

Blockchain-based Auxiliary Systems for Pseudonymization and Consent Management

Jiraphat Lapwattanaworakul¹, Chetneti Srisa-An¹, Thannob Aribarg¹

¹ College of Digital Innovation Technology, Rangsit University, Pathumthani, Thailand

Abstract – Stringent privacy regulations, exemplified by the General Data Protection Regulation (GDPR), create intricate challenges for businesses engaged in data sharing. In response to the risk associated with data disclosure and potential legal consequences, this research paper introduces a novel approach. It suggests the adoption of blockchain technology as an auxiliary system for managing consent. Our RSU-CMS consent management systems make use of smart contracts within a private blockchain environment. A new technique is employed to ensure data integrity and compliance with relevant laws. The experiment outlined in this paper provides an end-to-end illustration of the process using true experimental research, while the conclusion addresses the merits and demerits of this approach. Leveraging intelligent encryption, blockchain technology not only ensures anonymity but also enhances security, making it an attractive platform for consent management.

Keywords – Blockchain, pseudonymization, consent management, data privacy, GDPR.

1. Introduction

Data sharing on the Internet has been published freely on the Internet for decades.

DOI: 10.18421/TEM124-59

<https://doi.org/10.18421/TEM124-59>

Corresponding author: Jiraphat Lapwattanaworakul,
College of Digital Innovation Technology, Rangsit
University, Pathumthani, Thailand


Email: jiraphat.l65@rsu.ac.th

Received: 24 July 2023.

Revised: 16 October 2023.

Accepted: 23 October 2023.

Published: 27 November 2023.

 © 2023. Jiraphat Lapwattanaworakul, Chetneti Srisa-An & Thannob Aribarg; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

The article is published with Open Access at <https://www.temjournal.com/>

The General Data Protection Regulation (GDPR) was introduced in 2018 and applies to European countries. Since then, all famous data sources such as UCI Machine Learning Repository and Kaggle have had a big impact on sharing datasets that contain personal data. Normally, almost all datasets do not contain direct identification data such as real name and last name on a public dataset. However, a re-identification attack has taken place since 2009 [1]. This finding causes alerts on how to publish data on the Internet properly. This finding causes all publishers to care about the re-identification attack.

In 2019, Thailand established the Personal Data Protection Act (PDPA), which has been enforceable since June 1, 2022. The objective of the PDPA is to protect Thai data subjects or data owners from the lawless collection, sharing, or use of their personal information. PDPA mandates that explicit consent must be obtained before collecting any personal data information. The consent management system facilitates data controllers in managing the usage of personal data. Personal data and sensitive data should not be controlled by others without permission, because they are susceptible to attacks and misuse [2].

GDPR introduces two new terminologies in data privacy laws: data controllers and data processors. Companies that hold other personal data are known as “data controllers”, while individuals who work with other personal data to analyze it under the direction of “data controllers” are known as “data processors”. Both data processors and data controllers shall adhere to GDPR. Even though the data controller and processor are frequently the same, this is not necessarily the case.

The big new task of the GDPR data controller is consent management. Others who need to manipulate other personal data need consent from the data controller before operating. Not only approval but withdrawal and update also need consent from owners. The blockchain consensus scheme can solve consent management on GDPR easily. Blockchain can become a public logs repository permanently by laws. To avoid an expensive free, a private blockchain or consortium blockchain is adopted in this case.

Article 4(5) of the GDPR encourages a novel practice called pseudonymization, For independently kept personal data, it becomes extra information. Pseudonymization is an alternative method for processing personal data in E-Commerce because of its reversible scientific, historical, and statistical characteristics. Blockchain is a cutting-edge technological advancement for this century. Data on blockchains are recorded in a massive distribution network, making it nearly hard for hackers to alter or change them. A blockchain is used to store all personally identifiable information and sensitive data. All personal data can be protected from online data breaches using this method.

A review of a lot of literature found that there are few studies and applications of blockchain in PDPA practices. The first purpose of this study is to use blockchain technology as a pseudonymization technique. All mapping tables are stored in the blockchain. The hashing address is unique enough for a primary key that can link back to microdata. The hashing address is a box address when created combined with the row number of the table. Each mapping table is in a box. Each chain stores a history of each mapping table. The chain's last box is the mapping table's current version.

The rest of this paper is structured as follows: In section 2, the architecture design for consent management and pseudonymization is presented. Section 3 reviewed all relevant academic papers. Our proposed methodology is discussed in section 4. In section 5, the author demonstrates an experiment. Section 6 demonstrated the experiment result. In section 7, the author presented a conclusion of the study.

2. Architecture Design for Pseudonymization and Consent Management

Due to its robust qualities, this research intends to apply the blockchain concept to data privacy. Data on the blockchain is resistant to modification and is difficult to alter. Three articles in GDPR cause public blockchain not to comply with PDPA, including articles 14, 15, and 18 [2]. According to section 14, data owners possess the right to correct their data if they believe it is inaccurate.

If data owners believe that the current data is erroneous or incomplete, they can update new data and change any data controllers already hold on them. According to this section, blockchain alone is not applicable because data on the public blockchain are hard to change. All supplementary tables in the blockchain are reassembled to update data and redo the process. The chain in blockchain keeps the last updated data in the last box and keeps history in a chain.

Article 15 states that one can remove data from a blockchain; therefore, the data owner/subject cannot utilize the right to delete data in the blockchain. Data controllers cannot store EU citizens' personal data on a blockchain. For this reason, this research selects blockchain as an auxiliary system. The database server keeps all data as a centralized controller. When data is deleted on a database server, the link on the blockchain becomes invalid and useless.

Eventually, Article 18 provides the right to limit how data control processes the data. Since public blockchains are available to anyone, it does not comply with Article 18. A solution for Article 18 is an authorized blockchain instead of a public blockchain. Authorized blockchains are restricted to only parties who get permission to access them. The other words, permission blockchains are not for public access [3].

For public blockchain, data is accessible to everyone who joins a network. This property is unsuitable for data privacy; therefore, a permission blockchain is better than a public one. For those reasons above, permission blockchain is used as an auxiliary system for the following purposes. Purpose 1: Data Linkage schema. A secure server with reading and writing access simply stores personal data secretly. Then personal data segment, direct or indirect information that refers to each data on the main server is stored on our blockchain, as shown in Figure 1. Purpose 2 is to limit access to only relevant people involved.

Figure 1 demonstrates the system's architectural design. The system comprises a single database server and multiple blockchain networks. Blockchain networks are specifically dedicated to the storage of direct identifier segments.

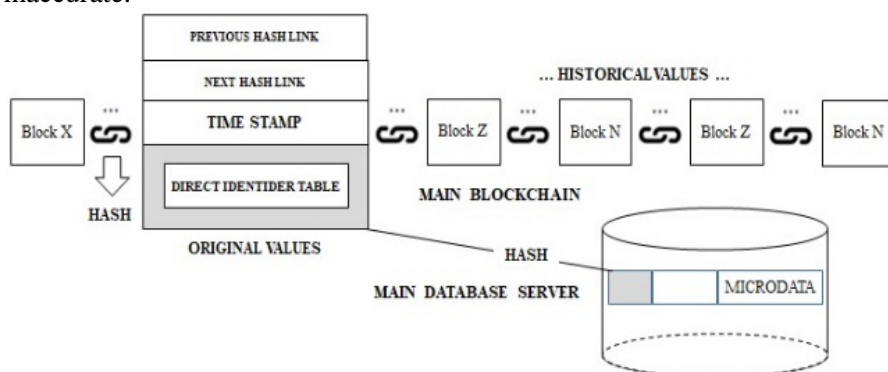


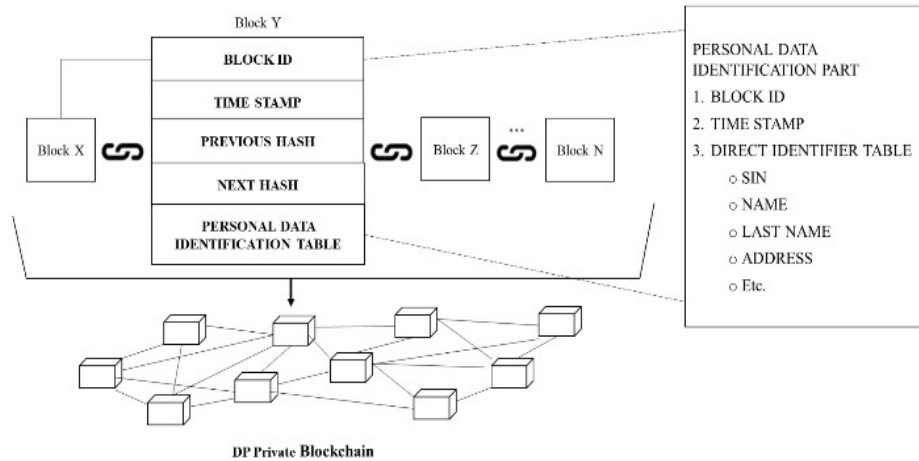
Figure 1. Main architecture diagram

A link between each node and the database server uses a hash function. The reason for using the hash technique is because of two properties. First, hashes are a one-way function. Once data is hashed, the result cannot be reversed back to the original version. Secondly, a hash function can prove if the suspicious file is ever modified or tampered with. Data on the server is connected to the box's hash.

The data controller simply deletes the actual data from the main server if any data owners exercise their right to erasure.

As a result, the hash on the blockchain becomes ineffective. It is no longer useful and regarded as "personal data".

Figure 2 shows the blockchain that stores a segment of direct identifier attributes. This chain acts as an auxiliary system supporting a central database server.



Purpose: This blockchain is to store an original direct identifier segment that is split from an original Personal Data table

Figure 2. Auxiliary-direct-identifier-table blockchain

In this paper, consent management has a responsibility as follows: Before collecting and processing a customer's data, the organizations/businesses must get consent from the owner and then secondly prove that a customer is a real person. Among promising technologies, blockchain and smart contracts for PDPA compliance are some of the solutions gaining popularity.

personal data is handled in compliance with the Personal Data Protection Act or similar data protection regulations. In this scenario, a module for personal management, designated as the data controller, is situated within the primary server of the data center, where all currently active customer records are stored.

Figure 3 is a visual representation that gives an overview of a system. Within this system, there is a component called "personal data management", which has the role of a "PDPA data controller". This suggests that it plays a critical role in ensuring that

A requester is a person who wants to get a permit to store/process, withdraw, or update from a data owner. From steps 1 to 5, there is no owner data in the consent block to avoid a data breach. Each block consists of a Requester ID, Owner ID, Consent ID, Status, and Date.

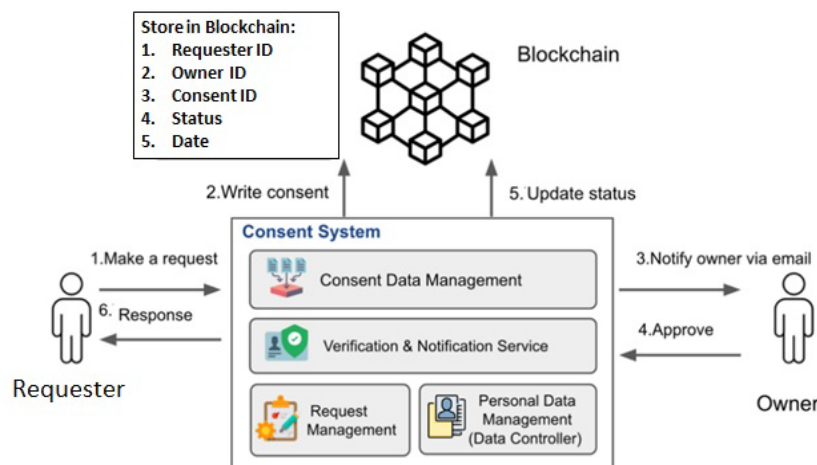


Figure 3. RSU-CMS architecture diagram

Figure 3 shows our consent management diagram using smart contracts in a private blockchain. The proposed system focuses on block creation and secures a smart contract. In this paper, a blockchain infrastructure and smart contracts are used to contract a consent management decentralized system. Consent management is as follows tasks. Task 1: Before collecting and processing a customer's data, the requesters such as organizations/businesses must get consent from the data subject, and Task 2: They must be able to prove that a data owner is a real person.

From Task 1: Consent enables the information owner to control usage parameters of their personal information. A smart contract is used as a permission token to comply with PDPA.

From Task 2: To prove the owner's identity, the public key infrastructure is used. The protection of privacy is ensured by employing blockchain encryption, which restricts data access to the owner's private key. This encryption mechanism guarantees that sensitive data remains confidential and secure, thus preserving individuals' privacy. The main benefit of blockchain is to improve privacy and security using cryptographic algorithms.

The blocks within the blockchain do not contain any personal data. Instead, they consist solely of consent smart contracts, which are translated into database queries as needed. This approach allows for on-demand retrieval of information without compromising the security and privacy of personal data within the blockchain. In step 2, the request block is signed with a requester's private key to prove his/her identification.

3. Related Work

Suripeddi [4] studied compatibility issues between blockchain and GDPR. The result shows that some articles in GDPR contradicted blockchain characteristics.

Mohanta [5] is concerned about the privacy of blockchain. The data saved on a blockchain resists being changed or deleted to allow the blockchain to be the first completely distributed system.

In comparison to conventional methods, the private blockchain may offer greater security and privacy [6]. It can be used to reduce the risk of improper data collection. The current widespread practice of centralizing the storage of personal data is not an ideal solution.

Zhang [7] suggests implementing the pseudonymity concept. To protect a user's real name. Pseudonymity is for private property. Pseudonymity is a new modern approach to disguised identity. He reviewed on page 25 that Proof of Authority (PoA) is a consensus paradigm that enables validators to quickly approve transactions within a blockchain network.

This paper implements the private blockchain network called "xCHAIN" as an auxiliary system using PoA.

The application development on blockchain by smart contract has been rapidly adopted since invited by Nick Szabo in the 1990s [8].

A new protocol using blockchain as a manager node that stores, queries, and shares sensitive data complying with GDPR is proposed in [9].

Sirur [10] studied and proposed recommendations using blockchain to comply with GDPR laws. They study both large enterprises/organizations and SMEs.

The most difficult challenge for deploying blockchain is to be GDPR compliant in Article 14 (right to be erasure) [11].

Kondova [12] proposes a new way to self-sovereign identity on public blockchains such as Hyperledger Indy.

Hristov [13] proposed Hyperledger Fabric as a backbone of GDPR-compliant frameworks. However, they are still confused about Article 14 on how to erase data from history boxes.

Bonneau [14] reviewed privacy-enhancing methods for Bitcoin and other cryptocurrencies. Both security and privacy are concerns in their paper.

Many re-identification attacks have been successfully done by using multiple public data sets since 2009 [1].

Hewa [15] interviewed 20 developers asking about obstacles and intensity for them working on smart contracts. The paper suggested many aspects beneficial for developers.

Ensuring adherence to data protection laws becomes essential when individuals employ smart contracts to assert their personal data rights, especially in cases where technologies such as blockchain-based smart contracts are leveraged to automate and enhance data protection procedures. This is the reason for the stability of smart contracts – the master data subject rights generate hassle in linking with smart contracts applying the blockchain. These are the right to erase and the right to correct, given the changelessness of the blockchain [16].

4. Proposed Method

Our methodology has two independent segments as follows: consent management system in segment I and pseudonymization in segment II.

4.1. Segment I: Consent Management System (CMS)

Figure 3 shows RSU-CMS architecture. There are six steps in a process as follows:

4.1.1. Step 1: Make a request

RSU-CMS consists of four modules including the consent data management module, verification & notification service module, request management module, and personal management (Data Controller) module. Figure 3 illustrates a scenario where anyone requests rights from data owners. The consent data management module constructs a block that contains as follows: Requester ID, Owner ID, Consent ID, Status, and Date.

4.1.2. Step 2: Write consent

A consent management software called RSU-CMS writes a log into the blockchain as shown in label number 2 in Figure 3. xCHAIN is one of the biggest private blockchains in Thailand. The winner will be the only one who can write a block in a chain. In this case, the log is kept in the blockchain forever. No one can change or alter it. Once a code is executed automatically, the block address is sent to the owner by both email and wallet.

4.1.3. Step 3: Notify the owner via email

After a block is created in step 2, a winner writes a block into the blockchain. All members of the data controller (firm/company/university) need to be pre-registered by creating a wallet. To make sure that the data owner knows the result of the contest. RSU-CMS notifies the data subject via email with public-key encryption.

4.1.4. Step4: Approve by the data subject

In step 4, the data subject approves his/her request by updating a flag in the blockchain. In our research, there are three types as follows: Type 1: the right to be informed, Type 2: the right to be forgotten (data erasure), and Type 3: the right to object. Status in a blockchain consists of three types. A new block is created and sent to a blockchain. Below the PDPA, data subjects have the right to object to the processing of their personal data under certain circumstances:

- 1) Individuals must have the right to object to the processing of their personal data if it is gathered without their consent and is connected to activities conducted in the public interest or justified by a legitimate interest.
- 2) When personal data is utilized for direct marketing purposes data subjects possess the right to object to its processing.
- 3) When personal data is employed for statistical, historical, or scientific research purposes, data subjects maintain the right to object to its processing [17].

Type 3 is requested directly from a data controller. No need to process steps 3 and 4.

4.1.5. Step5: Update the Status on the Block

In this step, a new block with a new status is created and then written to a blockchain again. In this way, we can keep track of history from a blockchain easily.

4.1.6. Step6: Response

The data controller answers the request with permission from the data owner in step 6. In this final step, a data controller must perform accordingly with permission as consent. As an example, if the right to be forgotten (data erasure) is exercised, the data owner's records will be completely removed from the database.

4.2. Segment II: Pseudonymization Section

In accordance with the GDPR, pseudonymization refers to the process of handling personal data in such a way that it can no longer be directly linked to a specific data subject without utilizing additional information [18]. To pseudonymize a dataset, the "additional information" must be "kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person".

5. Experiment

From section 4, all personal data tables are split and prepared in a data preparation process. The result of the conclusion section 7 provides anonymized microdata linked to two blockchains. One "main blockchain" has maintained a history of all identifier attributes when a new transaction comes. It is noticeable that both blockchains have maintained all original values of each personal data table. The main database server contains all anonymized tables that can trace back to all original values by combining both blockchains. Keep in mind that the main database server maintains microdata suppression and generalization.

The smart contract development process depicted in Figures 4 and 5 serves as a demonstration of a test for smart contract code written in solidity language on the blockchain. Before proceeding with the smart contract application, it is essential to establish an appropriate development ecosystem and load the necessary development toolkits. These steps are crucial for ensuring a smooth and efficient smart contract development process. The development ecosystem mostly consists of Ethereum Virtual Machine (EVM). Go-Ethereum (Geth), and Solidity.

The Ethereum Virtual Machine is the engine, software platform, or virtual machine, that executes, runtime, and deploys smart contracts on the Ethereum ecosystem. Go-Ethereum is an open-source tool and command line interface (CLI) for building decentralized applications on the Ethereum network written in the Go-programming language. Solidity language is an object-oriented, primary language used to create and develop smart contracts for EVM. Moreover, the utilization of smart contracts on Ethereum places significant reliance on the Ethereum node, often utilizing software such as Geth, which operates discreetly in the background. Hence, it becomes crucial to configure an Ethereum network for the optimal functioning of this node. The procedure encompasses several sequential steps: The Geth console utilizes a file name “genesis.json” to create the genesis block. Concurrently, the Geth console designates a directory to store the block data and the account’s personal keys. Starting the network, once the genesis block is created and the directory is set up, the network is initiated by running specific commands. Geth will read the files, store block data, and configure relevant parameters to establish a fully functioning node within the Ethereum network.

Smart contracts are uploaded to the blockchain network by employing bytecode through the transaction process. The deployment process of a smart contract results in the creation of a new smart contract account on the blockchain. During the implementation of a smart contract, the code written in Solidity, which is a high-level programming language utilized for creating Ethereum smart contracts, is compiled into EVM bytecode. This compilation process is facilitated by the Solidity compiler, also known as SOLC. Subsequently, smart contracts are constructed through transactions that contain sensitive data, such as smart contract address and content, and the creator’s account number. It is also necessary to keep data on the smart contract address, amount outstanding of the wallet, and smart contract binary code in the blockchain. And calling functions in smart contracts through the Web3.js library. Remote Procedure Call (JSON-RPC), and Application Binary Interface (ABI) to modify and read the data.

Figure 5 is our source code written in solidity language and runs on xCHAIN private blockchain. The proposed architectures were demonstrated using a private blockchain called xCHAIN. Our work shows that it consumes a low cost of development, has no subscription fee, and is easy to monitor the history of a whole process.

In this research paper, we have selected the “adult.csv” dataset, which can be accessed via the following URL:

<https://www.kaggle.com/datasets/wenruli/adult-income-dataset>.

This dataset, referred to as the “Adult” dataset [19], is hosted on Kaggle. To illustrate this experiment, we have integrated social security numbers, names, and addresses with the “Adult” dataset. The resulting combined dataset, named “Full-Adult-dataset.csv”, is employed as a prototype of our demonstration. We utilize Python and Scikit-Learn, both renowned machine-learning tools. In this experiment, we leverage these tools to perform various data manipulations, particularly formatting the dataset into three distinct segments: a Direct identifier segment, a Quasi-identifier segment, and an Anonymized segment.

6. Experiment Result

This experiment result shows a comprehensive comparison guide on blockchain platforms. There are two primary settings of blockchain platforms, namely: the global public and local public mechanisms, which the lab tests on the Internet network of Rangsit University (RSU-NET). Table 1 shows a head-to-head comparison of blockchain platforms setting the criteria for consideration when deciding on platforms the hosting Decentralized Apps (DApps) usually consist of performance (bandwidth, transaction time), transaction fees (transactions, gas), number of validators, and developer experience.

6.1. Global Public

This is a comparison between the Binance Smart Chain (BSC) and Ethereum (ETH). However, both BSC and ETH look very similar in a way. A quick-hit rundown of the parameter comparison as follows:

6.1.1. History

BSC is a new blockchain network launched in 2019 and was created by Binance CEO Changpeng Zhao that assents smart contract-based applications to be executed. This blockchain platform’s goal is to allow users to handle their digital assets cross-chain with substantial capacity and low latency. BSC has grown innumerable popularity in early 2021.

In contrast, Ethereum was founded and first proposed by Vitalik Buterin, Gavin Wood, and Charles Hoskinson in 2013 and made it launched as an independent blockchain in 2015. It is one of the oldest and most decentralized open-source blockchain platforms. This blockchain platform includes the smart contract which creates a peer-to-peer secure network that operates and validates application code.

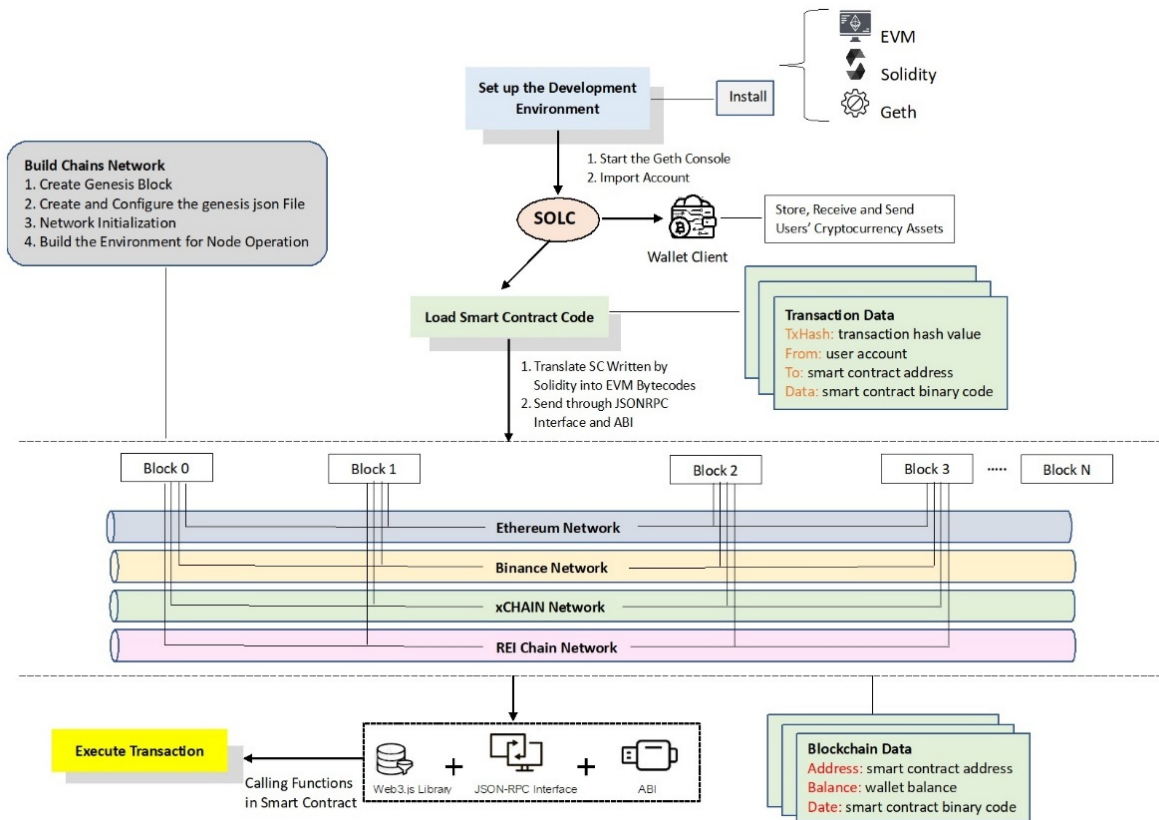


Figure 4. The development process of smart contracts on the blockchain

```

1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.15;
3
4 contract Demo{
5
6     struct Consent {
7         uint id;
8         address requester;
9         address owner;
10        uint consentId;
11        uint date;
12        bool status;
13    }
14    uint consentCount;
15
16    constructor(){
17        consentCount = 0;
18    }
19
20    mapping (uint => Consent) public consents;
21
22    function addConsentDetail(address _requester,
23                            address _owner,
24                            uint _consentId) public {
25        consents[consentCount] = Consent(consentCount,
26                                        _requester,
27                                        _owner,
28                                        _consentId,
29                                        block.timestamp,
30                                        false);
31        consentCount += 1;
32    }
33
34    function setConsentStatus(uint _id, bool _status) public {
35        require(msg.sender == consents[_id].owner, "Only Owner");
36        consents[_id].status = _status;
37    }
38 }
    
```

Figure 5. Exert in source code

6.1.2. Transaction Fees

From our results in Table 1, BSC transaction costs are \$0.68 (0.00210247 BNB) and \$1.19 (0.000726204866 ETH) for Ethereum. Transaction fees conclude that the BSC is very cheap, but ETH is very high on the transaction. However, this can be described thanks to the consensus paradigm used by BSC compared to the one implemented by Ethereum.

$$\text{Transaction Fees} = \text{Gas limit} * \text{Gas price per unit} * \text{Gwei denomination}$$

In our results = $420,494 * 5 * 0.000000001$
 = 0.00210247 BNB (\$0.68)
 and = $46,422 * 15.64353 * 0.000000001$
 = 0.0007262041726249 ETH (\$1.19)
 Note: 1 Gwei = 0.000000001 BNB or ETH

6.1.3. Transaction Time

Normally, the transaction time for BSC posts is about 3 seconds per block time which matches the lab result. Whereas Ethereum takes between 12 to 16 seconds per block which is consistent with the lab result (is equal to 15 seconds per block). Nonetheless, the transaction speed appears with tradeoffs. BSC has a nearly small number of participants running its network but can offer faster than Ethereum.

6.1.4. Gas Limit and Gas Used

The gas limit signifies the maximum amount of gas allocated for an operation in a transaction, as determined by the users' willingness to spend. Meanwhile, the gas used indicates the actual amount consumed, both in absolute values and as a percentage of the allocated limit. More complicated operations require more gas because they require more computation work.

- The lower limit is computations transaction processing can do less.
- The max limit is computations transaction processing can do more.

From our result, the gas used by BSC and Ethereum is 100% of the gas limit.

6.1.5. Gas Price

The gas prices are very cheap on the BSC and very high on the Ethereum blockchain. Anyway, this can be described as the gas model of the consensus mechanism used by BSC comparison with Ethereum. From Table 1, the gas prices show 5 Gwei and 15.643533 Gwei for BSC and Ethereum in sequence. Like BSC and Ethereum, q Gwei (gas unit) is equal to 1,000,000,000 wei or 0.000000001 BNB or ETH respectively. If you pay the lower price, your transaction will take a long time to live through.

- Lower price is slower time to process in a block.
- Higher price is faster time to process in a block.

6.1.6. Consensus Mechanism

BSC uses the Proof-of-Stake-Authority (PoSA) protocol to perform which is used to deploy stacking, token exchange, and smart contracts. BSC utilized a hybrid consensus mechanism, merging both Delegated Proof-of-Stake (DPoS) and Proof-of-Authority (PoA), to ensure blockchain security and establish network consensus. This protocol required the network validator to stake a specific number of BSC validators being compensated through fees charged for every validated transaction. The PoSA consensus algorithm allows cheaper and faster blockchain transactions for users.

Ethereum alternated from Proof-of-Work (PoW) to Proof-of-Stake (PoS) protocol on September 15, 2022.

That customized process, better known as "The Merge", has been years in the making. This protocol as a consensus algorithm needs node validators to lock away on stake their assets for the change to process network transactions and issue blocks. This PoS protocol is projected to facilitate the processing of 100,000 transactions per second (TPS), far surpassing even ordinary financial transactions. On the other hand, PoW could handle only 15 transactions per second, making it relatively slow for financial transactions.

6.1.7. Blockchain Traffic and DApps Ecosystem

It is tough to correctly estimate the accurate number of decentralized applications (DApps) on the BSC and the Ethereum platforms, as the number of DApps can change over time. In addition, there is no central repository or directory that lists all the DApps on the blockchain platforms, making it troublesome to correctly track and count them. Nevertheless, according to the data from <https://dappradar.com/rankings>, a website that traces and ranks DApps over various blockchain platforms, as of February 2, 2023, there are 3,815 DApps on the Ethereum platform and 4,567 DApps on the Binance Chain platform. These DApps cover a wide range of use cases, including social media, gambling, DeFi, marketplaces, exchanges, and more.

This is an important difference, but BSC has only grown since 2020, showing that BSC is a prosperous ecosystem. Active addresses are also a very important on-chain metric to think about. Despite being a newer blockchain, BSC recorded a peak of 2,271,060 addresses on December 1, 2021, which is higher than Ethereum's all-time high of 1,420,187 addresses on December 9, 2022.

6.1.8. Centralization

BSC is a community-driven, decentralized blockchain electrified by the Binance Coin token. Underneath a PoSA mechanism, BSC currently total operates on 43 network validators and only 21 active validators that run its blockchain.

In contrast, the number of Ethereum network validators has over 500,000 nodes, according to data from BeaconScan. Validators are important in guaranteeing the security and integrity of the Ethereum network.

Table 1. Page layout description

Parameters	Global Public		Local Public	
	Binance Smart Chain	Ethereum	xCHAIN	REI Chain
Launch	2019	2013	2021	2021
Website	www.binance.org/en/smartchain	https://ethereum.org/en	https://www.xchain.asia/	https://www.reichain.io/
Transaction Fees	0.00210247 BNB (\$0.68)	0.0007262041726249 Ether (\$1.19)	0.00421894 XTH (\$0.13)	0.000043822 REI (\$0.0013)
Transaction Time	3 sec	15 sec	4.4 sec	1 sec
Gas Limit	420,494	46,422	421,894	65,733
Gas Used	430,494 (100%)	46,422 (100%)	421,894 (100%)	43,822 (66.67%)
Gas Price	5 Gwei	15.64353 Gwei	10 Gwei	1 Gwei
Consensus Mechanism	PoSA	PoS	PoA	PoA
Blockchain Traffic & DApps Ecosystem	4,567	3,815	4	25
Validator Staking Requirement	Stake at least 10,000 BNB to be eligible	Stake 32 ETH (Eth2)	None	None
Centralization	43 Nodes	500,000+ Nodes	21 Nodes	3 Nodes

6.2. Local Public

This is a side-by-side comparison of xCHAIN versus REI Chain as follows:

6.2.1. History

xCHAIN is a centralized blockchain created by the Thailand Blockchain Working Group (TBWG) in 2021, which consists of key partners with the alliance of technology experts and Thailand’s leading blockchain, namely, 1) J Ventures Co., Ltd., which is a platform develop under Jay Mart Group, 2) I AM Consulting Co., Ltd., which is consulting company and develop IT systems for the enterprises, 3). Dome Cloud Co., Ltd., which is a comprehensive IT solution service, and 4). Satang Corporation is a leading blockchain developer and crypto trading website.

REI Chain is a Thai blockchain and centralized blockchain optimized by the Thai announced in 2021, intending to make blockchain technology easily accessible to all groups of people. REI Chain has an idea to bring the token system to try and apply it to the education industry as well. At present, 4 institutions participate in REI Chain: 1). the College of Digital Innovation Technology, Rangsit University, 2). the Faculty of Economics, Chiang Mai University, 3). the Faculty of Business, Economics and Communications, Naresuan University, and 4). the School of Integrated Innovation, Chulalongkorn University.

6.2.2. Transaction Fees

From our results in Table 1, xCHAIN transaction fees are \$0.13 (0.00421894 XTH) and \$0.0013 (0.000043822 REI) for REI Chain.

Transaction fees conclude that the REI Chain is very cheap, but xCHAIN is very high on the transaction. This can be explained by the consensus algorithm used by xCHAIN equated to the one implemented by REI Chain.

Transaction Fees = Gas Limit * Gas Price per unit *

$$\begin{aligned}
 & \text{Gwei denomination} \\
 \text{In our results} &= 421,804 * 10 * 0.000000001 \\
 &= 0.00421894 XTH (\$0.13) \\
 &= 65,733 * 1 * 0.000000001 \\
 &= 0.000043822 REI (\$0.0013)
 \end{aligned}$$

Note: 1 Gwei = 0.000000001 XTH or REI

6.2.3. Transaction Time

Mostly, the transaction time for REI Chain posts is about 1 second per block time which matches the lab test results, whereas xCHAIN takes less than 5 seconds per block time which is logical with the lab test results (4.4 seconds per block). However, the transaction speed occurs with tradeoffs. REI Chain has a nearly small number of participants running its network but can offer faster than xCHAIN.

6.2.4. Gas Limit and Gas Used

In our results, the gas limit of xCHAIN is 421,894 and 100% gas used, while the gas limit of REI Chain is 65,733 and 66.67% gas used.

6.2.5. Gas Price

The gas prices are very high on the xCHAIN and very cheap on the REI Chain. Anyway, this can be described as the gas model of the consensus algorithm used by xCHAIN comparison with REI Chain.

From Table 1, the gas prices show 10 Gwei for xCHAIN and 1 Gwei for REI Chain. The same as xCHAIN and REI Chain, 1 Gwei (gas unit) is equal to 1,000,000,000 wei or 0.000000001 XTH or REI. If you pay the lower price, your transaction will take a long time to live through.

6.2.6. Consensus Mechanism

All xCHAIN and REI Chain use Proof-of-Authority (PoA) which is an alternative consensus algorithm that provides efficient solutions and high performance for blockchain networks (particularly the private ones). The term was proposed by Ethereum co-creator and erstwhile CTO Garvin Wood in 2017.

6.2.7. Blockchain Traffic and DApps Ecosystem

xCHAIN and REI Chain are ready blockchain ecosystems. By receiving cooperation from partners from many sectors, whether education institutions, business enterprise organizations, software developers, and startups with participating validator nodes to create a strong blockchain ecosystem. Currently, xCHAIN has only 4 DApps, while REI Chain has 25 DApps.

6.2.8. Centralization

xCHAIN currently has 21 validator nodes which are universities and leading organizations in Thailand. Rangsit University is also one of them. On the other hand, currently, REI Chain is only 3 validator nodes such as KillSwitch, Inspex, and Arken.

7. Conclusion

In the first part of the paper on consent management systems, Blockchain is used as a log of consent history since its property is a chronological structure. It also gives decentralization and avoids a single point of failure. Personal data is kept in a controller node and his/her node. The anonymity and the absolute of the network are attained through the intelligent use of encryption. The experimental results indicate that blockchain is an appealing platform for the consent management system and can aid the PDPA act by supplying creditworthy environmental data and acceding for continuous monitoring by the data subject. This is why: The person has their transparency stolen when it reaches the consent stages. To become operational, a consent platform must earn the trust of its users.

In the second part of the paper on Pseudonymization, blockchain technology is suggested as an auxiliary system in this study.

All mapping tables are stored in the blockchain. The hashing address is unique enough for a primary key that can link back to the microdata. Each mapping table is in a box. Each chain stores a history of each mapping table. The last box of the chain is the current version of the dataset.

For the pseudonymization process: The proposed new technique outperformed other techniques as follows: Firstly, due to all original direct identifiers are kept secretly in the blockchain. There is little or no information loss because it is a reversible process anytime. Second, the security is still very strong, thanks to the robust and resilient blockchain architecture. In a distributed network like blockchain, no one can easily hack, Hackers must modify all 50% of the nodes to succeed. Third, businesses or enterprises can freely anonymize their data before publishing it for researchers. No need to worry about permanent data loss. Fourthly, our model operates within a private blockchain, ensuring that only authorized individuals have access to the system.

This paper discusses two key aspects: consent management using blockchain for data security and pseudonymization via blockchain. The use of blockchain in both areas offers enhanced data protection, security, and control, making it a promising solution for managing consent and safeguarding data privacy.

References:

- [1]. Henriksen-Bulmer, J., & Sheridan, J. (2016). Re-identification attacks – A systematic literature review. *International Journal of Information Management*, 36, 1184-1192.
- [2]. Zemler, F. (2019). Concepts for GDPR-compliant processing of personal data on blockchain: A literature review. *Anwendungen und Konzepte der Wirtschaftsinformatik*, (10), 96-107.
- [3]. Haque, A. B., Islam, A. K. M. N., Hyrynsalmi, S., Naqvi, B., & Smolander, K. (2021). GDPR compliant blockchains – A systematic literature review. *IEEE Access*, 9, 50593-50606.
- [4]. Suripeddi, M. K. S., & Parandare, P. (2021). Blockchain and GDPR – A study on compatibility issues of the distributed ledger technology with GDPR data processing. *Journal of Physics Conference Series*, 1964(4), 042005.
- [5]. Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. *Internet of Things*, 8.
- [6]. Melin, K. (2019). *The GDPR compliant of blockchain, A qualitative study on regulating innovative technology*. (Thesis, Uppsala, Sweden. Uppsala Universiteit.
- [7]. Zhang, R., Xue, R., & Liu, L. (2020). Security and Privacy on Blockchain. *ACM Computing Surveys*, 52(3), 1-34.

- [8]. Zou, W., Lo, D., Kochhar, P. S., Le, X. B. D., Xia, X., Feng, Y., et al. (2021). Smart contract development: Challenges and opportunities. *IEEE Transactions on Software Engineering*, 47(10), 2084-2106.
- [9]. Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *Proceedings of the IEEE Security and Privacy Workshop*, 180-184.
- [10]. Sirur, S., Nurse, J. R. C., & Webb, H. (2019). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security at ACM Conference on Computer and Communications Security (CCS)*, 88-95.
- [11]. Muma, S., Kappos, D., & Sumroy, R. (2021). The right to be forgotten meets the immutable: A practical guide to GDPR-compliant blockchain solutions. *The Center for Global Enterprise (CGE)*, 88-95.
- [12]. Kondova, G., & Erbguth, J. (2020). Self-sovereign identity on public blockchain and the GDPR. In *Proceedings of the 35th Annual ACM SAC Conference*, 342-345.
- [13]. Hristov, P., & Dimitrov, W. (2018). The blockchain as a backbone of GDPR-compliant frameworks. In *Proceedings of the 8th International Multidisciplinary Symposium – Challenges and Opportunities for Sustainable Development Through Quality and Innovation in Engineering and Research Management*, 20(1), 305-310.
- [14]. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies. *IEEE Symposium on Security and Privacy*, 104-121.
- [15]. Hewa, T. M., Hu, Y., Liyanage, M., Kanhare, S. S., & Ylianttila, M. (2021). Survey on blockchain-based smart contracts: Technical aspects and future research. *IEEE Access*, 9, 87643-87662.
- [16]. Voss, W. G. (2021). Data protection issues for smart contracts. In *Smart Contracts: Technological, Business, and Legal Perspectives*. Marcelo Corrales, 79-100. Hart Publishing, Bloomsbury.
- [17]. Bernal, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-Preserving solutions for blockchain review and challenges. *IEEE Access*, 7, 164908-164940.
- [18]. Bourka, A., Drogkaris, P., & Agrafiotis, I. (2019). *Pseudonymization techniques and best practices. Recommendations on shaping technology according to data protection and privacy provisions*. European Union Agency for Cybersecurity (ENISA).
- [19]. Lapwattanaworakul, J., Srisa-An, C., & Angsirikul S. (2022). Guidelines for data anonymization for data privacy in Thailand. *2022 6th International Conference on Information Technology (InCIT)*, Nonthaburi, Thailand, 211-215.