UM6P | College of Computing

A Comparative Analysis of Blockchain Redaction Techniques

Imane El Abid

imane.elabid@um6p.ma

Mohammed VI Polytechnic University, Morocco

Yahya Benkaouz

yahya.benkaouz@um5.ac.ma

Mohammed V University in Rabat, Morocco

IEEE DAPPS 2024
The 6th IEEE International Conference on Decentralized Applications and Infrastructures

Blockchain

Decentralized digital ledger technology operating on a peer-to-peer network.

Decentralization

A peer-to-peer network
No central authority
Nodes carry a copy of the ledger

Immutability

Tamper-proof ledger of transactions
Guarantees data integrity
Resilient to double-spending

Transparency

All participants in the network can view, verify and validate the transactions

Security

Use of cryptographic functions
Transactions are verified and validated using consensus.

Blockchain

Decentralized digital ledger technology operating on a peer-to-peer network.

Decentralization

A peer-to-peer network
No central authority
Nodes carry a copy of the ledger

Immutability

Tamper-proof ledger of transactions
Guarantees data integrity
Resilient to double-spending

Transparency

All participants in the network can view, verify and validate the transactions

Security

Use of cryptographic functions
Transactions are verified and validated using consensus.

Is Blockchain immutability always a VIRTUE ?

Outline

1 Introduction

2 Immutability Pillars

3 Need for redaction in the blockchain

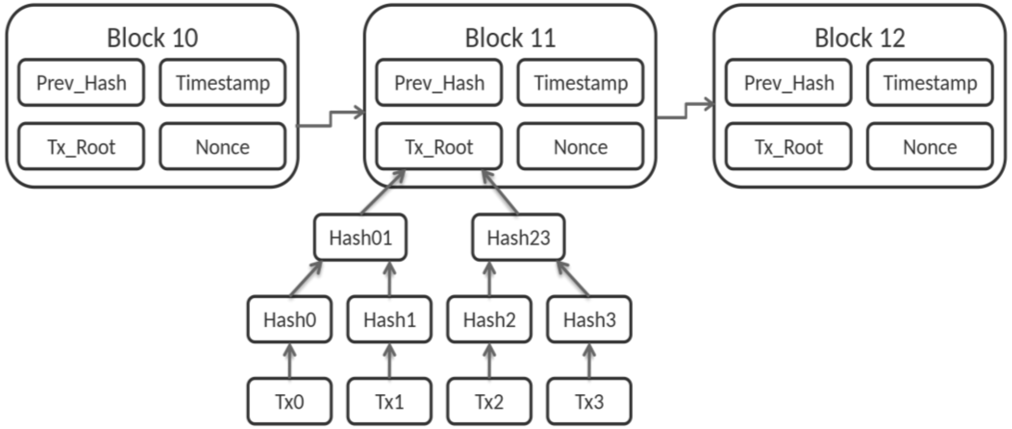
4 Redaction Methods

5 Evaluation & Discussion

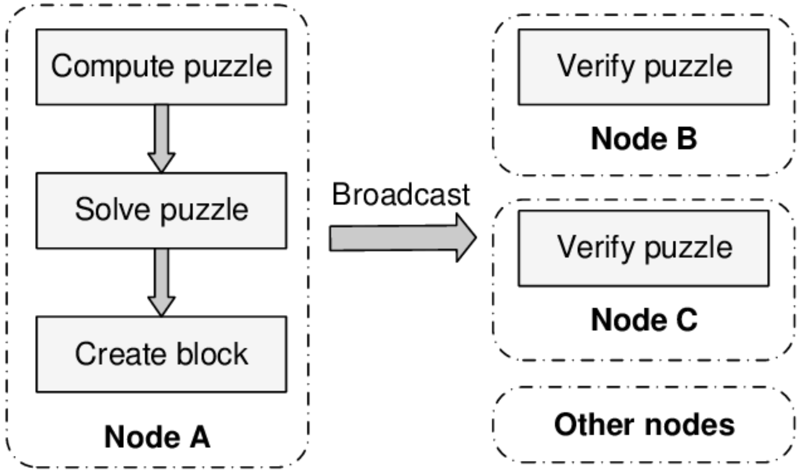
6 Conclusion & Perspectives

7 References

Immutability pillars



Hash Functions



Consensus

1.4% of Bitcoin transactions contained non-financial data in multiple types (text, images, URLs, Source code)

(Matzutt2018,Gregoriadis2022)

Why do we need mutable blockchain?

Data privacy

GDPR or equivalent data protection regulations dictate that users must have total control over their data, which means that users have control over who, when, and how their data is used.

Illegal content removal

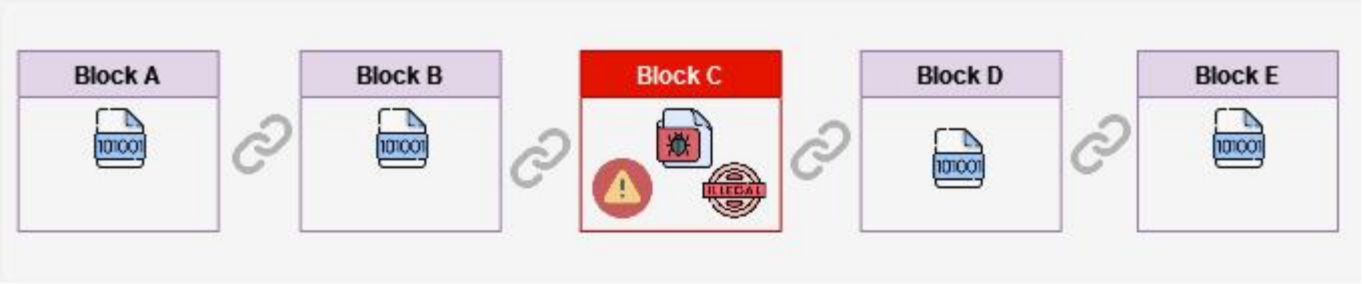
The disclosure or even the mere possession of particular data, including politically sensitive material, pirated data, blasphemy, and hate speech may be illegal in certain jurisdictions.

Operational error correction

Immutability limits the ability to correct errors or inaccuracies in the recorded data.

Software upgrade

Smart contracts are self-executed and typically irrevocable, any errors or vulnerabilities in the can have significant consequences Applications wherein constant review of software revisions and contractual terms is necessary!



Blockchain ledger

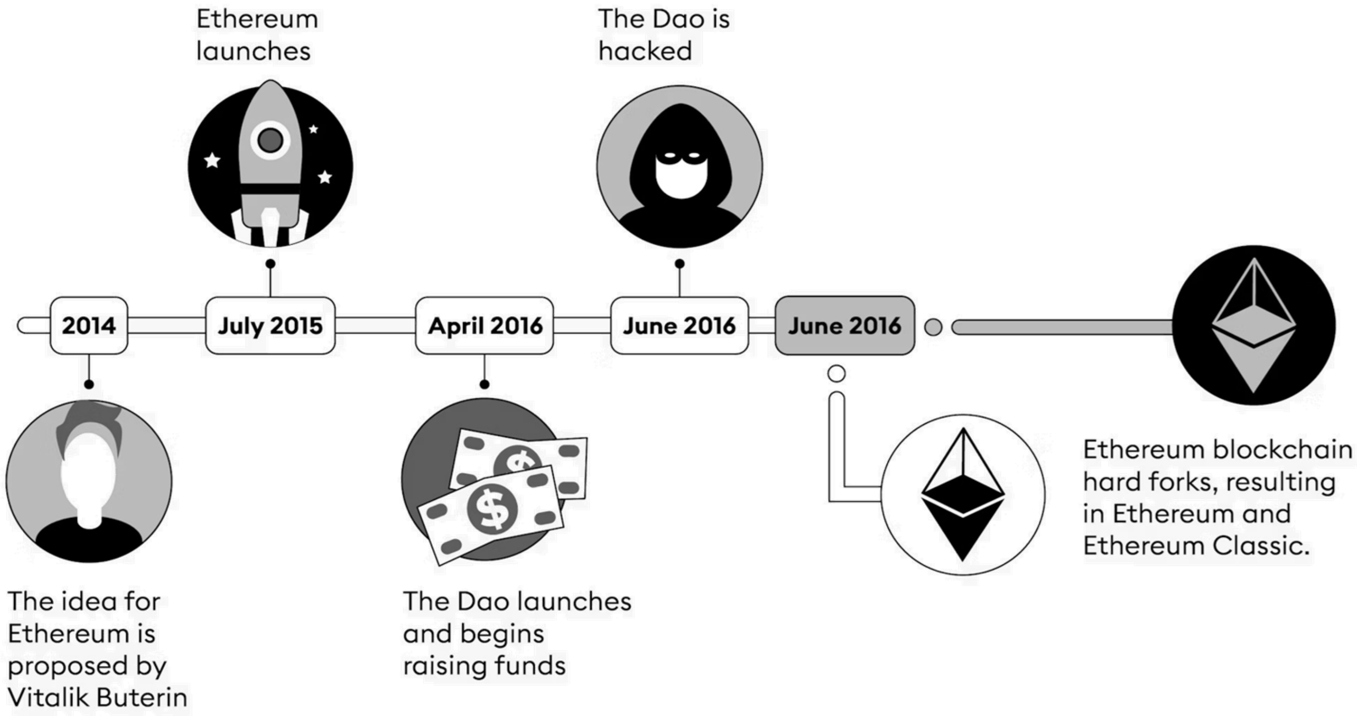
DAO Attack

18th of June 2016

+50,000,000$

A lot of money siphoned out

Solution???


Ethereum launches
The Dao is hacked
2014
July 2015
April 2016
June 2016
June 2016
The idea for Ethereum is proposed by Vitalik Buterin
The Dao launches and begins raising funds
Ethereum blockchain hard forks, resulting in Ethereum and Ethereum Classic.

Escaping immutability

Hard fork

-Undermine trust

-Energy Inefficient

-Blockchain splits

Off-chain storage

-Centralized storage facility

-Only hashes stored on-chain

-Discards blockchain features

Pruning

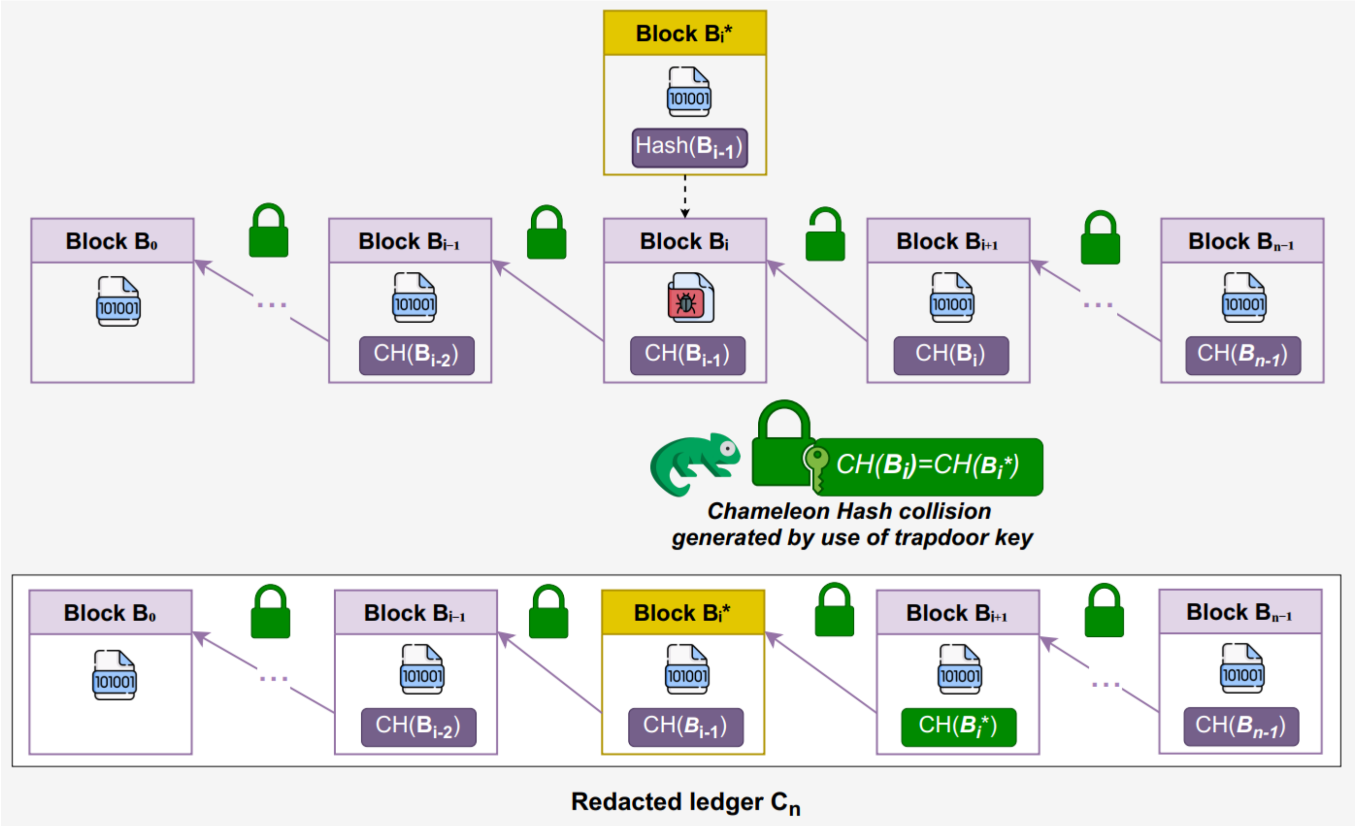
-Removing unnecessary data

-No traceability

-No tool for verification

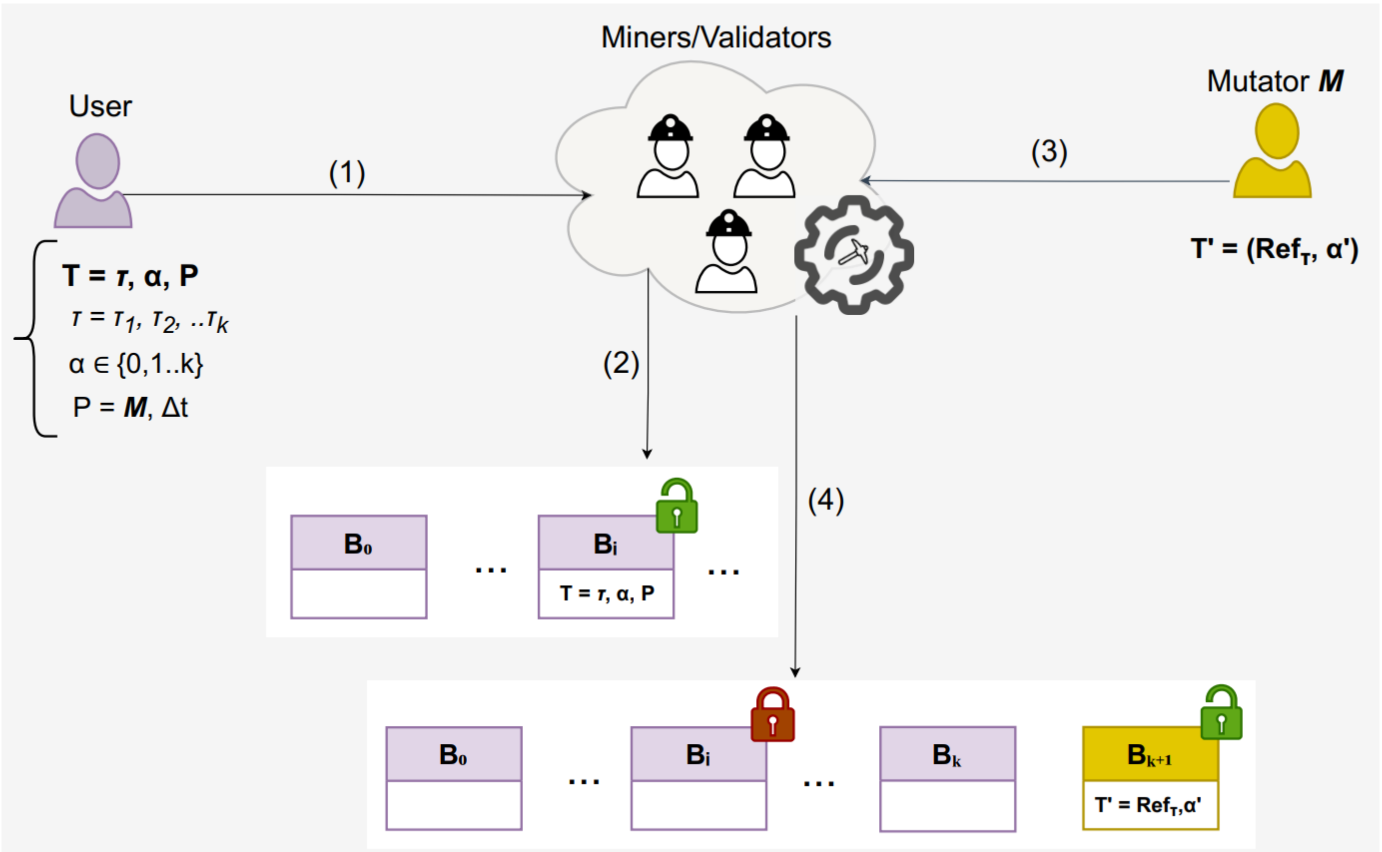
Chameleon-hash redaction

- 1st Blockchain redaction proposal using Chameleon Hash functions that allows the creator to find collisions
- Achieves data redaction without compromising the overall integrity of the blockchain.
- Trapdoor keys held by authorized parties that enable the redaction process.
- Only specific nodes with the trapdoor can perform redactions
- The rest of the blockchain remains valid because the new hash maintains the chain's cryptographic structure.



Mutation-based redaction

- µchain allows redactions through multiversioned transactions.
- A defined redaction policy dictates the rules and conditions under which redactions can be initiated and approved.
- µchain doesn't erase the original data but appends a new "redacted" version to the chain.
- Each block in µchain has multiple versions. The "current" version represents the latest state of the blockchain.



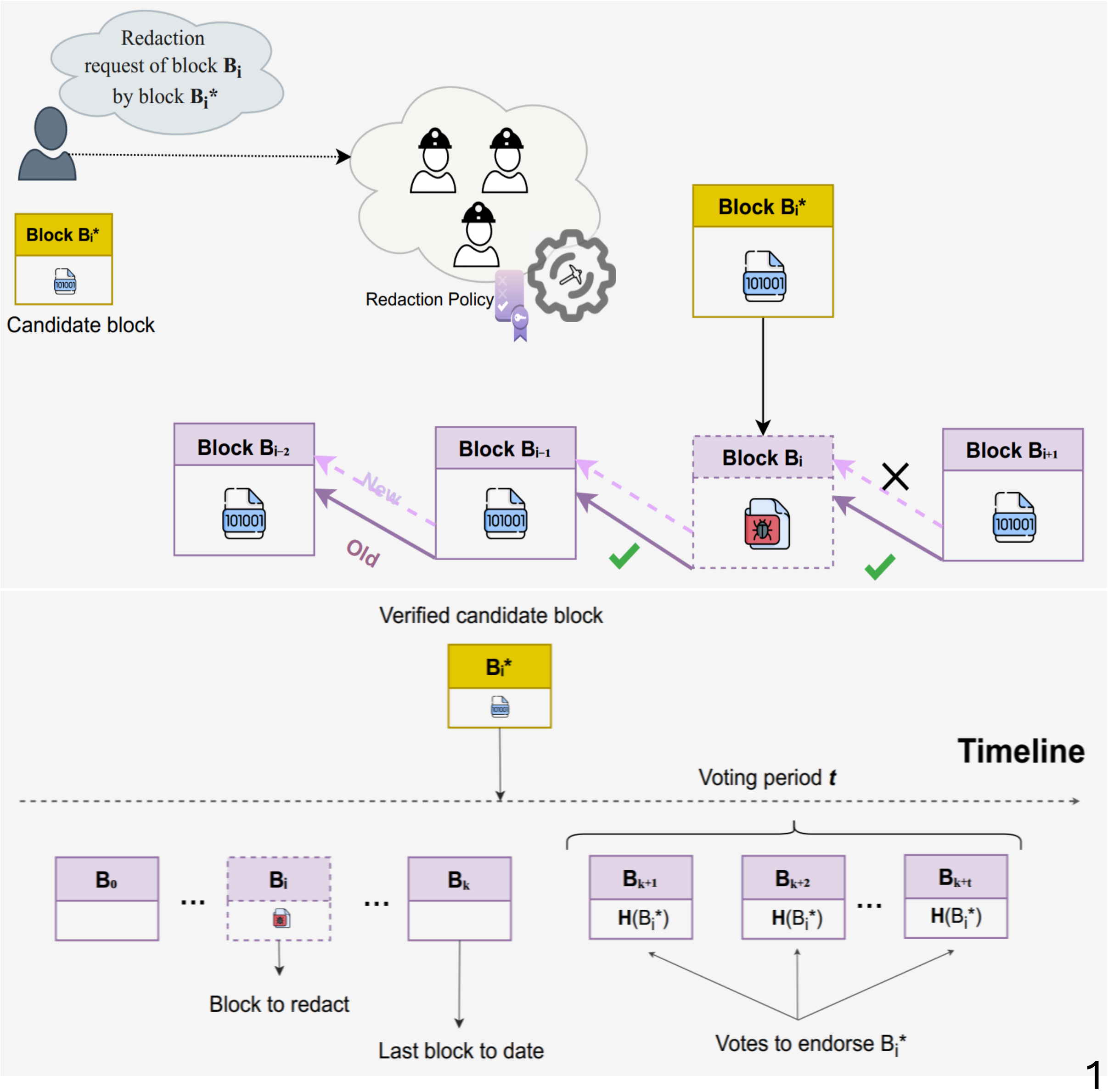
Voting-based redaction

- This approach leverages dual links between adjacent block to implement data modification.

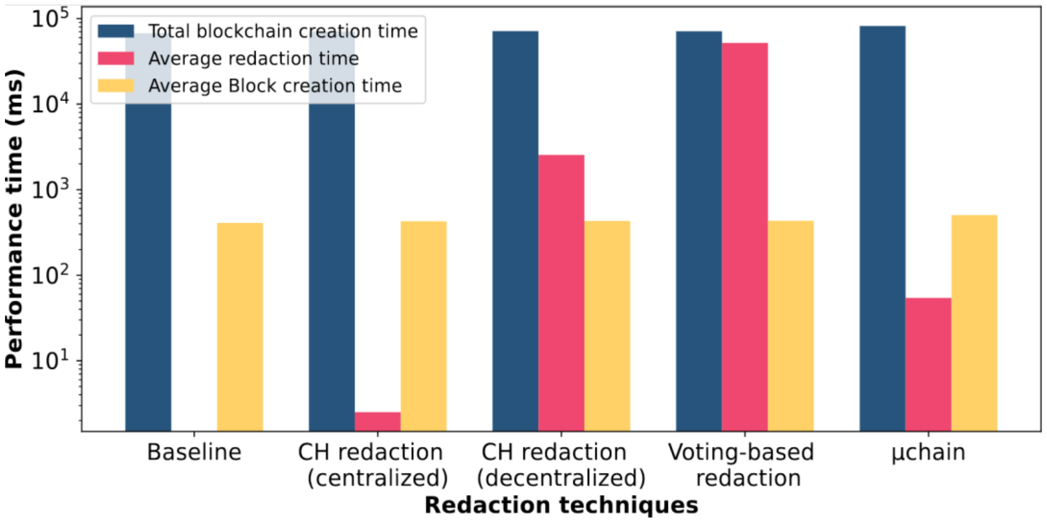
- Suitable for permissionless settings regardless
- of the deployed consensus protocols.

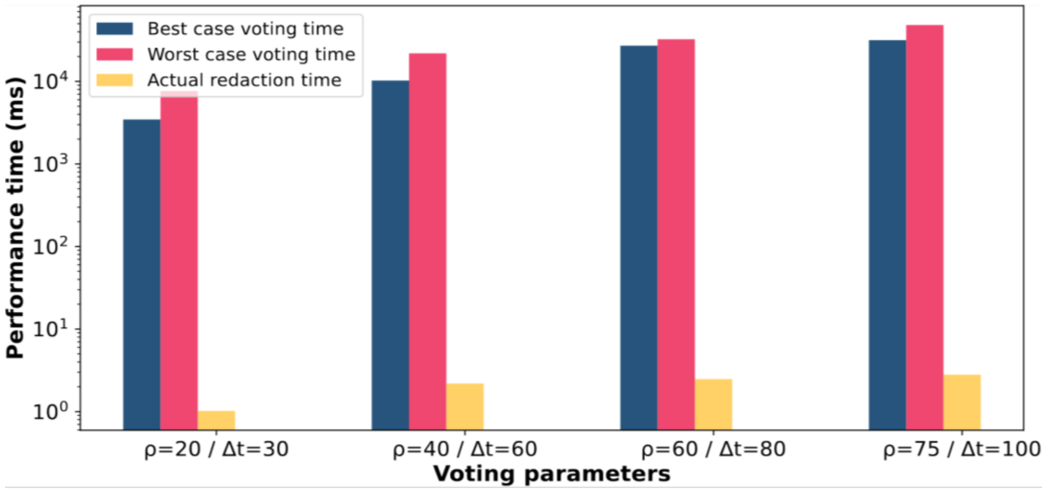
- Redaction proposals undergo a voting process among network participants to determine approval or rejection.

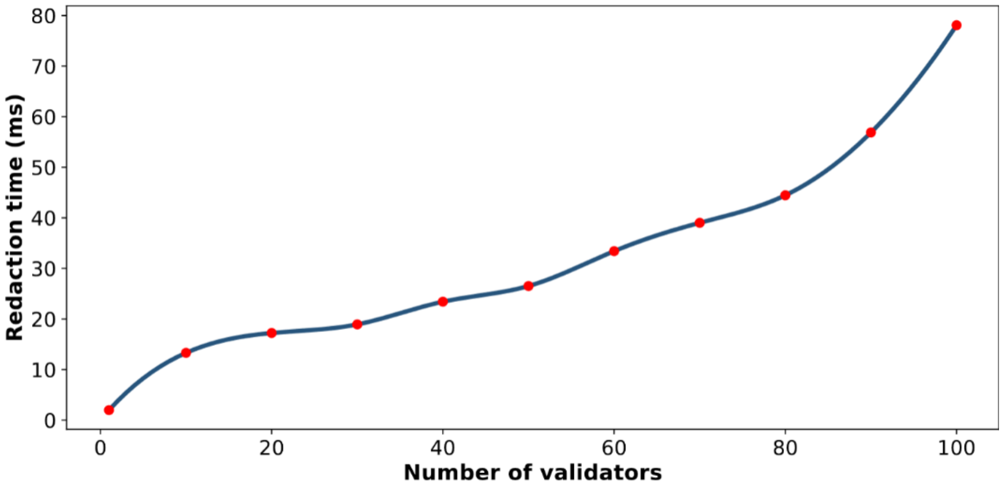
- Upon reaching the voting threshold, the candidate block can replace the old one.

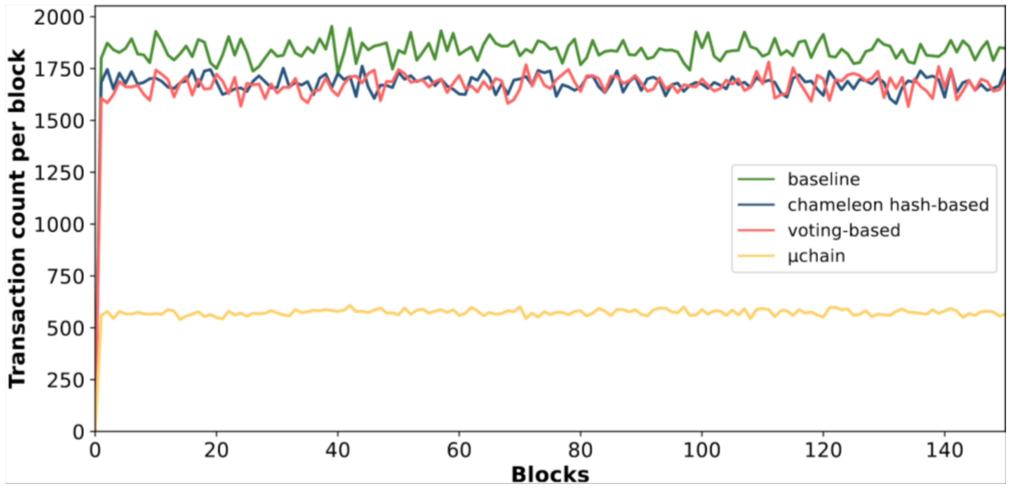


Benchmark and evaluation

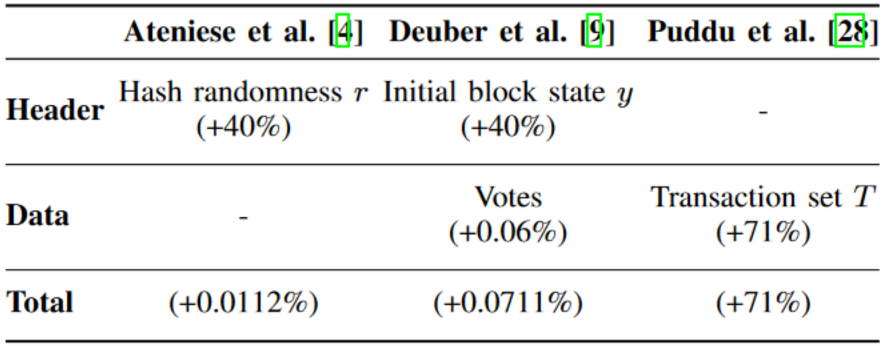




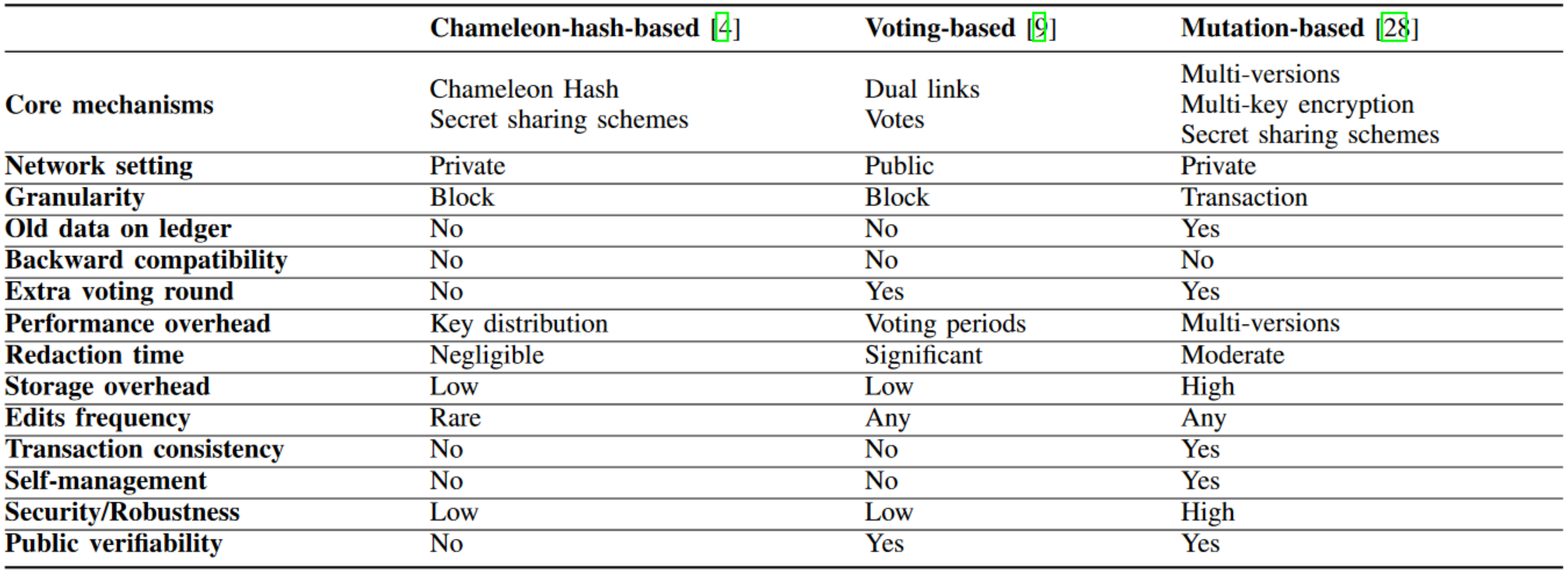




Additional analysis



	Ateniese et al. [4]	**Deuber et al. [9]**	**Puddu et al. [28]**
Header	Hash randomness r (+40%)	Initial block state y (+40%)	-
Data	-	Votes (+0.06%)	Transaction set T (+71%)
Total	(+0.0112%)	(+0.0711%)	(+71%)



	Chameleon-hash-based [4]	**Voting-based [9]**	**Mutation-based [28]**
Core mechanisms	Chameleon Hash Secret sharing schemes	Dual links Votes	Multi-versions Multi-key encryption Secret sharing schemes
Network setting	Private	Public	Private
Granularity	Block	Block	Transaction
Old data on ledger	No	No	Yes
Backward compatibility	No	No	No
Extra voting round	No	Yes	Yes
Performance overhead	Key distribution	Voting periods	Multi-versions
Redaction time	Negligible	Significant	Moderate
Storage overhead	Low	Low	High
Edits frequency	Rare	Any	Any
Transaction consistency	No	No	Yes
Self-management	No	No	Yes
Security/Robustness	Low	Low	High
Public verifiability	No	Yes	Yes

Open questions

- Conflict Resolution
- Scalability and Speed
- Consistency
- Incentives
- Content Scrutiny
- Adaptability
- …

Conclusion

&

Perspectives

- Chameleon hash-based techniques are superior in terms of redaction speed, particularly within permissioned blockchain environments.
- Voting-based techniques excel in decentralization at the expense of latency.
- Mutation-based techniques, despite being straightforward, induces high storage overhead exceeding baseline blockchains by several factors.

- Analysis of blockchain technology from the users' perspective.
- Better response to application requirements.
- Awareness of blockchain immutability.
- Considerate security properties.
- Control of who can perform redaction.

References

Matzutt 2018, Matzutt, Roman, et al. "Thwarting unwanted blockchain content insertion." 2018 IEEE International Conference on Cloud Engineering (IC2E). IEEE, 2018.

Ateniese2017, G. Ateniese, B. Magri, D. Venturi, and E. Andrade, “Redactable blockchain–or–rewriting history in bitcoin and friends,” in 2017 IEEE European symposium on security and privacy.

Camenisch2017, Camenisch, J., Derler, D., Krenn, S., Pöhls, H. C., Samelin, K., & Slamanig, D. (2017, March). Chameleon-hashes with ephemeral trapdoors. In IACR International Workshop on Public Key Cryptography.

Puddu2017, I. Puddu, A. Dmitrienko, and S. Capkun, “μchain: How to forget without hard forks,” Cryptology ePrint Archive, 2017.

Derler2019, Derler, D., Samelin, K., Slamanig, D., & Striecks, C. (2019). Fine-grained and controlled rewriting in blockchains: Chameleon-hashing gone attribute-based.

Ashritha2019, Ashritha K, Sindhu M, Lakshmy KV. Redactable blockchain using enhanced chameleon hash function. In: 2019 5th International Conference on Advanced Computing Communication Systems.

Deuber2019, Deuber, D., Magri, B., & Thyagarajan, S. A. K. (2019, May). Redactable blockchain in the permissionless setting. In 2019 IEEE Symposium on Security and Privacy (SP).

Thank you.

Any questions ?

You can contact me at:

Imane.elabid@um6p.ma