AN OPTIMIZED RESOURCE-EFFICIENT REDACTION MECHANISM WITH INTEGRITY VALIDATION SUPPORT FOR REDACTABLE BLOCKCHAIN

ABD ALI SHAMS MHMOOD ABD ALI

UNIVERSITI SAINS MALAYSIA

2025

AN OPTIMIZED RESOURCE-EFFICIENT REDACTION MECHANISM WITH INTEGRITY VALIDATION SUPPORT FOR REDACTABLE BLOCKCHAIN

by

ABD ALI SHAMS MHMOOD ABD ALI

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy

May 2025

ACKNOWLEDGEMENT

I would like to express our gratitude to Allah SWT for giving us the opportunity and helping me endlessly to achieve the current stage in formatting this thesis. Current collaborated efforts to develop my knowledge and understanding. I would like to thank Dr. Mohd Najwadi for his endless support, valuable comments and efficient training to be a researcher. Dr. Je Sen, for the valuable advice and endless efforts. Additionally, thank you to my husband, Hasan, for his sincere and loyal help, patience, advice, and support. To my kids, Ward and Zain. To my family, a simple and humble reward for your years of support and finally, to both my universities, USM and Aliraqia, for facilitating this effort to be accomplished.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ALGORITHMS

Page

LIST OF DEFINITIONS

Page

LIST OF ABBREVIATIONS

IoT	Internet-of-Things
GDPR	European General Data Protection Regulation
CH	Chameleon Hash
PBCH	Policy-Based Chameleon Hash
KDM	Key Distributed Management
CHET	Chameleon Hash Ephemeral Trapdoor
ABE	Attribute-Based Encryption
F.O	Fujisaki and Okamoto
TO	Transaction Owner
TM	Transaction Modifiers
CTA	Central Trusted Authority
etd	Ephemeral Trapdoor
Std	Second Trapdoor
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
KP-ABE	Key-Policy Attribute-Based Encryption
ORE	Optimized Resource Efficient
KRM	Key Reusability Mechanism
IV	Integrity Validation
OREIV	Optimized Resource Efficiency supported by the Integrity Validation
PoW	Proof of Work
PoS	Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
MT	Merkel Tree
MOF-BC	Memory-Optimized and Flexible Blockchain
CA	Certificate Authority
DOS	Denial Of Service
FPLE	Functionality Preserving Local Erasure
SPV	Simplified Payment Verification
TXID	Transaction ID
ECR	Enhanced Collision Resistance
PKE	Public-Key Encryption

NIZKP	Non-Interactive Zero-Knowledge Proof
MPC	Multiparty Computation
DCH	Distributed Chameleon Hash
TEE	Trusted Execution Environment
RCB	Redactable Consortium Blockchain
TCH	Threshold Chameleon Hash
ASCS	Sanitizable Chameleon Signature
SRB	Self-Redactable Blockchain Proposal
RCH	Revocable Hash Function
RCS	Revocable Chameleon Signature
TTCH	Threshold Trapdoor Chameleon Hash
TUCH	Time-Updatable Chameleon Hash
LRRS	Linkable-And-Redactable Ring Signature
CHCT	Chameleon Hash Changeable Trapdoor
STM	Standard Model
ROM	Random Oracle Model
FAME	Fast Attribute Message Encryption
LSSS	Linear Secret Sharing Scheme
DMBDH	Decisional Modified Bilinear Diffie-Hellman
DBDH	Decisional Bilinear Diffie-Hellman
CPA	Chosen Plaintext Attack
CCA	Chosen-Ciphertext Attacks
FABEO	Fast Attribute-Based Encryption with Optimal Security
PRG	Pseudorandom Generator
KEM	Key Encapsulation Mechanism
ABTT	Attribute-Based Traitor Tracing
HIBE	Hierarchical Identity-Based Encryption
UTXO	Unexpended Transaction Output
KERB	K-Time Modifiable and Epoch-Based Redactable Blockchain
DAPS	Double Authentication Prevents Signature
DGSS	Dynamic Group Signature Schemes
RFAME	Revocable FAME
MA-ABE	Multi-Authority Attribute-Based Encryption
RPCH	Revocable Policy-Based Chameleon Hash

ASM	Accountable Subgroup Multi-Signature
ABAC	Attribute-Based Access Control
DPBCH	Decentralized Policy-Based Chameleon Hash
BLS	Boneh-Lynn-Shacham
MAC	Message Authentication Code
PFRB	Policy-Hidden Fine-Grained Redactable Blockchain
RB	Redactable Blockchain
PRBFM	Privacy-Preserving Fine-Grained Redactable Blockchain with Policy Fuzzy Matching
PCHT	Policy-Based Chameleon Hash with Black-Box Traceability
ABET	Attribute-Based Encryption with Black-Box Traceability
PIRB	Privacy-Preserving Identity-Based Redactable Blockchain
PCHA	Policy-Based Chameleon Hash with Black Box Accountability
ABTT	Attribute-Based Traitor Tracing
IBS.	Identity-Based Signature
OO-RB-AOC	Online/Offline Rewritable Blockchain with Auditable Outsourced Computation
DSE-RB	Dynamic Searchable Encryption Framework on Redactable Blockchain
DPSS	Dynamic Proactive Secret Sharing
DS	Digital Signatures
DTCH	Dynamic Trust-Based CH Mechanism, Dubbed
DACH	Dynamic And Decentralized Attribute-Based CH
SDR-Chain	Securely And Dynamically Redactable Blockchain
PBC	Pairing-Based Cryptography
ICR	Insider Collision Resistance
BK	Boneh-Katz

MEKANISME REDAKSI SUMBER CEKAP YANG DIOPTIMUMKAN DENGAN SOKONGAN PENGESAHAN INTEGRITI UNTUK BLOK RANTAI BOLEH SUNTING

ABSTRAK

Teknologi Blockchain memperkenalkan era paradigma terpencar baharu yang mengelakkan pergantungan kepada pihak ketiga yang dipercayai. Ia adalah lejar yang telus dan diedarkan yang direka secara asas untuk mata wang kripto digital tetapi sejak itu telah diperluaskan kepada pelbagai industri. Walau bagaimanapun, kebolehubahannya mewajibkan cabaran penting termasuk menyimpan kandungan terlarang, pelanggaran peraturan privasi dan menyekat fleksibiliti pengurusan data. Oleh itu, blockchain boleh redactable telah muncul sebagai penyelesaian utama yang membolehkan pindaan kandungan tidak berubah terkawal. Penyuntingan peringkat urus niaga yang diperkukuh oleh kawalan capaian yang terperinci membentuk asas kepada mekanisme penyuntingan semasa. Konsep redaksi ini pada asasnya bergantung pada pengubahsuaian urus niaga boleh ubah yang dikawal oleh dasar capaian pratakrif yang ditentukan oleh pemilik transaksi. Pengubah suai yang dilengkapi dengan keistimewaan penulisan semula yang diperlukan dan yang memenuhi dasar akses yang berkaitan didayakan untuk melakukan pengubahsuaian. Walau bagaimanapun, infrastruktur mekanisme redaksi sedia ada adalah tidak cekap. Sebagai contoh, skim transformasi Chameleon Hash Ephemeral Trapdoor (CHET), Penyulitan Berasaskan Atribut Dasar Ciphertext (CP-ABE) dan Fujusaki-Okamutu (F.O.) memerlukan kos pengiraan. CP-ABE menawarkan kawalan capaian yang tepat ke atas data yang disulitkan yang membawa kepada mewujudkan kawalan capaian yang terperinci, tetapi varian semasa menanggung penggunaan sumber yang besar yang membawa

kepada ketidakcekapan dalam masa pengiraan, kos pengiraan dan kos penyimpanan. Selain itu, CHET mengenakan kemerosotan daya pengeluaran dan peningkatan overhed apabila ia gagal menyokong dasar tambahan transaksi yang berdaya tahan. Selain itu, mekanisme pengesahan integriti yang tidak cekap semasa mengenakan masa pengiraan yang berlebihan dan overhed komunikasi pada bahagian pengubah suai, dan juga tidak dapat menyokong tingkah laku jujur pihak redaksi. Penyelidikan ini mencadangkan mekanisme redaksi Cekap Sumber Dioptimumkan yang disokong oleh Pengesahan Integriti (OREIV). Ia bergantung pada tiga komponen utama yang cekap. Pertama, Cekap Sumber Dioptimumkan (ORE) memanfaatkan CP-ABE FABEO yang menghasilkan peningkatan masa pengiraan, kos pengiraan dan kos penyimpanan. Kedua, Mekanisme Kebolehgunaan Semula Utama (KRM) diperluaskan dengan ORE. Ia meningkatkan daya pemprosesan penambahan transaksi dan mengurangkan overhed komunikasi keseluruhan berdasarkan dasar tambahan yang dipratakrif dan dikawal ketat. Akhir sekali, mekanisme Pengesahan Integriti (IV) yang menawarkan keteguhan pengesahan teks sifir yang cekap dan memastikan gelagat redaksi yang jujur menangani batasan andaian tingkah laku jujur blockchain yang dibenarkan semasa. Akibatnya, OREIV menggabungkan komponen utama yang dicadangkan sebelum ini. Keputusan analisis perbandingan yang dijalankan antara OREIV dan terkini menunjukkan masa pengiraan yang lebih baik, kos pengiraan, kos penyimpanan dan mengurangkan overhed pengiraan tanpa menjejaskan keselamatan.

AN OPTIMIZED RESOURCE-EFFICIENT REDACTION MECHANISM WITH INTEGRITY VALIDATION SUPPORT FOR REDACTABLE BLOCKCHAIN

ABSTRACT

Blockchain technology introduces a new decentralized paradigm era avoiding the reliance on trusted third parties. It is a transparent and distributed ledger which is designed fundamentally for digital cryptocurrencies but has since been extended to various industries. However, its immutability obligates significant challenges including storing illicit contents, privacy regulations violations, and restricting data management flexibility. Therefore, redactable blockchain has emerged as a leading solution enabling controlled immutable contents amendment. Transaction-level redaction reinforced by fine-grained access control forms the cornerstone of the current redaction mechanisms. This redaction concept essentially depends on modifying mutable transactions governed by predefined access policies specified by the transaction owner. Modifiers equipped with necessary rewriting privileges and who fulfil the associated access policy are enabled to perform modifications. However, the existing redaction mechanisms infrastructures are inefficient. For instance, the Chameleon Hash Ephemeral Trapdoor (CHET), Ciphertext Policy Attribute-Based Encryption (CP-ABE), and Fujusaki-Okamutu (F.O.) transformation schemes are computationally costly. The CP-ABE offers precise access control over encrypted data that leads to establishing fine-grained access control, but current variants incur substantial resource consumption leading to inefficiencies in computational time, computational cost, and storage cost. Additionally, CHET imposes throughput degradation and increased overhead where it fails to support resilient transaction

appending policies. Moreover, the current inefficient integrity validation mechanism imposes an excessive computational time and communication overhead on the modifier side, and also unable to support redaction parties' honest behaviour. This research proposes an Optimized Resource Efficient redaction mechanism supported by Integrity Validation (OREIV). It relies on three key efficient components. First, Optimized Resource Efficient (ORE) leverages CP-ABE FABEO resulting in improving computational time, computational cost, and storage cost. Second, a Key Reusability Mechanism (KRM) extended with ORE. It enhances transaction appending throughput and reduces overall communication overhead based on predefined and strictly governed appending policies. Finally, an Integrity Validation (IV) mechanism that offers efficient ciphertext verification soundness and ensures honest redaction behaviour addressing the limitations of the current permissioned blockchain honest behaviour assumption. Consequently, OREIV combines previously proposed key components. The comparative analysis results conducted between OREIV and the current state-of-the-art demonstrate better computational time, computational cost, and storage cost, and reduce computational overhead without compromising security.

CHAPTER 1

INTRODUCTION

1.1 Introduction

Blockchain is a modern cutting-edge technology that recently rose to depict one of the perfect decentralized computing paradigms. It was essentially built to store Bitcoin transactions to eliminate third-party dominancy (Abidi et al., 2021). It functions as a transparent, immutable, publicly distributed ledger regulated by a peer-to-peer network. The transactions are validated by powerful elected nodes named miners who comply with specified regulating consensus algorithms that organize their operations (Uddin et al., 2021). Decentralization and security are the blockchain permanent characteristics. Decentralization is achieved by a local public distributed ledger possessed by every node where data relevancy and integrity are ensured, avoiding tampering attempts.

Meanwhile, the collection, storage, and processing are conducted by recording transactions into a block structure. Blocks are connected using cryptographically generated hash values to guarantee chain consistency, security, and validity. Each block hash value is stored in the previous block header, ensuring immutability (Sanka et al., 2021).

Blockchain services have recently extended to serve diverse industries witnessed by several applications adoption, including copyright dispute resolution (Ma et al., 2018), product traceability (Aitzhan and Svetinovic, 2018), electronic voting (Khan et al., 2020), storage services (Khan et al., 2022), healthcare services (Wang and Li, 2021), product tracking throughout the entire supply chain (Yiu, 2021), data management (Abidi et al., 2021) and Internet-of-Things (IoT) (Kapassa et al., 2021).

Immutability is the blockchain transparency and integrity protection technique where any amendment to a certain block will impact the block's consistency (Narayanan et al., 2016). Therefore, it prevents the modification of transactions once approved (Zheng et al., 2019; El Ioini and Pahl, 2018). However, immutability can be a growth obstacle via malevolent motives, such as illegal information storage and dissemination (Casino et al., 2020). Matzutt et al. (2018) have discovered eight records related to sexual content comprised of 274 child pornography. Further, 142 links are also associated with darknet services. Therefore, blockchain immutability is passively exploited by storing inappropriate content and illegal material, violating intellectual rights. Due to these issues, users might be reluctant to adopt blockchain technology to avoid illegal consequences. Hence, continuously appending the latest digital information would be infeasible without legal content being removed from the blockchain, which poses an essential prerequisite to further adoption by being obligatory for law enforcement agencies, including Interpol (Tziakouris, 2018).

The European General Data Protection Regulation (GDPR), which supports the user's "right to be forgotten, " rose as a rival to the blockchain’s immutability (Bai et al., 2022; Schellinger et al., 2022). It permits users to edit their personal information and anonymously amend personal data attached to previous blocks. Additionally, immutability might not support the emergence of blockchain-based applications, which request an adequate flexibility level of data redaction. Examples include, but are not restricted to, users' confidential and sensitive information, such as health and insurance records (Bigini et al., 2020; Gatteschi et al., 2018). The users might prefer to remove sensitive details from the platform while updating the information if required, including the contract amendment service and deleting redundant data to free more space in the IoT-based blockchain systems (Politou et al., 2018).

Thus, a redactable blockchain becomes a persistent demand to mitigate the issues mentioned above, resulting in diverse redaction mechanisms that rely mainly on cryptographic solutions. Recent solutions are classified as Non-Chameleon or Chameleon redaction mechanisms (Politou et al., 2021; Zhang et al., 2021). Non-chameleon redaction mechanisms vary among proposals regarding their conceptual buildings through multiple infrastructures like, data appending-based, voting-based, local, and a hard fork redaction. These solutions are considered infeasible in terms of cost due to blockchain infrastructure amendments or severely consuming time, bandwidth, and storage (Politou et al., 2021; Zhang et al., 2021).

The Chameleon redaction mechanism relies on the Chameleon Hash (CH) function. It is easy to implement due to no further amendments to the blockchain infrastructure. Meanwhile, it maintains consistency. Redaction mechanism-based CH was first devised by Ateniese et al. (2017) and adopted by Accenture. It is considered the cornerstone for the block-level proposed redaction mechanisms. It exploits the power of modifying certain content without changing the block hash, consequently preserving blockchain consistency using a secret trapdoor key (Krawczyk and Rabin, 1998). The replacement of the standard hash function with CH is specially performed in the permissioned blockchain. The CH trapdoor key possession must be held by a central authority that regulates and distributes the modifier's rewriting privileges. However, generating a single trapdoor key for the entire block remains a potential vulnerability. It can be disclosed by malicious modifiers, which facilitate the redaction of any transaction without being monitored. Consequently, data integrity is threatened, thus undermining the entire block consistency. The coarse-grained access control concept is also adopted where the transaction owner is not perceived of what has been modified or by whom Derler et al. (2019).

Derler et al. (2019) introduced the Policy Based Chameleon Hash (PBCH) redaction mechanism that enables transaction-level redaction with fine-grained access control constructed by combining Chameleon Hash Ephemeral Trapdoor (CHET) (Camenisch et al., 2017) and Cipher Policy Attribute-Based Encryption (CP-ABE) (Agrawal and Chase, 2017), CHET produces two keys the long-term key is generated for each modifying node and distributed during the setup phase. The transaction owner issues the short-term trapdoor key through the transaction hashing phase, leading to the hash value being appended in the blockchain. The short-term trapdoor key is then encrypted using CP-ABE according to predefined attributes to construct an access policy. Any modifier compliant with the access policy can decrypt the trapdoor key and perform redaction (Derler et al. 2019). However, the current PBCH-reliant constituent infrastructure results in significant computational resource consumption, adversely affecting the overall redaction mechanism efficiency and throughput regarding performance and resource demands.

Furthermore, the assumption of honest behaviour among redaction participants poses another critical challenge, impacting the validity of ciphertexts within permissioned blockchain environments. This assumption cannot always be guaranteed, leading to potential data integrity violations. This research mainly focuses on enhancing fine-grained access control with transaction-level redaction mechanisms efficiency and throughput without compromising security properties. It also ensures the validation of mutable transactions and participant's honest behaviour. Therefore, an efficient redaction construction with fine-grained access control supported by a behavioural validation mechanism in the redactable blockchain is proposed.

1.2 Research Motivation

The recent immutability is misused through injecting illicit and inappropriate content discovered and reported by Matzutt et al. (2018). It indicates serious and potential immutability failure to ethically maintain and manage data stored, such as Bitcoin-stored child pornography linked to darknet services. Moreover, the rise of compulsory GDPR demonstrates another immutability-challenging aspect, which emphasizes the importance of data privacy and the right of individuals to control their personal information (Bai et al., 2022; Schellinger et al., 2022). The abovementioned issues emphasize the redactable blockchain concept to provide a balanced ability to amend data without compromising immutability using strict redaction mechanisms governing such cases. It offers a precise approach to amend content within the blockchain, enabling controlled modifications in predefined scenarios.

This adaptability is crucial for aligning blockchain technology with legal mandates, such as GDPR, and addressing the ethical implications of storing and disseminating illicit content. Furthermore, the applicability of redactable blockchain across diverse industries such as healthcare (Hylock and Zeng. 2019), financial (Xu et al., 2020), education (Wei et al., 2022), supply chain (Zhang et al., 2023), marketing (Wang et al. 2022), sales (Wang et al., 2022), IoT (Huang et al., 2019, 2019, 2020, 2021; Yu et al., 2019), and more other applications like defence (Chen et al., 2014; Gao et al., 2022; Hou et al., 2021; Huang et al., 2022; Jia et al., 2021; Matzutt et al., 2022; Xu, 2021; Zhang et al., 2021) demonstrates its potential ability to transform data management practices to facilitate the secure, flexible, and compliant amendment of data.

It also addresses the critical need to balance immutability and adaptability, producing a more inclusive and ethically responsible blockchain ecosystem. This

research aims to contribute to the body of knowledge by examining and analyzing the current effective redaction mechanisms. The motivating aspect illustrates the need to be adopted in the different business applications, as illustrated in Table 1.1

Table 1.1 Redactable Blockchain Applications

Authors	**Applications**	**Business Sector**
Huang 2019	Industrial data management	Supply chain management
Xu 2020	Identity management	Financial sector
Mishra 2022	Secure data aggregation	Security
Wei 2022	Secure federal learning	Education
Wang 2022	Housing renting, listing	Marketing
Huang 2020; 2021	Data management distribution	IIOT, IOT
Hylock and Zeng, 2019	Health chain, EHR	Health care
Huang 2022	Credit Bank Supervision	Financial sector

1.3 Problem Statement

Redaction mechanism designs play a vital role in modifying blockchain content where they require control, preserving immutability, transparency, and security. Therefore, balanced approaches are highly required to increase wider applicability. Ateniese et al., 2017 were the first to propose a redaction mechanism by employing the CH function (Ateniese and de Medeiros, 2005). Their proposed mechanism relies mainly on replacing the standard one-way hash function with the CH. The latter generates a key pair of public and master trapdoors to amend data without violating the chain's consistency, resulting in having a similar hash representation. Therefore, transaction redactions are secured by safely replacing hash values in the block header. However, master trapdoor key exposure remains a potential vulnerability because of generating a single key for the entire block which can be prone to be disclosed by malicious modifiers. It enables them to redact any transaction without being monitored. Consequently, data integrity is threatened which in turn undermines the entire block consistency (Ateniese and Medeiros, 2005). Recent proposed redaction-

based chameleon solutions have mainly focused on Key Distributed Management (KDM) to prevent key exposure (Lv et al., 2020; Liu et al., 2021; Matzutt et al., 2022). However, the solutions mentioned above have relied on coarse-grained access control assumptions where the transaction owner is unaware of what has been modified or by whom.

Policy-based Chameleon Hash (PBCH) proposed by Derler et al. (2019) has represented a significant advancement in blockchain redaction. It overcomes Ateniese's drawbacks by adopting fine-grained access control within a transaction redaction level. It primarily relies on the Chameleon Hash Ephemeral Trapdoor (CHET) and Ciphertext Policy-based Attribute-Based Encryption (CP-ABE) and Fujisaki and Okamoto (F.O.) transformation scheme. Furthermore, three players are meant to run redaction operations. The Transaction owner (TO) issues and appends transactions to the blockchain while Transaction Modifiers (TM) redact and ensure the received transactions soundness; meanwhile, the Central Trusted Authority (CTA) generates and distributes required redaction privileges. CHET is an enhanced variant of the CH, which plays a redaction mechanism role via computing two secret trapdoor keys. First, the long-term trapdoor key is issued and distributed by CTA in the setup phase to all eligible modifiers. When the transaction is appended, the TO generates the ephemeral trapdoor (etd), where etd is dominant in the redaction process. Thereby, TM with both trapdoor keys can easily conduct transaction redaction (Camenisch et al., 2017).

The CP-ABE offers fine-grained access control over encrypted data, establishing Insider Collision Resistance (ICR), outsider collision resistance and indistinguishability security properties. Due to secure private key distribution management, it is currently adopted with a wide range in diverse industries such as

electronic health, messaging platforms, online social networks, and information-centric networking (Al-Dahhan et al., 2019). It mainly encrypts the etd key based on a set of predefined modifier's attributes, forming access policies.

Therefore, any modifier that complies with specified attributes can decrypt it and perform the demanded redaction safely. This methodology shapes the fine-grained access control-based redactable blockchain concept because it ensures that data access is strictly governed by predefined policies, enhancing the security and integrity of the data management process. The F.O. transformation scheme is employed as a validation mechanism in the PBCH. The TM conducts the received ciphertext verification through decrypting and re-encrypting operations. Eligible TM decrypts received ciphertext, checks the etd soundness, performs demanded modifications, and then re-encrypts the resulting outcomes. However, the reliance on used CP-ABE variants results in heavy resource consumption, degrading the system’s efficiency in terms of computational time, computational cost, and storage cost.

Moreover, generating etd for each appended transaction by CHET notably increases the communication overhead and decreases transaction throughput. Additionally, the current validation mechanism implementation enforces TM to decrypt received ciphertext to ensure extracted etd correctness. If true, modifications are performed, and the outcomes are re-encrypted, increasing computational time and overhead. Additionally, a modifier can also amend the access policy. Finally, the transaction owners' honest behaviour assumption poses another critical challenge, impacting ciphertext validity within permissioned blockchain environments. This assumption cannot always be guaranteed, leading to potential data integrity violations.

In summary, three main problems have been addressed in this research. First, heavy resource consumption in terms of computational time, computational cost, and

storage cost due to reliance on inefficient fine-grained access control and redaction mechanism infrastructure. Second, lack of an efficient Key Reusability Mechanism (KRM). The redundant ephemeral trapdoor (etd) key generation for each transaction, specifically in selective cases limits TO ability to append larger volumes of mutable transactions. It reduces redaction mechanism throughput and increases overall communication overhead. Third, recent fine-grained access control with transaction-level redaction mechanisms remains inefficient due to reliance on complex cryptographic primitives ensuring ciphertext soundness resulting in increasing TM side burdensome. Additionally, the participants' honest behaviour assumption adopted in the state-of-the-art solutions based on the permissioned blockchain nature does not always hold.

Previous extensive analysis presents a potential research question that can be formalized as follows:

a. How to enhance resource consumption in the current transaction level redaction aided by the fine-grained access control redaction mechanism, while maintaining similar security properties?
b. How to avoid fresh Ephemeral Trapdoor (etd) key usage, which causes low transaction throughput and increases overall redaction communication overhead?
c. How an efficient validation mechanism can be designed to verify redactions and participants' behaviour while ensuring transaction integrity and compliance with redaction regulations?

1.4 Research Objectives

There are three defined objectives in this research which can be described:

a. To optimize the efficiency of redaction mechanism resources by reducing resource consumption in terms of computational time, computational cost, and storage cost, while preserving its security properties in terms of Insider Collision Resistance (ICR) and indistinguishability.

b. To design a Key Reusability Mechanism (KRM) that allows the secure reuse of etd keys for appended transactions while preserving redaction permissions. It also compares transaction throughput, communication overhead, and the number of keys generated before and after KRM implementation.

c. To propose an Integrity Validation (IV) mechanism extended with the ORE, thereby verifying ciphertext soundness while ensuring that participating parties comply with the redaction regulation requirements and demonstrate honest behaviour.

1.5 Research Contribution

The contributions of this research to the body of knowledge are summarized as follows.

a. An Optimized Resource Efficiency (ORE) redaction mechanism that reduces resource consumption in terms of computational time, computational cost, and storage cost, concurrently preserving Insider Collision Resistance (ICR) and indistinguishability.

b. A Key Reusability Mechanism (KRM) extended with the previous resource consumption optimization, which increases transaction throughput and reduces overall communication overhead.

c. An Integrity Validation (IV) mechanism extended with the ORE, thereby verifying ciphertext soundness and ensuring that participating parties comply with the redaction regulation requirements and demonstrate honest behaviour.

1.6 Research Scope

This research mainly focuses on four aspects of fine-grained access control with transaction-level redaction mechanisms. First, current redaction mechanisms rely on a set of underlying components that severely consume available resources, thereby degrading overall redaction efficiency in terms of computational time, computational cost, and storage cost. Therefore, this research is proof of concept that focuses on optimizing these efficiency metrics via enhancing redaction mechanisms abilities without compromising security properties attained.

Second, the current mutable transaction appending strategy remains inefficient. It reduces throughput volumes and increases overall communication overhead. This research introduces an enhanced appending mechanism extended with previously proposed optimization for increasing transaction appending throughput and decreasing overall communication overhead.

Third, the recent ciphertext validation mechanism requires heavy decryption and re-encryption operations, impacting computational time and communication overhead. Thereby, an efficient validation mechanism is also developed to reduce computational time and communication overhead.

Finally, the assumption of honest behaviour relying on a permissioned blockchain nature cannot always be true. Therefore, an honest behaviour verifying

mechanism is also introduced to ensure authentic behaviour in following the obligation of the redaction mechanism. Figure 1.1 shows the scope of the research.

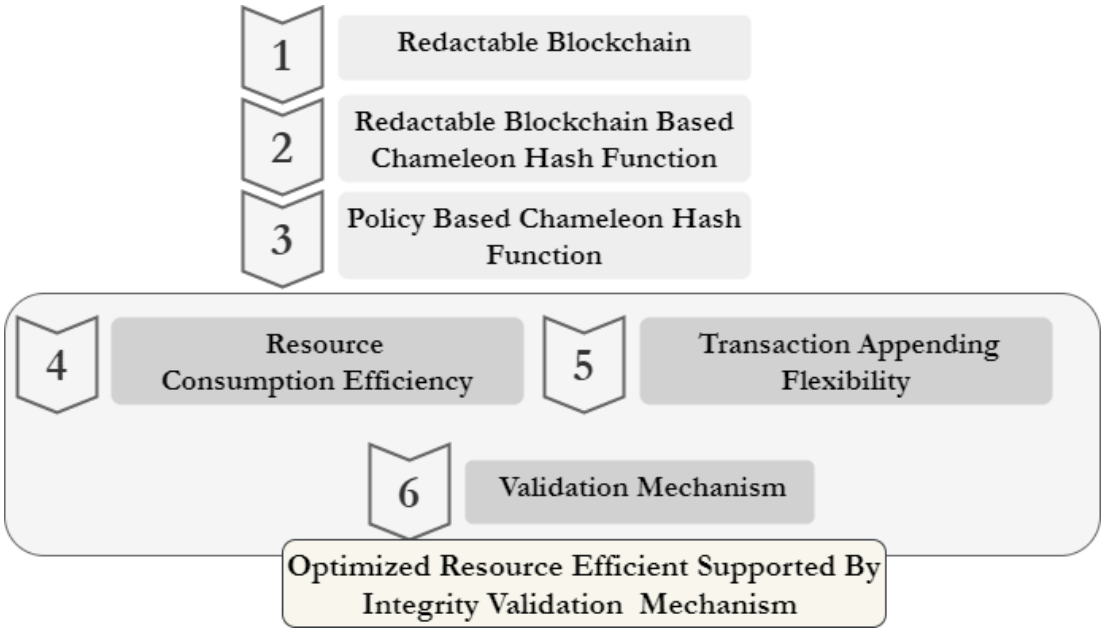

Figure 1.1 Research Scope.

1.7 Research Methodology

This section represents the methodology followed, as shown in Table 1.2, deduced from a current, in-depth review of the state-of-the-art redactable blockchain. The overall flow of the research is visually depicted in Figure 1.2 and assigned to each of the research objectives and expected results. This diagram summarizes the versions of the research methodology, where an expanded version is available in Chapter 3.

Table 1.2 Research Methodology.

Steps	Description	Objectives	Outcomes
1	1.1 Problem formulation and preliminaries. 1.2 Redactable blockchain mechanisms investigation. 1.3 Classifying redaction mechanisms into Chameleon and Non-Chameleon hash functions. 1.4 Analyzing transaction level redaction with fine-grained access control redacting mechanisms. 1.5 Investigation of PBCH's current state of the art. 1.6 Investigating PBCH ABE, CHET, and validation mechanism components. 1.7 Challenge determination.	All	1. Comprehensive literature review. 2. Identifying the research gap.
2	2.1 Investigate and analyze inefficient PBCH infrastructure. 2.2 Variants efficiency measurements. 2.3 Optimizing resource consumption regarding computational time, computational cost, and storage cost preserving security properties.	1	An Optimized Resource Efficient (ORE) redaction mechanism preserving similar security properties.
3	3.1 Investigating the currently implemented transaction appending mechanism. 3.2 Measuring and analyzing its overhead and throughput. 3.3 Proposing an optimized transaction appending mechanism. 3.4 Extending with the previously proposed enhancements.	2	A Key Reusability Mechanism (KRM) increases appended transactions throughput with decreased overhead.
4	4.1 Investigating and analyzing the current validation mechanisms leveraged. 4.2 Investigating honest behavior validation procedures. 4.3 Measuring its computational time and communication overhead. 4.4 Proposing an Integrity Validation Mechanism. 4.5 Extended with previously proposed enhancements.	3	An Integrity Validation (IV) mechanism that ensures valid appended transactions and honest redaction parties' behaviour.

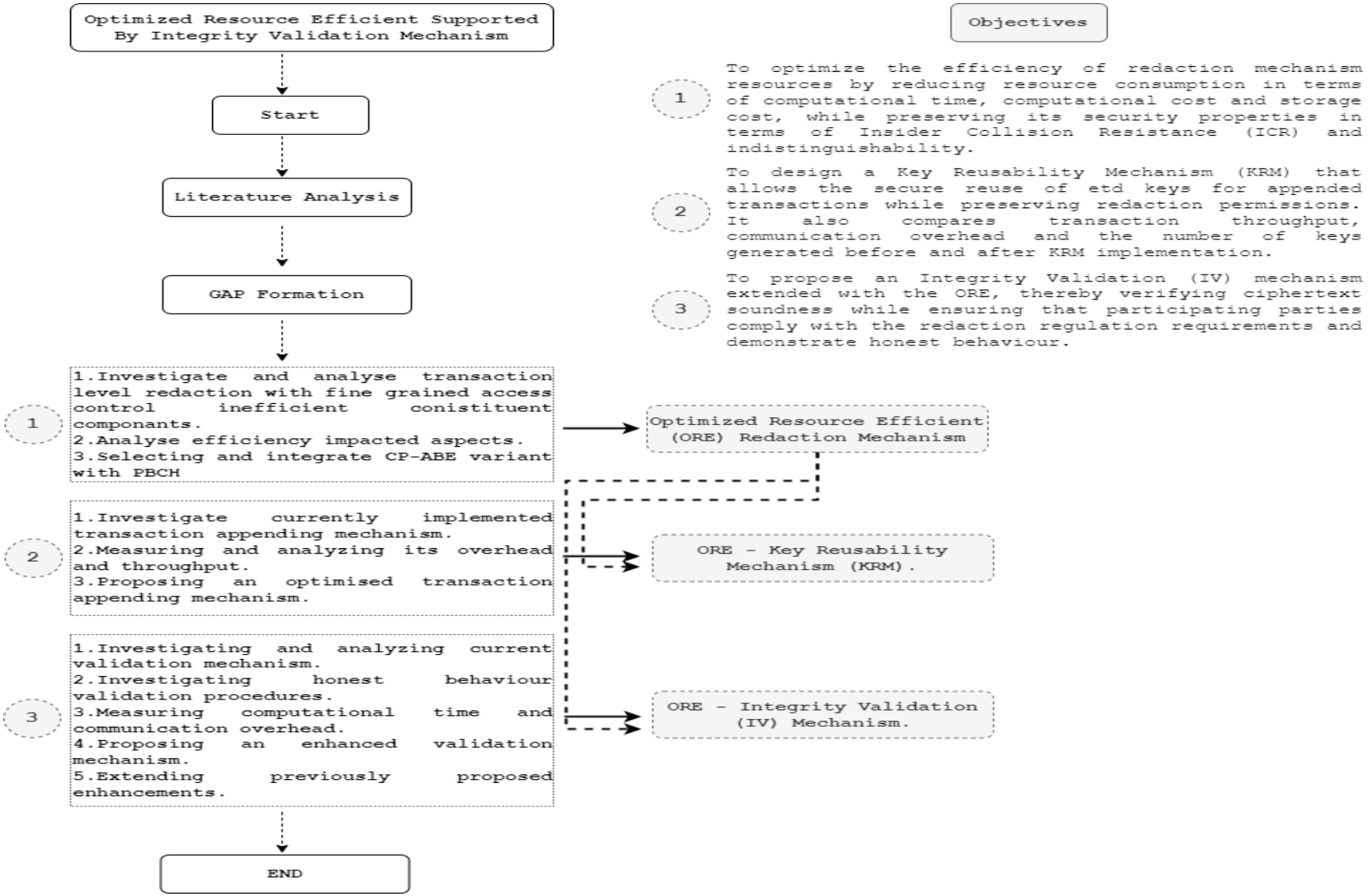

Figure 1.2 Research Questions, Objectives, and Contributions Mapping

1.8 Thesis Outlines

This Research is organized as follows:

Chapter 1 provides the necessary background information, declares the problem statement, presents the research questions, outlines the research objectives, specifies the research contributions, defines the research scope and boundaries, discusses the research methodology, and describes the organization of the thesis. This chapter serves as an introduction to the thesis and outlines the research's purpose and structure, guiding the readers through the subsequent chapters.

Chapter 2 presents a comprehensive literature review of redactable blockchain, discussing its mechanisms and the challenges in achieving the scoped problem. Introduces PBCH and outlines its core concepts while analyzing proposed schemes and challenges. Furthermore, it analyses backboned components like ABE, which have been studied thoroughly with its variants; meanwhile, Current CHET as a transaction appending mechanism used is also analyzed deeply, and finally, the transaction validation mechanism has been overviewed thoroughly. It is worth noting that the efficiency impact caused by these components has been analyzed precisely. Challenges and gaps are also determined. This chapter serves as a foundation for the subsequent chapters, providing a comprehensive overview of the PBCH construction and its associated challenges.

Chapter 3 presents the methodological steps taken to achieve the predefined objectives outlined in Chapter 1. It provides a detailed description of the methodology used to carry out this research.

Chapter 4: It demonstrates the first objective and proposed contribution by illustrating the building of an Optimized Resource Efficiency (ORE) redaction mechanism, including a system model, a formal definition, a security model, and concrete construction. The experiments presented a theoretical analysis, experimental analysis, and security analysis.

Chapter 5: It expresses the second objective and proposed contribution by explaining the build of the Key Reusability Mechanism (KRM), which is extended with ORE, presenting a formal definition, concrete construction, and experiments conducted to measure variants efficiency measures.

Chapter 6 shows the third objective and proposed contribution by proposing an Integrity Validation (IV) mechanism integrated with ORE, forming finally the Optimized Resource Efficiency supported by the Integrity Validation (OREIV) mechanism. It presents a system model, formal definition, security model, and concrete construction expressing its lifecycle architecture. The OREIV application within redactable blockchain feasibility is also demonstrated. Theoretical, implementation, literature comparison, and security analysis are presented.

Chapter 7: This chapter highlights the conclusion and future work.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter provides a broad overview of current blockchain types and constituent properties. Additionally, a full analysis of the current redactable blockchain state and the importance of redaction mechanisms has been conducted. Section 2.2 provides an overview of blockchain, including its types and construction features while in Section 2.3, the current redaction state of the art and their categorized solutions include further grouped solutions-based techniques. Section 2.4 illustrates the Policy-Based Chameleon Hash (PBCH) redaction mechanism's extensive refined review outlining its core building components in section 2.5. After that, its current state of the art, analysis conducted, and summary illustrated in section 2.6. In section 2.7, the research gap has been identified based on current PBCH redaction limitations, and finally, the chapter summary depicts briefed outcomes achieved. Chapter Two taxonomy is presented in Figure 2.1.

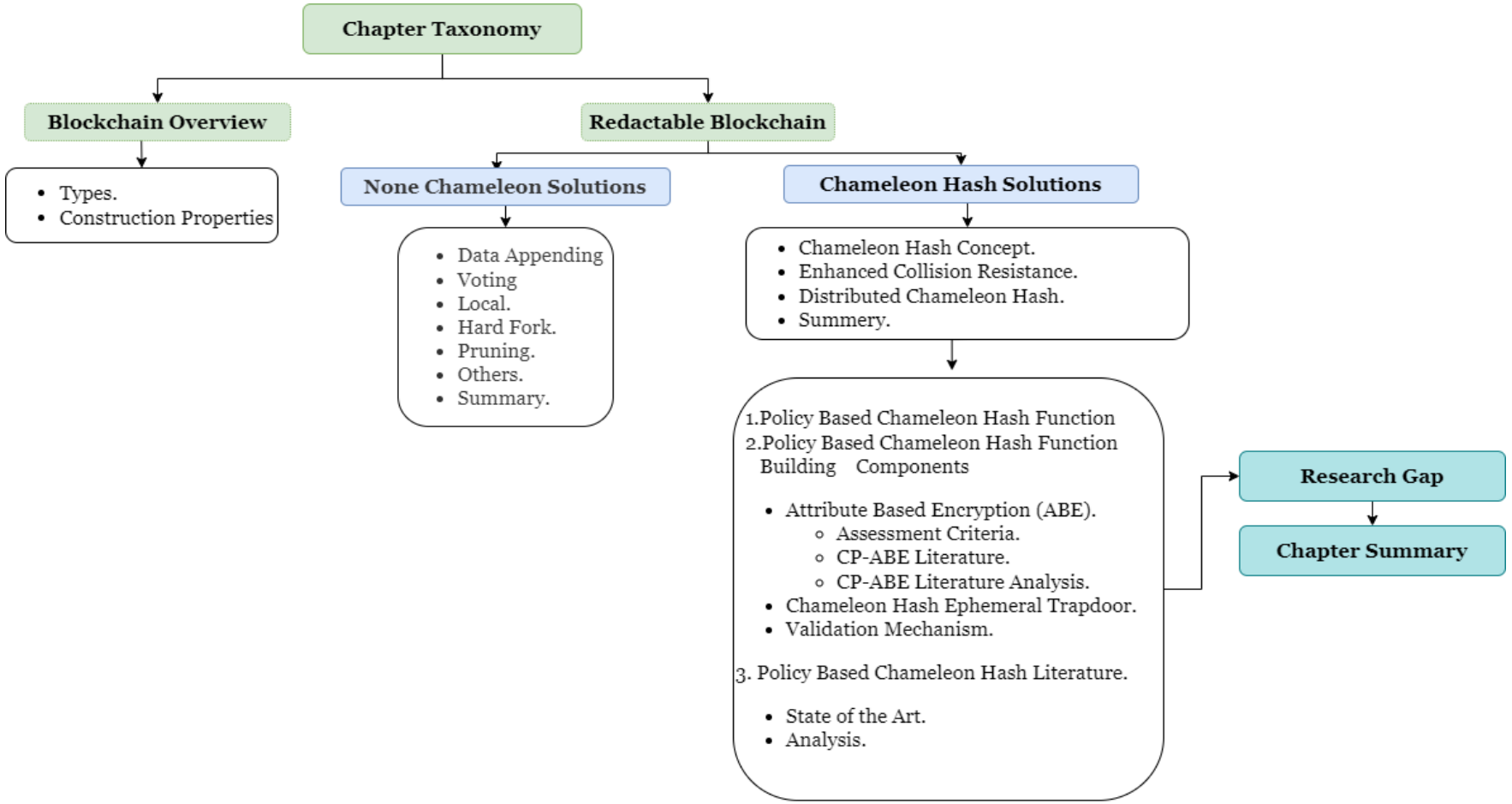

Figure 2.1 Chapter Two Taxonomy

2.2 Blockchain Overview

Blockchain is a fundamental storing technology that has aided Bitcoin's growth while recently serving various industries. The underlying infrastructure comprises a distributed public ledger, blocks, miners, and a consensus mechanism. The distributed public ledger functions as a publicly accessible registry encompassing all validated transactions, organized into blocks that remain immutable once approved. The decentralized nature of the blockchain eliminates the requirement for centralized authorities or replicas, reinforcing a trustless environment. (Zheng et al., 2017). Miners serve as powerful nodes in the blockchain, elected based on their resources, power, and financial abilities. They are rewarded fees for validating transactions via solving certain mathematical puzzles given to them by the consensus algorithm. The consensus algorithm is the primary regulator that organizes, approves, and rewards all miners based on authentic transaction validation, resulting in appending transactions finally within a block (Romano and Schmid, 2017). Figure 2.2 illustrates the blockchain infrastructure.

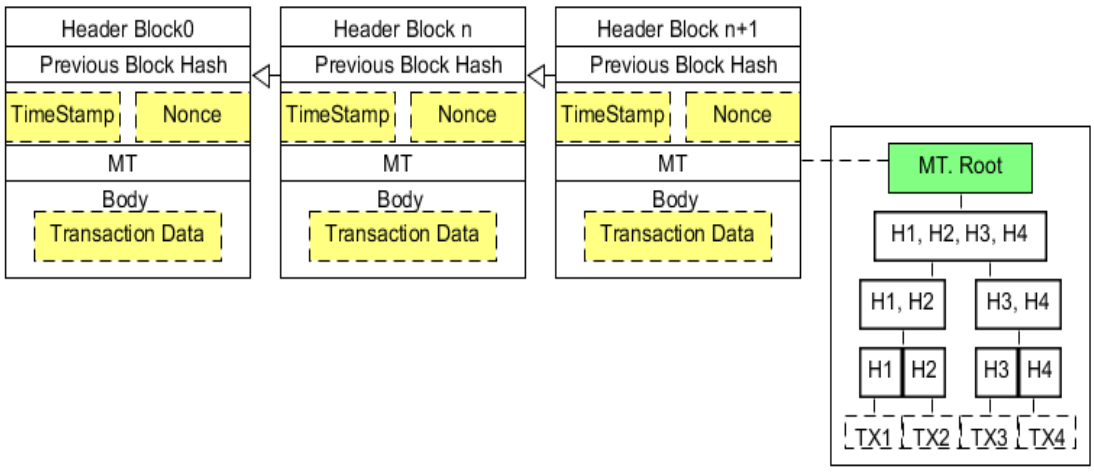

Figure 2.2 Blockchain Basic Structure

Additionally, various consensus protocols are available, each designed to suit different network environments. These protocols provide other mechanisms for achieving consensus among participants in the blockchain network. These protocols include Proof-of-Work (PoW), Proof-of-Stake (PoS), Proof-of-Activity (PoA), Byzantine Fault Tolerance (BFT), and hybrid BFT algorithms. PoW protocol is the official blockchain consensus mechanism where nodes independently solve cryptographic puzzles to create blocks containing valid transactions (S. Zhang & Lee, 2020). In the case of Bitcoin's blockchain protocol, the longest chain is selected as the main chain (Nakamoto, 2008). However, PoW protocols are known for their high computational costs and low throughput.

In the PoS protocol proposed by (King and Nadal 2012), stakeholders produce blocks. The probability of a PoS miner proposing a block is proportional to their stake value in the network. This approach reduces the need for intensive computational work. The PoA protocol is a hybrid approach that combines PoW and PoS elements. Stakeholders associated with a pseudo-random series create blocks based on their probabilities, reflecting their stake volumes. BFT protocols allow each participant to suggest an alternative block to be agreed upon by a group. This enables higher transaction throughput but may lead to increased communication overhead. The goal of every consensus protocol is to ensure that the most honest nodes can reach a consensus on a unified blockchain history (Wang et al., 2019; Monrat et al., 2019). Transactions become immutable once approved, preventing modifications without repeating the approval process. Immutability is a crucial feature that ensures data integrity and blockchain consistency (Hafid et al., 2020; Wang et al., 2023). Each block in the blockchain comprises two main sections. The first section is the unique block header, which

includes the previous block's hash value, nonce, and timestamp. The second section contains the verified transactions. Any attempt to alter the transactions will result in different hash values, revealing unauthorized activities (Deng et al., 2023). To calculate the hash value, the previous block's header is combined with the current block's timestamp, nonce, Merkel tree, and bits, following the order: SHA256 (Version || PrevHash || Merkle Root || Timestamp || Bits || Nonce).

This process facilitates the continuous expansion of the blockchain by generating and appending new blocks (Wang et al., 2019; Monrat et al., 2019). It also efficiently detects any tampering with previous blocks, ensuring the overall integrity of the blockchain's data. The timestamp records the time the block is created, providing a chronological order to the connected blocks. The nonce is used to develop and validate block contents, adding blockchain security. These blocks are then added to the main chain and chosen based on specific consensus algorithm rules.

2.2.1 Blockchain Construction Feature

Blockchain introduces several different features that can be leveraged to suit a wide range of industries beyond financial services (Antonopoulos, 2014); Habib et al., 2022). These features are outlined in Table 2.1:

Table 2.1 Key Features of Blockchain

Features	Definition
Decentralization	It allows the blockchain to serve as a decentralized, duplicating, and disseminating data repository across all networked users.
Neutrality	It facilitates continuous valid transaction records inclusion on a blockchain public ledger by credible payments or trust levels individuals.
Replication	It authorizes consensus algorithms to replicate all valid transactions across all network nodes.
Audibility	It ensures that all transactions are publicly displayed and audited due to every performed transaction being appended to the Genesis block.

Integrity	Transactions are verified by the hashing algorithm before being published on the distributed ledger. Specifically, the SHA256 algorithm is frequently used to provide a digital fingerprint that cannot be reverse-engineered (Makridakis and Christodoulou, 2019). Thus, every amendment could not be executed without invalidating the signature before eventually invalidating the transaction.
Anonymity	It permits users to conduct transactions through pseudonyms generated by respective secret keys rather than actual identities or real-life addresses to prevent exposing personal particulars (Gong et al., 2021).
Traceability	It provides detailed records between transactions to trace all transactions on the blockchain and reveal the entire flow.
Immutability	It issues signatures to guarantee transaction authenticity and integrity. The Merkel Tree (MT) structure maintains an efficient integrity check process, prohibiting malicious block tampering (Yu et al., 2019).

Immutability is the utmost important block and transaction consistency feature. For instance, assuming that there are TX1, TX2, TX3, and TX4. The TX3 has been altered on the nth block, where the hash value becomes different on the MT root. Therefore, the n^{th} block's hash value is invalidated with the $(n+1)^{th}$ block recorded copy value. As such, the modification was invalid and difficult to approve without other nodes possessing more than 51% hashing power to accept the modification and regenerate an alternative chain from the $(n+1)^{th}$ block. Consequently, data immutability is ensured. Figure 2.3 represents data immutability.

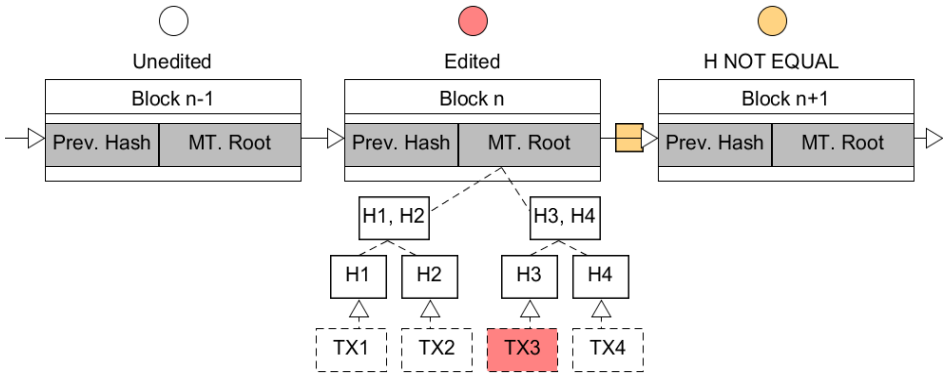

Figure 2.3 Blockchain Immutability Methodology.

2.2.2 Types of Blockchain

Blockchains are categorized into numerous types depending on their respective purposes and distinctive features, as illustrated in Table 2.2. The permissionless or public blockchain does not necessitate platform users to participate in the network, which is fully decentralized as the participation is based on the process of consensus and perusal before sharing the transaction record to maintain the distributed ledgers (Xie et al., 2019; Cai et al., 2018). Additional blocks are posted, examined, and verified by all users that possess a copy of the entire blockchain, ensuring high security in establishment and operation, as the blocks are corroborated by computationally challenging consensus procedures, such as decoding cryptograms or investing more personal cryptocurrency. Therefore, any form of data tampering in blockchain content is prevented by hashes and decentralized, consistent with other benefits of anonymity and privacy (Bodziony et al., 2021). However, permissionless blockchains pose multiple research issues. For example, efficiency is negatively impacted by numerous participants and computationally expensive consensus procedures. Another type is permissioned or private blockchains developed for a single organization, where participants join the network by invitation and are required to maintain the decentralization characteristic of the blockchain (Cai et al., 2018).

Permissioned blockchains contrast with permissionless blockchains in that only approved entities can participate in the network and maintain the blocks, providing higher security and efficiency levels by preventing data tampering through hashes and consensus. However, private blockchain nodes are not anonymous, as internally authorized users could breach networks (Xie et al., 2019). Meanwhile, consortium blockchains serve as private blockchains for

various organizations, wherein merely invited and approved users are permitted to participate and support the network. The consensus process is comparatively more time-consuming than permissioned blockchains, although swifter than permissionless platforms. Regarding security, consortium blockchains could process data in a more protected manner to avoid alterations and hacking activities than permissioned blockchains due to monitoring by different organizations (Cai et al., 2018).

Table 2.2 Blockchain Type

Type	**Public (Permissionless)**	**Private (Permissioned)**	**Consortium**
Network	Decentralized	Partially Decentralized	Hybrid Among Public and Private
Access	Any participant	Predefined Participant	Multiple Predefined Participants
Concept	1. Read and write transactions. 2. Vote to add pooled transactions. 3. Validate transactions, and consequently, they are secured.	1. Conditional read and write operations. 2. Conditional verification. 3. Public reading might be allowed.	1. Permission read/write by multi-controlling nodes. 2. Participants are selected differently 3. Public reading might be allowed.
Consensus	PoW/PoS	Multi-party	Multi-party
Approval Time	10 Minutes	100 ms	100 ms
Scalability	Slow	Fast, Light	Fast, Light
Security, Privacy	Lack of privacy and anonymity.	High Privacy	High Privacy
Cost	Costive.	Costive.	Costive.
Energy	High Consumption	Low Consumption	Low Consumption
Efficiency	Non-Efficient	Efficient	Efficient
Immutability	Non-tempered	Can Be Tampered	Can Be Tampered
Centralization	No	Yes	Partially
Use Cases	Cryptocurrency	Supply Chain	Banking, Insurance
Application	Bitcoin	Ethereum	Edexa