Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems

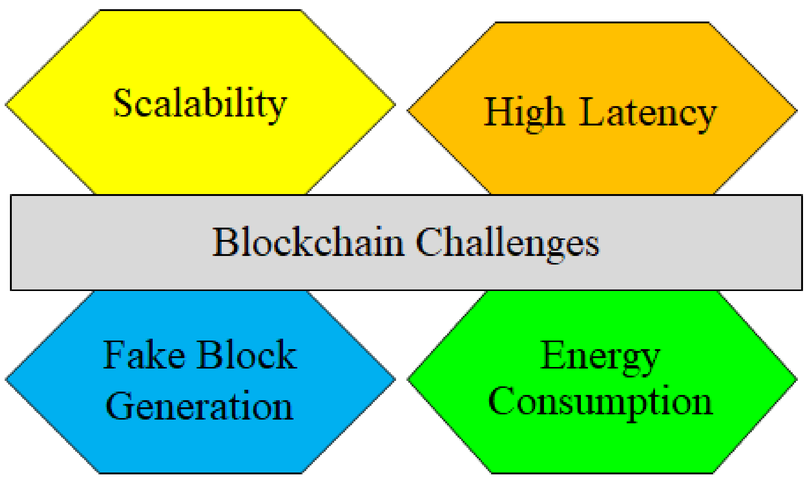
Deepak Puthal[1], Saraju P. Mohanty[2], Priyadarsi Nanda[3], Elias Kougianos[4], and Gautam Das[5]

[1,3]Faculty of Engineering and Information Technologies, University of Technology Sydney, Australia, Email:
[1]Deepak.Puthal@uts.edu.au, [3]Priyadarsi.Nanda@uts.edu.au

[2]Department of Computer Science and Engineering, University of North Texas, USA, Email: Saraju.Mohantyg@unt.edu

[4]Department of Engineering Technology, University of North Texas, USA, Email: Elias.Kougianosg@unt.edu

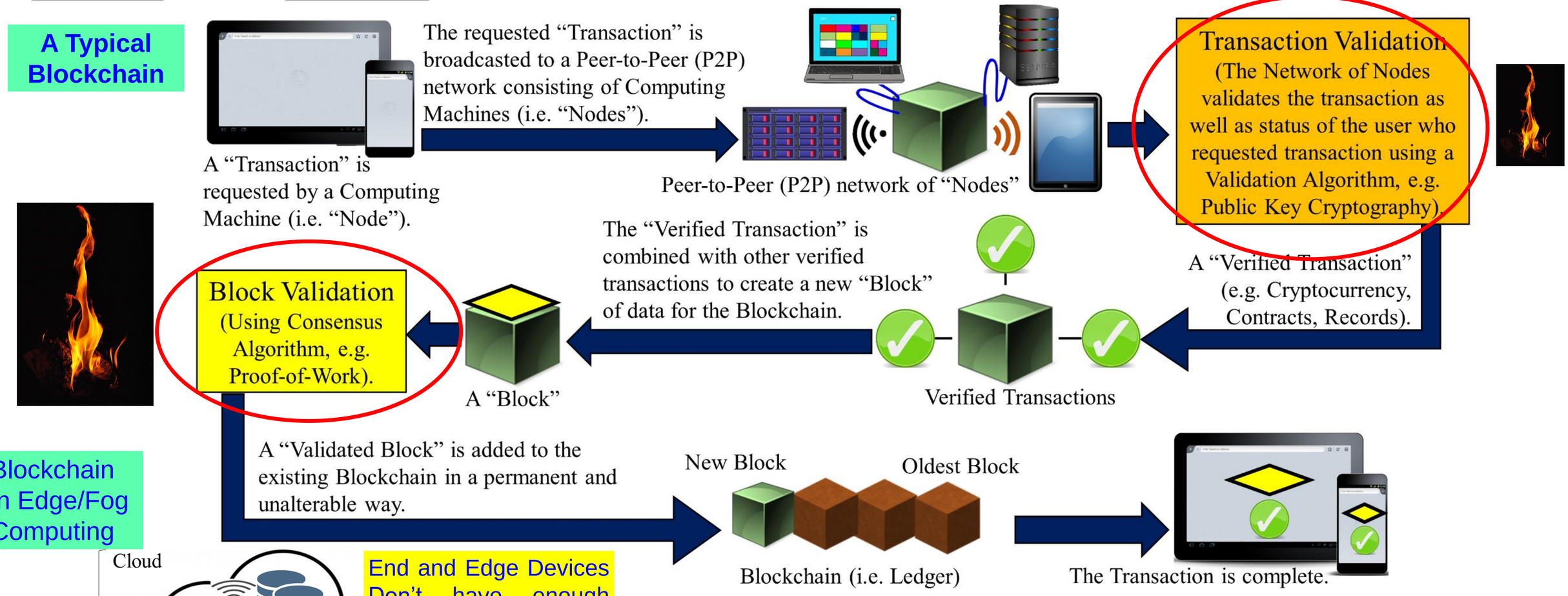
[5]Department of Computer Science and Engineering, The University of Texas at Arlington, USA, Email: gdas@uta.edu



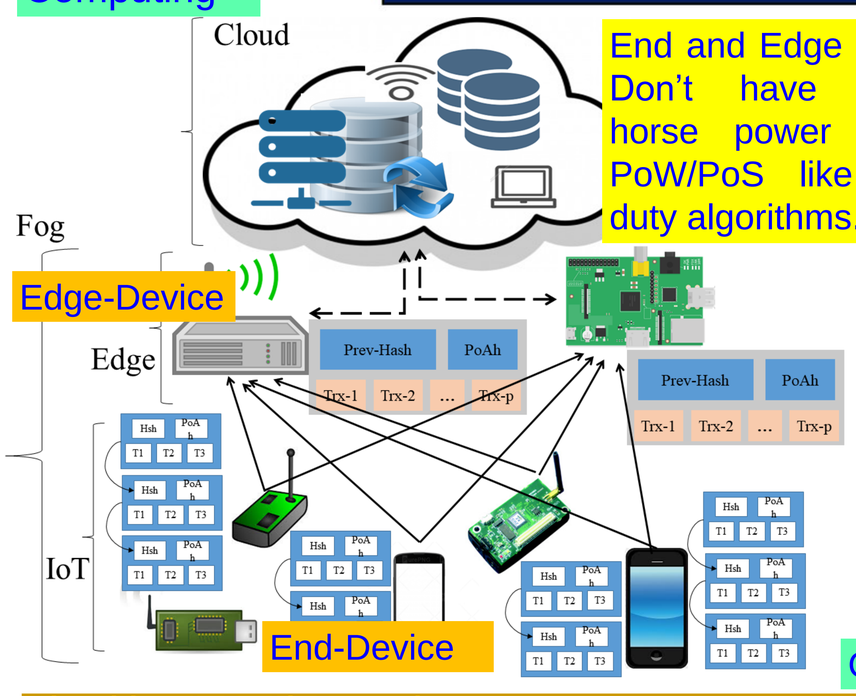
- Energy for mining of 1 bitcoin → 2 years consumption of a US household.
- Energy consumption for each bitcoin transaction → 80,000X of energy consumption of a credit card processing.
- Proof-of-Work (PoW) requires huge resources i.e. electricity consumption is equivalent to 1.5 household electricity for one day in the USA.
- Estimated that bitcoin transactions (that used PoW) will consume close to the electricity in Denmark by 2020.

The novel contributions of the current paper that advance the blockchain technology are:
(1) A new consensus algorithm called Proof-of-Authentication (PoAh) is proposed which is suitable for lightweight blockchain to allow blockchain to run using minimal resources and energy requirements.
(2) The new consensus algorithm is validated for resource-constrained distributed systems.
(3) Proof-of-Authentication is evaluated in both simulation and testbed environments.

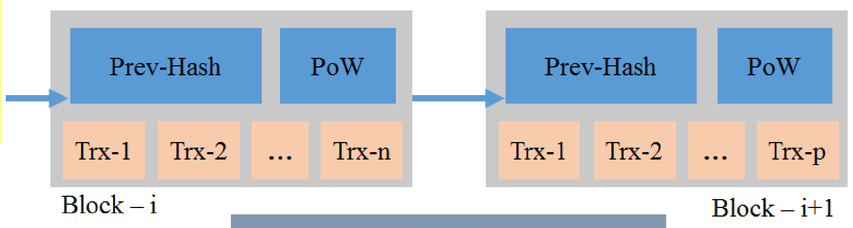
A Typical Blockchain



Blockchain in Edge/Fog Computing



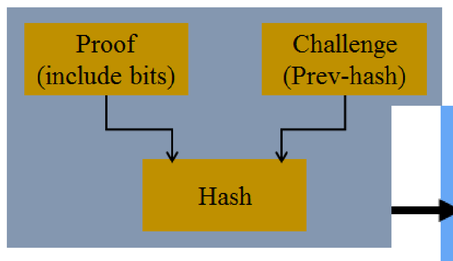
End and Edge Devices Don't have enough horse power to run PoW/PoS like heavy duty algorithms.



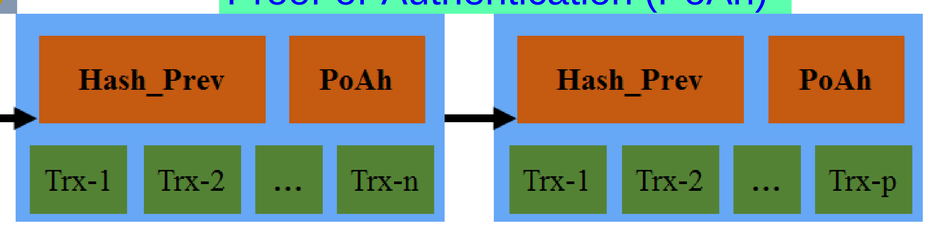
PoW

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

Proof-of-Work (PoW) transactions



Proof-of-Authentication (PoAh)



Consensus Algorithms - Comparative Perspective

	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

Algorithm 1: PoAh Procedure

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

PoAh

- Private/Permissioned blockchain – Trusted or partially-trusted nodes
- Solving cryptographic puzzle is not necessary
- A node doing false authentication → Loose a unit of trust value → a normal node after certain number of false authentication.

Our proposed Proof-of-Authentication (PoAh) - 200X faster than classic Proof-of-Work (PoW): PoW – 10 min in cloud versus PoAh 3 sec in Rasperry Pi. Consumes negligible energy as compared to the PoW.

Smart Electronic Systems Laboratory (SESL)
UNT DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING College of Engineering EST. 1890