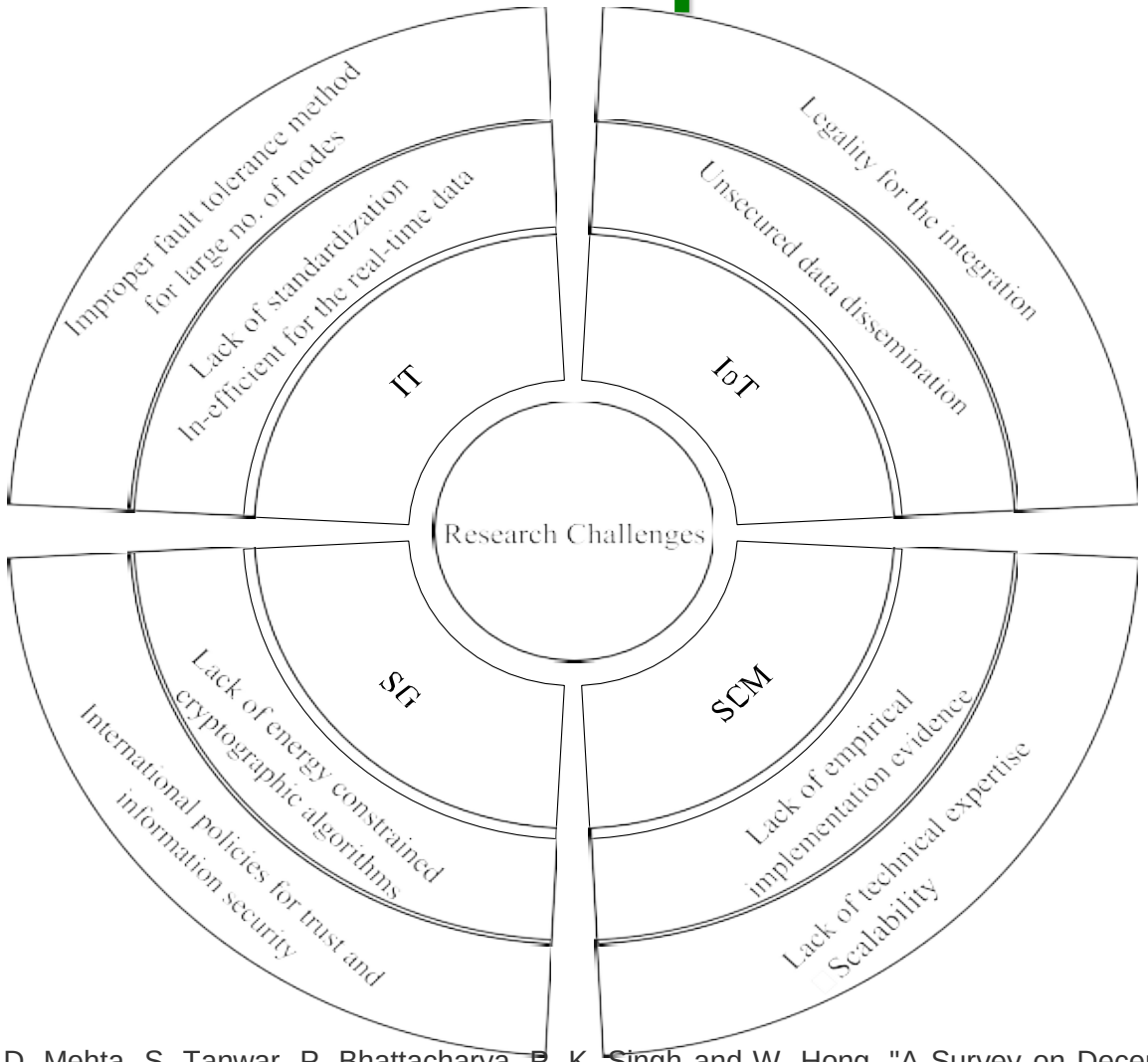
Conclusions

- Blockchain technology has many advantages and applicability in different fields.
- Blockchain is a secure platform that could contribute in smart healthcare, smart transportation, and smart agriculture.
- Blockchain could consolidate IoT applications in smart environments.
- DAG is an alternative technique for blockchain 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

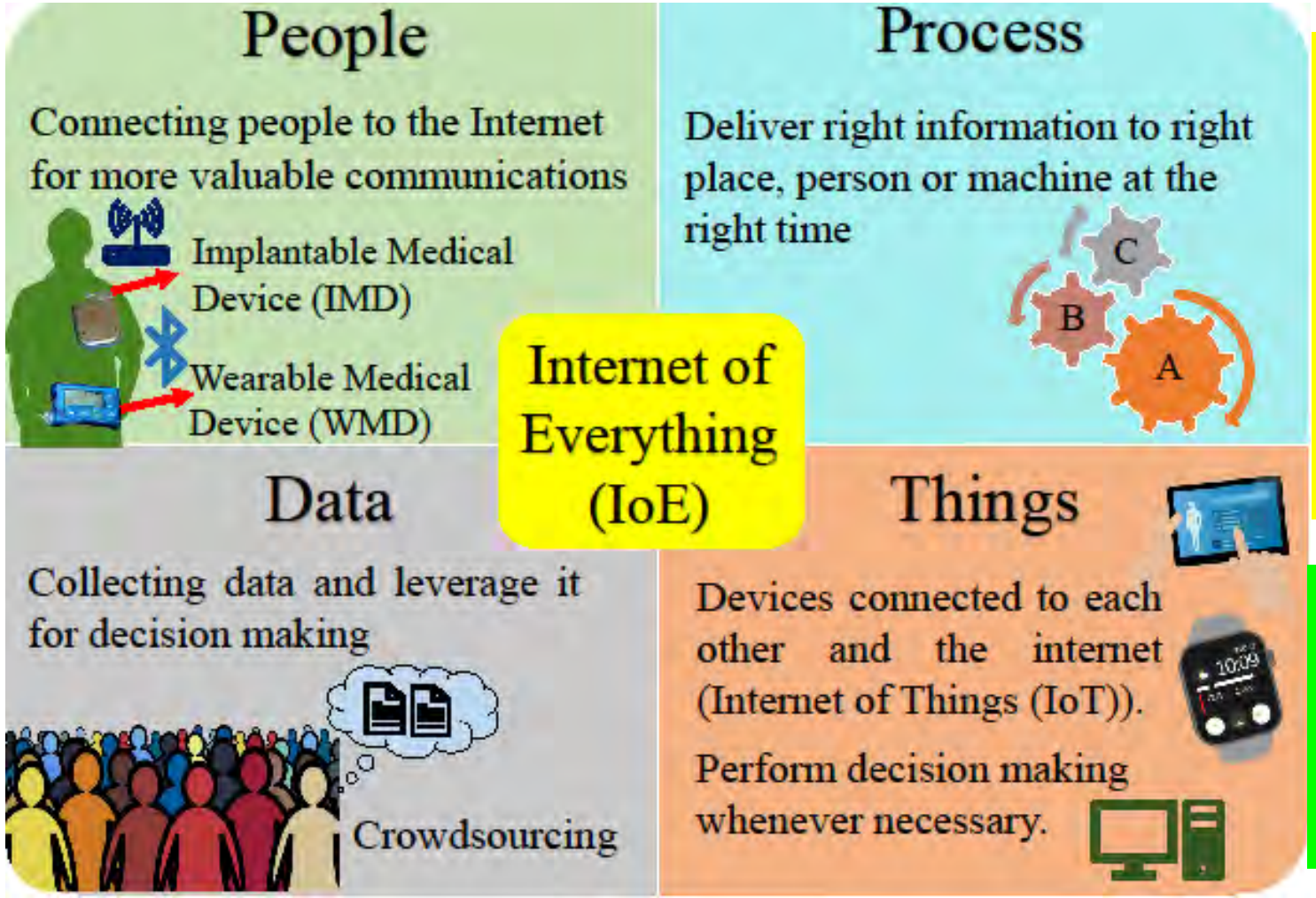
- As future directions, more efficient and low power algorithms for blockchain can be developed.
- Even though Blockchain has many advantages, it has some limitations.
- These limitations created opportunities for researchers, and companies to figure out a way to overcome it.

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.