PUFchain 3.0: Hardware-Assisted Distributed Ledger for Robust Authentication in the Internet of Medical Things

Presenter: Venkata K. V. V. Bathalapalli

Venkata K. V. V. Bathalapalli[1], S. P. Mohanty[2], E. Kougianos[3]
Babu K. Baniya[4], and Bibhudutta Rout[5]

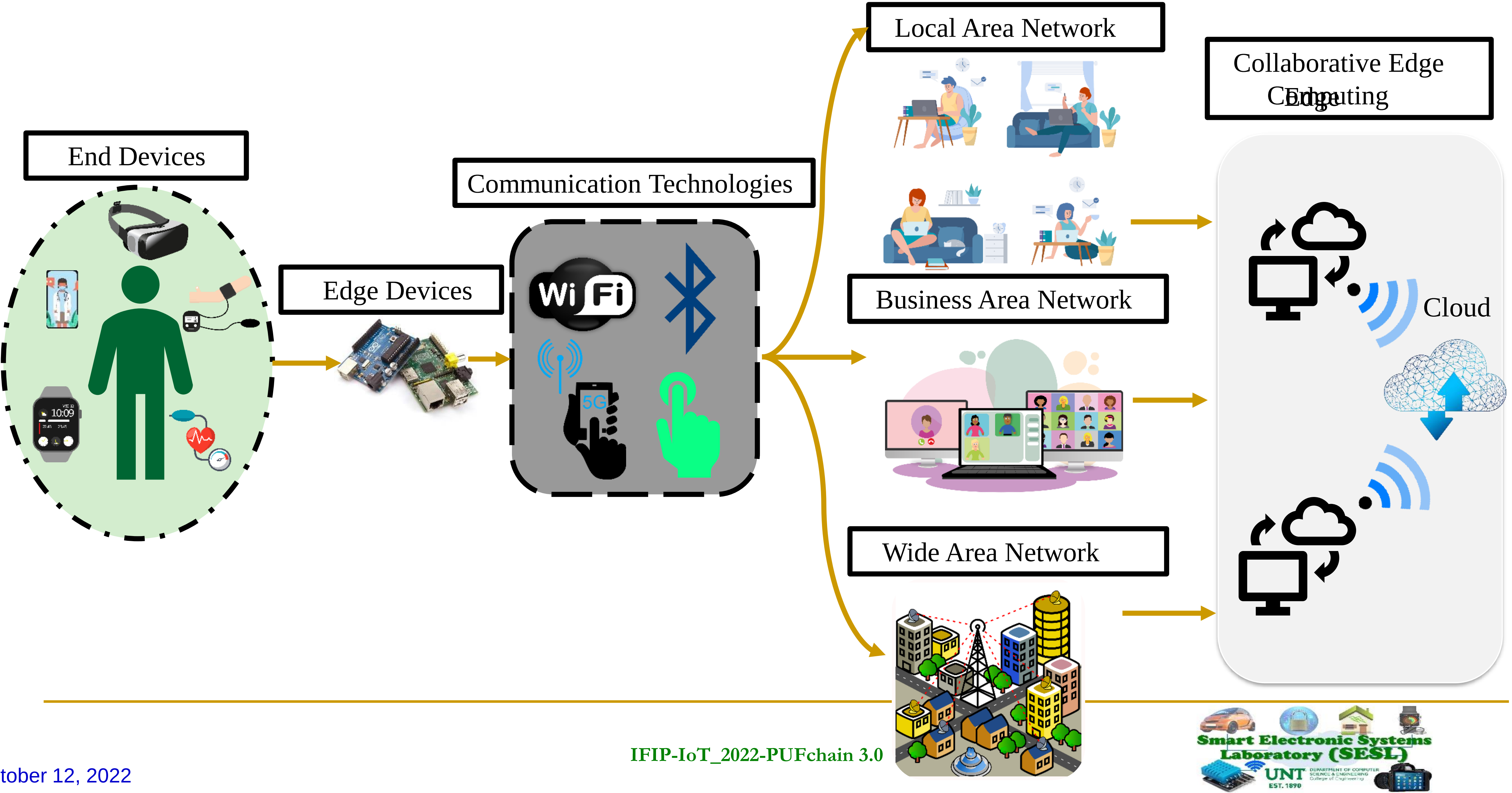
University of North Texas, Denton, TX, USA.[1,2,3,5] and Grambling State University[4].

Email: **vb0194@unt.edu, saraju.mohanty@unt.edu[2], elias.kougianos@unt.edu[3], Baniyab@gram.edu[4], bibhudutta.rout@unt.edu[5]**

Outline

- The Big Picture
- Novel Contributions
- Related Works
- Working Flow of PUFchain 3.0
- Implementation and Validation
- Conclusions & Future Work

Architecture of H-CPS



End Devices

Edge Devices

Communication Technologies

Local Area Network

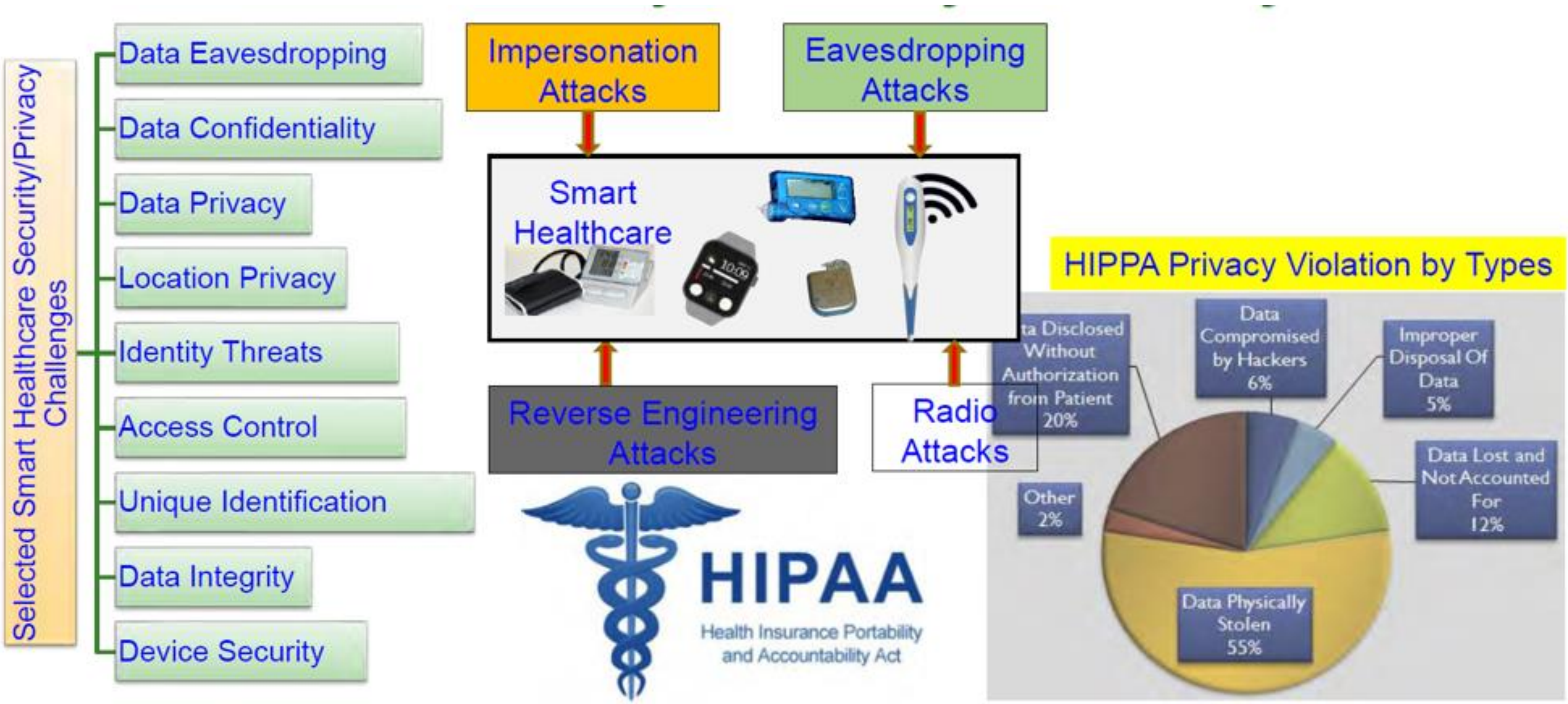
Business Area Network

Wide Area Network

Collaborative Edge Computing Edge

Cloud

Smart Healthcare Cybersecurity Issues



Selected Smart Healthcare Security/Privacy Challenges

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

Impersonation Attacks

Eavesdropping Attacks

Smart Healthcare

Reverse Engineering Attacks

Radio Attacks

HIPAA

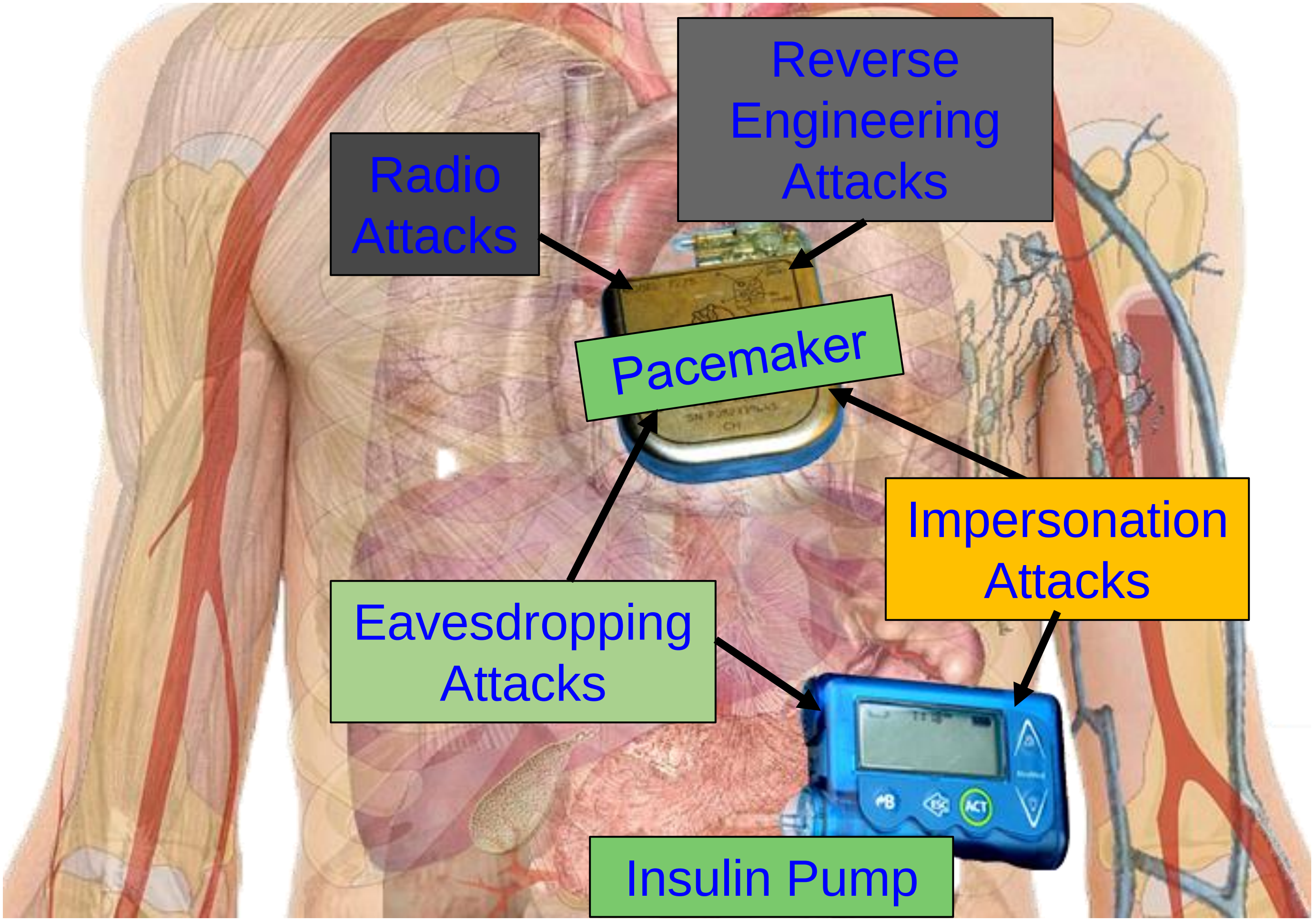
Health Insurance Portability and Accountability Act

HIPPA Privacy Violation by Types

ta Disclosed Without Authorization from Patient 20%
Data Compromised by Hackers 6%
Improper Disposal Of Data 5%
Data Lost and Not Accounted For 12%
Other 2%
Data Physically Stolen 55%
10:09

Source: Expert Lecture - Workshop on VLSI Device and Circuit Design Tools, School of Electronics Engineering, VIT-AP University - 23 June 2022 (Physical Unclonable Function (PUF) as the Hardware-Assisted Security (HAS) Primitive)

Cybersecurity Measures in Healthcare Cyber-Physical Systems is Hard



Collectively (WMD+IMD): Implantable and Wearable Medical Devices (IWMDs)

Implantable and Wearable Medical Devices (IWMDs):

→ Longer Battery life

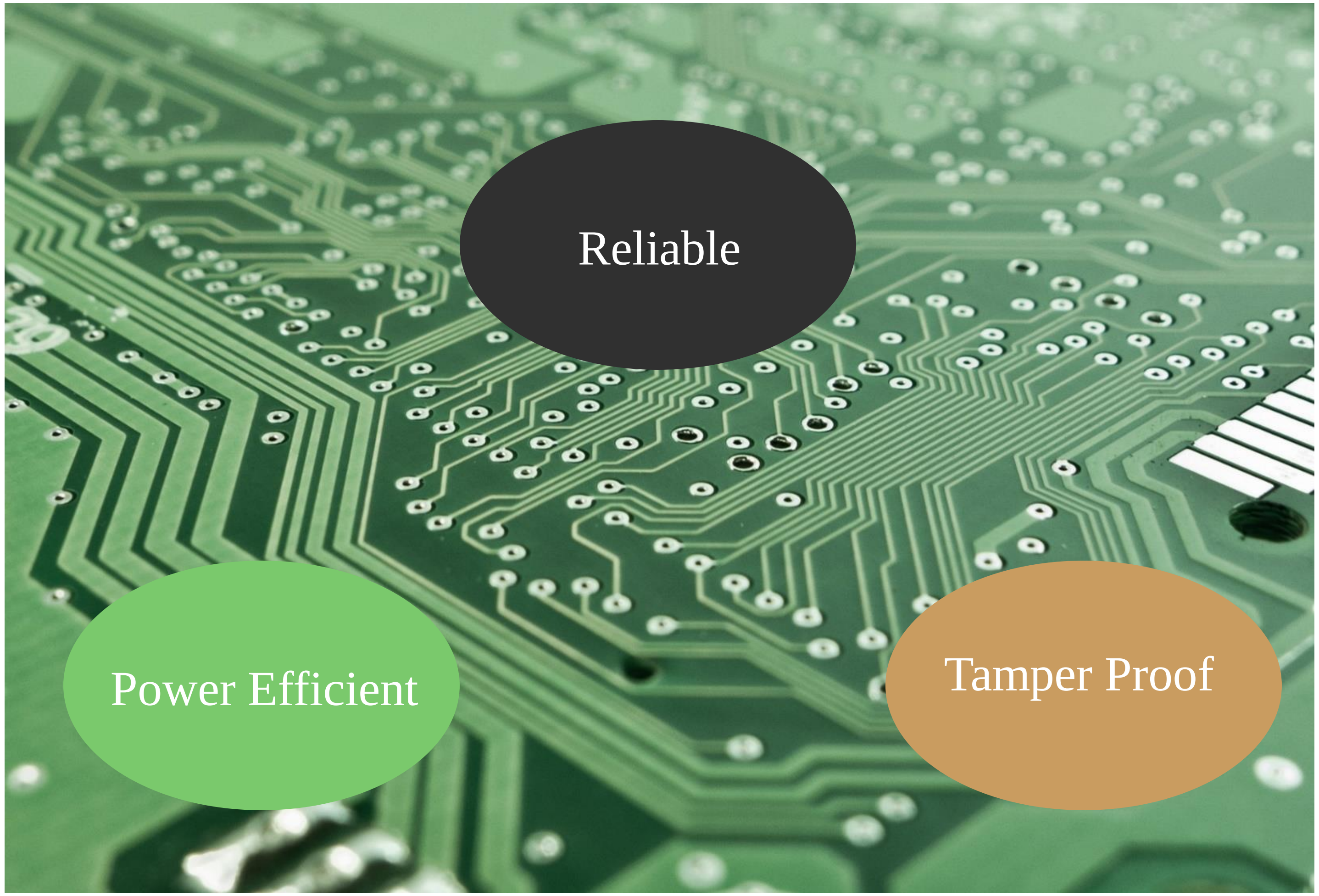
→ Safer device

→ Smaller size

→ Smaller weight

→ Not much computational capability

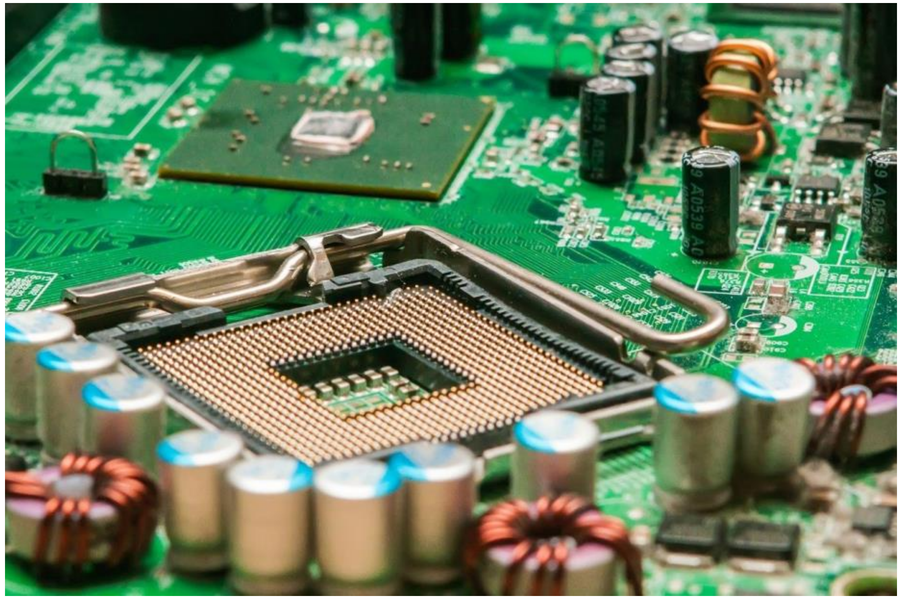
PUF: A Hardware-Assisted Security Primitive



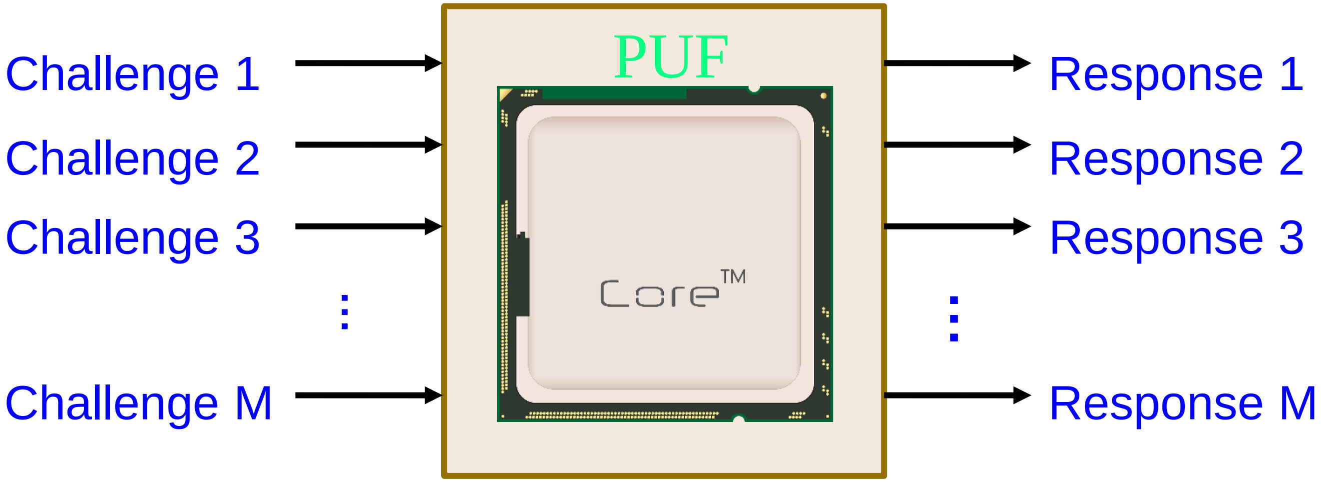
- A secure fingerprint generation scheme based on process variations in an Integrated Circuit
- PUFs don’t store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.
- A simple design that generates cryptographically secure keys for the device authentication

PUF: A Hardware-Assisted Security Primitive

- ✓ PUF has a Challenge as an Input and Response as an Output
- ✓ Response output from the PUF design will be unique for the challenge input on that PUF design
- ✓ Arbiter and Ring Oscillator PUFs are the most widely used PUF designs for IoT applications
- ✓ Delay based PUF designs support higher number of Challenge Response pairs (CRP)



PUF Key Generation and Working



Challenge 1

Challenge 2

Challenge 3

⋮

Challenge M

PUF

Core™

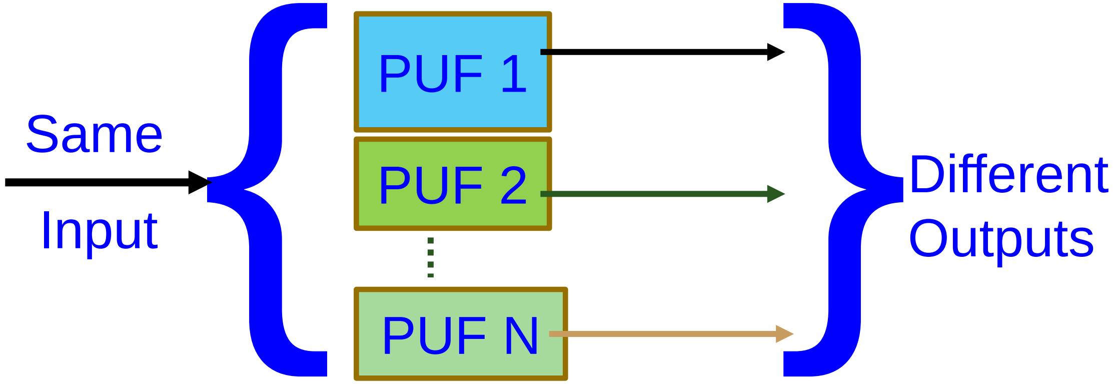
Response 1

Response 2

Response 3

⋮

Response M



Same Input

PUF 1

PUF 2

⋮

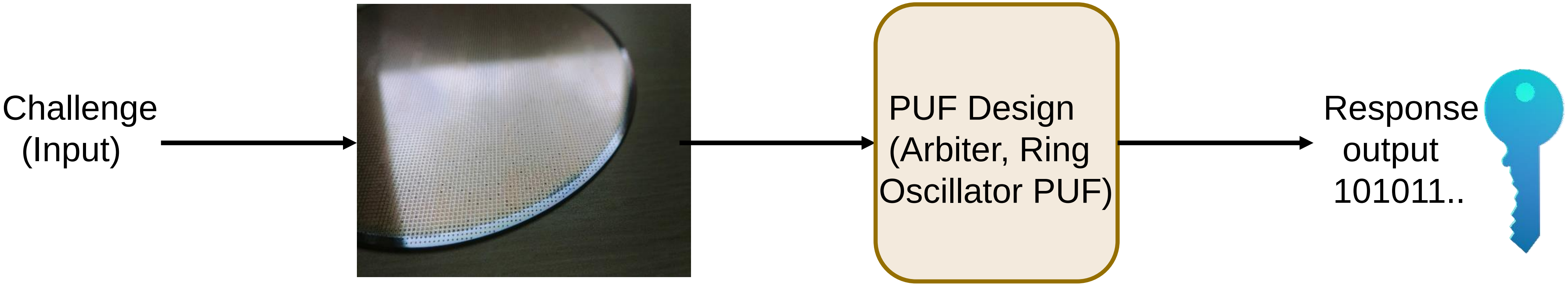
PUF N

Different Outputs

Source: iSES 2019 Demo (PUFchain: Hardware-Integrated Scalable Blockchain)

PUF-Principle

- PUF keys are not stored in the digital memory. But the keys are generated using silicon manufacturing process variations.

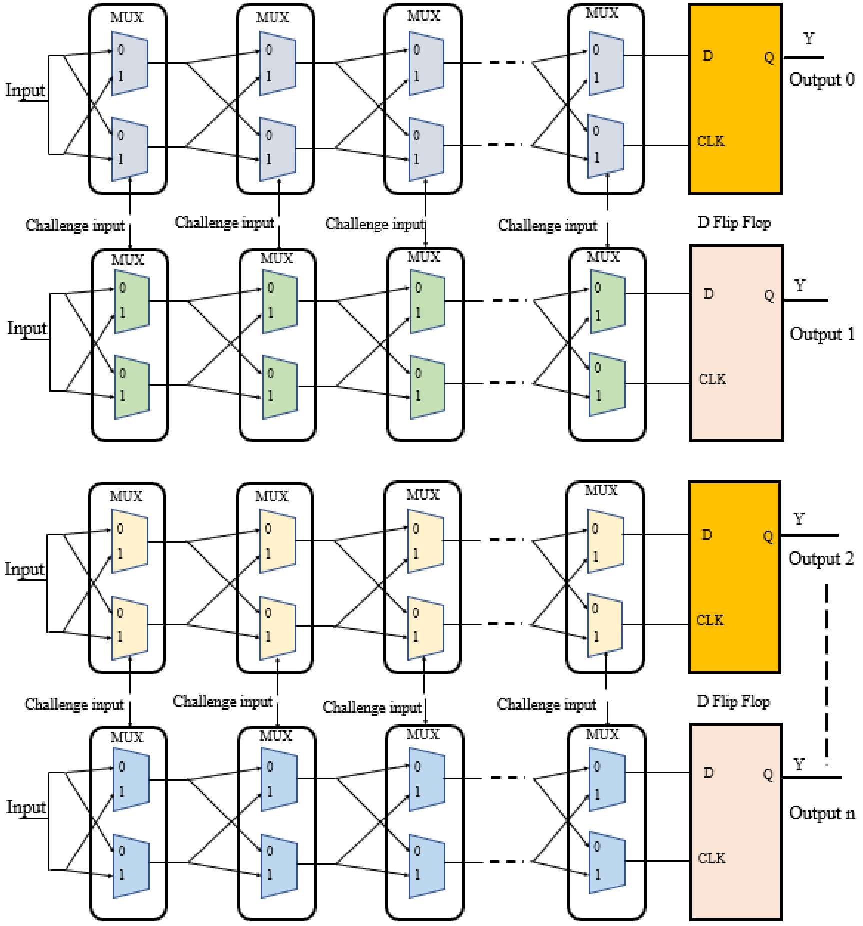


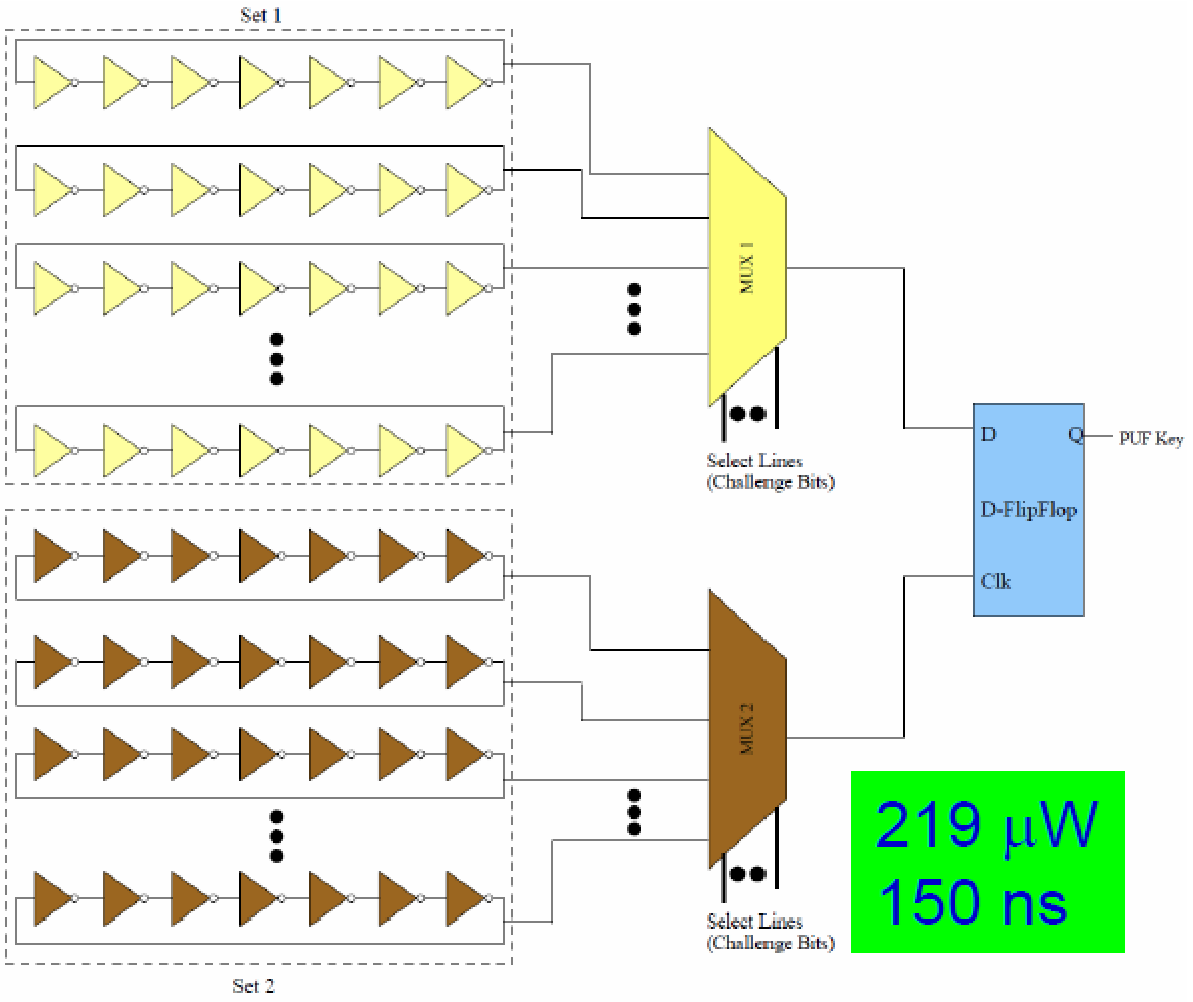
Silicon Wafer

Parameters: Oxide growth, Ion Implantation, Lithography

Source: OCIT 2021 Talk (A PUF Based Approach for Sustainable Cybersecurity in Smart Agriculture)

PUF Designs

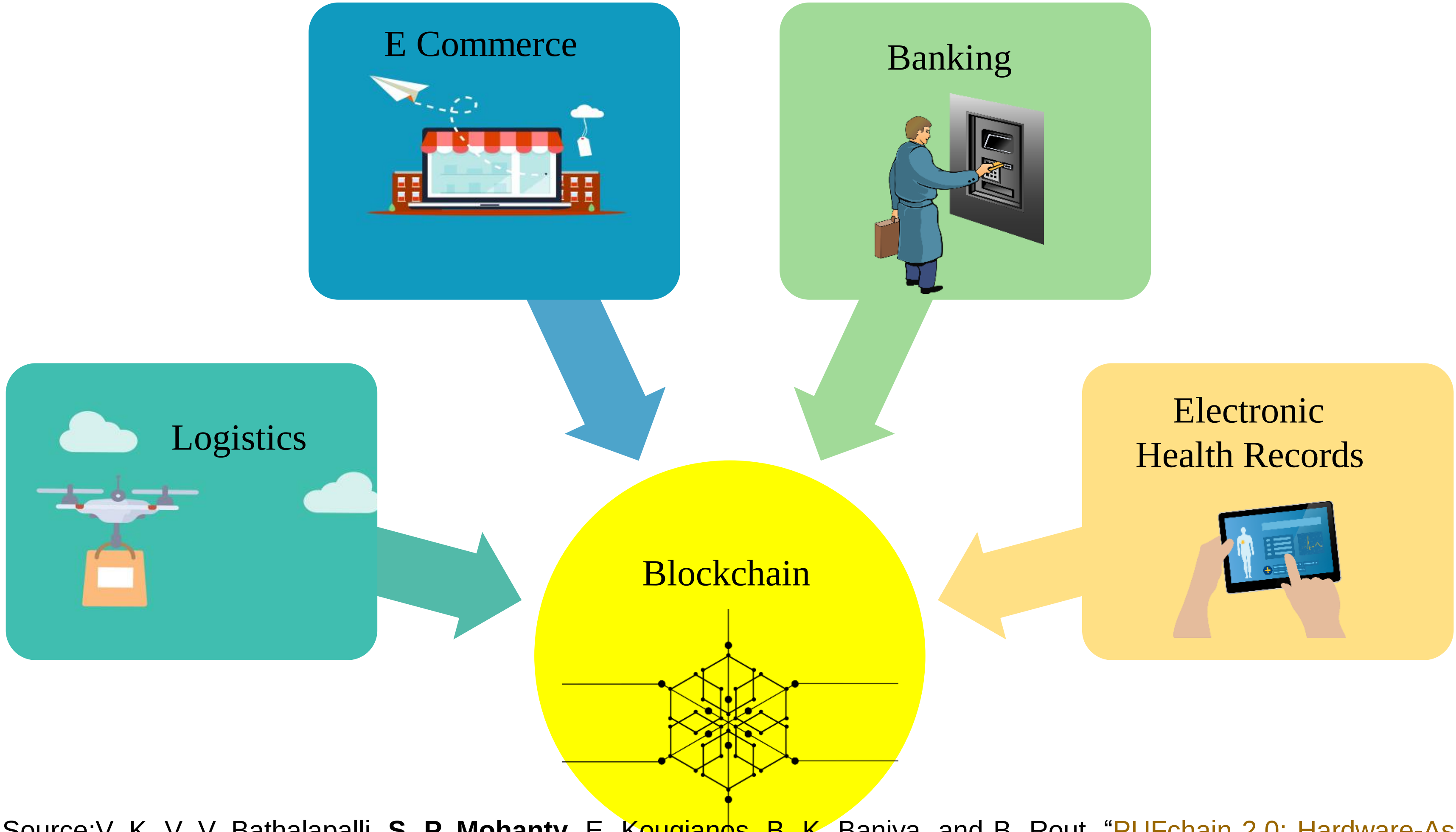




219 µW
150 ns

Source: iSES 2019 Demo (PMsec: PUF-Based Energy-Efficient Authentication of Devices in the Internet of Medical Things (IoMT))

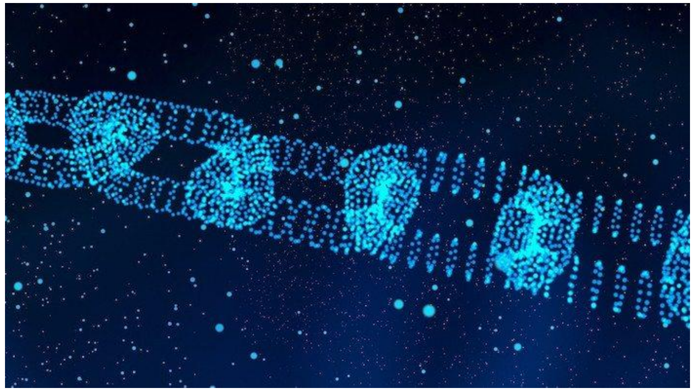
Applications of Blockchain

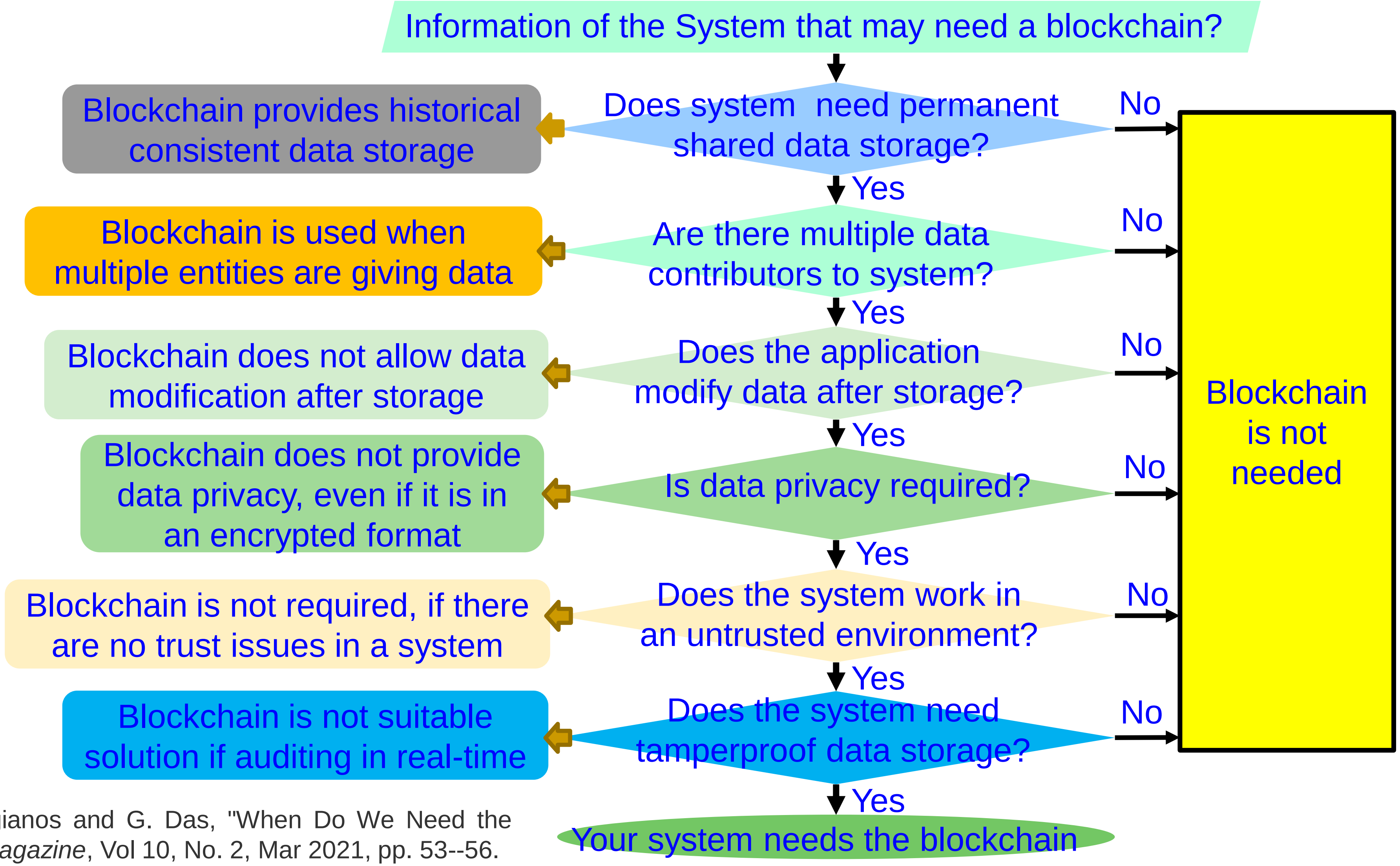


- Blockchain can be Public, Private, and Consortium
- Proof of Work (PoW), Proof of Stake(PoS), and Proof of Authentication(PoAh) are prominent consensus algorithms
- PoAh is 1000 times faster than PoW

Source:V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344, 19-pages, DOI: https://doi.org/10.1007/s42979-022-01238-2.

When do You Need the Blockchain?





Information of the System that may need a blockchain?

Does system need permanent shared data storage?

Blockchain provides historical consistent data storage

Are there multiple data contributors to system?

Blockchain is used when multiple entities are giving data

Does the application modify data after storage?

Blockchain does not allow data modification after storage

Is data privacy required?

Blockchain does not provide data privacy, even if it is in an encrypted format

Does the system work in an untrusted environment?

Blockchain is not required, if there are no trust issues in a system

Does the system need tamperproof data storage?

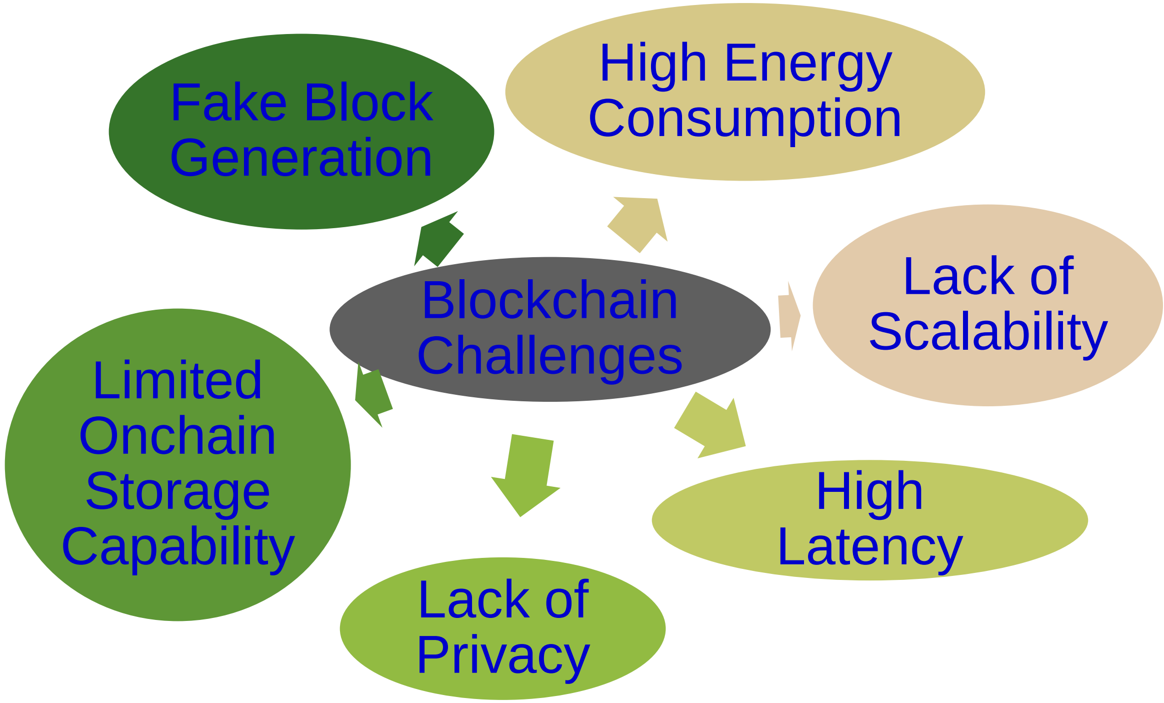
Blockchain is not suitable solution if auditing in real-time

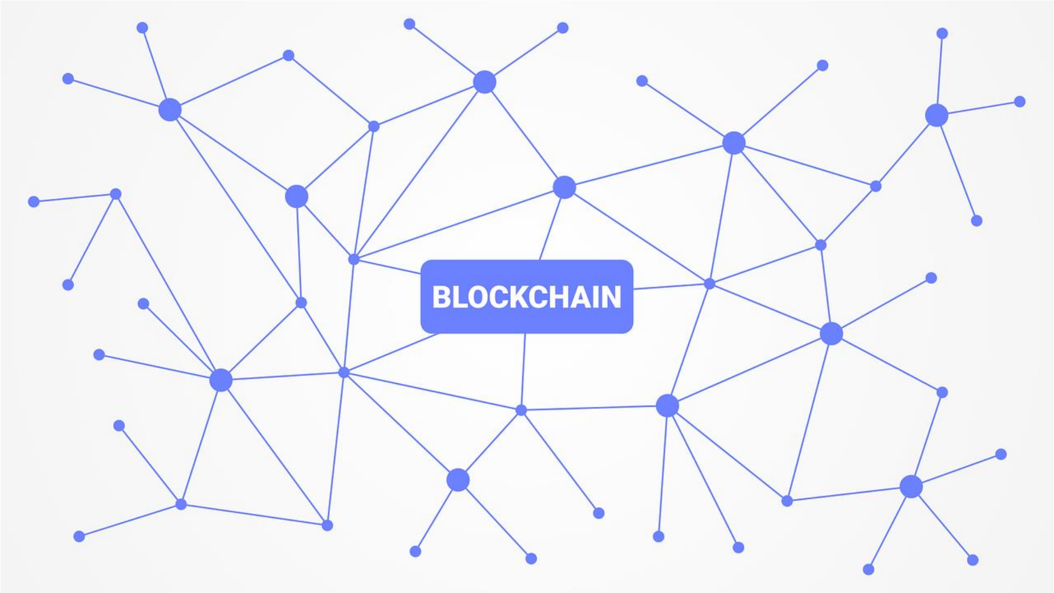
Your system needs the blockchain

Blockchain is not needed

Source: D. Puthal, S. P. Mohanty, E. Kougianos and G. Das, "When Do We Need the Blockchain?," *IEEE Consumer Electronics Magazine*, Vol 10, No. 2, Mar 2021, pp. 53--56.

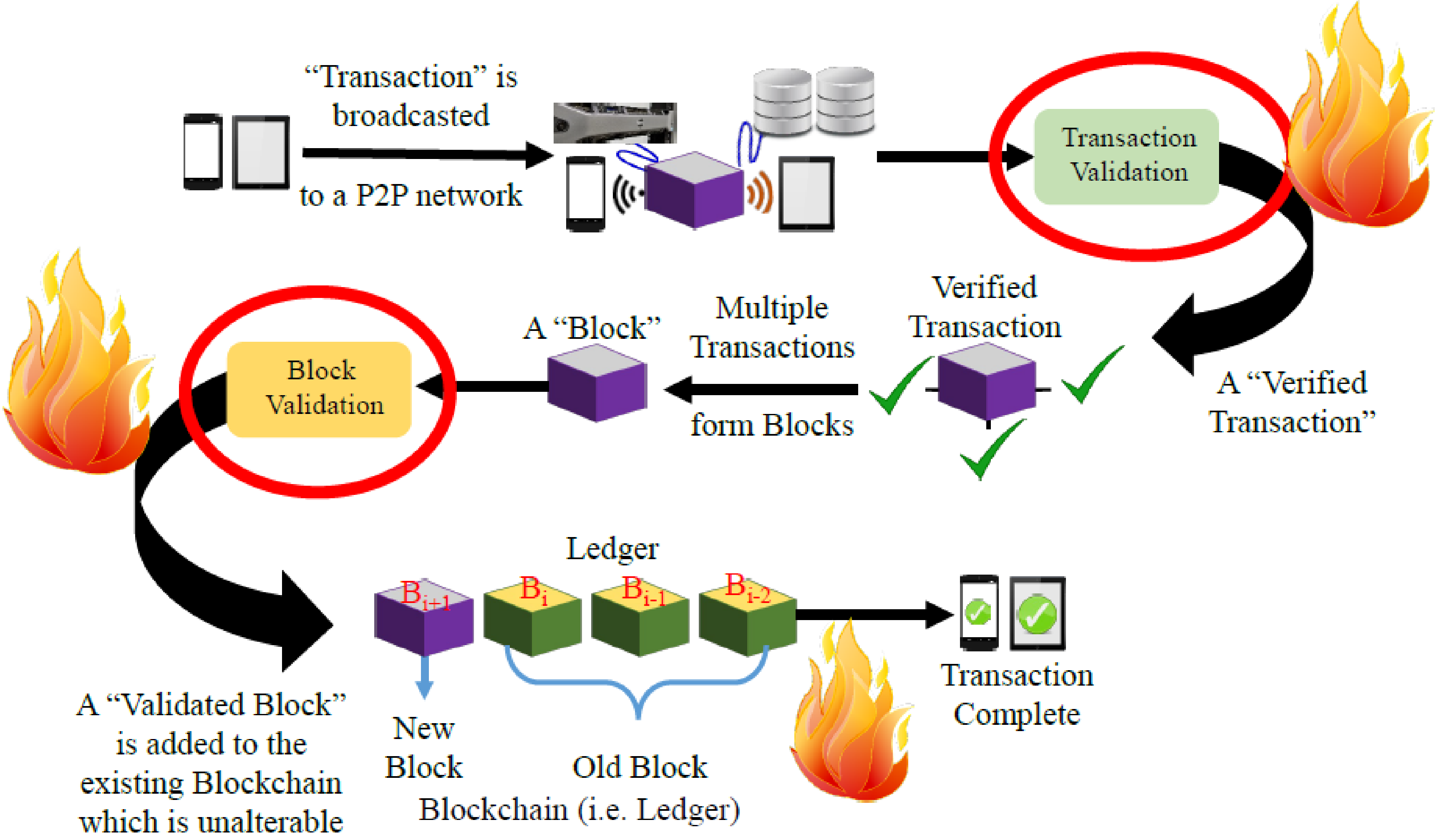
Blockchain has Many Challenges





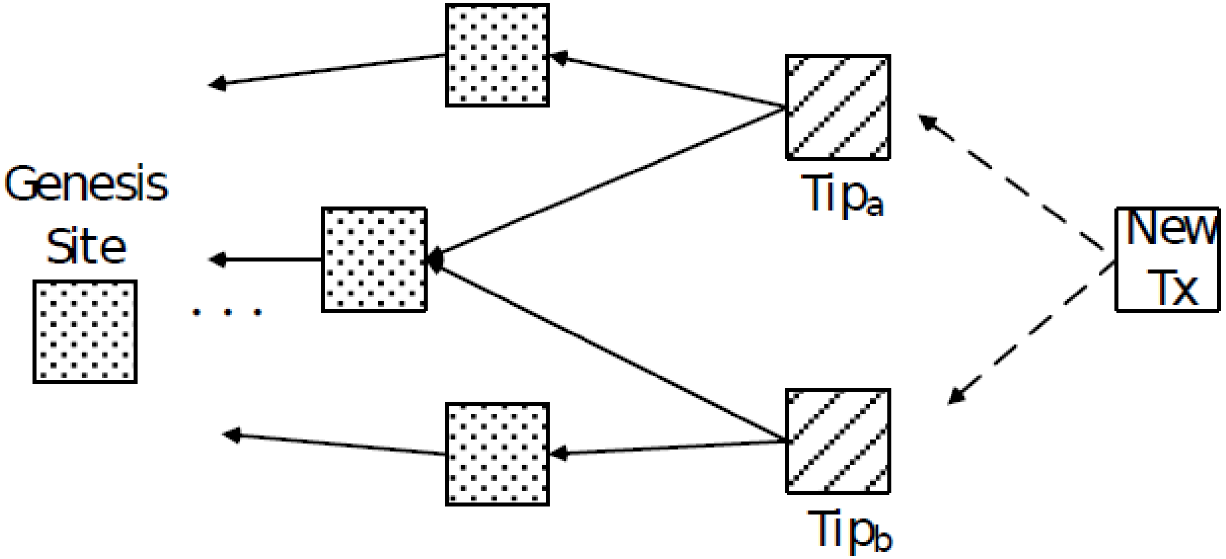
Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, “Everything you Wanted to Know about the Blockchain”, *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 4, July 2018, pp. 06--14.

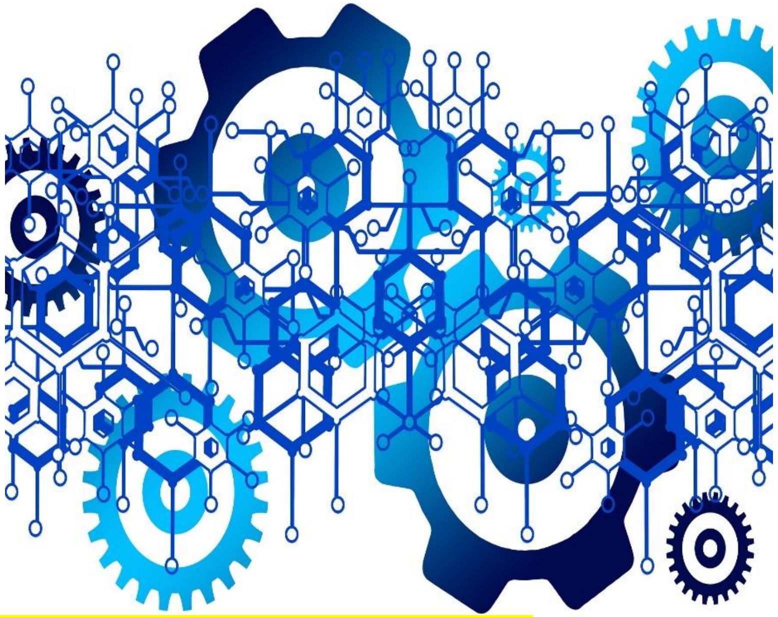
Block Validation and Addition Process



Source: D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems," *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 2019, pp. 1-5, doi: 10.1109/ICCE.2019.8662009.

Transaction Validation in IOTA Tangle

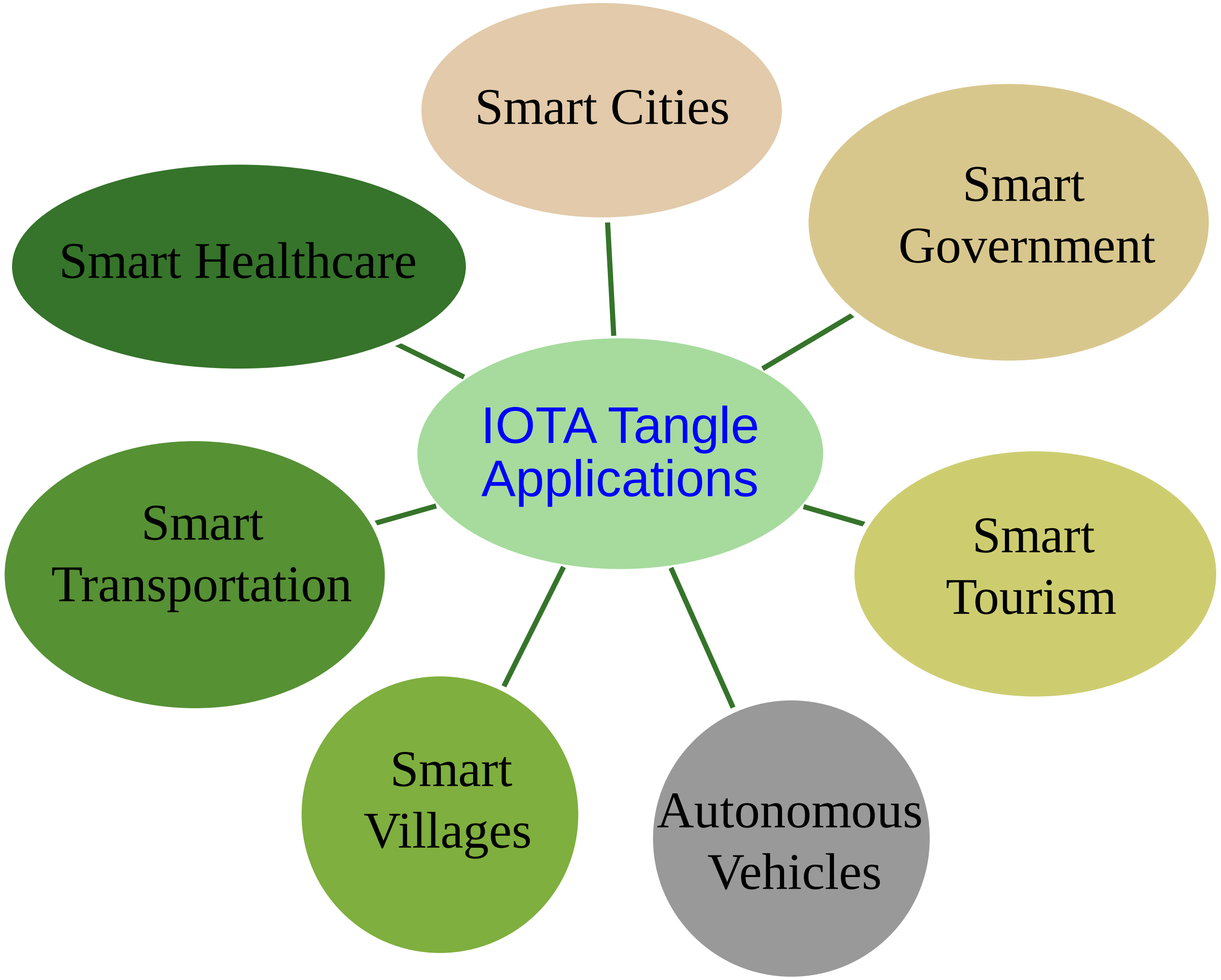




- Tips are unverified transactions in the Network
- Incoming transaction must validate tips to become part of Tangle Network

Source: F. Guo, X. Xiao, A. Hecker and S. Dustdar, "Characterizing IOTA Tangle with Empirical Data," *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, 2020, pp. 1-6, doi: 10.1109/GLOBECOM42002.2020.9322220.

Applications of IOTA Tangle



- Miner less and Fee less Distributed ledger technology
- Minimal amount of Proof of Work to negate the possibility of fraud transaction approval
- MAM Channel: A secure data communication protocol for IoT-b based applications

Novel Contributions

- Providing a miner-less, low-cost decentralized DLT for device authentication using PUFs and creating a secure channel for communicating IoMT data through MAM.

- A DLT that utilizes Proof of Work requires minimal computational resource requirements.

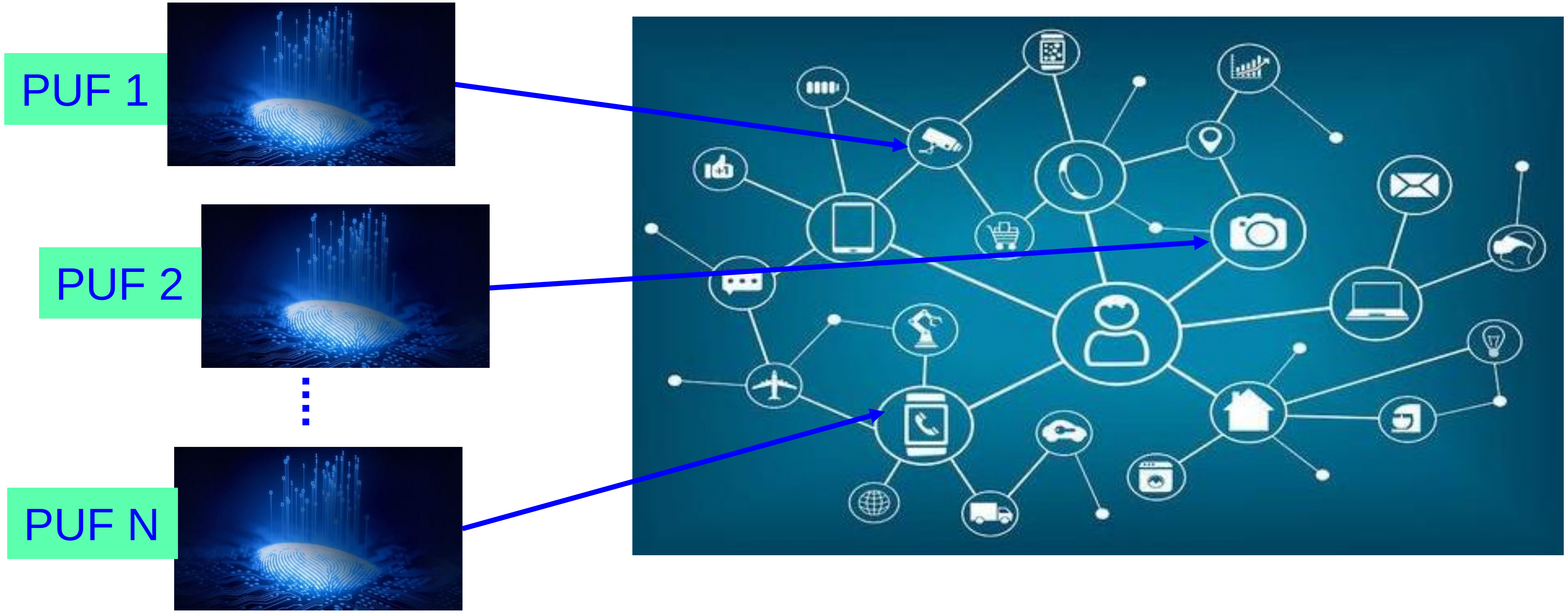
- A PUF-based security approach where a PUF module can be integrated inside wearable and implantable IoMT devices and can generate a unique device fingerprint.

- A system that doesn’t require transaction fees and allows secure communication through MAM.

- A robust multi-level device authentication system for edge computing-driven SC.

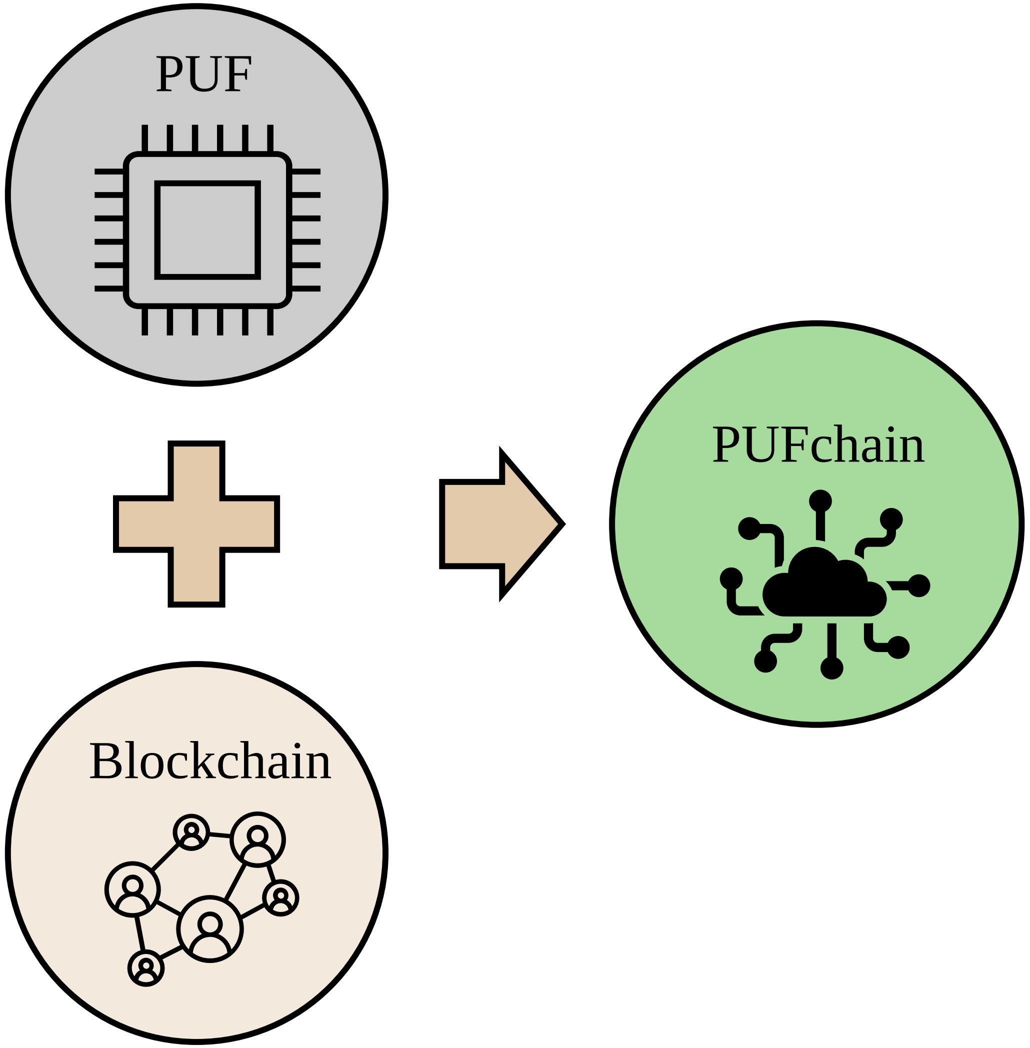
- A sustainable security solution that works in the Restricted mode of MAM where an authorization key is created to restrict unauthorized access to the MAM channel.

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



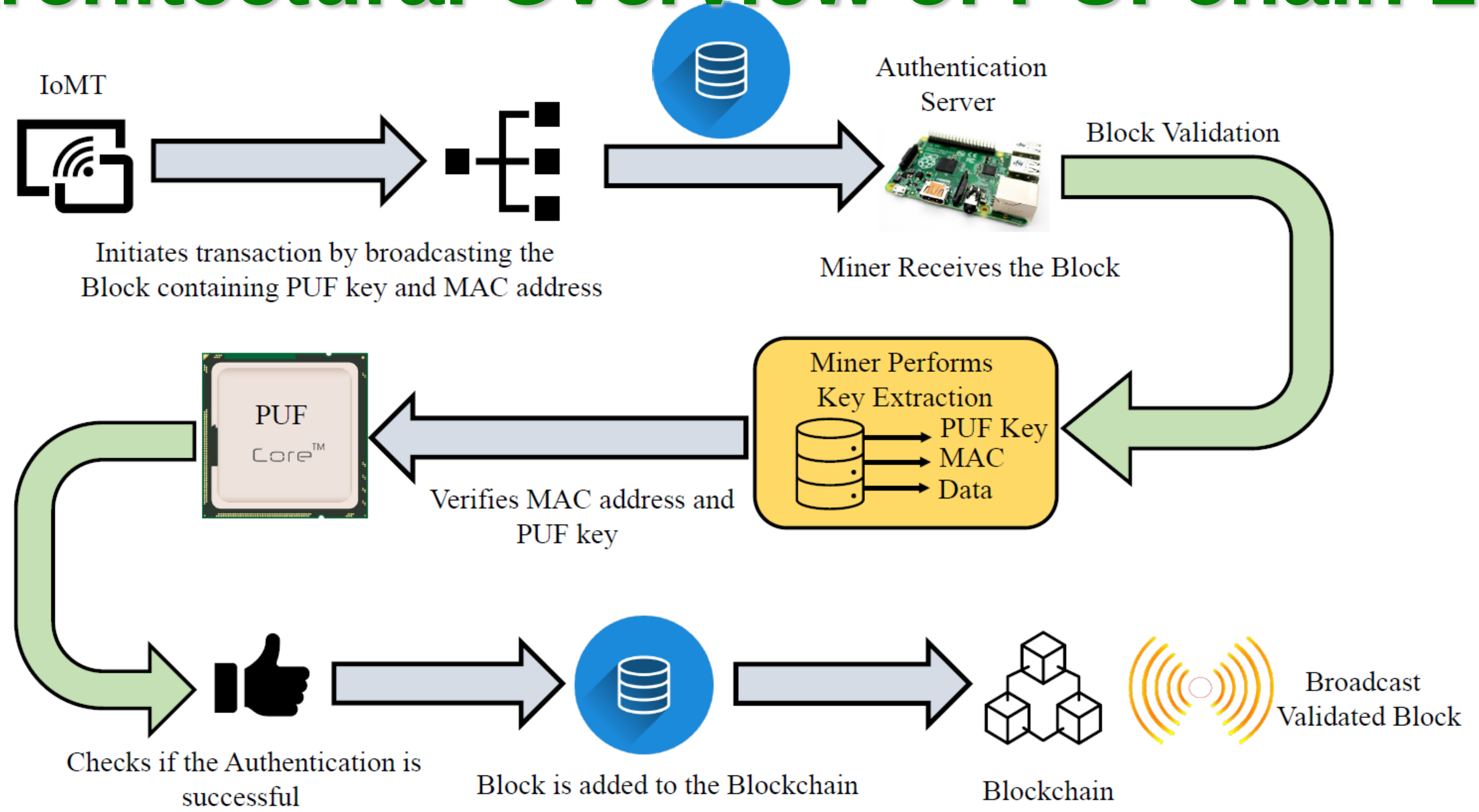
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, “PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

PUFchain – Another Way



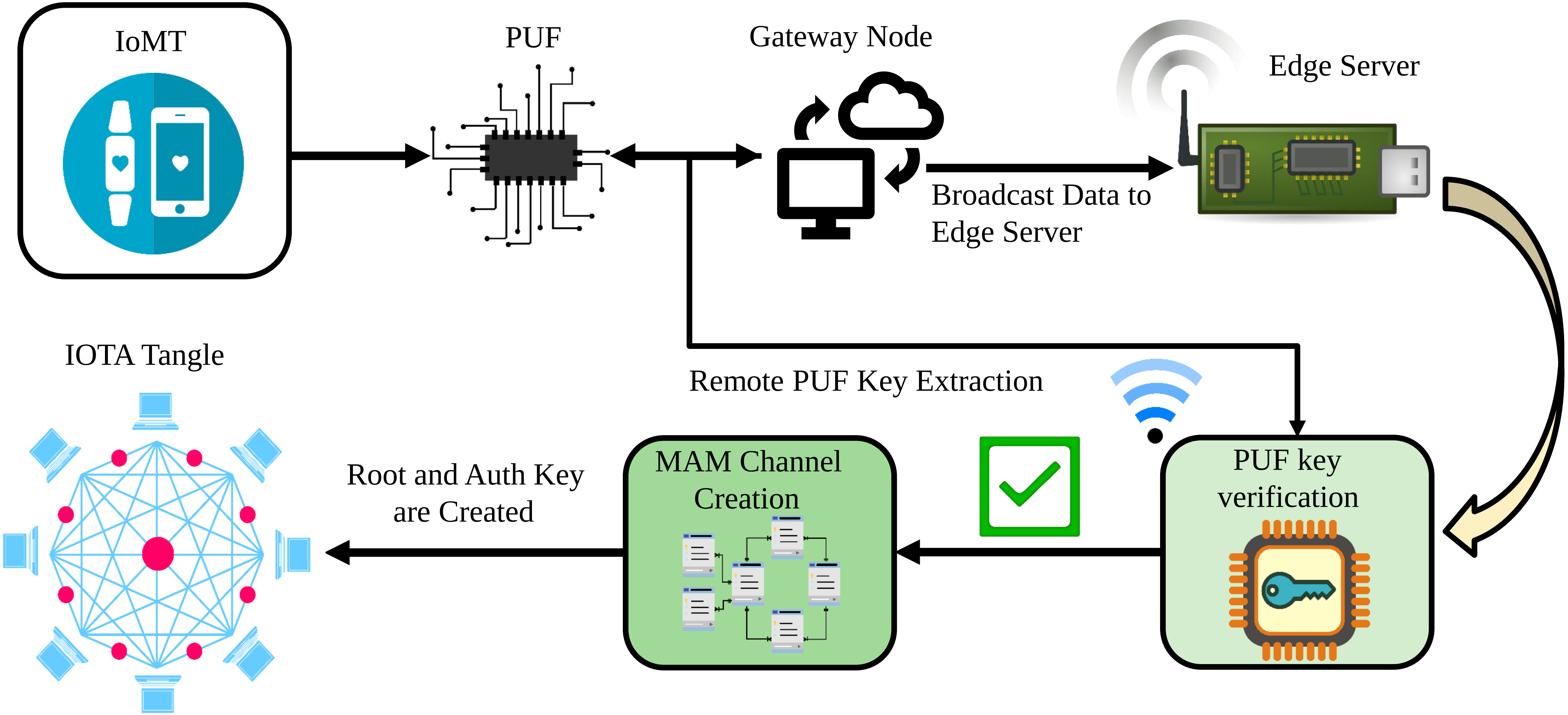
Blockchain Technology is integrated with Physically Unclonable Functions such as PUFchain by storing the PUF Key in an immutable Blockchain

Architectural Overview of PUFchain 2.0


IoMT
Initiates transaction by broadcasting the Block containing PUF key and MAC address
Authentication Server
Miner Receives the Block
Block Validation
Miner Performs Key Extraction
PUF Key
MAC
Data
Verifies MAC address and PUF key
PUF
Core™
Checks if the Authentication is successful
Block is added to the Blockchain
Blockchain
Broadcast Validated Block

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344, 19-pages, DOI: https://doi.org/10.1007/s42979-022-01238-2

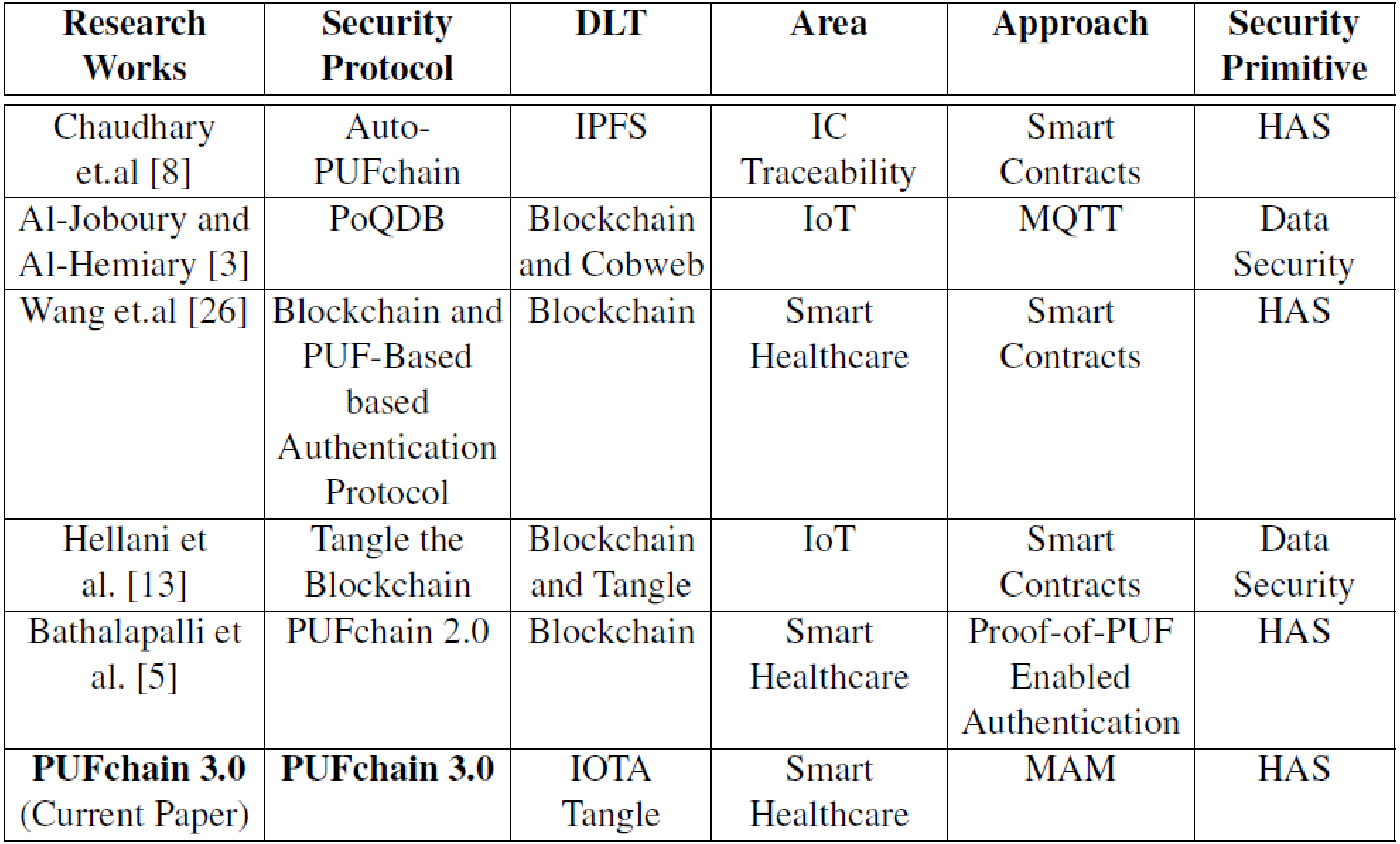
Architectural Overview of PUFchain 3.0


IoMT
PUF
Gateway Node
Edge Server
Broadcast Data to Edge Server
IOTA Tangle
Remote PUF Key Extraction
Root and Auth Key are Created
MAM Channel Creation
PUF key verification

Smart Electronic Systems Laboratory (SESL)

UNT EST. 1890 DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING College of Engineering

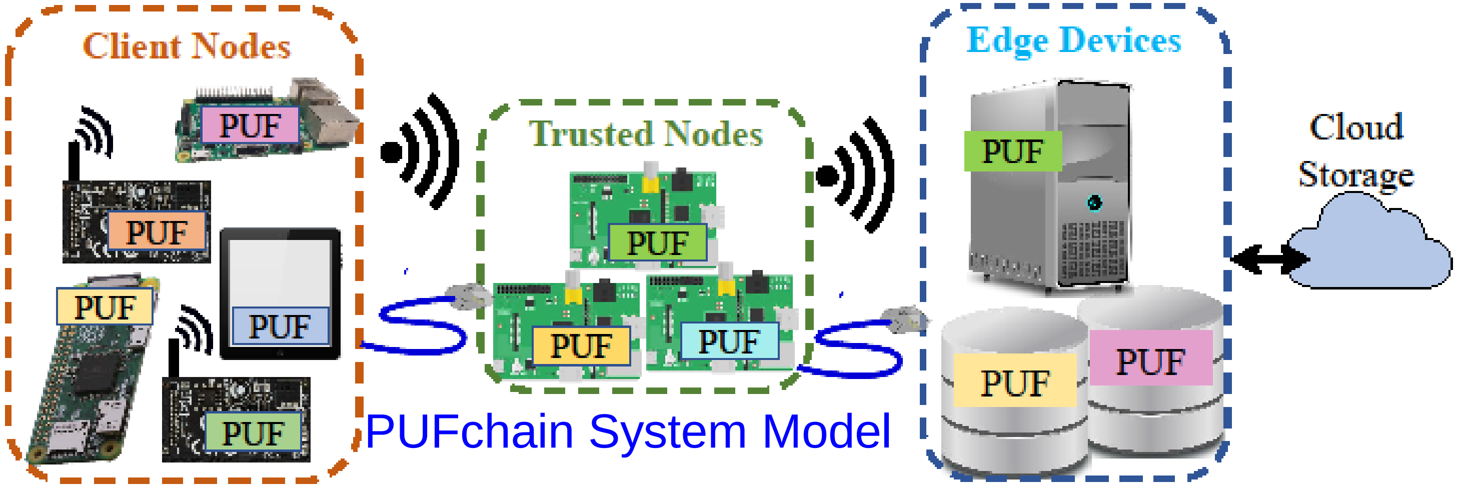
Related Prior Works



Research Works	Security Protocol	DLT	Area	Approach	Security Primitive
Chaudhary et.al [8]	Auto-PUFchain	IPFS	IC Traceability	Smart Contracts	HAS
Al-Joboury and Al-Hemiary [3]	PoQDB	Blockchain and Cobweb	IoT	MQTT	Data Security
Wang et.al [26]	Blockchain and PUF-Based based Authentication Protocol	Blockchain	Smart Healthcare	Smart Contracts	HAS
Hellani et al. [13]	Tangle the Blockchain	Blockchain and Tangle	IoT	Smart Contracts	Data Security
Bathalapalli et al. [5]	PUFchain 2.0	Blockchain	Smart Healthcare	Proof-of-PUF Enabled Authentication	HAS
PUFchain 3.0 (Current Paper)	**PUFchain 3.0**	IOTA Tangle	Smart Healthcare	MAM	HAS

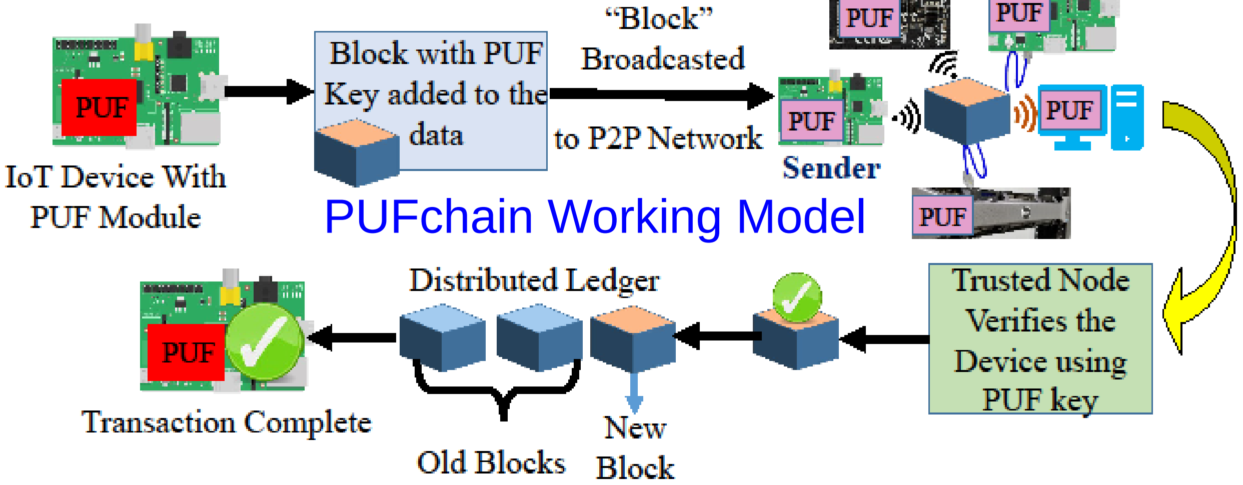
PUFchain: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare

PUFchain: Our Hardware-Assisted Scalable Blockchain



PUFchain System Model

Can provide:
Device, System, and
Data Security



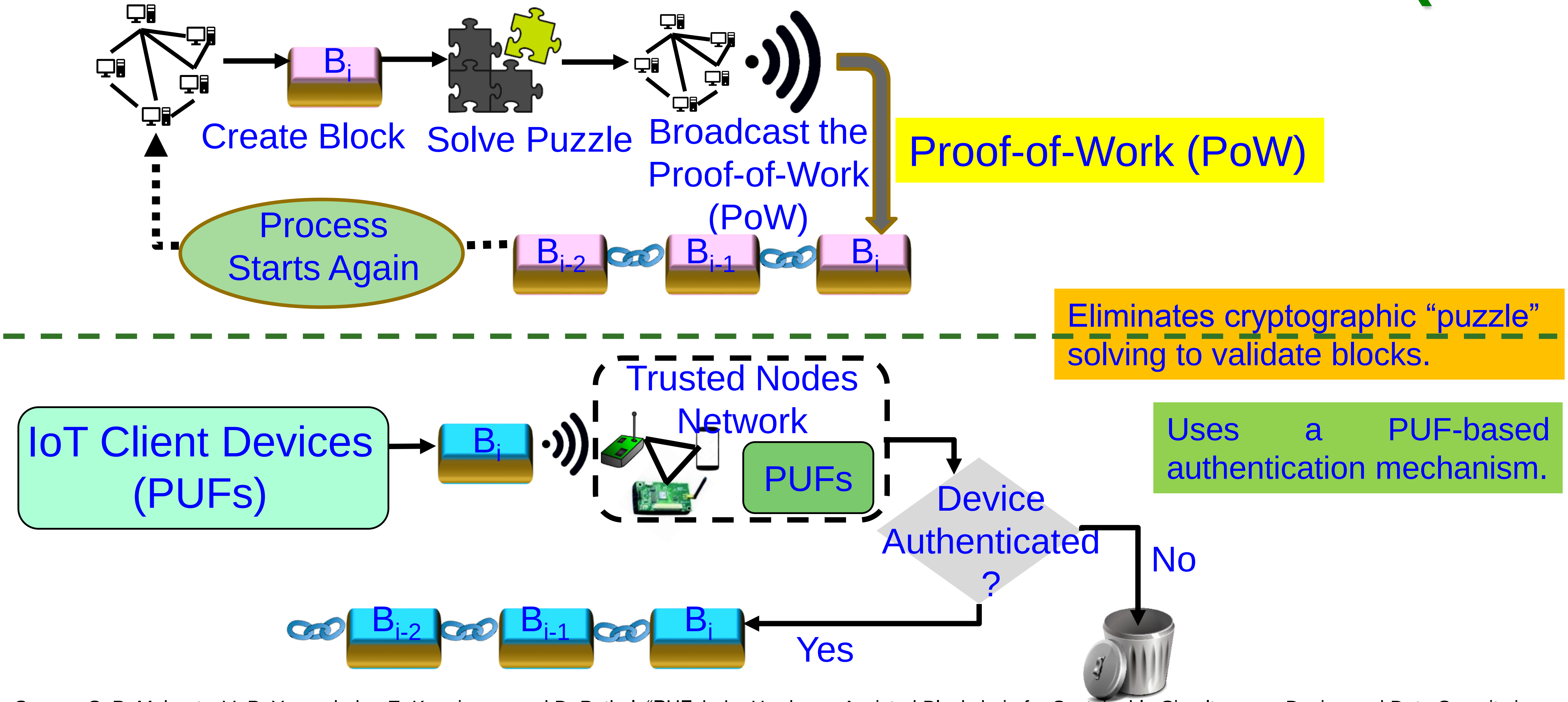
PUFchain Working Model

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

- ✓ 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 Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

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



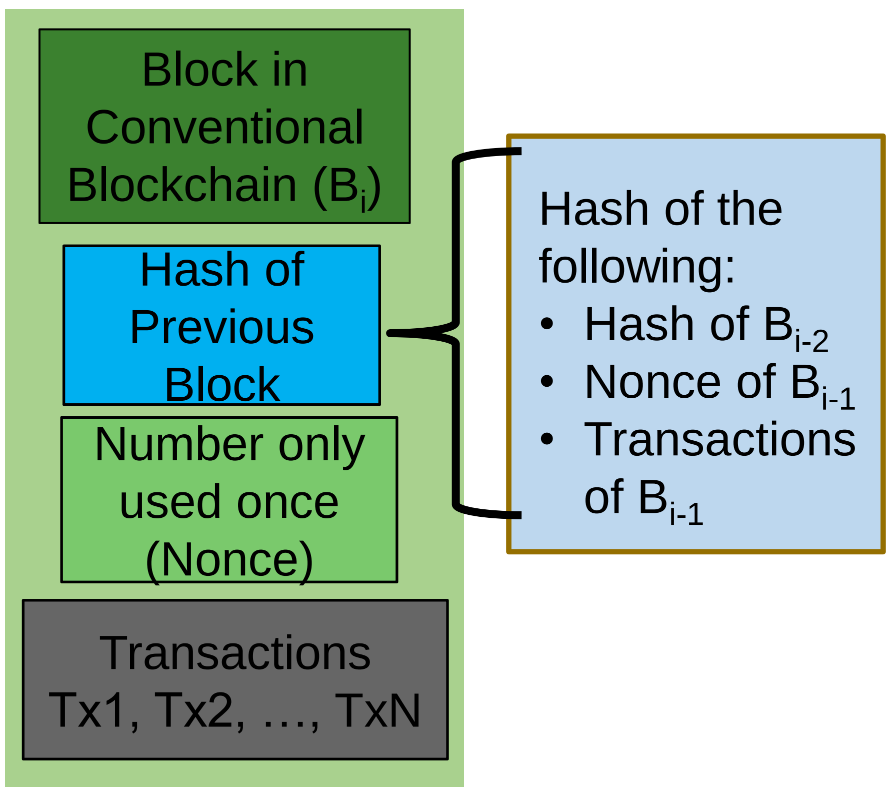
Proof-of-Work (PoW)

Eliminates cryptographic “puzzle” solving to validate blocks.

Uses a PUF-based authentication mechanism.

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. 8-16.

PUFchain: Proposed New Block Structure



Block in Conventional Blockchain (B_i)

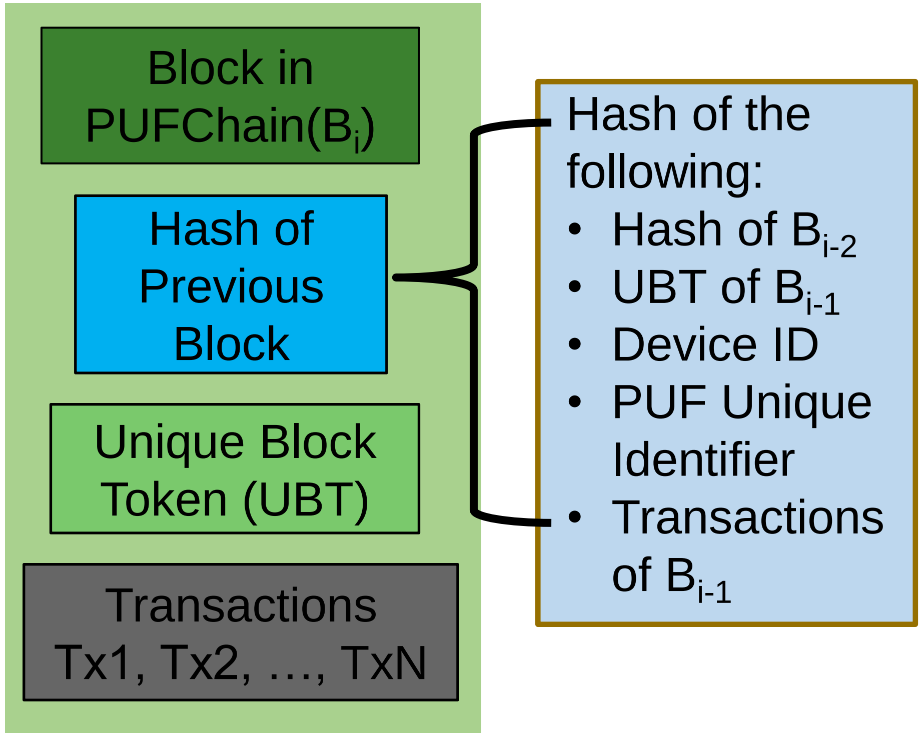
Hash of Previous Block

Number only used once (Nonce)

Transactions Tx1, Tx2, …, TxN

Hash of the following:
- Hash of B_{i-2}
- Nonce of B_{i-1}
- Transactions of B_{i-1}

Conventional Block Structure



Block in PUFChain(B_i)

Hash of Previous Block

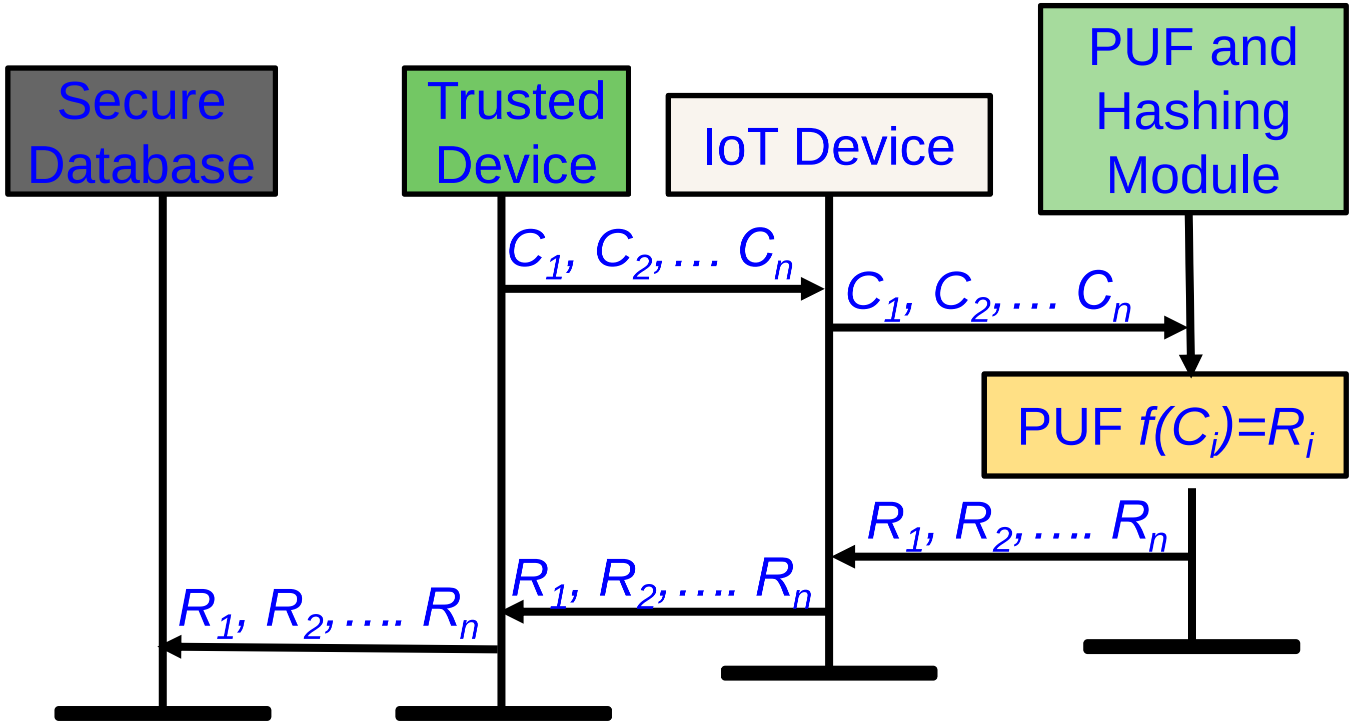
Unique Block Token (UBT)

Transactions Tx1, Tx2, …, TxN

Hash of the following:
- Hash of B_{i-2}
- UBT of B_{i-1}
- Device ID
- PUF Unique Identifier
- Transactions of B_{i-1}

Proposed Block Structure for PUFchain

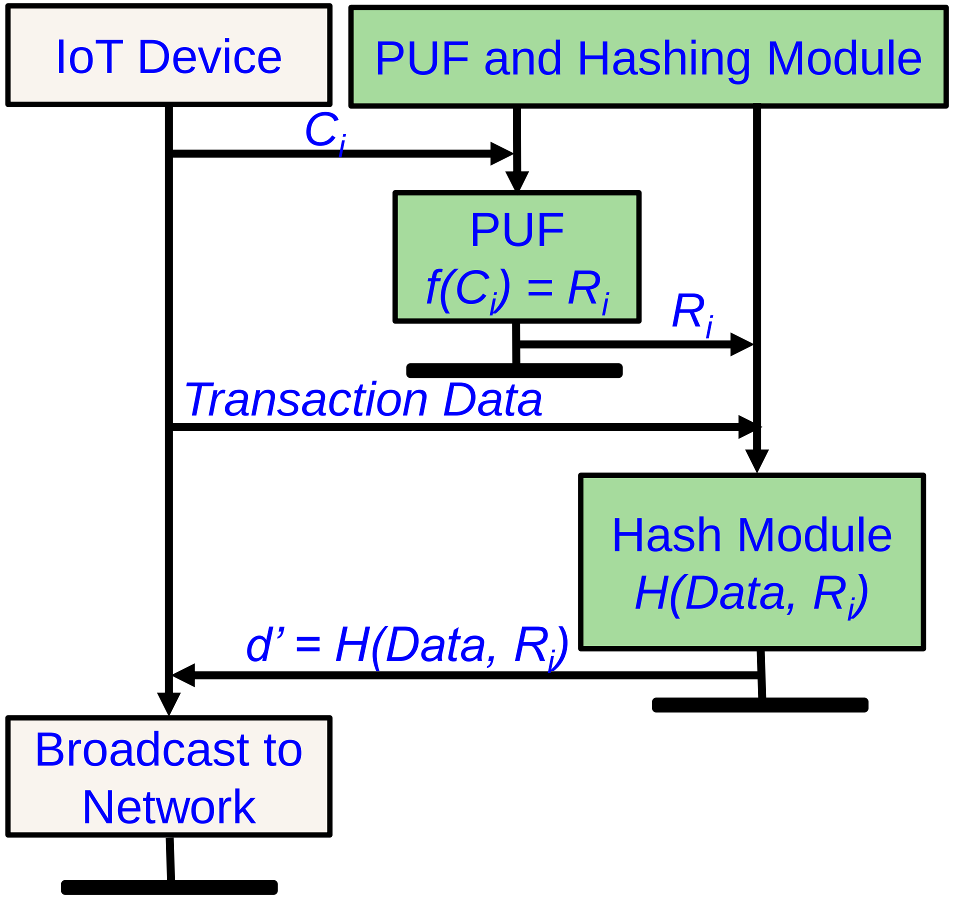
PUFchain: Device Enrollment Steps



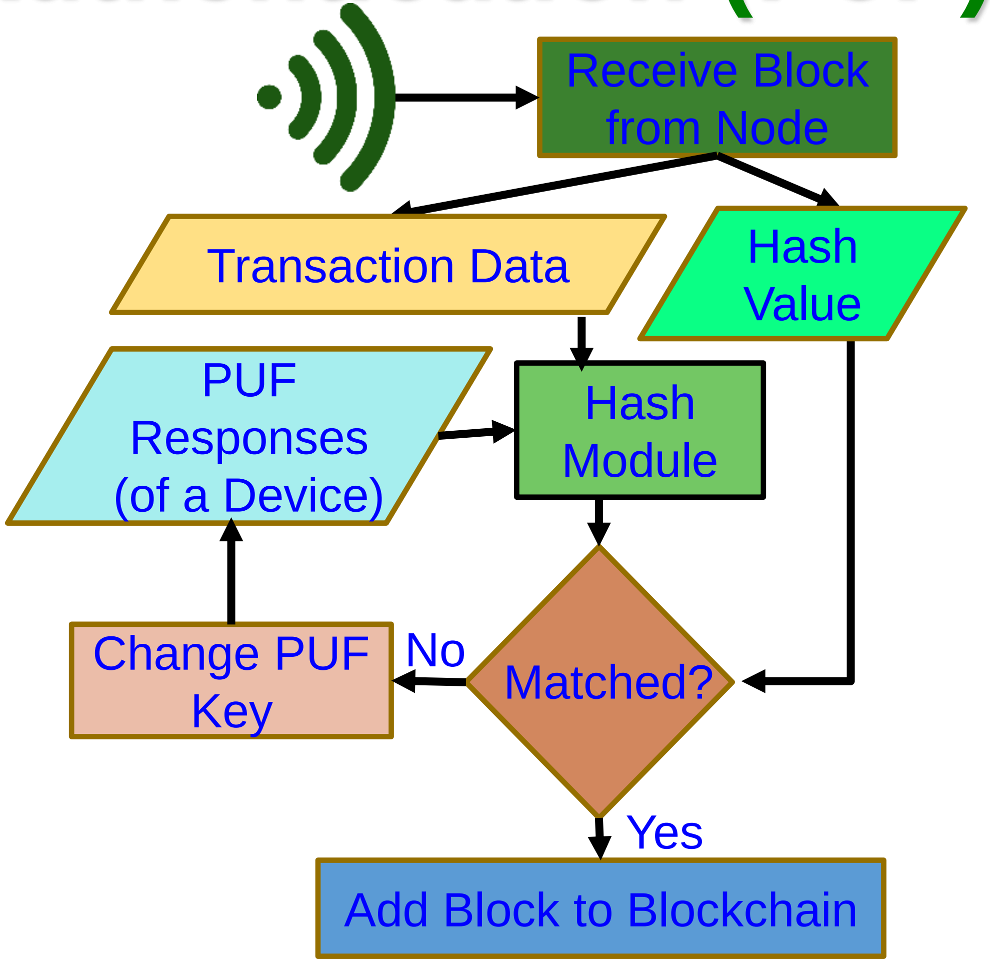
Device Enrollment Steps

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.

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



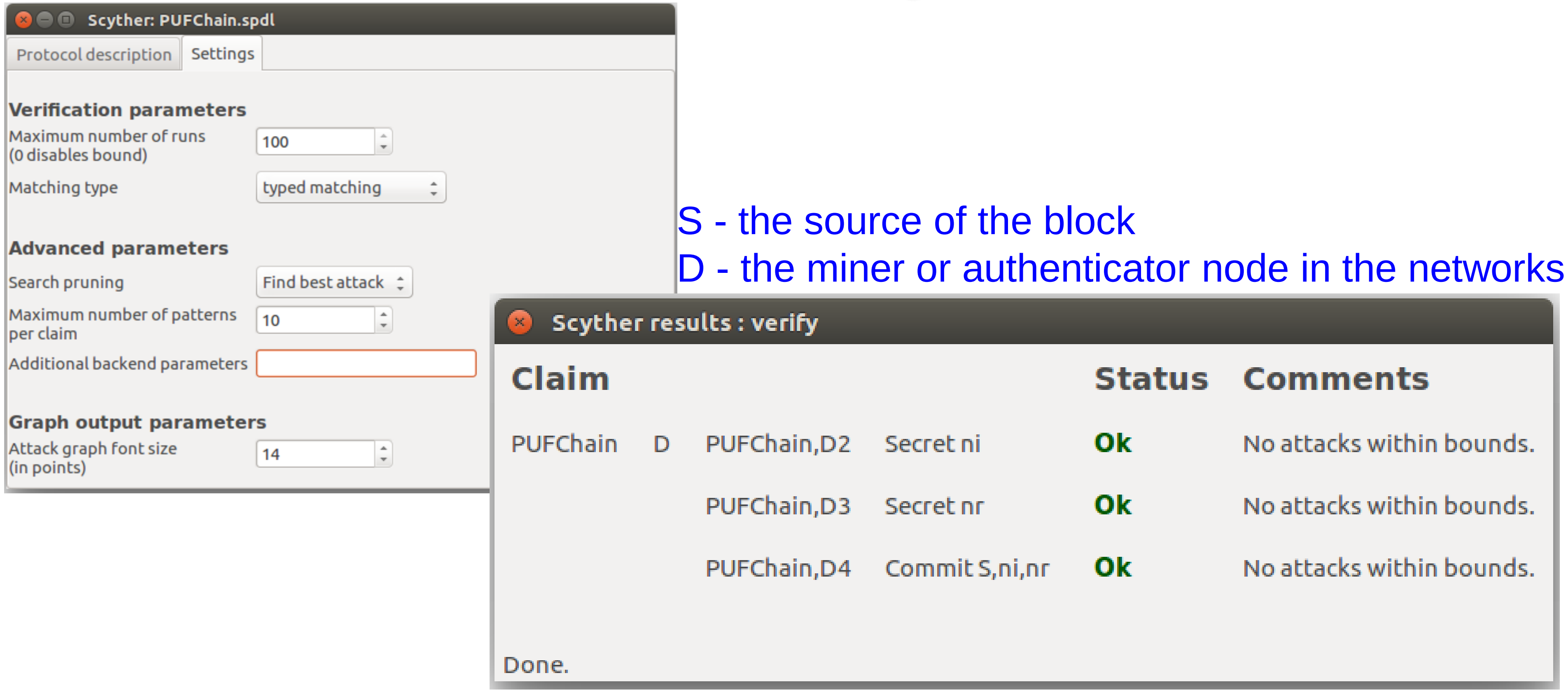
Steps for Transactions Initiation



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. 8-16.

PUFchain Security Validation



Scyther: PUFChain.spdl

Protocol description | Settings

Verification parameters

Maximum number of runs (0 disables bound): 100

Matching type: typed matching

Advanced parameters

Search pruning: Find best attack

Maximum number of patterns per claim: 10

Additional backend parameters:

Graph output parameters

Attack graph font size (in points): 14

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

Scyther results : verify

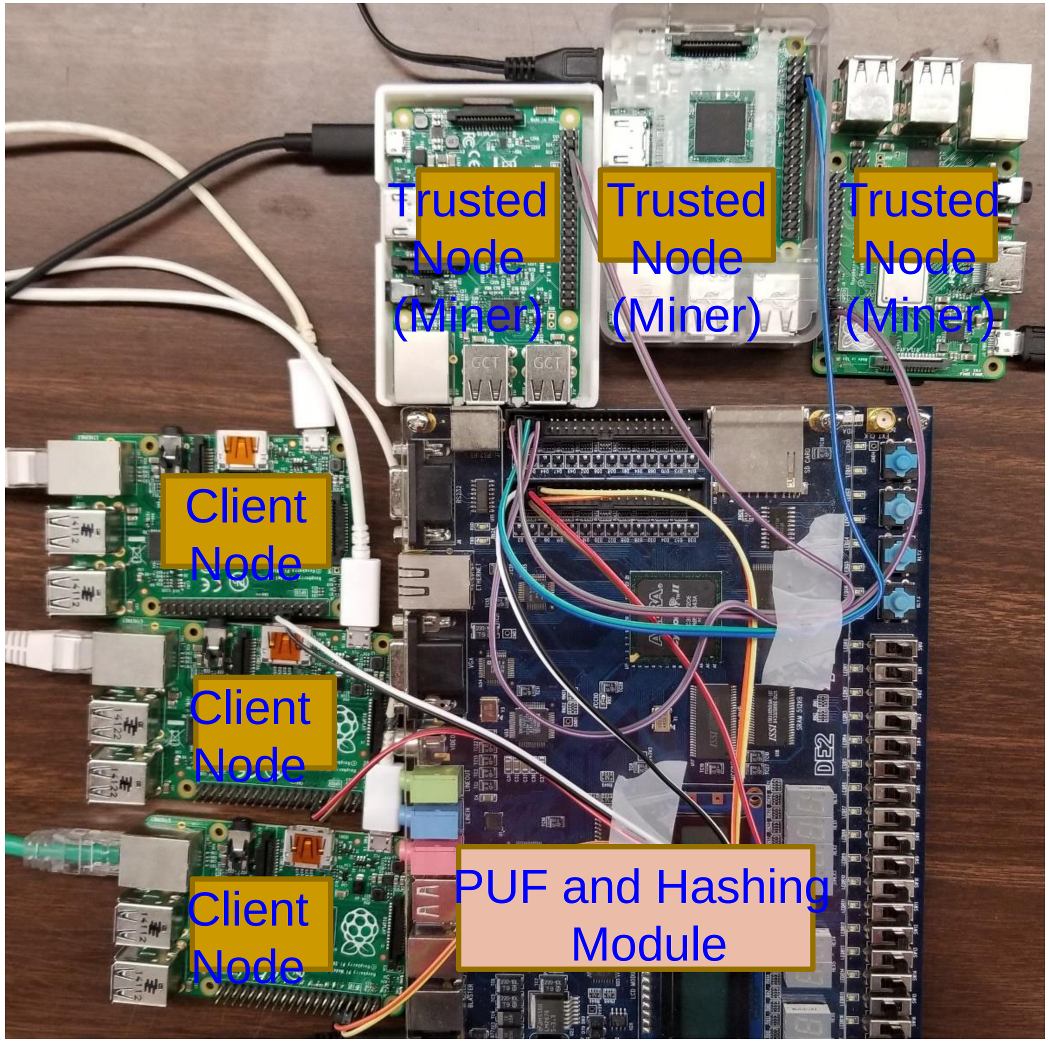
Claim				Status	Comments
PUFChain	D	PUFChain,D2	Secret ni	Ok	No attacks within bounds.
		PUFChain,D3	Secret nr	Ok	No attacks within bounds.
		PUFChain,D4	Commit S,ni,nr	Ok	No attacks within bounds.

Done.

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

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. 8-16.

Our PoP is 1000X Faster than PoW



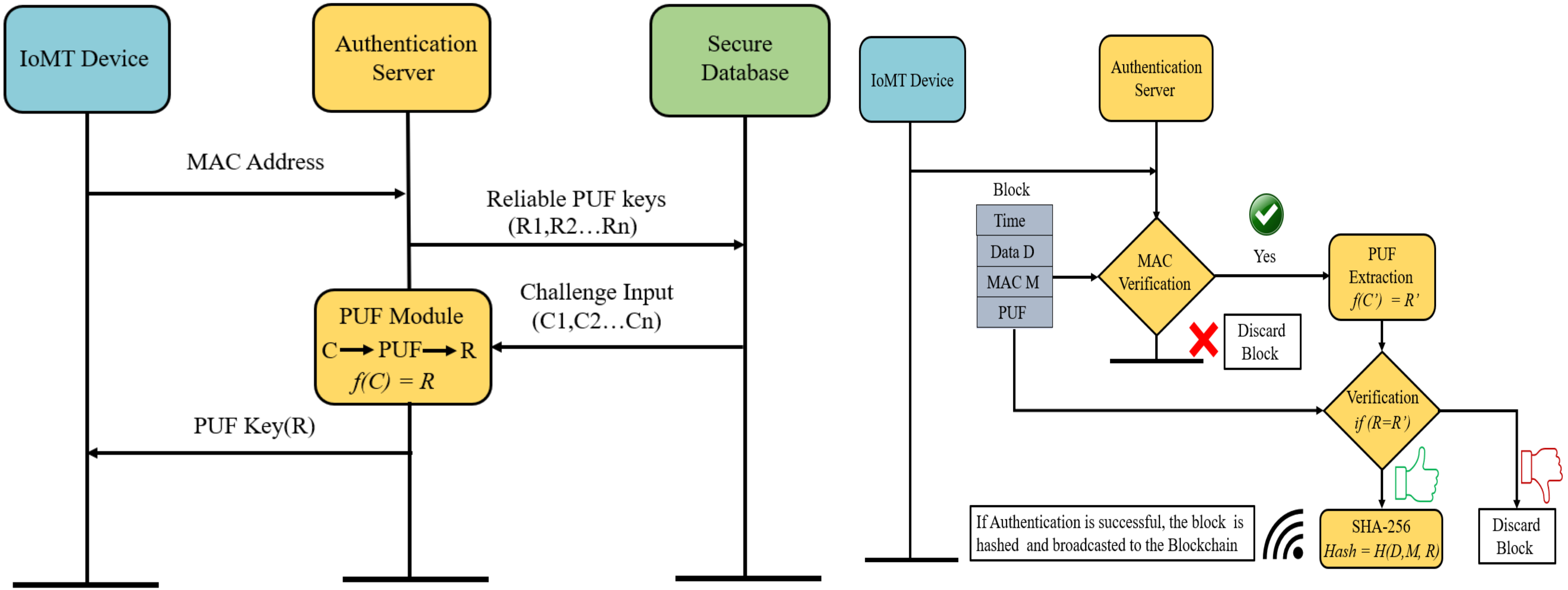
PoW - 10 min in cloud	PoAh – 950ms in Raspberry Pi	PoP - 192ms in Raspberry Pi
High Power	3 W Power	5 W Power

- ✓ 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 Data Security in Internet of Everything (IoE)”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

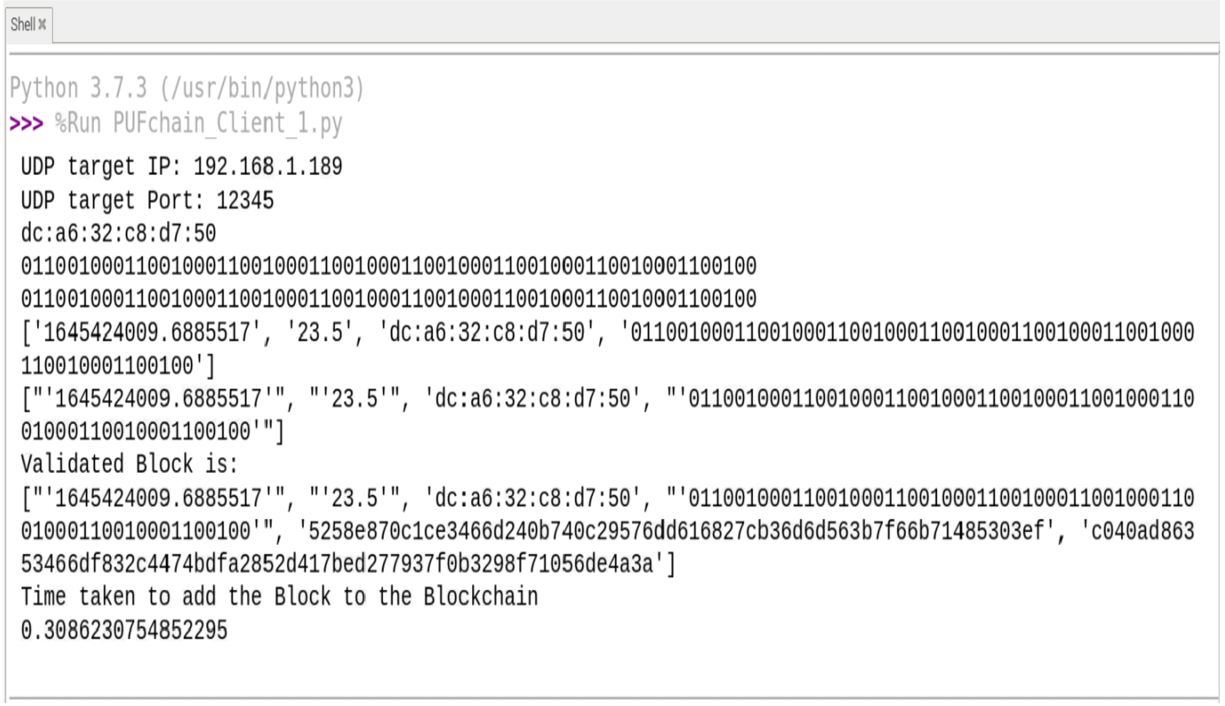
PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare

PUFchain 2.0 Enrollment and Authentication

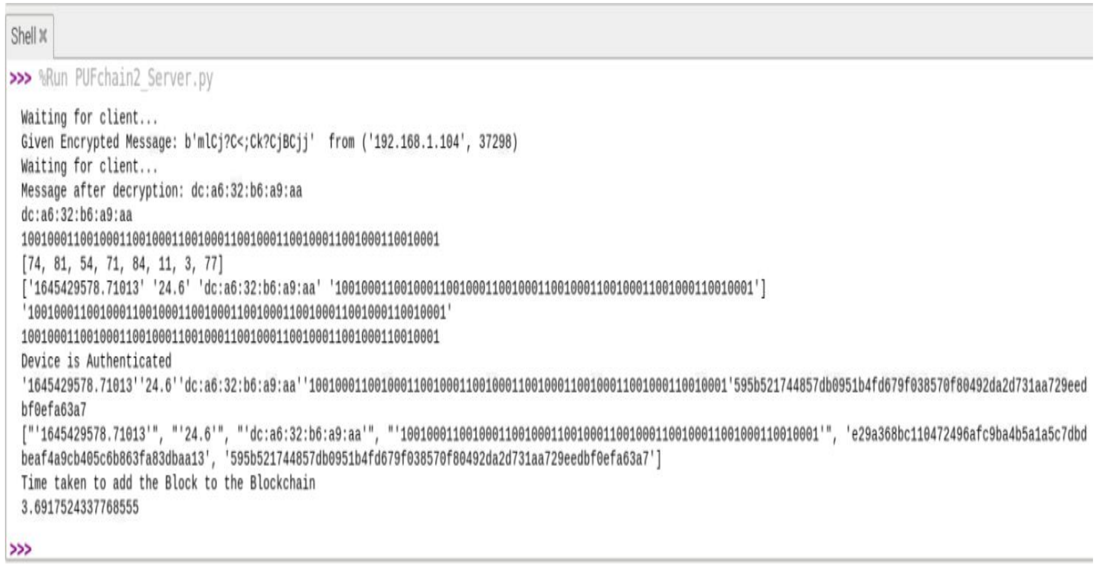


Source:V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344, 19-pages, DOI: https://doi.org/10.1007/s42979-022-01238-2.

Implementation and Validation of PUFchain 2.0



```
Python 3.7.3 (/usr/bin/python3)
>>> %Run PUFchain_Client_1.py
 UDP target IP: 192.168.1.189
 UDP target Port: 12345
 dc:a6:32:c8:d7:50
 0110010001100100011001000110010001100100011001000110010001100100
 0110010001100100011001000110010001100100011001000110010001100100
 ['1645424009.6885517', '23.5', 'dc:a6:32:c8:d7:50', '0110010001100100011001000110010001100100011001000
 110010001100100']
 ["'1645424009.6885517'", "'23.5'", 'dc:a6:32:c8:d7:50', "'01100100011001000110010001100100011001000110
 01000110010001100100'"]
 Validated Block is:
 ["'1645424009.6885517'", "'23.5'", 'dc:a6:32:c8:d7:50', "'01100100011001000110010001100100011001000110
 01000110010001100100'", '5258e870c1ce3466d240b740c29576dd616827cb36d6d563b7f66b71485303ef', 'c040ad863
 53466df832c4474bdfa2852d417bed277937f0b3298f71056de4a3a']
 Time taken to add the Block to the Blockchain
 0.3086230754852295
```



```
>>> %Run PUFchain2_Server.py
 Waiting for client...
 Given Encrypted Message: b'mlCj?C<;Ck?CjBCjj'  from ('192.168.1.104', 37298)
 Waiting for client...
 Message after decryption: dc:a6:32:b6:a9:aa
 dc:a6:32:b6:a9:aa
 1001000110010001100100011001000110010001100100011001000110010001
 [74, 81, 54, 71, 84, 11, 3, 77]
 ['1645429578.71013' '24.6' 'dc:a6:32:b6:a9:aa' '1001000110010001100100011001000110010001100100011001000110010001']
 '1001000110010001100100011001000110010001100100011001000110010001'
 1001000110010001100100011001000110010001100100011001000110010001
 Device is Authenticated
 '1645429578.71013''24.6''dc:a6:32:b6:a9:aa''1001000110010001100100011001000110010001100100011001000110010001'595b521744857db0951b4fd679f038570f80492da2d731aa729eed
 bf0efa63a7
 ["'1645429578.71013'", "'24.6'", "'dc:a6:32:b6:a9:aa'", "'1001000110010001100100011001000110010001100100011001000110010001'", 'e29a368bc110472496afc9ba4b5a1a5c7dbd
 beaf4a9cb405c6b863fa83dbaa13', '595b521744857db0951b4fd679f038570f80492da2d731aa729eedbf0efa63a7']
 Time taken to add the Block to the Blockchain
 3.6917524337768555

>>>
```

Source:V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344, 19-pages, DOI: https://doi.org/10.1007/s42979-022-01238-2.

PUFchain 2.0 Results

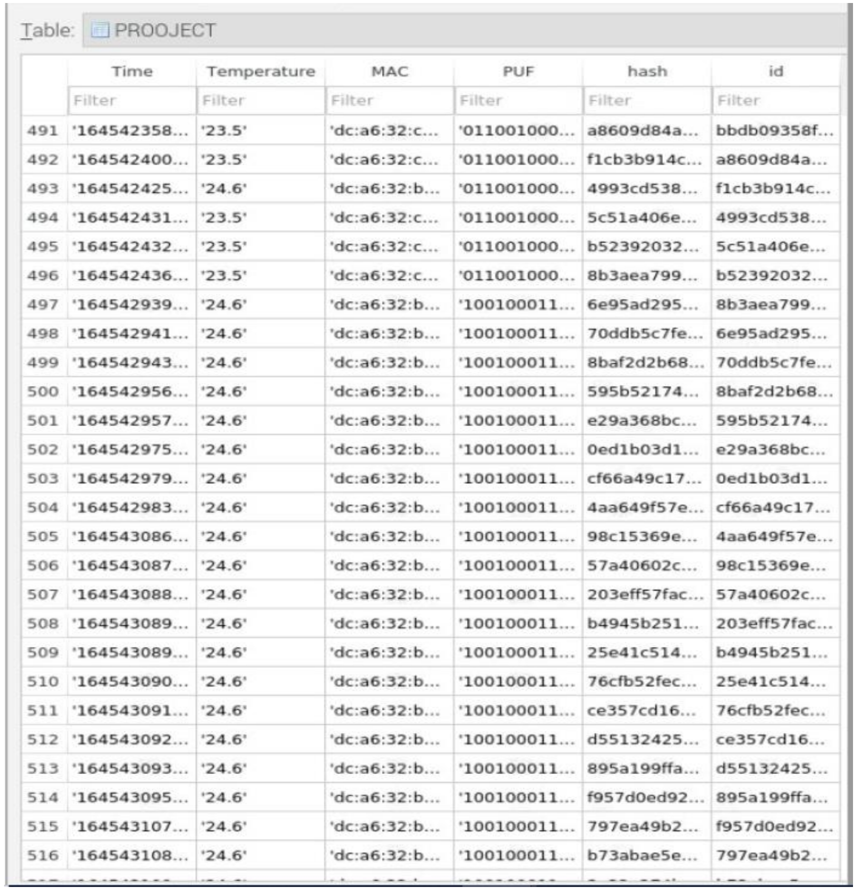
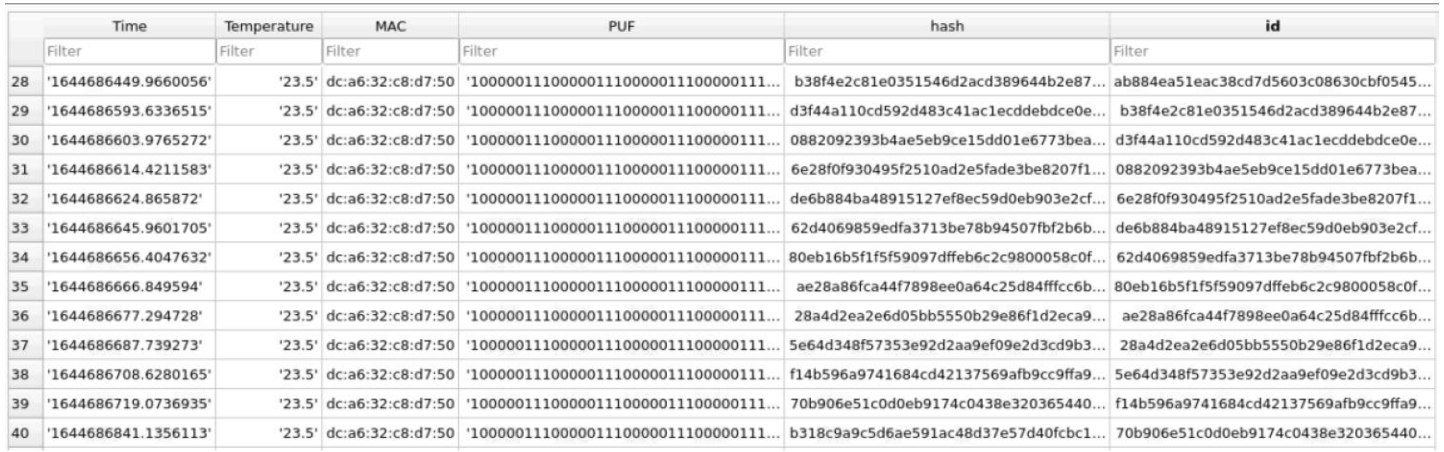


Table: PROOJECT

	Time	Temperature	MAC	PUF	hash	id
	Filter	Filter	Filter	Filter	Filter	Filter
491	'164542358...	'23.5'	'dc:a6:32:c...	'011001000...	a8609d84a...	bbdb09358f...
492	'164542400...	'23.5'	'dc:a6:32:c...	'011001000...	f1cb3b914c...	a8609d84a...
493	'164542425...	'24.6'	'dc:a6:32:b...	'011001000...	4993cd538...	f1cb3b914c...
494	'164542431...	'23.5'	'dc:a6:32:c...	'011001000...	5c51a406e...	4993cd538...
495	'164542432...	'23.5'	'dc:a6:32:c...	'011001000...	b52392032...	5c51a406e...
496	'164542436...	'23.5'	'dc:a6:32:c...	'011001000...	8b3aea799...	b52392032...
497	'164542939...	'24.6'	'dc:a6:32:b...	'100100011...	6e95ad295...	8b3aea799...
498	'164542941...	'24.6'	'dc:a6:32:b...	'100100011...	70ddb5c7fe...	6e95ad295...
499	'164542943...	'24.6'	'dc:a6:32:b...	'100100011...	8baf2d2b68...	70ddb5c7fe...
500	'164542956...	'24.6'	'dc:a6:32:b...	'100100011...	595b52174...	8baf2d2b68...
501	'164542957...	'24.6'	'dc:a6:32:b...	'100100011...	e29a368bc...	595b52174...
502	'164542975...	'24.6'	'dc:a6:32:b...	'100100011...	0ed1b03d1...	e29a368bc...
503	'164542979...	'24.6'	'dc:a6:32:b...	'100100011...	cf66a49c17...	0ed1b03d1...
504	'164542983...	'24.6'	'dc:a6:32:b...	'100100011...	4aa649f57e...	cf66a49c17...
505	'164543086...	'24.6'	'dc:a6:32:b...	'100100011...	98c15369e...	4aa649f57e...
506	'164543087...	'24.6'	'dc:a6:32:b...	'100100011...	57a40602c...	98c15369e...
507	'164543088...	'24.6'	'dc:a6:32:b...	'100100011...	203eff57fac...	57a40602c...
508	'164543089...	'24.6'	'dc:a6:32:b...	'100100011...	b4945b251...	203eff57fac...
509	'164543089...	'24.6'	'dc:a6:32:b...	'100100011...	25e41c514...	b4945b251...
510	'164543090...	'24.6'	'dc:a6:32:b...	'100100011...	76cfb52fec...	25e41c514...
511	'164543091...	'24.6'	'dc:a6:32:b...	'100100011...	ce357cd16...	76cfb52fec...
512	'164543092...	'24.6'	'dc:a6:32:b...	'100100011...	d55132425...	ce357cd16...
513	'164543093...	'24.6'	'dc:a6:32:b...	'100100011...	895a199ffa...	d55132425...
514	'164543095...	'24.6'	'dc:a6:32:b...	'100100011...	f957d0ed92...	895a199ffa...
515	'164543107...	'24.6'	'dc:a6:32:b...	'100100011...	797ea49b2...	f957d0ed92...
516	'164543108...	'24.6'	'dc:a6:32:b...	'100100011...	b73abae5e...	797ea49b2...

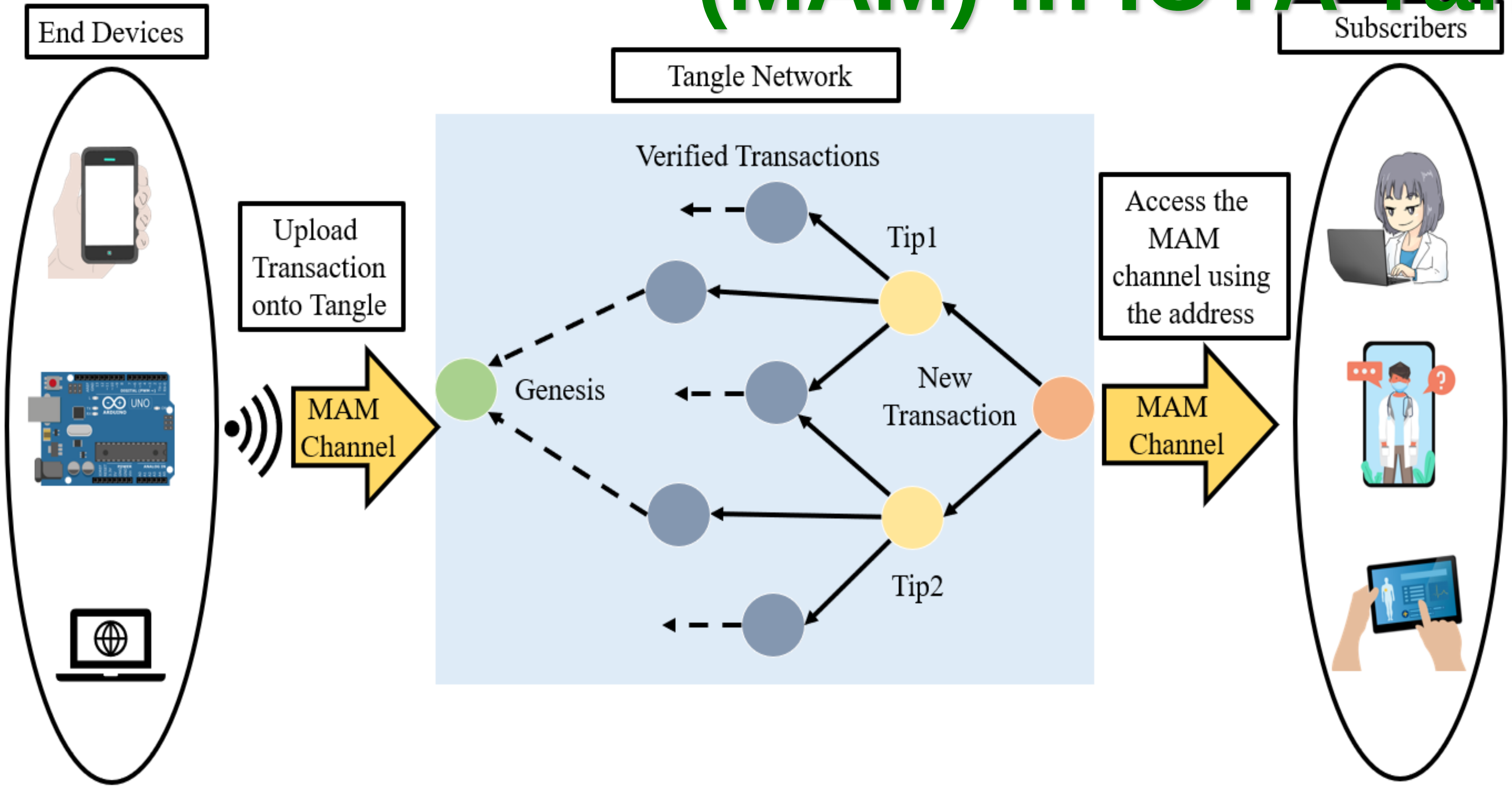


	Time	Temperature	MAC	PUF	hash	id
	Filter	Filter	Filter	Filter	Filter	Filter
28	'1644686449.9660056'	'23.5'	dc:a6:32:c8:d7:50	'100000111000001110000011100000111...	b38f4e2c81e0351546d2acd389644b2e87...	ab884ea51eac38cd7d5603c08630cbf0545...
29	'1644686593.6336515'	'23.5'	dc:a6:32:c8:d7:50	'100000111000001110000011100000111...	d3f44a110cd592d483c41ac1ecddebdce0e...	b38f4e2c81e0351546d2acd389644b2e87...
30	'1644686603.9765272'	'23.5'	dc:a6:32:c8:d7:50	'100000111000001110000011100000111...	0882092393b4ae5eb9ce15dd01e6773bea...	d3f44a110cd592d483c41ac1ecddebdce0e...
31	'1644686614.4211583'	'23.5'	dc:a6:32:c8:d7:50	'100000111000001110000011100000111...	6e28f0f930495f2510ad2e5fade3be8207f1...	0882092393b4ae5eb9ce15dd01e6773bea...
32	'1644686624.865872'	'23.5'	dc:a6:32:c8:d7:50	'100000111000001110000011100000111...	de6b884ba48915127ef8ec59d0eb903e2cf...	6e28f0f930495f2510ad2e5fade3be8207f1...
33	'1644686645.9601705'	'23.5'	dc:a6:32:c8:d7:50	'100000111000001110000011100000111...	62d4069859edfa3713be78b94507fbf2b6b...	de6b884ba48915127ef8ec59d0eb903e2cf...
34	'1644686656.4047632'	'23.5'	dc:a6:32:c8:d7:50	'100000111000001110000011100000111...	80eb16b5f1f5f59097dffeb6c2c9800058c0f...	62d4069859edfa3713be78b94507fbf2b6b...
35	'1644686666.849594'	'23.5'	dc:a6:32:c8:d7:50	'100000111000001110000011100000111...	ae28a86fca44f7898ee0a64c25d84fffcc6b...	80eb16b5f1f5f59097dffeb6c2c9800058c0f...
36	'1644686677.294728'	'23.5'	dc:a6:32:c8:d7:50	'100000111000001110000011100000111...	28a4d2ea2e6d05bb5550b29e86f1d2eca9...	ae28a86fca44f7898ee0a64c25d84fffcc6b...
37	'1644686687.739273'	'23.5'	dc:a6:32:c8:d7:50	'100000111000001110000011100000111...	5e64d348f57353e92d2aa9ef09e2d3cd9b3...	28a4d2ea2e6d05bb5550b29e86f1d2eca9...
38	'1644686708.6280165'	'23.5'	dc:a6:32:c8:d7:50	'100000111000001110000011100000111...	f14b596a9741684cd42137569afb9cc9ffa9...	5e64d348f57353e92d2aa9ef09e2d3cd9b3...
39	'1644686719.0736935'	'23.5'	dc:a6:32:c8:d7:50	'100000111000001110000011100000111...	70b906e51c0d0eb9174c0438e320365440...	f14b596a9741684cd42137569afb9cc9ffa9...
40	'1644686841.1356113'	'23.5'	dc:a6:32:c8:d7:50	'100000111000001110000011100000111...	b318c9a9c5d6ae591ac48d37e57d40fcbc1...	70b906e51c0d0eb9174c0438e320365440...

Source:V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344, 19-pages, DOI: https://doi.org/10.1007/s42979-022-01238-2.

PUFchain 3.0: Hardware-Assisted Distributed Ledger for Robust Authentication in the Internet of Medical Things

Masked Authentication Messaging (MAM) in IOTA Tangle



- ➢ Provides Device and Data security in IoT
- ➢ Works in Three modes: Public, Private and Restricted

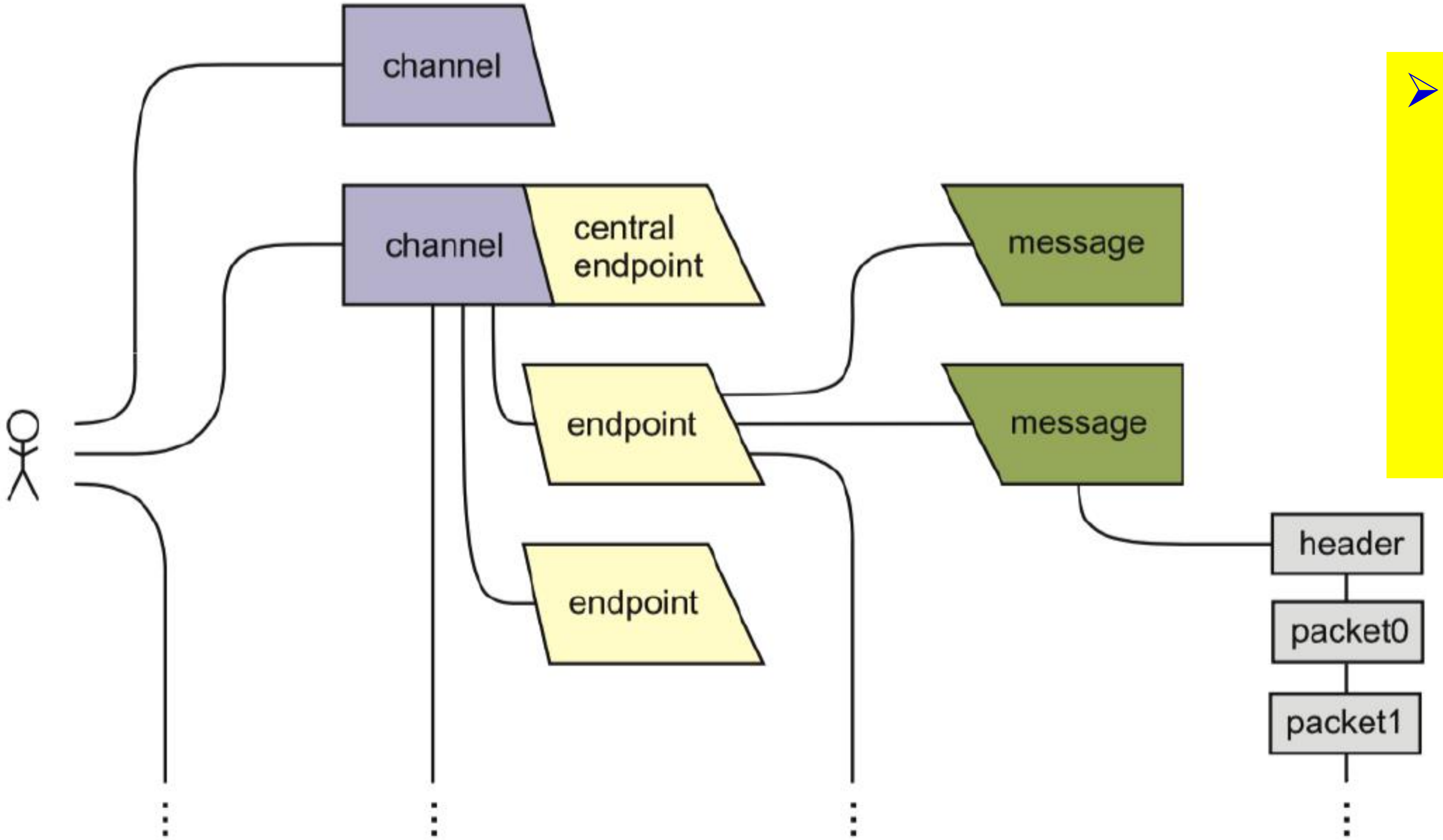
MAM Modes

Public Mode: In Public mode, the IoT device which is the source collects the data and uploads it onto Tangle. A MAM channel with an address is generated for the secure exchange of information. The address of the channel will be the root of the Merkle Tree. The subsequent transaction must be submitted to the MAM channel using this fetched root.

Private Mode: For applications requiring privacy and confidentiality, as in the case of health record management, the root of the Merkle tree is hashed and the obtained hash is used as the address of the channel to publish and access the data.

Restricted Mode: The restricted mode of MAM works by using a channel Authorization key or Side key along with the Merkle root. The address of the channel for the next transaction is generated by computing the hash of the Merkle root and side key.

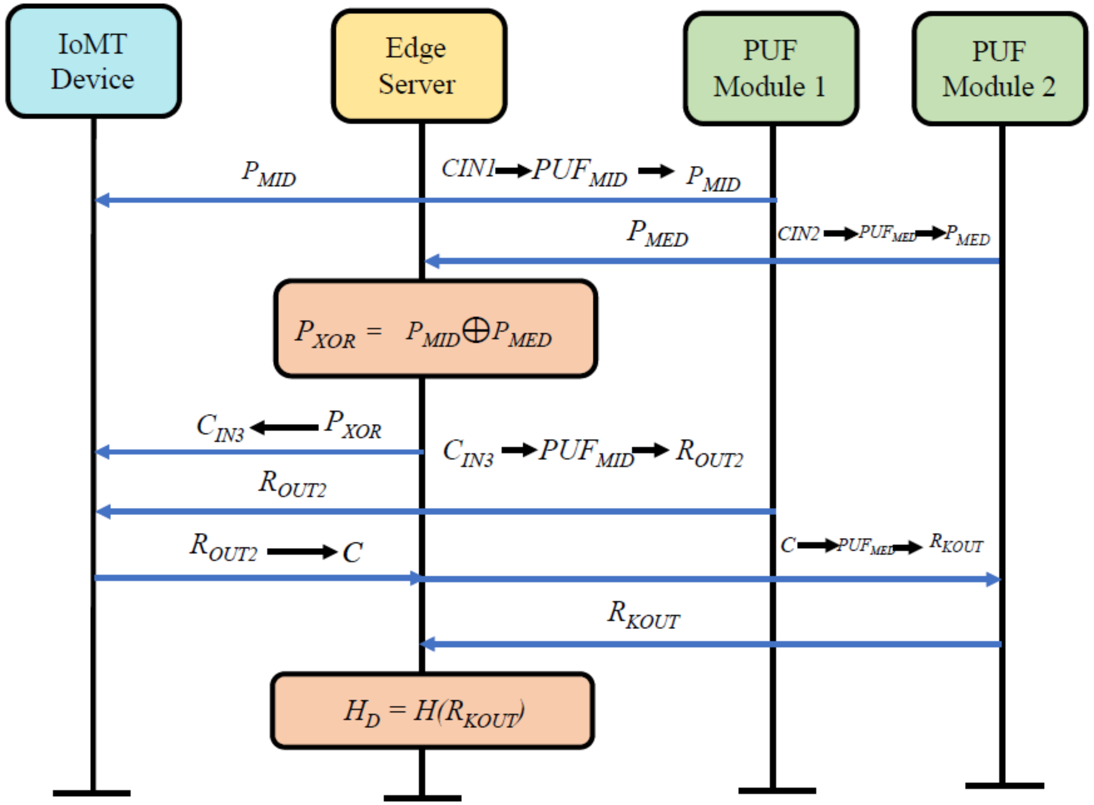
MAM Channel



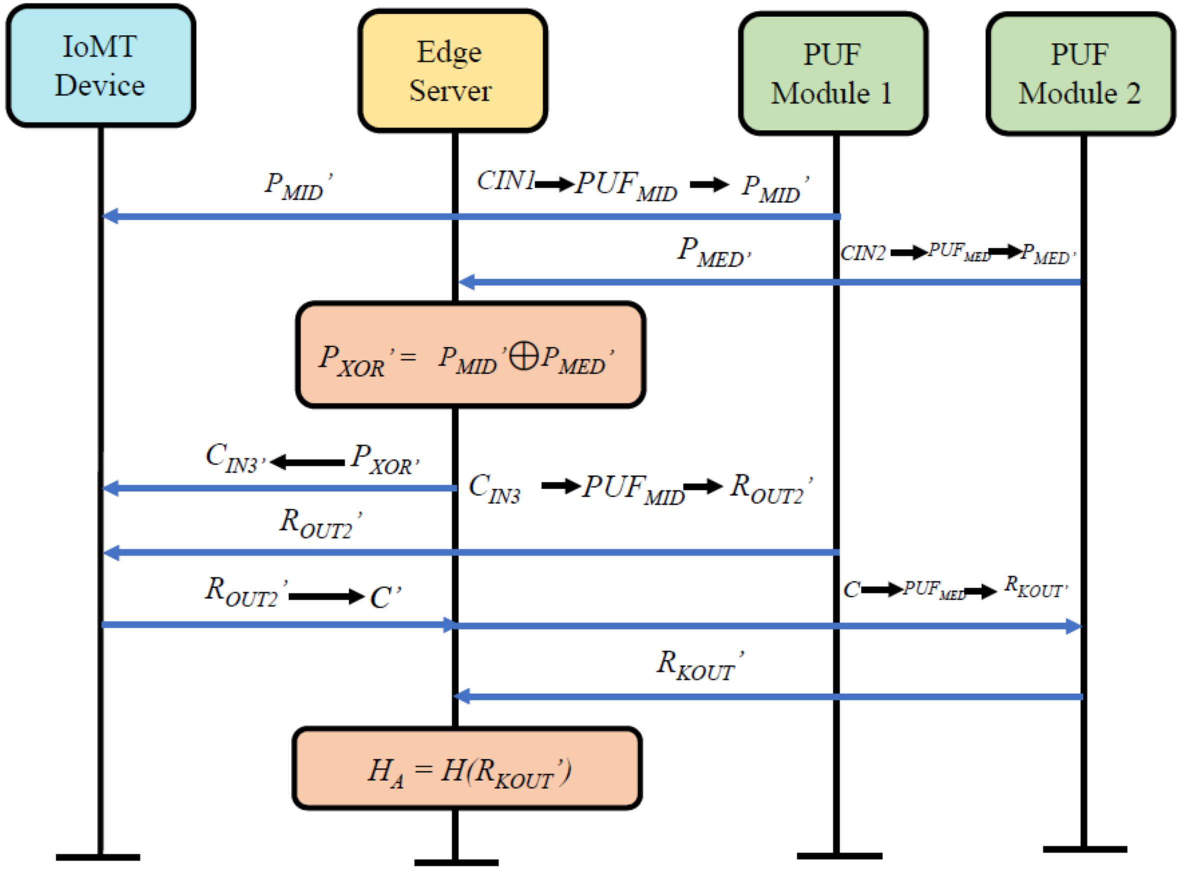
- MAM Channel once initiated consists of a sequence of transactions where each transaction provides an address for the next transaction

Source: Lamtzidis, O.; Pettas, D.; Gialelis, J. A Novel Combination of Distributed Ledger Technologies on Internet of Things: Use Case on Precision Agriculture. *Appl. Syst. Innov.* **2019**, *2*, 30. https://doi.org/10.3390/asi2030030

Working Flow of PUFchain 3.0

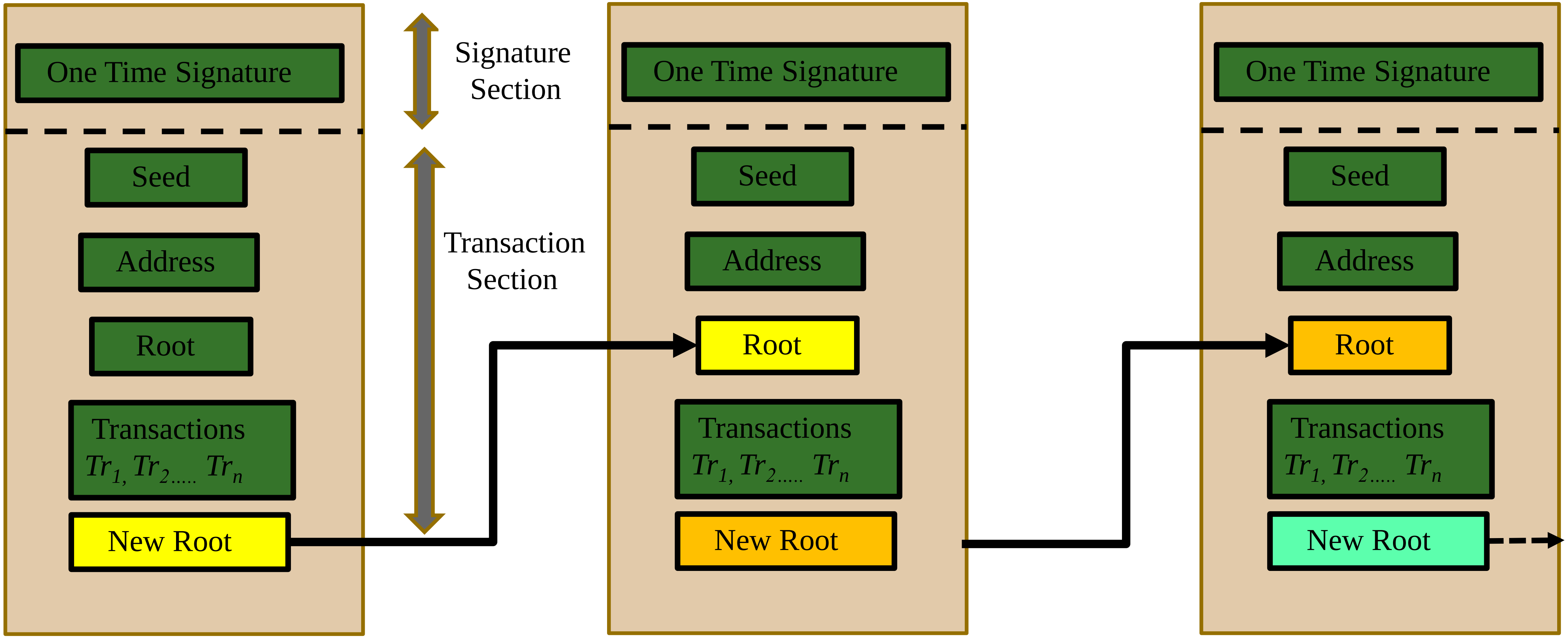

IoMT Device
Edge Server
PUF Module 1
PUF Module 2
P_{MID}
$CIN1 \rightarrow PUF_{MID} \rightarrow P_{MID}$
P_{MED}
$CIN2 \rightarrow PUF_{MED} \rightarrow P_{MED}$
$P_{XOR} = P_{MID} \oplus P_{MED}$
$C_{IN3} \leftarrow P_{XOR}$
$C_{IN3} \rightarrow PUF_{MID} \rightarrow R_{OUT2}$
R_{OUT2}
$R_{OUT2} \rightarrow C$
$C \rightarrow PUF_{MED} \rightarrow R_{KOUT}$
R_{KOUT}
$H_D = H(R_{KOUT})$

Steps for Device Registration

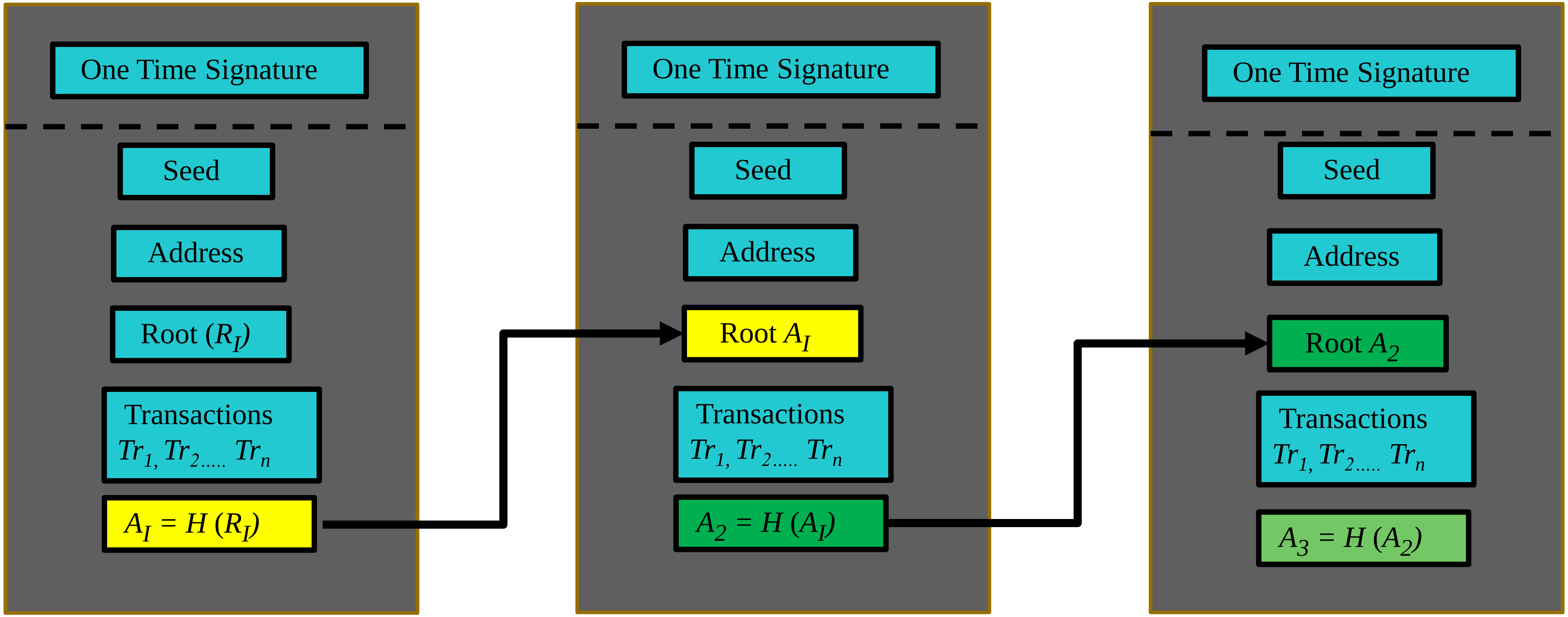

IoMT Device
Edge Server
PUF Module 1
PUF Module 2
P_{MID}'
$CIN1 \rightarrow PUF_{MID} \rightarrow P_{MID}'$
P_{MED}'
$CIN2 \rightarrow PUF_{MED} \rightarrow P_{MED}'$
$P_{XOR}' = P_{MID}' \oplus P_{MED}'$
$C_{IN3}' \leftarrow P_{XOR}'$
$C_{IN3} \rightarrow PUF_{MID} \rightarrow R_{OUT2}'$
R_{OUT2}'
$R_{OUT2}' \rightarrow C'$
$C \rightarrow PUF_{MED} \rightarrow R_{KOUT}'$
R_{KOUT}'
$H_A = H(R_{KOUT}')$

Steps for Authentication

MAM in Public Mode



MAM in Private Mode



One Time Signature

Seed

Address

Root (R_I)

Transactions

$Tr_{1,} Tr_{2.....} Tr_n$

$A_I = H\,(R_I)$

One Time Signature

Seed

Address

Root A_I

Transactions

$Tr_{1,} Tr_{2.....} Tr_n$

$A_2 = H\,(A_I)$

One Time Signature

Seed

Address

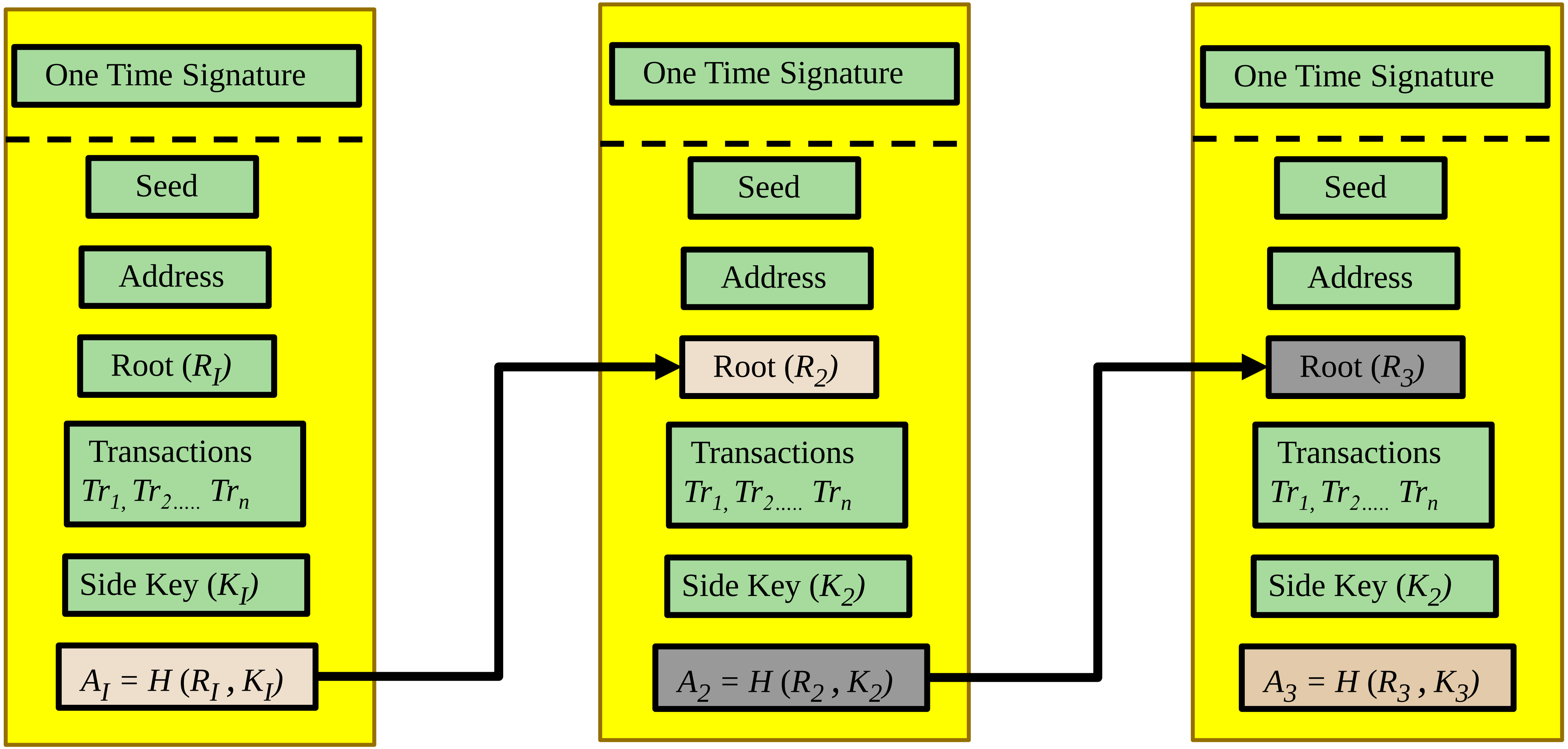
Root A_2

Transactions

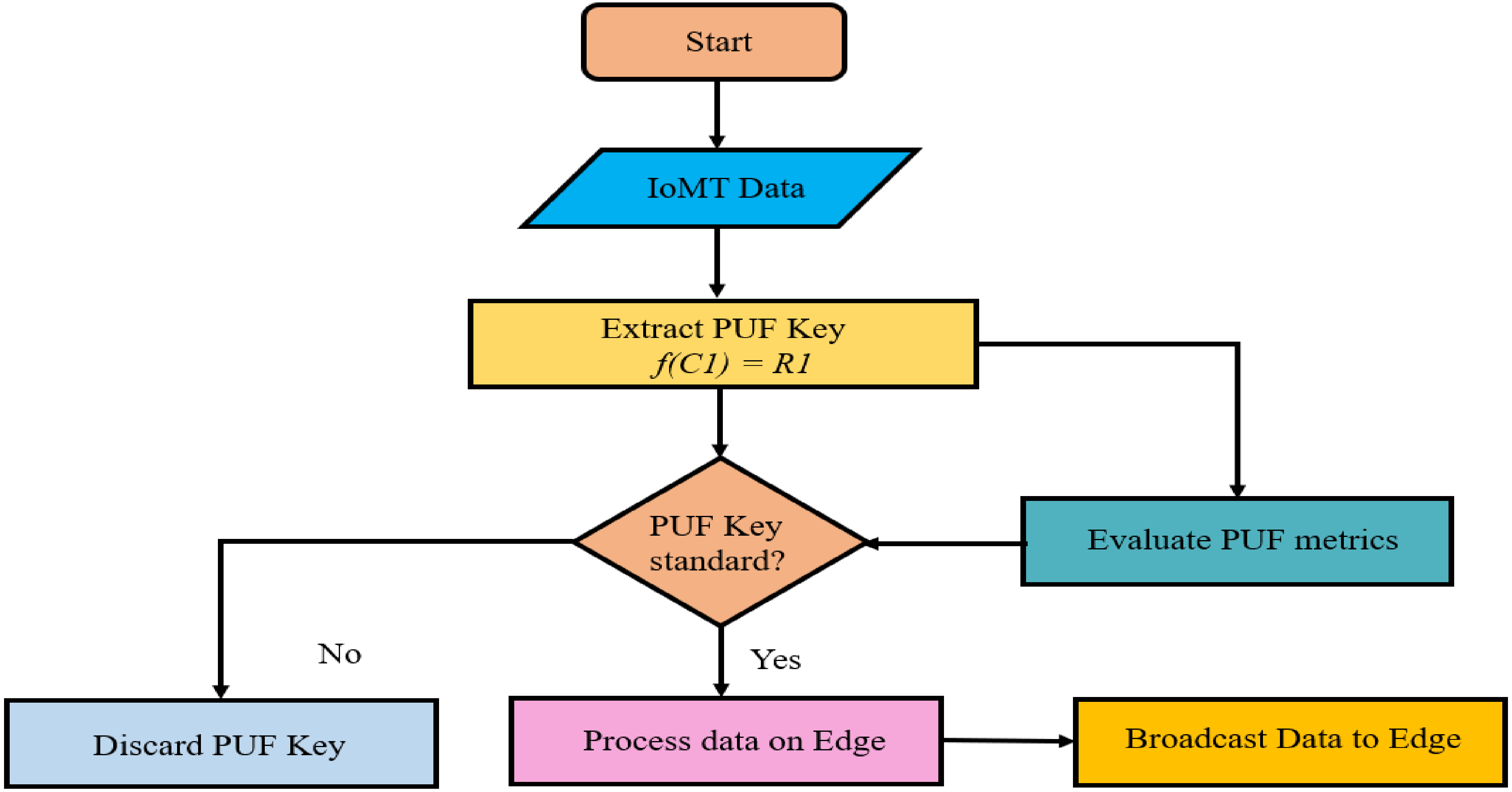
$Tr_{1,} Tr_{2.....} Tr_n$

$A_3 = H\,(A_2)$

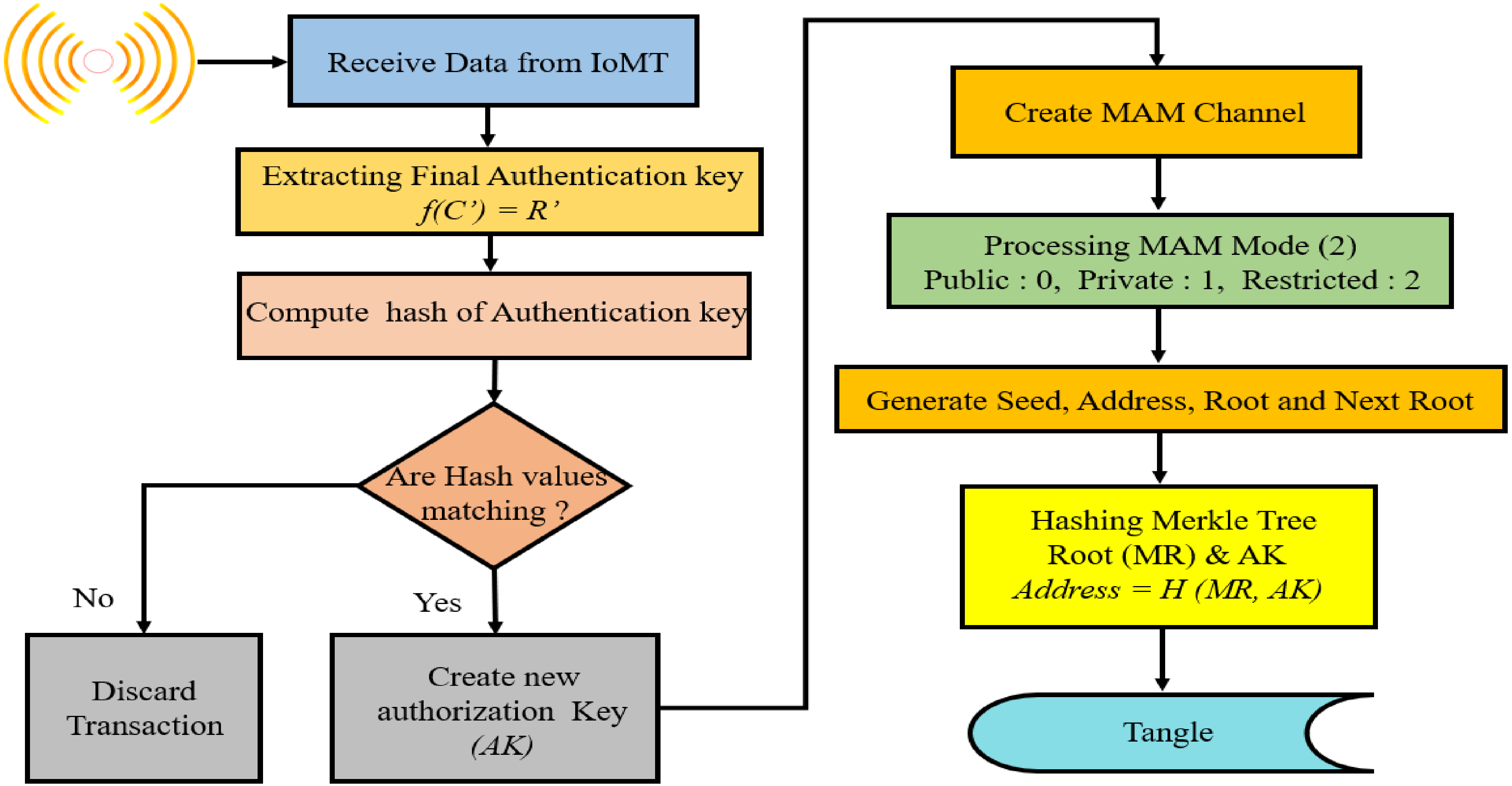
MAM in Restricted Mode



PUFChain 3.0 Enrollment



Authentication



Receive Data from IoMT

Extracting Final Authentication key
$f(C') = R'$

Compute hash of Authentication key

Are Hash values matching ?

No

Discard Transaction

Yes

Create new authorization Key (AK)

Create MAM Channel

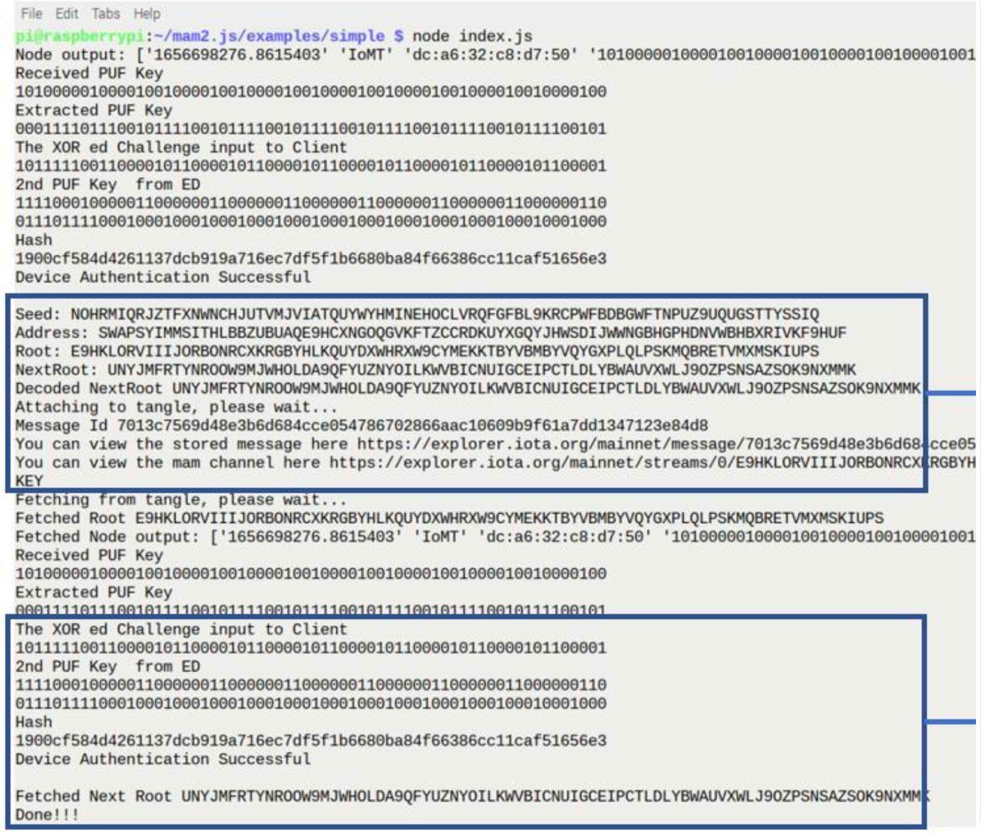
Processing MAM Mode (2)
Public : 0, Private : 1, Restricted : 2

Generate Seed, Address, Root and Next Root

Hashing Merkle Tree Root (MR) & AK
$Address = H\ (MR, AK)$

Tangle

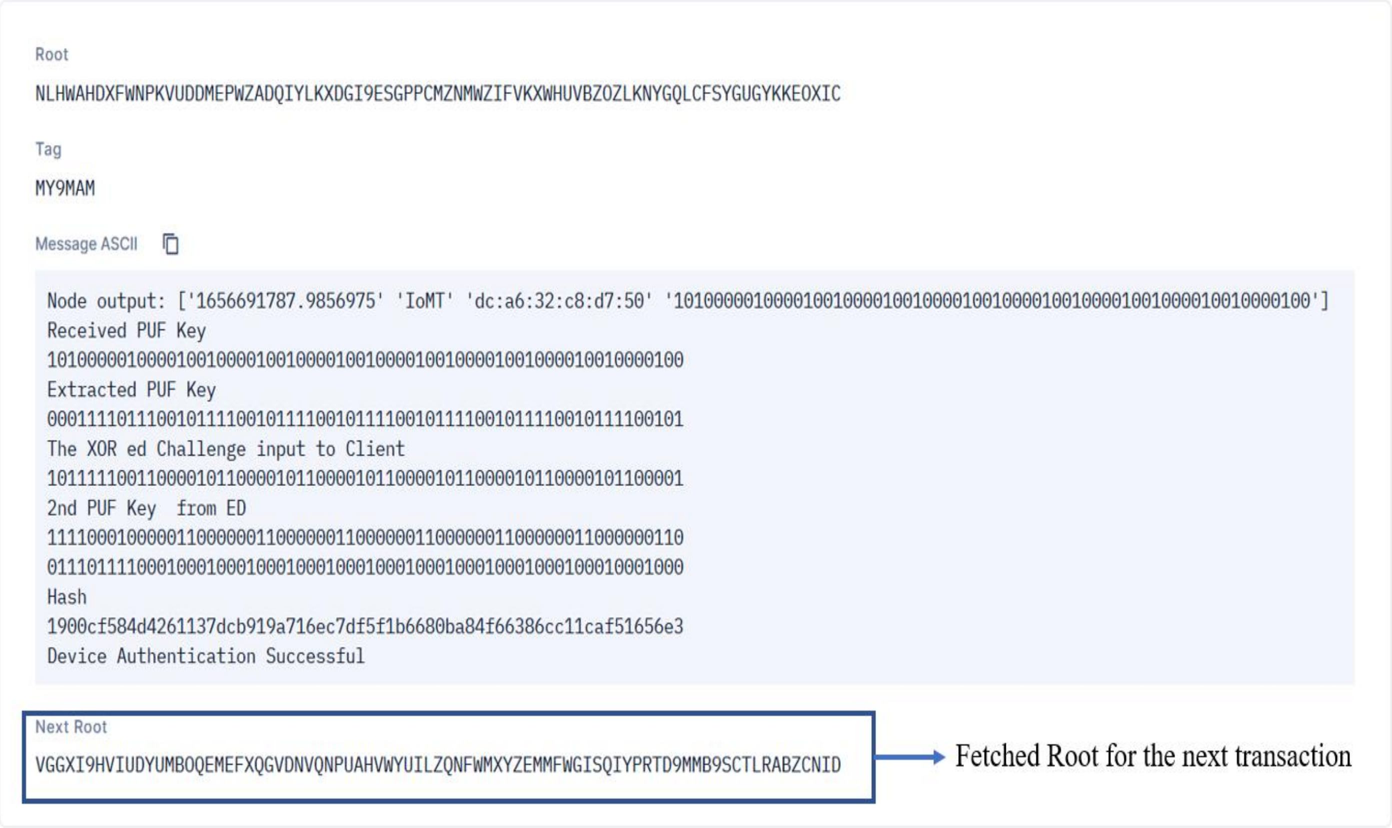
Implementation and Validation



```
pi@raspberrypi:~/mam2.js/examples/simple $ node index.js
Node output: ['1656698276.8615403' 'IoMT' 'dc:a6:32:c8:d7:50' '1010000010000100100001001000010010000100
Received PUF Key
1010000010000100100001001000010010000100100001001000010010000100
Extracted PUF Key
0001111011100101111001011110010111100101111001011110010111100101
The XOR ed Challenge input to Client
1011111001100001011000010110000101100001011000010110000101100001
2nd PUF Key  from ED
1111000100000011000000110000001100000011000000110000001100000110
0111011110001000100010001000100010001000100010001000100010001000
Hash
1900cf584d4261137dcb919a716ec7df5f1b6680ba84f66386cc11caf51656e3
Device Authentication Successful

Seed: NOHRMIQRJZTFXNWNCHJUTVMJVIATQUYWYHMINEHOCLVRQFGFBL9KRCPWFBDBGWFTNPUZ9UQUGSTTYSSIQ
Address: SWAPSYIMMSITHLBBZUBUAQE9HCXNGOQGVKFTZCCRDKUYXGQYJHWSDIJWWNGBHGPHDNVWBHBXRIVKF9HUF
Root: E9HKLORVIIIJORBONRCXKRGBYHLKQUYDXWHRXW9CYMEKKTBYVBMBYVQYGXPLQLPSKMQBRETVMXMSKIUPS
NextRoot: UNYJMFRTYNROOW9MJWHOLDA9QFYUZNYOILKWVBICNUIGCEIPCTLDLYBWAUVXWLJ9OZPSNSAZSOK9NXMMK
Decoded NextRoot UNYJMFRTYNROOW9MJWHOLDA9QFYUZNYOILKWVBICNUIGCEIPCTLDLYBWAUVXWLJ9OZPSNSAZSOK9NXMMK
Attaching to tangle, please wait...
Message Id 7013c7569d48e3b6d684cce054786702866aac10609b9f61a7dd1347123e84d8
You can view the stored message here https://explorer.iota.org/mainnet/message/7013c7569d48e3b6d684cce05
You can view the mam channel here https://explorer.iota.org/mainnet/streams/0/E9HKLORVIIIJORBONRCXKRGBYH
KEY
Fetching from tangle, please wait...
Fetched Root E9HKLORVIIIJORBONRCXKRGBYHLKQUYDXWHRXW9CYMEKKTBYVBMBYVQYGXPLQLPSKMQBRETVMXMSKIUPS
Fetched Node output: ['1656698276.8615403' 'IoMT' 'dc:a6:32:c8:d7:50' '1010000010000100100001001000010010000100
Received PUF Key
1010000010000100100001001000010010000100100001001000010010000100
Extracted PUF Key
0001111011100101111001011110010111100101111001011110010111100101
The XOR ed Challenge input to Client
1011111001100001011000010110000101100001011000010110000101100001
2nd PUF Key  from ED
1111000100000011000000110000001100000011000000110000001100000110
0111011110001000100010001000100010001000100010001000100010001000
Hash
1900cf584d4261137dcb919a716ec7df5f1b6680ba84f66386cc11caf51656e3
Device Authentication Successful

Fetched Next Root UNYJMFRTYNROOW9MJWHOLDA9QFYUZNYOILKWVBICNUIGCEIPCTLDLYBWAUVXWLJ9OZPSNSAZSOK9NXMMK
Done!!!
```



Root

NLHWAHDXFWNPKVUDDMEPWZADQIYLKXDGI9ESGPPCMZNMWZIFVKXWHUVBZOZLKNYGQLCFSYGUGYKKEOXIC

Tag

MY9MAM

Message ASCII

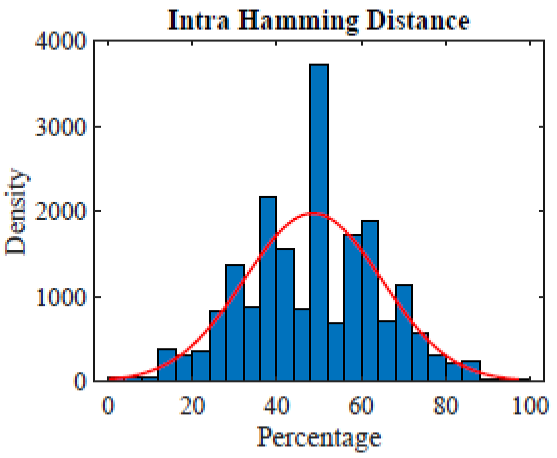
```
Node output: ['1656691787.9856975' 'IoMT' 'dc:a6:32:c8:d7:50' '1010000010000100100001001000010010000100100001001000010010000100']
Received PUF Key
1010000010000100100001001000010010000100100001001000010010000100
Extracted PUF Key
0001111011100101111001011110010111100101111001011110010111100101
The XOR ed Challenge input to Client
1011111001100001011000010110000101100001011000010110000101100001
2nd PUF Key  from ED
1111000100000011000000110000001100000011000000110000001100000110
0111011110001000100010001000100010001000100010001000100010001000
Hash
1900cf584d4261137dcb919a716ec7df5f1b6680ba84f66386cc11caf51656e3
Device Authentication Successful
```

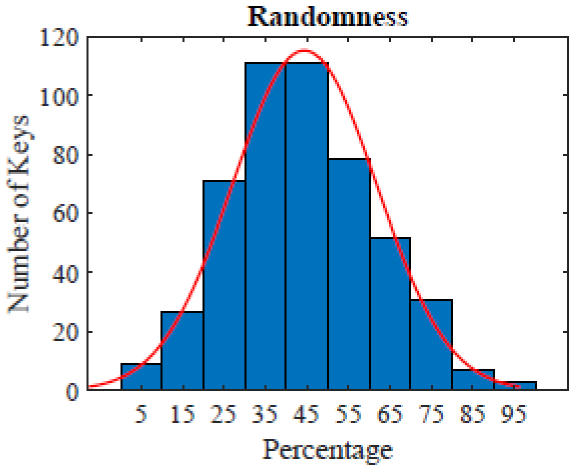
Next Root

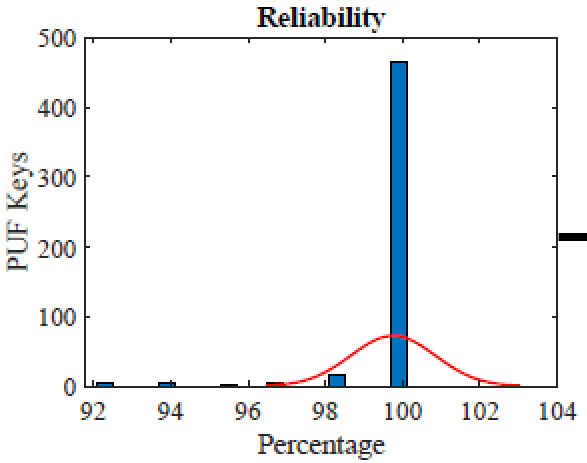
VGGXI9HVIUDYUMBOQEMEFXQGVDNVQNPUAHVWYUILZQNFWMXYZEMMFWGISQIYPRTD9MMB9SCTLRABZCNID

Fetched Root for the next transaction

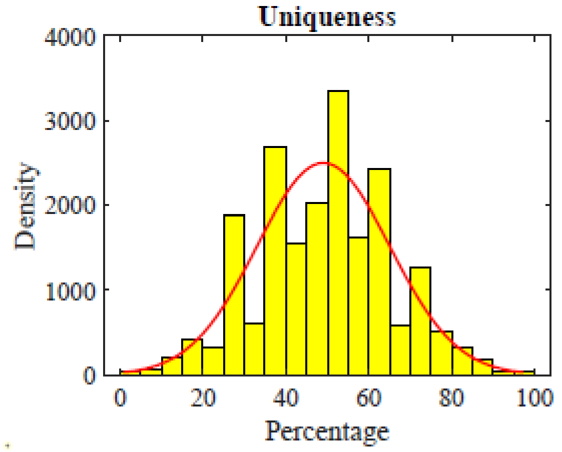
PUF Metrics

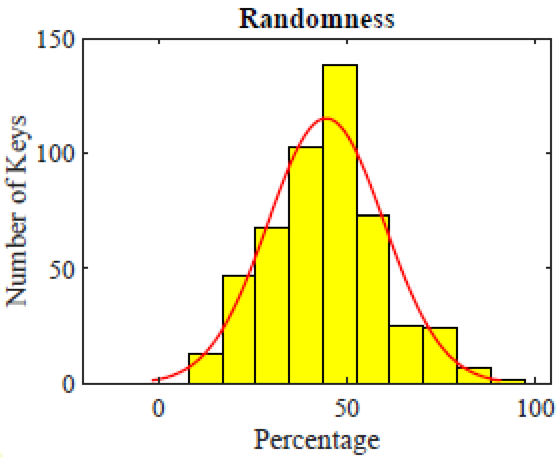


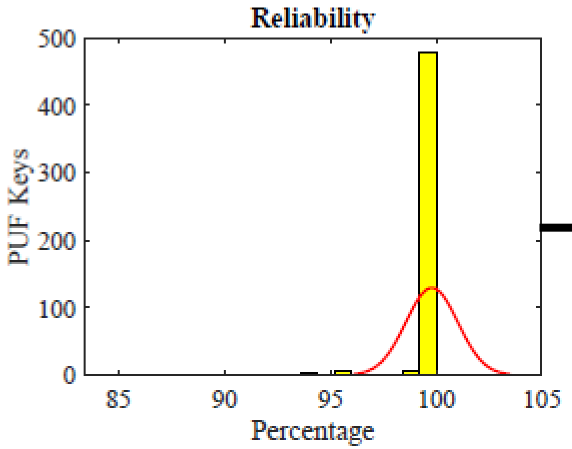




PUF Module 1

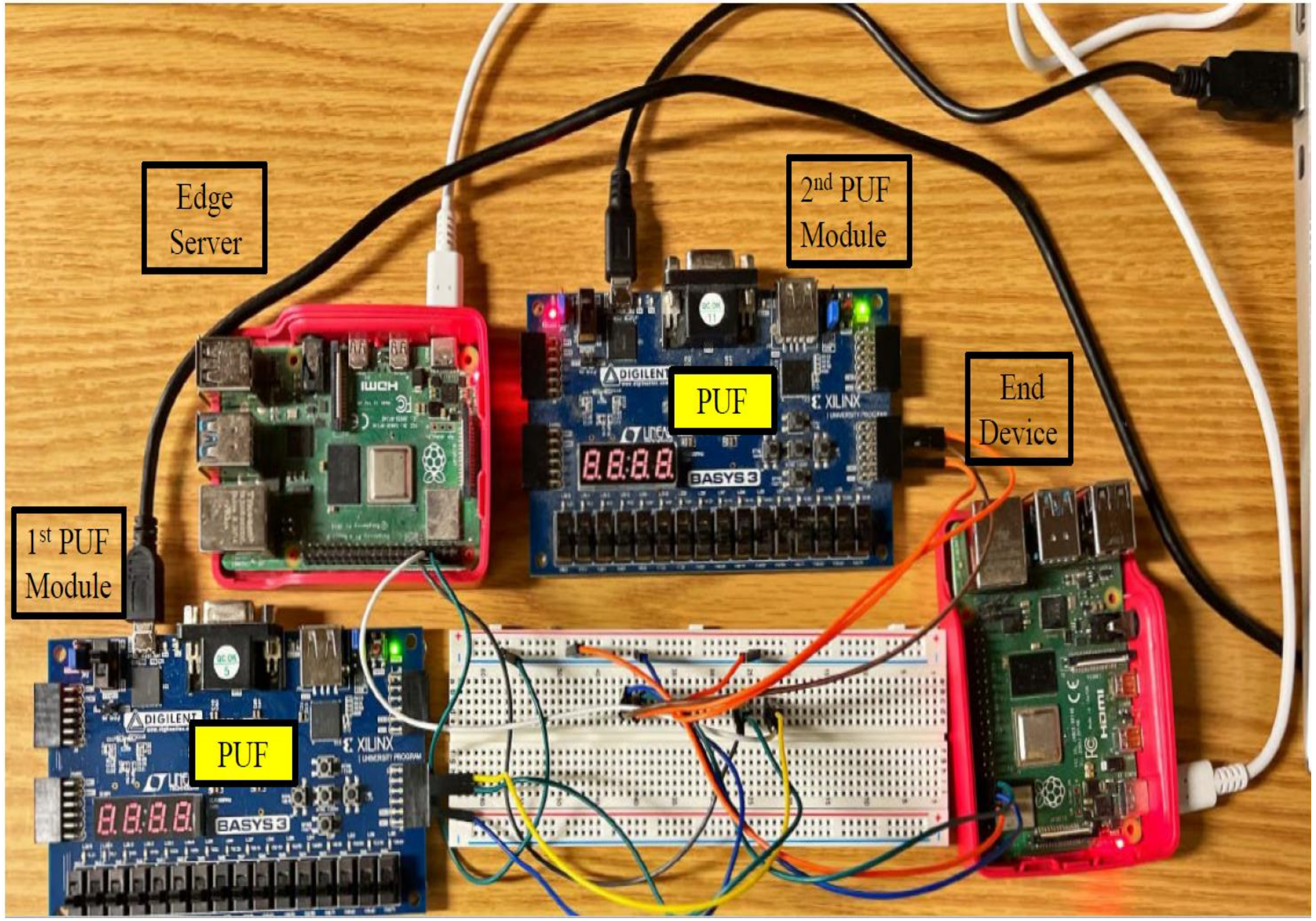






PUF Module 2

Prototype



Parameters	Results
Application	Smart Healthcare
DLT	IOTA Tangle
Communication Protocol	MAM
PUF Module	Arbiter PUF
Programming	JavaScript, Verilog, Python
Working Mode	Restricted
IOTA Network	Mainnet
Number of PUFs	2
PUF	xc7a35tcpg236-1
Edge Server	Single Board Computer

Summary

- This paper proposed and validated a sustainable security approach for device authentication and data confidentiality by utilizing PUF and IOTA Tangle.
- IOTA Tangle is becoming an alternative for Blockchain in IoT applications due to its capability in offering robust security for data as the Blockchain while being ‘Miner and Transaction Free’
- A robust security protocol for device authentication using Arbiter PUF which supports higher number of CRPs has been implemented and stored in Tangle using MAM in a restricted mode

Future Research

- Exploring the possibility of a scalable Blockchain based consensus mechanism using PUF and IOTA Tangle to achieve the objective of Security-by-Design could be a direction for future research.
- Idea of implementing PUF based authentication in Public and Private modes of MAM depending on the security requirements could be explored.
- Exploring the feasibility of a Trusted Platform Module (TPM) integrated PUF-based cryptographic scheme to attain the objective of Security by Design (SbD) in IoMT.

Thank You !!