Article

Not peer-reviewed version

An Efficient Privacy and Anonymity Setup on Hyperledger Fabric for Blockchain-enabled IoT Devices

Muhammad Saad , Saqib Ali Haidery , Aavash Bhandari , Muhammad Raheel Bhutta , Dong-Joo Park , Tae-Sun Chung *

Posted Date: 23 May 2024

doi: 10.20944/preprints202405.1485.v1

Keywords: Privacy; Anonymity; Blockchain; Hyperledger; IoT

Article

An Efficient Privacy and Anonymity Setup on Hyperledger Fabric for Blockchain-enabled IoT Devices

Muhammad Saad [1], Saqib Ali Haidery [1], Aavash Bhandari [1], Muhammad Raheel Bhutta [2], Dong-Joo Park [3] and Tae-Sun Chung [1,*]

[1] Department of Artificial Intelligence, Ajou University, Suwon, 16499, Rep. of Korea; muhammadsaad@ajou.ac.kr (M.S); saqib@ajou.ac.kr (S.A.H); aavashbhandari@gmail.com (A.B)
[2] Department of Electrical and Computer Engineering, University of UTAH Asia Campus, Incheon, 21985, Rep. of Korea; raheel.bhutta@utah.edu (M.R.B)
[3] School of Computer Science and Engineering, Soongsil University, Seoul, 06978, Rep. of Korea; djpark@ssu.ac.kr (D.J.P)
* Correspondence: tschung@ajou.ac.kr (T.S.C)

Abstract: The rise in IoT (Internet of Things) devices poses a significant security challenge. Maintaining privacy and ensuring anonymity within the system is a sought-after feature with inevitable trade-offs, such as scalability and increased complexity, making it incredibly challenging to handle. To tackle this, we introduce our proposed work for managing IoT devices using Hyperledger fabric. We integrated our system on the blockchain with a closed-circuit television (CCTV) security camera fixed at a rental property. The CCTV security camera redirects its feed whenever a new renter walks in. We have introduced the web token for authentication from the renter to the owner. Our contributions include the proposition of efficient framework architecture, a novel chain code algorithm, and stealth addresses with modified ring signatures. We performed different analyses to show the system's throughput and latency through stress testing. We have shown the advantages of the proposed architectures by comparing similar existing schemes. Our proposed scheme enhances the security of blockchain-enabled IoT devices and mitigates the single point of failure issue. Our future work includes scaling it up to cater to the needs of the healthcare system.

Keywords: Privacy; Anonymity; Blockchain; Hyperledger; IoT

1. Introduction

The Internet of Things (IoT) system is a complex environment where multiple entities and devices interact. These systems are centralized and trust-dependent [1]. They interconnect numerous devices to exchange and update data for various applications used in a smart city, smart home, smart car, healthcare, and other environments [2]. As the usage of IoT has become widespread, there have been attempts to replace the existing centralized access control methods with distributed ones [3]. One of the major challenges in replacing centralized systems is security [4].

The technological industry and information security have been evolving quickly and developing exponentially [5]. Many new devices are being surfaced daily, and security features need to be investigated. Security and privacy are two main primary concerns that need to be implemented for data protection against different attacks [6]. Privacy is one of the system's top priorities, and this feature attracts more studies to focus on it. Maintaining the anonymity of users across all platforms is another challenge when it comes to security. Privacy is about the controlled sharing of information. It can exist along a spectrum, allowing varying levels of disclosure. At the same time, anonymity represents the end of the privacy spectrum, where no identifying information is disclosed, and the individual remains wholly concealed.

With the introduction of blockchain in 2008 through Bitcoin by Satoshi Nakamoto, it is now used in various fields beyond cryptocurrencies and payment verification systems [7]. Because of its decentralized architecture and transparency, it is used in healthcare [8], transportation [9], and education areas [10]. Systems that require a third party as a key player, cost a lot, and have access to all

 doi:10.20944/preprints202405.1485.v1

the data are now shifting their focus to this area. [11]. As a distributed ledger technology, blockchain is widely used in trusted resource management [12]. Blockchain-based computing resource trading is established to guarantee security and privacy [13]. Smart contracts are an attractive feature that has led to increased research in various areas. In [14], the authors propose a blockchain-independent smart contract infrastructure suitable for resource constraint IoT devices.

Hyperledger Fabric is built on the principles of blockchain technology, with an open architecture that allows for modification of the consensus mechanism to enhance performance [15]. The modular approach of Hyperledger fabric allows users to make the system according to their desired needs and add functionalities that help achieve the desired results. It is a permissioned blockchain architecture that allows only the participants to register through the Membership Service Provider (MSP). The certificate authority issues a certificate during the process. The Private Data Collection (PDC) feature helps create channels among the blockchain participants according to the desired privacy. Unlike a public blockchain, this feature removes the overhead of creating separate channels. Like public blockchain, many mobile IoT devices are implemented in Hyperledger fabric for authentication. In [16], the authors propose authenticating mobile IoT devices using Hyperledger fabric as a broker, making the system more scalable and manageable .

A considerable amount of research is carried out in the healthcare field using Hyperledger fabric. In [17], the authors propose a patient-centric architectural framework for enhancing healthcare management during COVID-19. The solution tracks COVID-19 patients and mitigates the risk of patient data loss by maintaining privacy and security. An efficient chain code for access control in Hyperledger fabric system is proposed in [18]. Another healthcare monitoring system based on IoT-blockchain architecture on the Hyperledger framework is presented in [19]. Surveillance systems have been using the Hyperledger fabric due to its enhanced privacy features. In [20], the authors propose a data verification system for CCTV surveillance cameras in smart cities. They present a system that guarantees the trustworthiness of the stored recordings, allowing the authorities to validate whether a video has been altered. A decentralized approach for secure and sustainable networks with distributed video footage from vehicle-mounted cameras in smart cities is proposed in [21]. The authors combine vehicle cameras, blockchain technology, and certification authority to ensure video data's secure and sequential storage, protecting it against tampering and unauthorized access. In [22], the authors propose a two-level blockchain system for digital crime evidence management. The system separates the evidence into hot and cold blockchains.

Hyperledger fabric is also being used in the energy sector to maintain privacy and security in the smart grids. In [23], the authors propose a secure data aggregation scheme for smart grids. They present a decentralized and secure data aggregation method to protect the privacy, integrity, authentication, and confidentiality of individual consumption data. In [24], the authors conducted a comprehensive empirical study to understand validator peers in Hyperledger fabric and to improve the energy efficiency of permissioned blockchains using FPGAs. Hyperledger Fabric is consistently used in the field of land registrations and rental agreements. In [25], the authors developed a system that facilitates secure and transparent land transactions from planning to certificate issuance and integrates the management of land sales, significantly reducing the need for intermediaries. A residential smart rental platform, compliant with GDPR and based on blockchain technology, designed to facilitate secure rental contracts and payments for both landlords and tenants in [26].

Online voting systems have been implemented on Hyperledger Fabric to ensure anonymity within the system. In [27], the authors tackle some of the drawbacks and limitations of current systems and assess some well-known blockchain frameworks to build a blockchain-based electronic voting system. A similar system has been proposed in [28], where authors focus on the security and reliability of online voting systems through Hyperledger fabric. In [29], the authors propose a method for transmitting transaction data encrypted by homomorphic encryption through a secure channel and recording it on the blockchain after the voting is over. Most studies focus on either privacy [30] or anonymity [31]. In [32], the authors propose an architecture that addresses both privacy and anonymity. They adopt

 doi:10.20944/preprints202405.1485.v1

the K-anonymity method to construct a unified request to hide the location information of Electric Vehicles (EVs) based on undirected graphs. However, this scheme has a limitation due to the use of a consortium blockchain, where there are controlling nodes to verify and validate the transactions. In this scheme, attackers can obtain the location coordinates of EVs, although it is difficult to distinguish which EV coordinate belongs to them.

Hyperledger Fabric technology deployment in IoT systems is becoming common nowadays. Since our system works for both privacy and anonymity and is distributed, we have used this to cater to our needs. Scalability is an essential feature for any system, and due to Hyperledger fabric's modular approach, our system is very scalable. The feature of private data collection helped us group different users on different channels without creating individual channels. Since our system is private, a membership service provider adds a scanner to our system. Because of this, no unauthorized person can enter the system, thus cushioning the concerns about destabilizing blockchain. The chain code and endorsement policies realize the real-world scenarios that strengthen our system.

We present a Hyperledger Fabric design for a CCTV security camera rental system. The key contributions of our work are outlined below.

- Our framework devises a novel chain code algorithm to ensure the system's seamless operation. The endorsement policies are designed with real-world scenarios in mind.
- Our system uses a single key to invalidate the previous keys at once. Due to the modular approach of Hyperledger fabric, our system is much more scalable than the previously developed system.
- The concept of a token is introduced in the system for authentication purposes to mitigate the single point of failure, as the token can be re-generated if lost.
- The system ensures anonymity by adding an extra layer of security over the previously modified ring signatures. We add stealth addresses to our scheme to enhance the anonymity of both the user and the recipient.

The remainder of this paper is organized as follows: Section 2. reviews the related work. The proposed framework architecture is explained in Section 3. Experimental analyses are discussed in Section 4 along with the comparisons, while Section 5 concludes the paper with future research directions.

2. Related Works

Since the inception of Hyperledger fabric, various studies have been conducted in various fields. Some of the studies are related to preserving privacy and maintaining anonymity in the system. Since privacy is everyone's major desire, this area has been touched upon more than anonymity. Other than surveillance systems, privacy and anonymity have been a focus in areas like health care, voting systems, and smart grids.

In [33], the authors propose a design for the blockchain-based management of video surveillance systems. The proposed system involves trusted internal managers in the blockchain network. Figure 1 shows the proposed architecture. The video's metadata is recorded on the blockchain's distributed ledger to block data forgery. In this architecture, the video is first encrypted and then stored. Then, a license is created within the blockchain, and that license is used to export the video. The private database of the blockchain manages the video's decryption key; therefore, the internal managers cannot leak it unauthorizedly. The internal managers also manage and export videos safely by exporting the license issued within the blockchain. The authors utilize the private data collection feature of Hyperledger fabric, which collects, commits, and queries private data without creating individual channels. The membership service provider is used to make the network private. This scheme has security limitations as it uses internal managers. Though the system is well managed, and the internal managers need authorization to manage the decryption key, there is no concrete evidence that it cannot be breached. Furthermore, there may be a chance of hacking the video's decryption key.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 23 May 2024 doi:10.20944/preprints202405.1485.v1

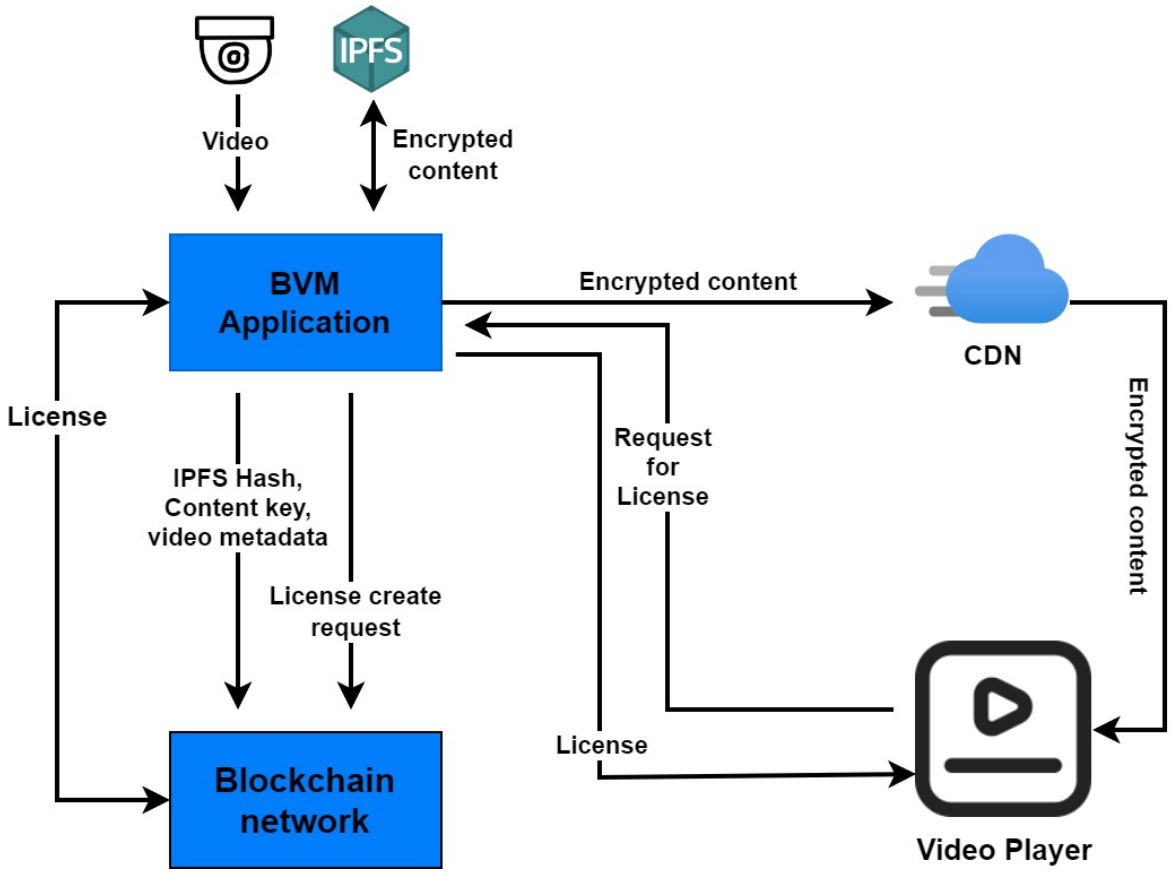

Figure 1. Architecture of Video Surveillance System.

In [34], the authors present a trustworthy and secure house rental system using blockchain and smart contracts. The authors propose blockchain with smart contracts to mitigate data security, third-party dependence, fraudulent agreements, payment delays, and ambiguous contracts. The proposed system works on Hyperledger's off-chain and on-chain transactions. Based on mutual understanding, the rental contract between the tenant and the landlord is carried out through off-chain communication. On-chain communication includes deposit and rental payments, digital key generation, and contract dissolution. This system ensures immutability and no dependence on third parties but lacks extensive protection for privacy. No concept of anonymity is used in the system; thus, the system lacks critical security parameters.

Smart grids systems have been using blockchain technology for a long time due to inherent advantages of privacy and security. In [35], the authors propose incorporating privacy and transparency into blockchain-based smart grid operations. They introduce a new method to achieve a balance between privacy, transparency, accountability, and verifiability. They utilized cryptographic tools to reach this objective, incorporating secure multiparty computations and verifiable secret sharing within the distributed components of a multi-channel blockchain and its associated smart contracts. The system implements demand response to enhance efficiency by measuring demand and supplying energy accordingly. Furthermore, the authors address potential accidental crashes by ensuring that the solution is suitable for low-performance IoT devices. They also maintain customer privacy by using different channels with the grid operator. Figure 2 shows the demand workflow with a blockchain-based energy management system. This system uses blockchain with different channels to maintain customer privacy. Instead of separate channels, if the Hyperledger fabric was used, the PDC feature could have been utilized for channel creation without the need for creating individual channels. Furthermore, the Hyperledger fabric's modular approach could have reduced the computational complexity of different consensus algorithms used in the public blockchain network.

 doi:10.20944/preprints202405.1485.v1

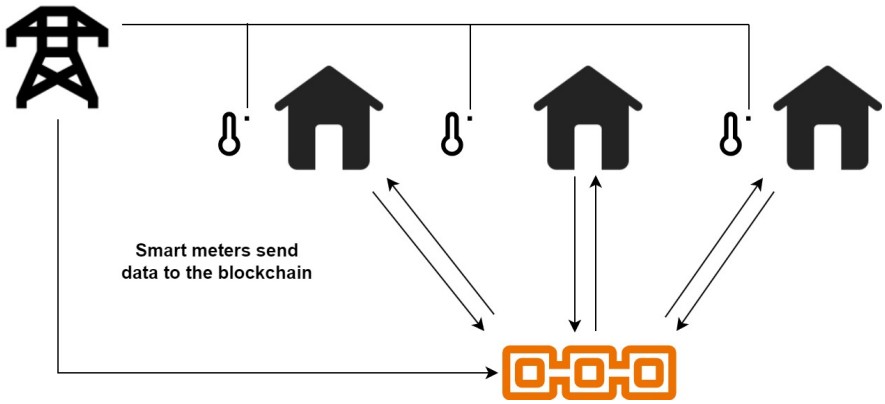

Figure 2. Demand response workflow with a blockchain-based energy management system.

In [36], a framework for a secure privacy and anonymity system for blockchain-enabled IoT devices is proposed. The system proposed is called SPAS. This original SPAS architecture is the basis for the proposed improvement in this paper. Figure 3 shows the basic architecture of SPAS. In this framework, the CCTV security camera feed is redirected to the renter when renting a property. At the same time, the old keys of the CCTV security camera are invalidated, and the feed to the owner is stopped. The owner generates the temp_ID for the renter and sends it on their mobile phone, and the renter verifies that temp_ID on the web portal. Though this system provides extreme security and anonymity by using modified ring signatures, some limitations still exist. The single point of failure issue with the mobile service and the temp_ID getting hacked if the mobile phone is stolen remains unsolved.

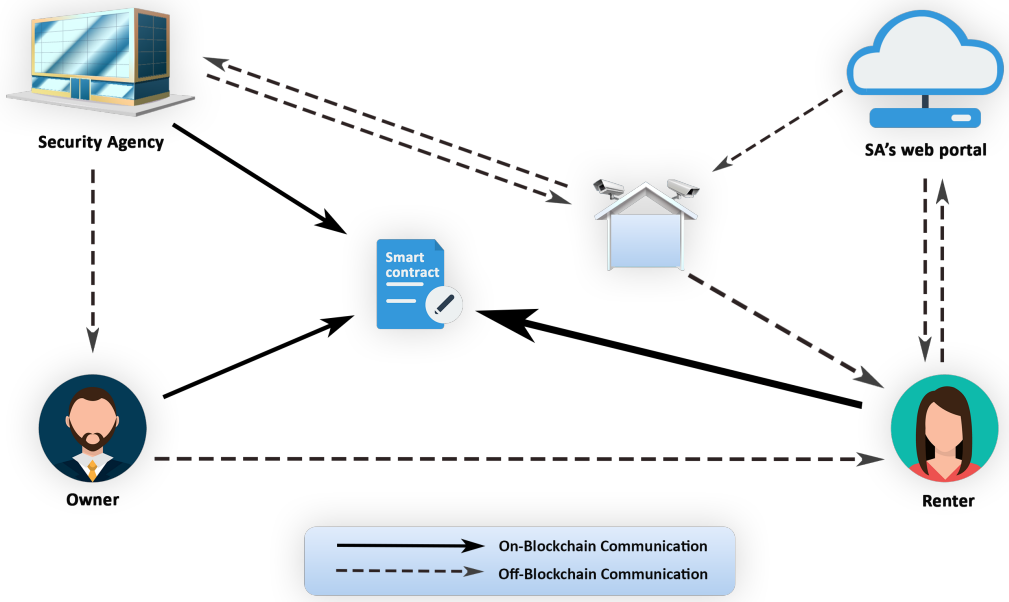

Figure 3. Secure privacy and anonymity setup (SPAS).

In this paper, we present our efficient privacy and anonymity setup on Hyperledger fabric based on the original SPAS architecture presented in [36]. Our proposed system maintains privacy and anonymity while meeting the basic needs of no dependence on third parties, less computationally extensive schemes, and immutable transactions. The modular approach of Hyperledger fabric allows us to add different entities and incorporate our core entities with them. This system is comparable to any mentioned systems for security enhancement.

 doi:10.20944/preprints202405.1485.v1

3. Proposed System

Privacy and anonymity have become the desired features of almost every existing system. Our system focuses on CCTV security camera feed, which requires a substantial level of privacy for the user and maintaining anonymity altogether. In this system, the CCTV security camera feed can be viewed either by the owner of the property or the renter who acquires the property one at a time. There can be several scenarios where this system can be applied, which include neighborhood watch programs where a community organization owns a network of CCTV security cameras placed strategically throughout a neighborhood and provides access to these cameras for a small fee. Another scenario is construction project rentals, where a construction equipment rental company owns CCTV security cameras designed to monitor construction sites. They rent out these CCTV security cameras to various construction companies on a project-to-project basis, providing real-time surveillance to enhance site security. All three scenarios, including our focused system, have a common thing: the desire for privacy and anonymity.

This section is organized as follows: Section 3.1 briefly introduces Hyperledger fabric technology. Section 3.2 will describe the basic architecture of our proposed system. While presenting the overall architecture of our system, we will detail our approach to preserving privacy and avoiding a single point of failure. In Section 3.3, we described the detailed flow of SPAS-H working. This includes a step-by-step workflow of the system and an algorithm. In Section 3.4, we propose an additional anonymity layer over the modified ring signatures for key management in the form of stealth addresses.

3.1. Overview of Hyperledger Fabric

Hyperledger Fabric is a blockchain platform that requires permission to access and has a modular architecture. This allows for the development of blockchain-based applications, solutions, and networks. Some key aspects of Hyperledger Fabric include a permissioned network, modular architecture, chain code (similar to a smart contract in a public blockchain), channel support (enabling private communication and transactions among multiple parties within a subset of a network), endorsement policy (defining the required criteria for a transaction to be considered valid), and ledger features such as world state and transaction log. Additionally, it supports pluggable consensus algorithms, allowing network participants to select the most suitable consensus mechanism for their specific case.

3.2. Basic Architecture of the Proposed System

Since this system extends our previous system from public blockchain to Hyperledger fabric, we call our system Secure Privacy and Anonymity Setup on Hyperledger (SPAS-H). Hyperledger fabric's modular nature helped us utilize its features to our desired requirements. The permissioned network feature helped us limit the anonymous users in the network and have scalability in control. Due to channel support in the fabric, our system enhances confidentiality among the participating entities. As our system requires several conditions to be satisfied before access is granted, the endorsement policies of fabric come into play as the policies can be customized based on the requirements, ensuring the proper validation and authorization of transactions. Other features, which include limiting the dependence on the third party for central operations, access of every node to the entire database, and its history and immutability, are the inherent features of blockchain technology utilized in this system, too.

A combination of different components makes up our SPAS-H system. These components work together to give the system the desired results. These include:

- CCTV security camera: Device for outputting the video feed.
- Owner: The one who owns the property. One owner can own multiple properties in multiple buildings, each with a single CCTV security camera.
- Renter: The one who rents the property and receives the CCTV security camera feed.

 doi:10.20944/preprints202405.1485.v1

- Security agency: It is responsible for deploying CCTV security cameras at owners' properties. The security agency also has a blockchain network that contains transactional information and all registered owners and renters.
- Web portal: This is the portal where the validation and authorization work takes place, both at the owner's and renter's end.
- SPAS-H API: It is the interface between the entities and the Hyperledger fabric network, used by the owners and renters and authenticated by the membership service.
- Keys management: The key generation platform is where the entities involved generate the key pairs. This enhances the anonymity feature of our system by incorporating multiple security layers. A single key at one time and key invalidation are important parts of the system.
- Chain code: It defines the rules that govern the transactions.
- Blockchain network: Private blockchain network based on Hyperledger fabric.

Figure 4 shows the architecture of SPAS-H. Different types of flows are indicated in different colors. Also, on-blockchain and off-blockchain communication, a key feature of our advanced system, is carried out throughout. The security agency deploys the CCTV security camera and waits for the public key, which is then sent to the property owner. The camera feed is directed toward the owner. Communication between the owner and renter is carried out through the SPAS-H interface via blockchain, which includes the money transfer. Further, on-blockchain communication exists between the owner and the SPAS-H interface and between the renter and the SPAS-H interface. The owner and renter also communicate off-blockchain with the web portal for authentication purposes, which comes under the umbrella of information flow. The CCTV security camera communicates with the SPAS-H interface off-blockchain to transfer public key information to the renter.

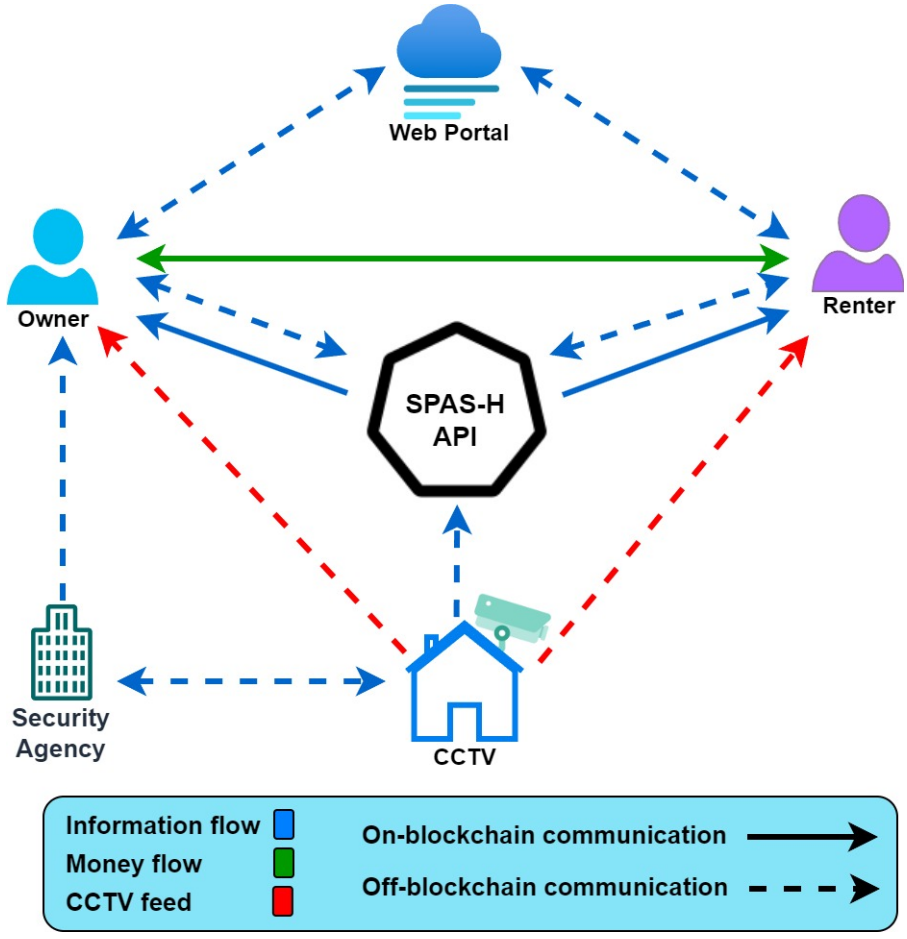

Figure 4. SPAS-H architecture.

 doi:10.20944/preprints202405.1485.v1

The property owner originates the system by giving the listing to the security agency. The listing contains the owner's vacant properties, which can be rented out. The security agency deploys CCTV security cameras at the vacant properties. The security agency has a private blockchain network deployed on Hyperledger fabric containing multiple channels, each with multiple peers. These peers are the endorsers and committers in the system and the owners or renters of some properties. The owner and renter register through the membership service provider and get the certificate from the certificate authority. Then, they generate their public and private keys through symmetric key encryption and enter the public keys and remaining details information in the SPAS-H and the chain code. After this, redirecting the CCTV security camera feed from the owner to the renter occurs. Before this, the money is transferred to the owner, and the transaction is encrypted through a modified ring signature and masked by stealth addresses to hide the identity of both the owner and the renter.

3.3. Flow of the SPAS-H Working

Like SPAS, SPAS-H also works in three main phases: deploying CCTV security cameras, renting property, and expiring the contract. The deployment and expiration of contracts mainly remain the same with minor amendments. The phase of renting property has extensive changes that strengthen privacy preservation in SPAS-H as it adds a new layer of security. Furthermore, compared to SPAS, SPAS-H removes the concept of receiving temp_ID and communication on mobile phones, thereby limiting the chances of temp_ID getting hacked by anyone and the single point of failure regarding mobile service outage.

When the renting procedure begins, the renter selects a property from SPAS-H and registers on the blockchain. They then generate a token on the web portal for authentication. This token, known as JSON Web Token (JWT), is used for web authentication, authorization, and information exchange. It grants access to specific routes, services, and resources. In the case of SPAS-H, the token authorizes the renter to access the CCTV security camera feed. The token serves as a verification of the renter's identity and intent to rent the property from the owner. Once generated, the token is sent to the owner via the SPAS-H interface for authentication on the web portal. This process adds an extra layer of security to the system, eliminating the need for temporary ID generation and mobile phone verification.

After the token authentication, the owner adds details of the renter with the CCTV security camera, and the procedure is carried forward through the Hyperledger fabric endorsement procedure, abiding by the defined endorsement policy in the system set by the property owner. This endorsement policy is different for different properties, as some properties might need the endorsement of all peers while others may require semi-agreement of the peer. This depends on factors that are outside the scope of our current work. Figure 5 shows the flow of SPAS-H and workflow explanation is detailed as follows.

1. Property listing: The property owner lists all the properties with the security agency. This includes all the vacant and occupied properties, which will help the future renters choose.
2. The process of CCTV security camera deployment and the feed commencement
    - 2.1 The security agency installs CCTV security cameras at all properties and asks the CCTV security camera to generate the key pair.
    - 2.2 The CCTV security camera generates key pairs (public and private keys) through key management, which uses symmetric key encryption.
    - 2.3 The security agency transfers the CCTV security camera public key to the owner. After generating their key pairs, the owner uses their private key to access the CCTV security camera feed. The CCTV security camera starts streaming the video feed to the owner.
3. The process of the owner joining SPAS-H and blockchain network
    - 3.1 The security agency asks the owner to join SPAS-H and blockchain network.
    - 3.2 The owner signs up for SPAS-H and logs in using their ID and password.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 23 May 2024 doi:10.20944/preprints202405.1485.v1

3.3 The owner joins the blockchain network of the security agency through a membership service provider as the certificate authority issues the certificate.
3.4 The owner now bears the SPAS-H ID, blockchain address, and a certificate.
3.5 The owner enters their details in the chain code and saves them in the SPAS-H database. SPAS-H maps the owner's information against their properties.

4. The process of the renter joining SPAS-H and blockchain network

4.1 The renter signs up for SPAS-H and logs in using their ID and password.
4.2 The renter can view the available properties on SPAS-H and select their preferred one.
4.3 The renter joins the blockchain network of the security agency through a membership service provider as the certificate authority issues the certificate.
4.4 The renter now bears the SPAS-H ID, blockchain address, and a certificate.

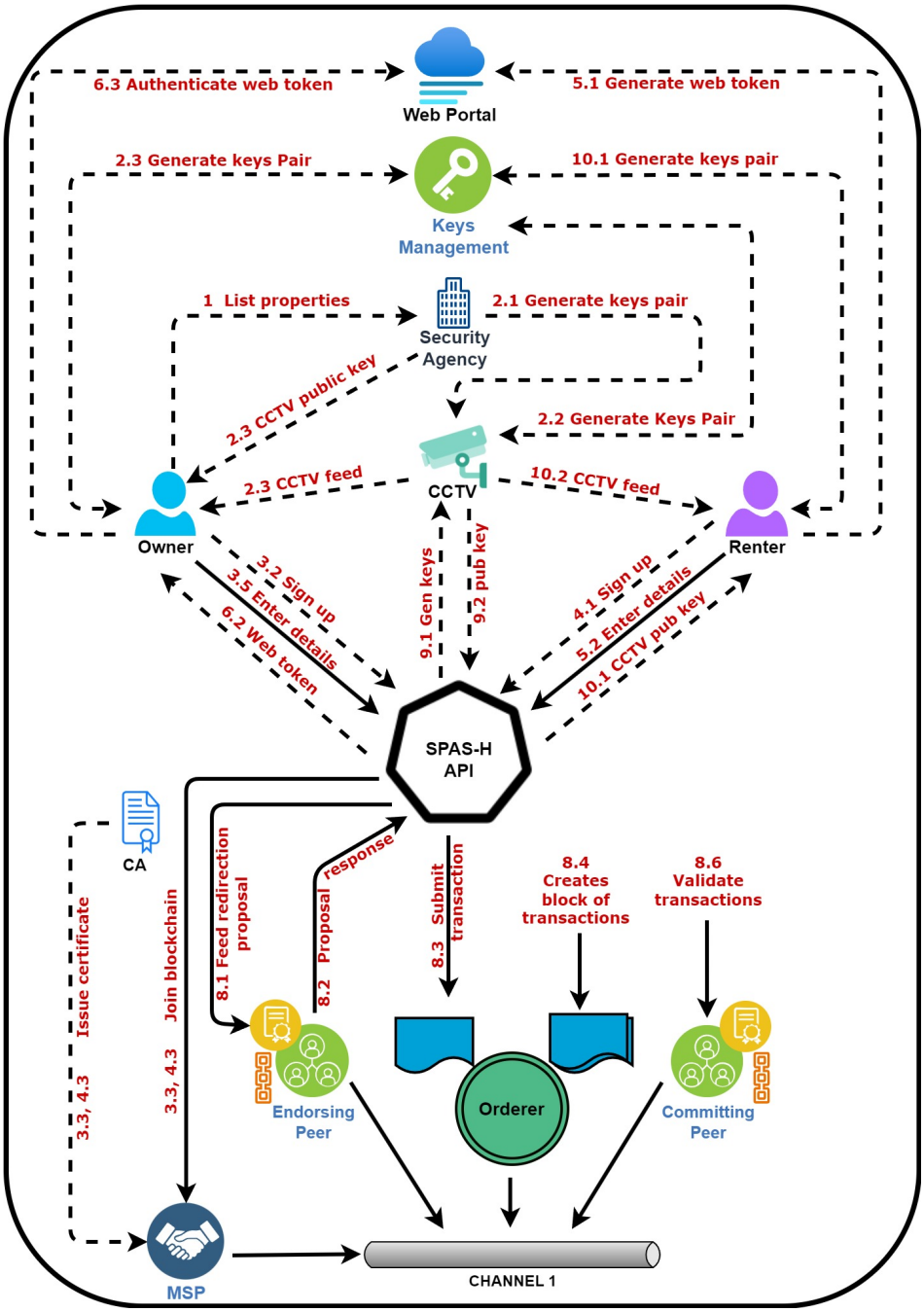

Figure 5. Workflow of SPAS-H.

 doi:10.20944/preprints202405.1485.v1

The following algorithm is for the redirection of camera feed from the owner to the renter which does not include the Hyperledger endorsement process.

Algorithm 1: CCTV security camera feed redirection to renter

Definitions: $O_i \in O$: set of Owners
$R_i \in R$: set of Renters
$C_i \in C$: set of Contracts
$P_i \in P$: set of Properties of Owners
SA: Security Agency
Input : Blockchain address, public key, and token
Output : CCTV camera feed redirection

Initialization: SC.Expiry ← false
SC.duration = renter defined ; `/* according to the renter requirement */`
SA.CCTV_access ← false
SA.CCTV_key = generate()
Send $O_i[P_i] \rightarrow SA$
foreach *Property* P_i, *Owner* O_i **do**
  Send $O_i[BC\_addr, pub\_key]$ to SA
  $SA.P_i \leftarrow$ **NULL**
end
foreach *Renter* R_i *after choosing property* $P_i \in P$ **do**
  Generate token from web portal
  return R_i.token
end
foreach *Renter* R_i *after generating token* **do**
  Send $R_i[BC\_addr, pub\_key, SPAS\text{-}H\_ID, token]$ to O_i
  O_i verifies token on web portal
  if $O_i.token$ *equals* $R_i.token$ **then**
    $O_i.P_i.CCTV == R_i.SPAS\text{-}H\_ID$
    Set SA.CCTV_access == true
    Set SC.expiry == true
    SC.duration ← getRentDuration()
    return SA.CCTV_key to R_i
  end
end

5. Web token generation process

   5.1 The renter utilizes the web portal to create a JSON Web Token.
   5.2 The renter enters their details in the chain code, including their blockchain address and certificate. The renter also saves the generated token on SPAS-H for the selected property.

6. Web token authentication process

   6.1 SPAS-H notifies the owner about any information entered regarding their property.
   6.2 The property owner requests and receives the web-generated token from the potential renter through SPAS-H.
   6.3 The owner uses a web portal to authenticate the token and validate whether the renter is a verified renter or an adversary who wishes to harm the property. The authentication process, initiated by the renter and completed by the owner, is an added layer of security in the system and is also logically correct. If the owner generates the token, they must wait indefinitely for the renter to select their property and authenticate the token.

7. The process of rental duration confirmation

   7.1. The owner looks up SPAS-H, the information mapped against their property, and gets the renter's SPAS-H ID. The owner maps the renter's SPAH-H ID with the CCTV security camera ID.
   7.2 The owner queries the rental duration from the renter.
   7.3 After entering the rental duration, the renter deposits the rent and asks SPAS-H for the CCTV security camera key after generating their key pairs through key management.

8. The process of updating ledger and adding block to the blockchain network

 doi:10.20944/preprints202405.1485.v1

8.1 SPAS-H sends a CCTV security camera feed redirection proposal to the endorsing peer.
8.2 The endorsing peer runs the chain code to simulate the CCTV security camera redirection to the renter proposal.
8.3 After executing the chain code, the endorsing peer sends the proposal response to SPAS-H.
8.4 SPAS-H submits transaction to the ordering service.
8.5 The ordering service generates a block of transactions and then sends the block to the committing peer.
8.6 The committing peer validates each transaction, verifies the endorsement policy, and then commits the block to the blockchain. The endorsement policy for SPAS-H is described briefly below in Table 1.

9. The process of the CCTV security camera generating new keys

9.1 After the ledger has been updated, SPAS-H requests the public key from the CCTV security camera.
9.2 The CCTV security camera generates new key pairs and sends the public key to SPAS-H. The old CCTV security camera key is invalidated, and the video feed to the owner is discontinued.

10. The process of initiating the CCTV security camera feed for the renter.

10.1 SPAS-H sends the CCTV security camera's public key to the renter. The renter generates their key pairs and uses their private key to access the video feed.
10.2 The CCTV security camera feed is redirected to the renter.

Table 1. Endorsement policy

Configuration	A building of two floors Each floor has three houses
Peer nodes	floor1 house1 (f1h1), floor1 house2 (f1h2), floor1 house3 (f1h3) floor2 house1 (f2h1), floor2 house2 (f2h2), floor3 house3 (f2h3)
Orderer node	Orderer
Endorsement Policy	3/3 from the same floor and 2/3 from other floor Consider a property selected on floor 1 The endorsement policy will be: [(f1h1.f1h2.f1h3). ((f2h1.f2h2) | (f2h1.f2h3) | (f2h2.f2h3))]

Several control mechanisms are employed to safeguard the blockchain network from potential collapse due to the continuous invocation of chain code. Some of these control mechanisms include attribute-based access control, role-based access control, and reputation-based access control. Additionally, the use of distributed identity server control, where users are registered first, can contribute to the resilience and stability of the blockchain network. A total of five entities are involved in SPAS-H which perform their roles and processing. Figure 6 shows the activity diagram of SPAS-H with all five entities.

 doi:10.20944/preprints202405.1485.v1

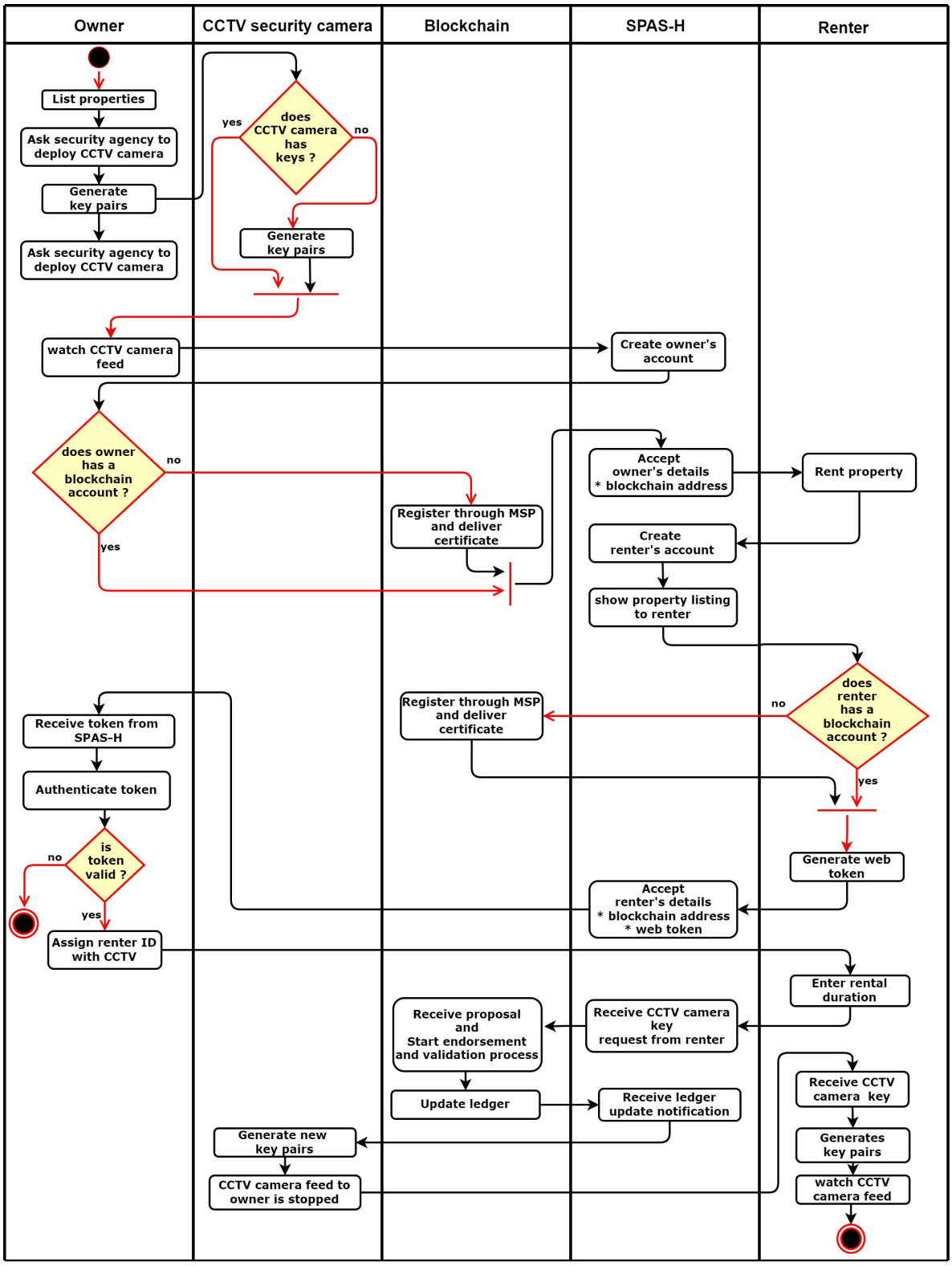

Figure 6. SPAS-H activity diagram.

3.4. Maintaining Anonymity

In the original SPAS, the key management part of the scheme involved the owner, the renter, and the CCTV security camera generating a key pair to be used for different operations. After the keys were generated, anonymity was maintained by using modified ring signatures [37,38] to mask the identities of both the owner and the renter. In SPAS-H, we build on the scheme used in the original

 doi:10.20944/preprints202405.1485.v1

SPAS by adding an additional layer of security, thereby enhancing the value of maintaining anonymity in the system.

In SPAS-H, we add an additional layer of identity masking, specifically for the recipient of the transaction, using stealth addresses [39]. The addition of stealth addresses ensures strong end-to-end anonymity in the system, a feature desired by almost everyone. Unlike conventional public addresses, stealth addresses provide unique, one-time addresses for every transaction. Monero also utilizes stealth addresses along with ring signatures to enhance user anonymity. The fundamental mathematical formulation of stealth addresses remains the same as [40].

When a sender initiates a transaction using a stealth address, the recipient can derive their private key to claim the funds securely without disclosing their public address. This method helps protect user identities and transaction details from prying eyes on the blockchain network. By incorporating stealth addresses into transactions, cryptocurrency users can enjoy increased privacy, confidentiality, and security. Using stealth addresses represents a valuable tool for safeguarding sensitive information and ensuring higher anonymity in blockchain transactions. Figure 7 shows the abstract workflow of stealth addresses.

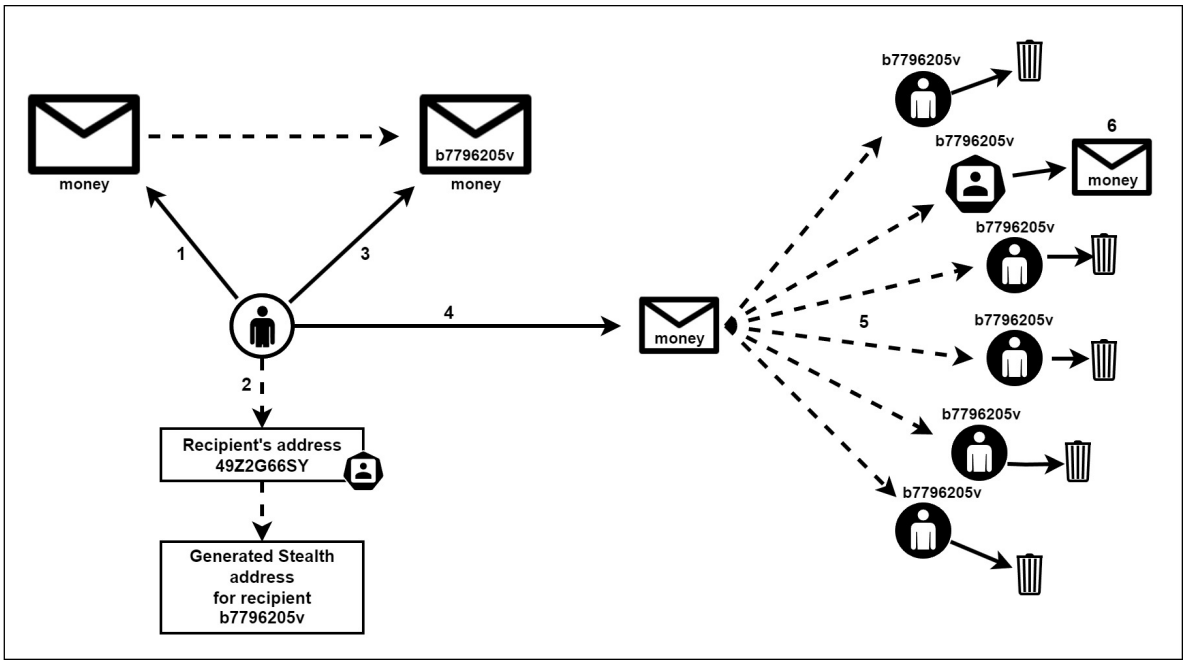

Figure 7. Stealth addresses workflow.

The sender wants to send money to the receiver, so they first generate the stealth address of the original sending address. After this, the money is sent to all potential receivers. Upon receiving the message, the receivers use their private keys to decrypt the message. Only the intended person can decrypt it and claim the money, while the others discard the transaction.

4. Discussion and Analysis

Our proposed scheme focuses on preserving privacy and maintaining anonymity. To achieve privacy, we use a novel chain code algorithm that employs one key at a time without reuse, and generates a new key at every redirection of the camera feed. For anonymity, we use stealth addresses with modified ring signatures from the original SPAS architecture. These mechanisms help mitigate security threats such as double usage, single point of failure, blockchain collapse, and system hacking. Moreover, we address the scalability issue by using the modular approach of Hyperledger Fabric, which allows for the addition of modules as needed.

During the implementation phase, we encountered various challenges. One of the challenges was integrating on-blockchain and off-blockchain communication. We addressed this challenge with the

 doi:10.20944/preprints202405.1485.v1

emergence of oracles, which are third-party services that fetch data from external sources and feed it into the blockchain. Another challenge was using stealth addresses with modified ring signatures. We overcame this challenge by leveraging mathematical modeling of ring signatures and stealth addresses, combining them to achieve our desired goal. Lastly, combining both privacy and anonymity setups posed another challenge, which we addressed through extensive experimentation.

4.1. Implementation

The permissioned nature of Hyperledger Fabric makes it an excellent tool for companies to use internally without the fear of outside manipulation. A CPU with 4 GB of RAM was deployed to host the private blockchain network. Using Fabric version 2.5.7, an endorser peer, a single orderer, and two committer peers were established. These nodes share a common channel for instantiating the developed chaincode. Hyperledger is highly configurable through its modular design and use of chaincodes. Chaincode drives the functionality of the blockchain, acting as the logic for the blockchain and being the fundamental aspect of the proposed solution. Unlike many blockchains that require smart contracts to be written in domain-specific languages, Hyperledger Fabric allows them to be written in general-purpose programming languages like Java, Go, and Node.js. The developed chaincode is written in Node.js.

4.2. Transactional Analysis

We conducted transactional analysis by stress testing the system, varying the number of operations per second. We closely monitored the impact on throughput and latency. Transaction latency is a crucial network-wide measure of the time taken for a transaction's effect to be usable across the network. Figure 8. illustrates a consistent decrease in network transaction latency, indicating that our system performs better as it scales to handle a higher number of operations per second. This adaptability also ensures that the overall performance remains stable even when multiple channels, such as additional renters and CCTV security cameras, are added to the system.

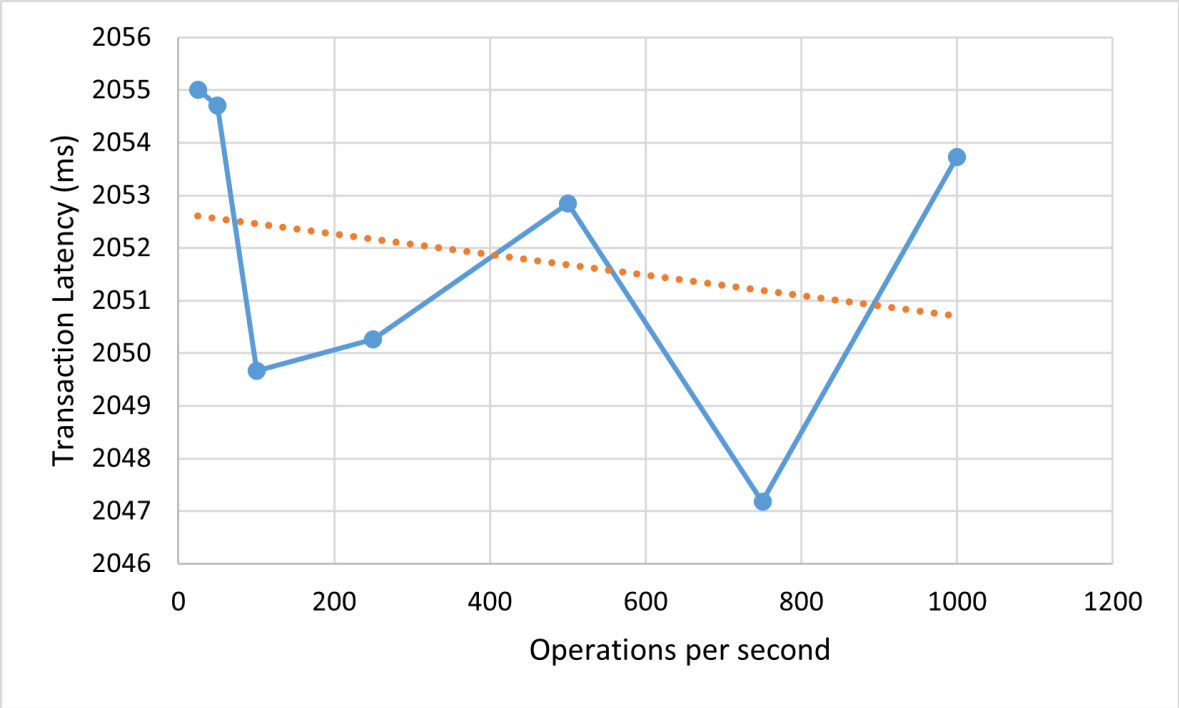

Figure 8. Transaction Latency.

Read latency is the time between when the read request is submitted and when the reply is received. Figure 9. shows the read latency of our system has decreased, indicating a reduction in

 doi:10.20944/preprints202405.1485.v1

response time as the number of operations increases. Both latency measures demonstrate an overall reduction as the system scales up, showcasing its ability to adapt to larger systems in the future.

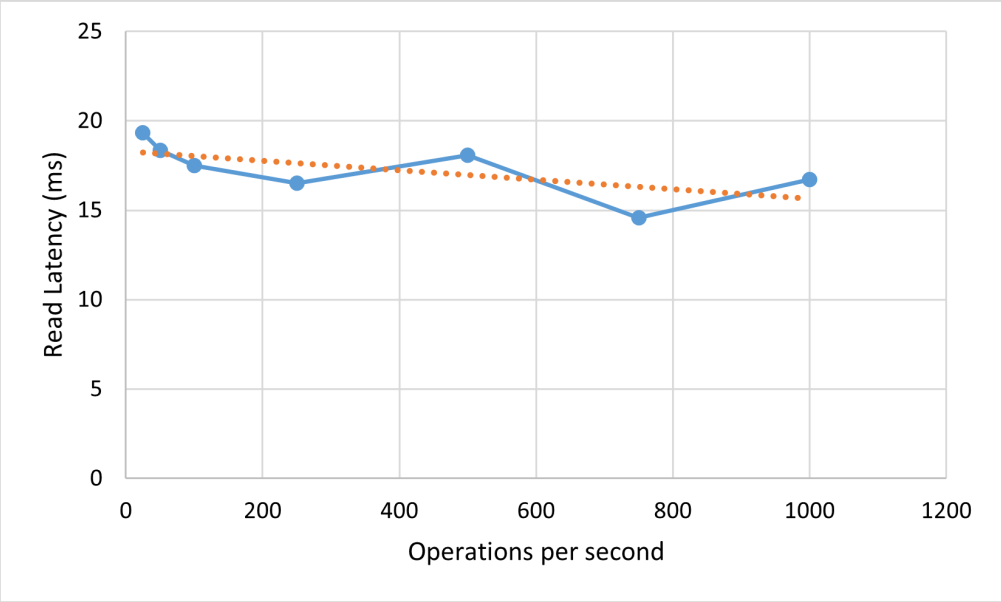

Figure 9. Read Latency.

Transaction throughput is the rate at which valid transactions are committed by the blockchain in a defined period. This is not the rate at a single node but committed at all nodes of the network. Figure 10 shows the transaction throughput of the system which remains constant no matter how much the operations are run per second.

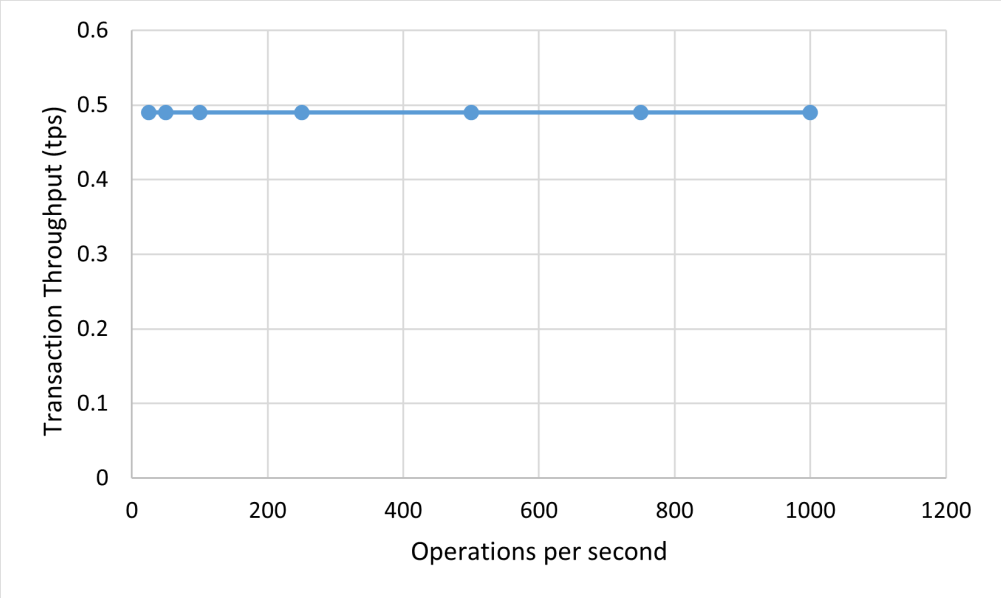

Figure 10. Transaction Throughput.

Read throughput is a measure of how many read operations are completed in a defined period, expressed as reads per second. Figure 11 shows the increasing read throughput of the system demonstrating its efficiency and resilience in overburdened environments. This shows that when dealing with very large systems and an increasing number of operations, the system is capable of performing as required.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 23 May 2024 doi:10.20944/preprints202405.1485.v1

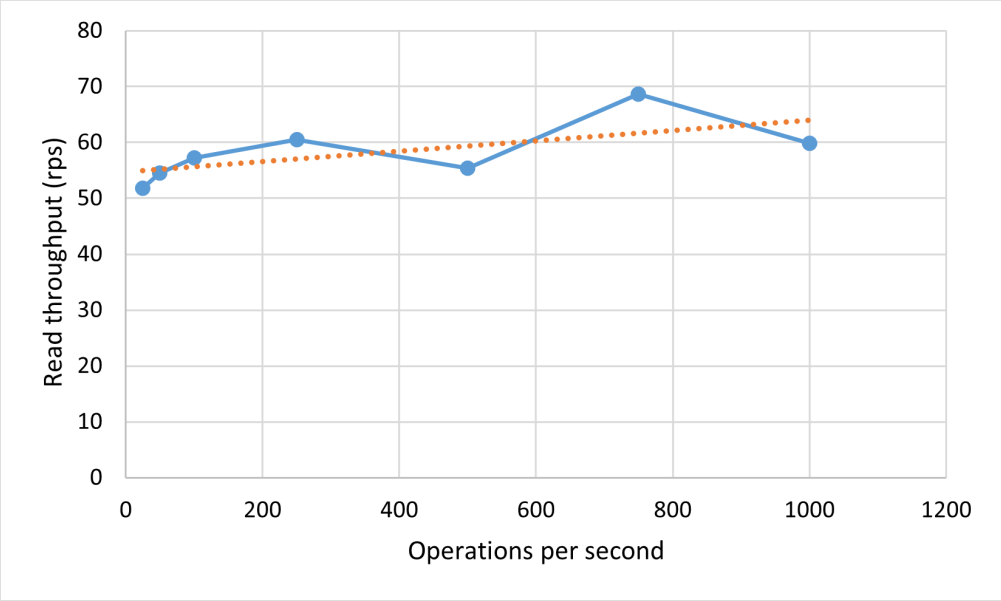

Figure 11. Read Throughput.

Some qualitative analysis is done between SPAS and SPAS-H to show the precedence of SPAS-H. For privacy comparison, the parameters chosen are confidentiality, proof complexity, and verification efficiency index. Figure 12 shows the privacy level comparison. The measure of confidentiality is encryption strength, proof complexity, proof size, and verification efficiency. SPAS-H excels in confidentiality and verification efficiency due to its stronger encryption and greater scalability through its use of Hyperledger Fabric. Additionally, SPAS-H has higher proof complexity as it employs multiple encryption schemes.

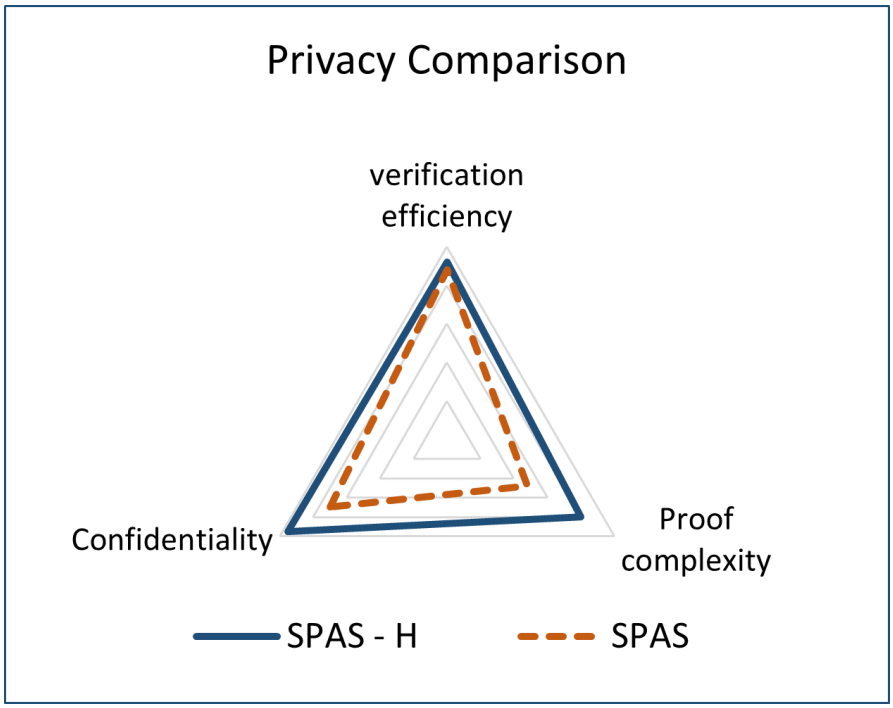

Figure 12. Privacy Level Comparison.

For anonymity analysis, we compared SPAS and SPAS-H systems for anonymity level, traceability resistance, and smart contracts integration. Figure 13 shows the anonymity level comparison. The

 doi:10.20944/preprints202405.1485.v1

parameters used to measure anonymity level are unlinkability and pseudonymity. Transaction privacy is the parameter for traceability resistance, while functionality and use-cases are the parameters for smart contracts integration. SPAS-H is considered better in terms of anonymity level and traceability resistance due to its use of stealth addresses, but it is the same as SPAS in terms of smart contract integration.

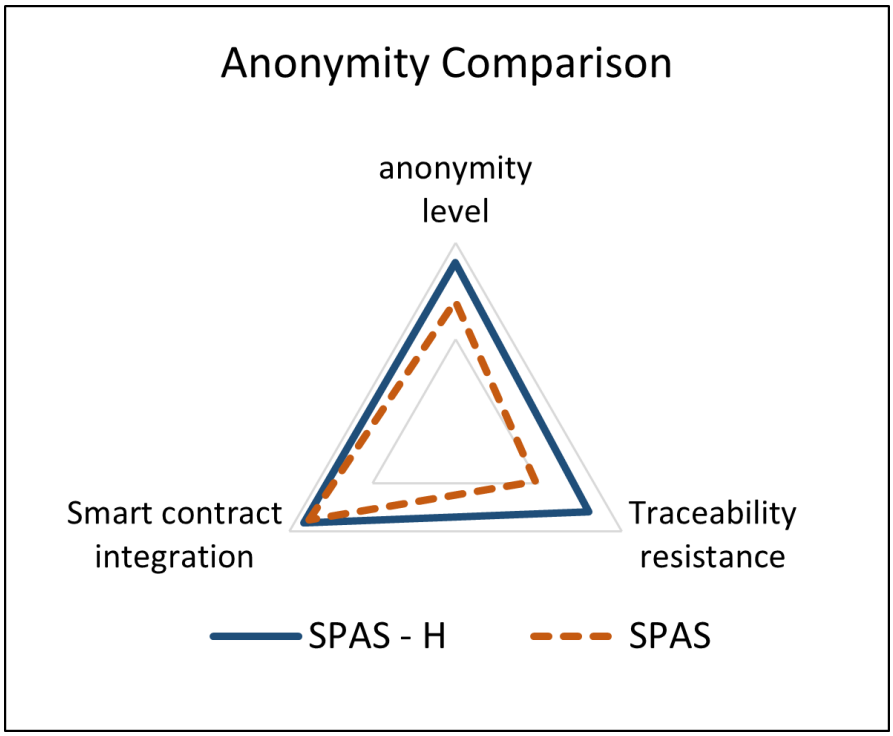

Figure 13. Anonymity Level Comparison.

4.3. Comparative Analysis

We give a comparative analysis of SPAS-H with other schemes mentioned in Section 2. The compared parameters include privacy, anonymity, authentication, smart contracts usage, key usage and confidentiality. Below is Table 2. showing the comparative analysis. The purpose of this comparison is to demonstrate which scheme fully or partially achieves the specified parameters. It's crucial to illustrate that our proposed architecture accomplishes the desired features when compared to existing schemes. This is attributed to the generation of new keys each time the tenant changes, ensuring privacy, the use of tokens for authentication, and the implementation of stealth addresses to ensure anonymity.

Table 2. Comparative Analysis.

Categories	BVM	Smart Grids	SPAS	SPAS-H
Privacy	achieved	achieved	achieved	achieved
Anonymity	partially achieved	partially achieved	achieved	achieved
Authentication	no	no	use of temp id	use of web token
Smart Contract	yes	yes	yes	yes
Key Usage	re-used	re-used	always new	always new
Confidentiality	low	low	low	high

 doi:10.20944/preprints202405.1485.v1

5. Conclusion

The SPAS-H system is an innovative solution that addresses privacy and anonymity concerns within the existing framework. It effectively mitigates challenges associated with traceability and linkability. Our system employs a sophisticated mechanism incorporating web token authentication, stealth addresses, and modified ring signatures. This unique combination enhances our scheme's resilience in preserving individuals' anonymity. The architecture's applicability extends beyond its current implementation, finding relevance in various IoT domains where privacy-sensitive data is at risk. In smart homes, the architecture safeguards data from IoT devices, such as facial and voice recognition, by securely storing it on the blockchain.

Furthermore, the practical implications of this architecture are truly inspiring, especially in the automotive sector. Smart contracts enable smart car parking and fuel payments, ensuring the confidentiality of identity-sensitive and monetary transactions. A significant contribution of our research is the introduction of a new chain code algorithm, notably characterized by the web token authentication architecture that enhances the efficiency of our system. The scalability of our system to diverse fields reliant on sensitive data, where preserving anonymity is crucial, underscores the versatility and relevance of our approach. Hyperledger Fabric opens the doors modularly, making it easier to scale up the system. Beyond IoT, the architecture has potential implementation in the pharmaceutical industry, particularly in scenarios involving the development and distribution of drugs through wholesalers, dispensers, and end customers.

Author Contributions: Conceptualization, M.S.; methodology, M.S., S.A.H., and A.B.; formal analysis, M.S., M.R.B. and D.J.P.; writing—original draft preparation, M.S..; writing—review and editing, M.S., S.A.H., A.B., M.R.B., D.J.P., and T.S.C.; supervision, D.J.P. and T.S.C.; funding acquisition, T.S.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) under the Artificial Intelligence Convergence Innovation Human Resources Development (IITP-2024-RS-2023-00255968) grant and the ITRC (Information Technology Research Center) support program (IITP-2021-0-02051) funded by the Korea government(MSIT).

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Agrawal, R.; Verma, P.; Sonanis, R.; Goel, U.; De, A.; Kondaveeti, S.A.; Shekhar, S. Continuous security in IoT using blockchain. 2018 IEEE international conference on acoustics, speech and signal processing (ICASSP). IEEE, 2018, pp. 6423–6427.
2. Khor, J.H.; Sidorov, M.; Woon, P.Y. Public blockchains for resource-constrained IoT devices—A state-of-the-art survey. *IEEE Internet of Things Journal* **2021**, *8*, 11960–11982.
3. Hwang, D.; Choi, J.; Kim, K.H. Dynamic access control scheme for iot devices using blockchain. 2018 international conference on information and communication technology convergence (ICTC). IEEE, 2018, pp. 713–715.
4. Xu, L.; Shah, N.; Chen, L.; Diallo, N.; Gao, Z.; Lu, Y.; Shi, W. Enabling the sharing economy: Privacy respecting contract based on public blockchain. Proceedings of the ACM workshop on blockchain, cryptocurrencies and contracts, 2017, pp. 15–21.
5. Krishnan, K.N.; Jenu, R.; Joseph, T.; Silpa, M. Blockchain based security framework for IoT implementations. 2018 international CET conference on control, communication, and computing (IC4). IEEE, 2018, pp. 425–429.
6. Kashif, M.; Kalkan, K. BCPriPIoT: BlockChain utilized privacy-preservation mechanism for IoT devices. 2021 Third International Conference on Blockchain Computing and Applications (BCCA). IEEE, 2021, pp. 201–209.
7. Pouraghily, A.; Wolf, T. A lightweight payment verification protocol for blockchain transactions on IoT devices. 2019 International Conference on Computing, Networking and Communications (ICNC). IEEE, 2019, pp. 617–623.

 doi:10.20944/preprints202405.1485.v1

8. Andrew, J.; Isravel, D.P.; Sagayam, K.M.; Bhushan, B.; Sei, Y.; Eunice, J. Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. *Journal of Network and Computer Applications* **2023**, p. 103633.
9. Jiang, S.; Cao, J.; Wu, H.; Chen, K.; Liu, X. Privacy-preserving and efficient data sharing for blockchain-based intelligent transportation systems. *Information Sciences* **2023**, *635*, 72–85.
10. Alsobhi, H.A.; Alakhtar, R.A.; Ubaid, A.; Hussain, O.K.; Hussain, F.K. Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review. *Knowledge-Based Systems* **2023**, *265*, 110238.
11. Van Saberhagen, N. CryptoNote v 2.0 **2013**.
12. Pan, Q.; Wu, J.; Bashir, A.K.; Li, J.; Vashisht, S.; Nawaz, R. Blockchain and AI enabled configurable reflection resource allocation for IRS-aided coexisting drone-terrestrial networks. *IEEE Wireless Communications* **2022**, *29*, 46–54.
13. Lin, X.; Wu, J.; Mumtaz, S.; Garg, S.; Li, J.; Guizani, M. Blockchain-based on-demand computing resource trading in IoV-assisted smart city. *IEEE Transactions on Emerging Topics in Computing* **2020**, *9*, 1373–1385.
14. Saquib, N.; Bakir, F.; Krintz, C.; Wolski, R. A Resource-Efficient Smart Contract for Privacy Preserving Smart Home Systems. 2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI). IEEE, 2021, pp. 532–539.
15. Klaokliang, N.; Teawtim, P.; Aimtongkham, P.; So-In, C.; Niruntasukrat, A. A novel IoT authorization architecture on hyperledger fabric with optimal consensus using genetic algorithm. 2018 Seventh ICT International Student Project Conference (ICT-ISPC). IEEE, 2018, pp. 1–5.
16. Banoun, N.; Diarra, N. Authentication of Mobile IoT Devices using HyperLedger Fabric Blockchain. 2021 Eighth International Conference on Software Defined Systems (SDS). IEEE, 2021, pp. 1–6.
17. Khatri, S.; al Sulbi, K.; Attaallah, A.; Ansari, M.T.J.; Agrawal, A.; Kumar, R. Enhancing Healthcare Management during COVID-19: A Patient-Centric Architectural Framework Enabled by Hyperledger Fabric Blockchain. *Information* **2023**, *14*, 425.
18. Sujihelen, L.; others. An efficient chain code for access control in hyper ledger fabric healthcare system. *e-Prime-Advances in Electrical Engineering, Electronics and Energy* **2023**, *5*, 100204.
19. Attia, O.; Khoufi, I.; Laouiti, A.; Adjih, C. An IoT-blockchain architecture based on hyperledger framework for health care monitoring application. NTMS 2019-10th IFIP International Conference on New Technologies, Mobility and Security. IEEE Computer Society, 2019, pp. 1–5.
20. Khan, P.W.; Byun, Y.C.; Park, N. A data verification system for CCTV surveillance cameras using blockchain technology in smart cities. *Electronics* **2020**, *9*, 484.
21. Moolikagedara, K.; Nguyen, M.; Yan, W.Q.; Li, X.J. Video Blockchain: A Decentralized Approach for Secure and Sustainable Networks with Distributed Video Footage from Vehicle-Mounted Cameras in Smart Cities. *Electronics* **2023**, *12*, 3621.
22. Kim, D.; Ihm, S.Y.; Son, Y. Two-level blockchain system for digital crime evidence management. *Sensors* **2021**, *21*, 3051.
23. Mahmood, A.; Khan, A.; Anjum, A.; Maple, C.; Jeon, G. An efficient and privacy-preserving blockchain-based secure data aggregation in smart grids. *Sustainable Energy Technologies and Assessments* **2023**, *60*, 103414.
24. Santoso, N.; Javaid, H. Improving Energy Efficiency of Permissioned Blockchains Using FPGAs. 2022 IEEE 28th International Conference on Parallel and Distributed Systems (ICPADS). IEEE, 2023, pp. 177–184.
25. M. Zein, R.; Twinomurinzi, H. Information Sharing in Land Registration Using Hyperledger Fabric Blockchain. *Blockchains* **2024**, *2*, 107–133.
26. Proença, A.S.; Dias, T.R.; Correia, M.P. Blockchain Based Residential Smart Rent. *arXiv preprint arXiv:2402.05737* **2024**.
27. Singh, S.; Singh, A.; Verma, S.; Dwivedi, R.K. Designing a Blockchain-Enabled Methodology for Secure Online Voting System. 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT). IEEE, 2023, pp. 178–184.
28. Chovancová, E.; Chovanec, M.; Ádám, N.; Hurtuk, J. Online voting management system based on Blockchain. 2023 IEEE 27th International Conference on Intelligent Engineering Systems (INES). IEEE, 2023, pp. 000169–000174.

 doi:10.20944/preprints202405.1485.v1

29. Tang, B.; Tan, M.; Liu, M.; Liu, Z.; Tian, W. A Privacy Protection Method of Blockchain-Based E-Voting Using Homomorphic Encryption and Order-Preserving Encryption. 2023 5th International Conference on Artificial Intelligence and Computer Applications (ICAICA). IEEE, 2023, pp. 86–90.
30. Islam, M.N.; Kundu, S. Preserving IoT privacy in sharing economy via smart contract. 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI). IEEE, 2018, pp. 296–297.
31. Li, X.; Mei, Y.; Gong, J.; Xiang, F.; Sun, Z. A blockchain privacy protection scheme based on ring signature. *IEEE Access* **2020**, *8*, 76765–76772.
32. Long, Y.; Chen, Y.; Ren, W.; Dou, H.; Xiong, N.N. Depet: A decentralized privacy-preserving energy trading scheme for vehicular energy network via blockchain and k-anonymity. *Ieee Access* **2020**, *8*, 192587–192596.
33. Jeong, Y.; Hwang, D.; Kim, K.H. Blockchain-based management of video surveillance systems. 2019 International Conference on Information Networking (ICOIN). IEEE, 2019, pp. 465–468.
34. Yadav, P.; Sharma, S.; Muzumdar, A.; Modi, C.; Vyjayanthi, C. Designing a Trustworthy and Secured House Rental System using Blockchain and Smart Contracts. 2022 IEEE 19th India Council International Conference (INDICON). IEEE, 2022, pp. 1–6.
35. Loreti, P.; Bracciale, L.; Raso, E.; Bianchi, G.; Sanseverino, E.R.; Gallo, P. Privacy and Transparency in Blockchain-based Smart Grid Operations. *IEEE Access* **2023**.
36. Saad, M.; Bhutta, M.R.; Kim, J.; Chung, T.S. A Framework for Enhancing Privacy and Anonymity in Blockchain-Enabled IoT Devices. *Computers, Materials & Continua* **2024**, *78*.
37. Bender, A.; Katz, J.; Morselli, R. Ring signatures: Stronger definitions, and constructions without random oracles. Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3. Springer, 2006, pp. 60–79.
38. Okamoto, T.; Tso, R.; Yamaguchi, M.; Okamoto, E. A k-out-of-n Ring Signature with Flexible Participation for Signers. *Cryptology ePrint Archive* **2018**.
39. Courtois, N.T.; Mercer, R. Stealth address and key management techniques in blockchain systems. ICISSP 2017-Proceedings of the 3rd International Conference on Information Systems Security and Privacy, 2017, pp. 559–566.
40. Yu, G. Blockchain stealth address schemes. *Cryptology ePrint Archive* **2020**.