information

MDPI

Article

A Blockchain-Based Decentralized Public Key Infrastructure for Information-Centric Networks

Jia Shi [1,2], Xuewen Zeng [1,2] and Rui Han [1,2,*]

[1] National Network New Media Engineering Research Center, Institute of Acoustics, Chinese Academy of Sciences, No. 21, North Fourth Ring Road, Haidian District, Beijing 100190, China; shij@dsp.ac.cn (J.S.); zengxw@dsp.ac.cn (X.Z.)
[2] School of Electronic, Electrical and Communication Engineering, University of Chinese Academy of Sciences, No. 19(A), Yuquan Road, Shijingshan District, Beijing 100049, China
* Correspondence: hanr@dsp.ac.cn

Abstract: How to achieve secure content distribution and accountability in information-centric networking (ICN) is a crucial problem. Subscribers need to verify whether the data came from a reliable source, rather than from a spoofing adversary. Public key cryptography was introduced to achieve a method of authentication that binds the data packet to its owner. In existing prototypes, PKIs, identity-based signatures (IBSs) and recommendation networks are the common schemes used to ensure the authenticity and availability of public keys. However, CA-based PKIs and KGC-based IBSs have been proven to be weak when it comes to resisting security attacks, with recommendation networks being too complex to deploy. In this respect, we designed a novel distributed authentication model as a secure scheme to support public key cryptography. Our model establishes a decentralized public key infrastructure by combining the smart contracts of blockchain and optimized zero-knowledge proof-verifiable presentations by utilizing the DID project, which realizes the management of public key certificates through blockchain and ensures the authenticity and availability of public keys in decentralized infrastructure. Our scheme fundamentally solves the issues of security and feasibility in existing schemes and provides a more scalable solution with respect to authenticating data sources. An experiment demonstrated that our proposal is 20% faster than the original zero knowledge proof scheme in registration.

Keywords: decentralized public key infrastructure (DPKI); verifiable presentations; zero-knowledge proof; ICN; blockchain

Citation: Shi, J.; Zeng, X.; Han, R. A Blockchain-Based Decentralized Public Key Infrastructure for Information-Centric Networks. *Information* **2022**, *13*, 264. https://doi.org/10.3390/info13050264

Academic Editor: Kun She

Received: 31 March 2022
Accepted: 21 May 2022
Published: 23 May 2022

1. Introduction

Information-centric networking (ICN) is a focus of research in the Next Generation. Internet (NGI) paradigm, which has been included in 5G standards by the International Telecommunication Union (ITU) [1]. By decoupling content identifiers and network addresses, ICN realizes high throughput and low latency data distribution. Caching, multihoming, multicast and multipathing are inherently supported by this paradigm [2]. DONA (data-oriented network architecture) [3], CCN (content-centric networking) [4], NDN (named data networking) [5], NetInf (network of information) [6] et al. are typical architectures of ICN [7]. ICN considers the security at the beginning of design. Its security model is attached directly to the data and its naming scheme, which is called intrinsic security [8]. Public key cryptosystems are a pivotal technology in making the design of ICN a reality. In the original design, PKIs [9] were the most-commonly used scheme to manage and distribute public keys. With the maturation of ICN architecture and naming design, the inadaptability of this scheme has been noticed. Considering that ICN is a highly distributed system [10], the centralized PKI model greatly limits the development and security of ICN [11,12]. Therefore, researchers have reconsidered distributed models based on identity-based cryptography (IBC) and recommendation networks. However, identity-based based

signatures suffer from the inherent key escrow problem, and the recommendation mechanism can only be applied in small group scenarios, which requires a certain amount trust among group members, and cannot be extended to large-scale network application scenarios as an authentication method. The question of how to complete distributed public key distribution and authentication in ICN architecture remains unresolved [13,14]. The decentralized public key infrastructure (DPKI) based on distributed identity proposed in recent years provided a breakthrough in addressing this problem. DPKI solves the problems of security and flexibility associated with centralized PKI systems by designing an efficient and reliable decentralized public key authentication scheme, which can provide strong support for the further deployment of an ICN network.

Therefore, we designed a DPKI-based distributed authentication model for ICN by combining blockchain and verifiable presentations [15]. The public key certificates realize distributed management and verification through the smart contract and distributed ledger technology of blockchain. Meanwhile, the verifiable presentations enable users to prove their identification claims to semi-trusted consensus nodes without unnecessary undermining privacy. In this way, the consensus nodes on the blockchain can authenticate the true identity of the users applying for reliable certificate registration. Our scheme fundamentally solves the binding between public key and physical identity and realizes the distributed management of public key certificates so as to provide a complete decentralized public key infrastructure. The main contributions of this paper are as follows:

(1) We propose a secure identification approach without revealing the privacy of users to semi-trusted nodes and define a certificate generation and management protocol to bind their true identity based on blockchain, which is a decentralized and secure alternative for public key authentication in ICN.
(2) An optimized zero-knowledge proof scheme was designed in the verifiable presentations, which increase the efficiency and security of the verifiable presentations. We introduced the Schnorr signature and Schnorr zero-knowledge proof for verifiable presentation verification, which is compatible with efficiency and security and is easier to deploy. An aggregate signature scheme was presented to support multi-attribute rapid verification. An experiment demonstrated that our proposal is 20% faster than the original zero knowledge proof scheme in registration.
(3) The process of secure communication was introduced and proved to be reliable. Our model registers the certificate ID in the standalone name resolution approach (SNR) system along with the network address (NA), which ensures the security of issuing certificate ID during the initial interaction.

The structure of this paper is organized as follows. In Section 2, we briefly introduce the related work of our scheme. Section 3 illustrates the system requirements and architectural model of our proposal. The design protocol for certificate generation and management is detailed in Section 4, including its working process and the related algorithms. Section 5 provides an analysis of the security of the whole scheme. The simulation results are presented and analyzed in Section 6. Finally, Section 7 offers our conclusion.

2. Related Work

In order to realize reliable asynchronous data exchange in an untrusted network environment, publishers and subscribers establish a trust model based on public key cryptography. Public key management schemes have also become the key to ensure network security, which has attracted the wide attention of researchers. Yu et al. [16] presented a centralized public key management in NDN. The certificate format, distribution and revocation were discussed and provide a starting point for the definition of a PKI. Mauri et al. [17] described an up-to-date key management method for ICN. The method is to keep a public key repository for trusted TA institutions and each consumer. After each key update, TA modifies it for all consumers. Li et al. [18] introduced a distributed authentication and authorization scheme based on identity-based cryptography (IBC) in ICN architecture. The authentication of the data source is integrated with a distributed scheme through the

use of an identity-based signature. Hamdane et al. [19] proposed a hybrid scheme which combines public-key infrastructure (PKI) and hierarchical identity-based cryptography (HIBC) for CCN and NDN, which realized reliable public key management though a private key generator (PKG) and a PKI. Yu et al. [20] proposed building automatic trust network applications in ICN network architecture to protect communication security. In the proposed method, taking the recommendation result as proof, the newly added users in the groups are accepted by the existing users. Yang et al. [21] demonstrated a hierarchical public key authentication in which the namespace matches the trust delegation hierarchy. The key with a specific name issued by each layer can only sign the specified data package. When the subscribers receive the data packet, they can verify the public key from bottom to top through the hierarchical relationship until they find the root key to complete the authentication of the data packet. This authentication method is applicable to ICN architectures with hierarchical names such as NDN and CCN.

To sum up, there are three main directions to address with respect to the authenticity and availability of public keys: PKIs, identity-based signatures and the recommendation trust model. Combined with the introduction in the previous section, we provide a comparison of existing works. The limitations of the existing literature are briefly summarized in Table 1.

Table 1. The limitations of the existing literature.

	Key Management	**System Model**	**Security**	**Scenario**
PKI	CA	Centralized	Weak (single point attack)	All
IBS	KGC	Distributed	Weak (KGC single point attack)	All
Trust network	Self-verifying	Distributed and decentralized	Weak (collusion Attacks)	Small group
DPKI	Blockchain	Distributed and decentralized	High (tamper resistant)	All

In addition, research on decentralized public key authentication is also in progress. The authors of [22–26] focus on the public and decentralized PKI system model and described a detailed scheme and the application of decentralized, PKI-based secure communication. Their designs provide the essential functions of PKIs, such as the registering, updating, revoking and verifying of the ownership of a public key. Furthermore, decentralized identifiers (DIDs) [27] and verifiable credentials [28] have become a project of primary concerned and represent a new type of identifier that enables verifiable, decentralized digital identities. Relevant research has also been conducted in the form of in-depth discussions [29–31]. The authors of [32,33] discussed the applicability of DIDs and VCs in ICN networks. Compared with these schemes, we hope to design a more secure, efficient and suitable DPKI scheme for ICNs. The following sections outline the proposed scheme based on these goals.

3. System Overview

In this section, we briefly introduce the design requirements and architectural model of our proposal.

3.1. Design Goals

The goal behind our model was to build a decentralized public key infrastructure (DPKI) on an ICN, which would allow for the identity and attributes to be retrieved and validated by other peers during secure data communication. The functions of DPKI systems include the granting of certificates as well as their generation and management and the

updating, revocation and establishment of new and old user certificate libraries. Blockchain is used as the underlying support to provide the infrastructure with distributed reliability. In order to realize the basic DPKI model, the design is divided into three basic functions:

(1) An input as a proof (P) for identity confirmation without CA;
(2) A verification procedure (V) for P to grant system management (generation, update, revocation);
(3) An output in the form of a certificate (G) for secure communication.

3.2. Adversarial Model

Based on the above design, we mainly considered three malicious adversary models:

(1) The miner nodes are semi-trusted. They truthfully perform the contracts of the blockchain, verify the registration request and add the certificates to a distributed ledger of the blockchain after verifying the identity. However, they may reveal the user data and lead to the leakage of private data;
(2) Malicious adversaries will try to steal the P of legitimate users to forge the identity of legitimate users in the process of certificate registration;
(3) Malicious adversaries will try to steal the certificates or private keys of legitimate users to forge the identity of legitimate users in the process of data exchange.

In addition, our system allows for the adversary to corrupt up to t of the n consensus nodes, for t is less than the fault tolerance threshold of the consensus algorithm.

Therefore, the P and V should be carried out using the zero-knowledge proof method to protect users' privacy and provide reliability with respect to proof of identity. Additionally, the functions of P, G and V should have the following properties (i and j are two peer user nodes in public key verification):

(1) $P_i \neq P_j$, i.e., in this sense, P should be a one-way function which should be hard to break. This prevents adversaries impersonating legal identities;
(2) Miners on blockchain can verify a user's identity via V and the P must not reveal any information not intended to be revealed by users;
(3) $G\ (i, sk_i) \neq G\ (k, sk_i)$, i.e., k is an attacker who steals the private key sk_i of a legitimate user i. k should not be able to generate i's certificate using sk_i without proof P_i. Otherwise, k can impersonate i;
(4) $P_i(\mathrm{n}) \neq P_i(\mathrm{n}+1)$, i.e., a user should be able to generate different proofs given different challenges. Meanwhile, the P should add the timestamp. This prevents adversaries from using an old proof to impersonate legal identities.

3.3. System Model

The system model for our proposal is illustrated in Figure 1. We will describe the main parts in detail.

1. Issue Credentials: Steps 1 and 2 illustrate the process for issuing verifiable credentials [34–36]. Users submit the necessary documents to credential issuers, which creates a verifiable credential from these claims and transmits the verifiable credential to applying users. Verifiable credentials can be used to build verifiable presentations [37], which can also be cryptographically verified as proof of identity attributes.
2. Certification generation and management: The verifiable presentations using derived credentials will be the proof of users for identity confirmation in certification generation and management. A decentralized architecture was developed using blockchain as a database to store metadata such as public keys, digital signatures and other attributes. Smart contracts enable users to create and manage their identities and related attributes on a blockchain network.
3. Secure communication: Communication verifiers including network devices and peer users' information interactions. Devices or peers can retrieve the active public key certificates from the immutable ledger of the blockchain. If they find the certificate, it performs the signature verification process. It should be noted that the certificate ID

is obtain from the SNR in the NA lookup process. When accessing the ICN, users will register their user ID along with a certificate ID in the SNR.

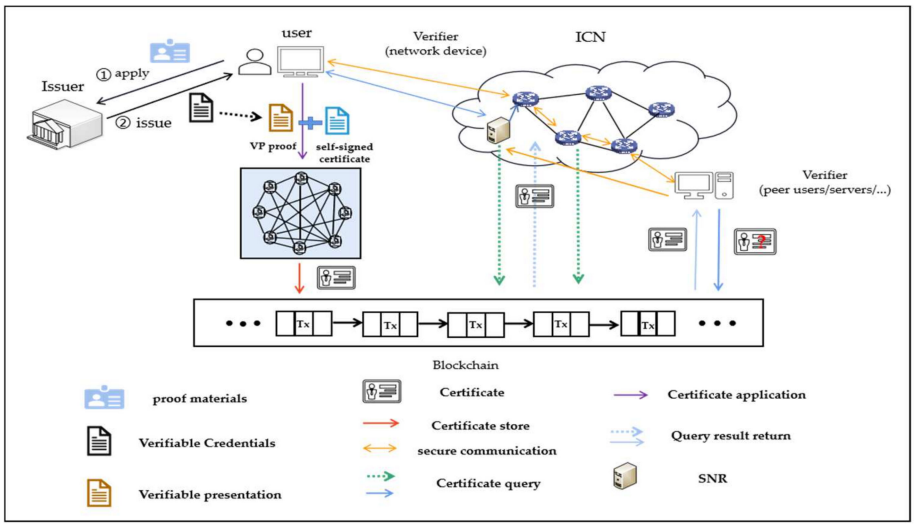

Figure 1. System model.

In next section, the generation rules of P and V used to grant certificate management (its generation, update and revocation) will be described in detail.

4. Optimization Scheme

We introduce an authentication presentation using zero-knowledge proof to illustrate the scheme of P and V in Section 4.1. The corresponding certificate management scheme is described in Section 4.2. Verifiable presentations offer the possibility of integrating various identity attributes into certificates, which associates the certificates of individuals or organizations with their real identities. This process ensures the unforgeability of public key certificates and solves the identification dilemma via private key disclosure in an anonymous authentication scheme. The scheme of secure data exchange using DPKI is described in Section 4.2.

4.1. An Authentication Scheme Using Zero-Knowledge Proof

Zero-knowledge proof (ZKP) mechanisms [38] introduce key capabilities to express multiple verifiable credentials from multiple issuers into a single proof without revealing any unnecessary information. The W3C Model [39] represents one way of using a Camenisch–Lysyanskaya (CL) signature method [40] in verifiable presentations as zero-knowledge proof, which provides a unique feature to support issuing of an anonymous credential. The CL ZKP has been shown to increase the system overhead. Related research has considered the BBS+ [41] signature. However, BBS+ signatures do not support claims aggregation. Research on the zero-knowledge proof of verifiable presentations is ongoing. We present a practical method based on the Schnorr signature [42] and Schnorr ZKP [43] for the purpose of designing a public key certificate system. The digital signature property of a CL signature can be completed by a Schnorr signature. Meanwhile, the linear nature of the Schnorr signature can provide aggregation verification and reduce the overhead. The Schnorr ZKP can realize the zero-knowledge property of a CL signature. Our scheme realizes computational security based on the integer factoring problem and discrete logarithm problem. Compared with the existing research, our scheme is efficient, secure and easier to deploy. The process of zero-knowledge identity authentication is as follows:

First of all, our scheme is a tripartite scheme involving the issuer, user (prover) and verifier. The interactive proof process is divided into two stages: issuers issue the verifiable credential to users and the user as a prover submits the verifiable presentation derived from

the verifiable credentials based on zero-knowledge proof to the verifier for the verification. It should be noted that the EC group is a trusted third-party endorsement signature that verifies the reliability of the verifiable credential certificate, and the modular group is necessary to complete a VP proof verification of the zero-knowledge proof between the user and verified nodes. We will explain the details of the tripartite process in the following description.

- **Issuer:**

The issuer publishes the system parameters as a trusted third party and uses the private key to sign the parameter v which ensures that the subsequent verifiers can verify the authenticity of the zero-knowledge proof parameters v through an asymmetric signature. The steps of the issuing process are as follows:

a. Setting up the system parameters: choosing large prime p, q, g and $p - 1 = 0 \bmod q$. A cyclic group $G \subset Z_p^*$ of prime order q is chosen, in which it is assumed that the DLP is difficult, along with a generator $g \in G$. A hash function H: $\{0, 1\}^* \rightarrow G$ is chosen. The public parameters are $pp = (p, q, g, G, H)$. A prime field of order p is represented by the symbol F_p. The base point of the elliptic curve F_p is Q. Asymmetric keys (SK_{issuer}, PK_{issuer}) meet the equality $PK_{issuer} = (SK_{issuer})\ Q$;
b. Generating an endorsement signature: The applicant defines a secret value ***s*** which is only shared by the issuer and the applicant. It can be chosen according to the privacy information (e.g., ID number) submitted by the applicant. Then the issuer calculates a parameter $v = g^s \bmod p$ as a private authenticator with the modular group and the endorsement signature $Sig1 = kQ = K$, $Sig2 = SIG\ \{H\ (v||K||credential), SK_{issuer}\} = k + H\ (v||K||credential)^*\ SK_{issuer}$ with the EC group, where k is random, $k \in Z_p^*$. These three parameters (v, $Sig1$, $Sig2$) are written as the proof statement in the verifiable credential with other credential metadata and the verifiable credential is sent to the credential applicant. The parameters ($Sig1$, $Sig2$) are the Schnorr signature result. V is the ZKP parameter of the hidden knowledge s. It should be noted that the issuers are a completely trusted third party (e.g., government or police bureaus), which can obtain the user's privacy for identity authentication and will not reveal it.

- **Prover:**

Prover wants to prove the knowledge s, which is hidden as $v = g^s \bmod p$, to prove that the prover providing the VP proof is indeed a legal user with the correct identity, who knows the secret s and does not steal and reproduce the proof of others. The validation parameters are calculated by the prover from their verifiable credential according to the following steps:

(1) Pick $r \in Z_p^*$ and compute $x = g^r \bmod p$;
(2) Calculate $e = Hash(v||K||credential)$;
(3) Calculate $y = r + se \bmod q$;
(4) Publish v, e, x, y, $Sig1$, $Sig2$ to verifier.

- **Verifier:**

The verifier conducts a zero-knowledge proof interaction with the prover and between the two parties. The steps of the verification process are as follows:

(1) Check $Ver\ \{(Sig2)Q = Sig1 + Hash(v||K||credential)^*\ PK_{issuer}\} \stackrel{?}{=} true$;
(2) Check $x \stackrel{?}{=} g^y v^{-e} \bmod p$;
(3) Accept if (1) and (2) are true.

Meanwhile, if the verifiable presentation is provided by multiple verifiable credentials, the aggregation nature of Schnorr can be utilized to reduce the verification overhead. For instance, a film company's certificate verification does not only attribute their identity but also the qualification credentials, which can be regarded as a service attribute. According to Schnorr's linear properties, verifiers can check the signature by using following calculation:

(1) $Sum\ \{Sig1_i\} = (Sig1_1)Q + (Sig1_2)Q + \ldots + (Sig1_n)Q = \{Sig1_1 + Sig1_2 + \ldots + Sig1_n\}Q$;

(2) $Sum\ \{Sig2_i\} = Sum\{K_i + e_i{}^* PK_{issueri}\} = Sum\{K_1 + K_2 + \ldots + K_n\} + Sum\{e_1{}^* PK_{issuer1} + e_2{}^* PK_{issuer2} + \ldots + e_n{}^* PK_{issuern}\}$;

(3) Check $x \stackrel{?}{=} g^y v^{-e} \ mod\ p$. Provers can select the same v when applying for credentials to reduce the verification overhead.

4.2. Essential Functions

In this sub-section, we describe a detailed scheme for building a decentralized PKI. In order to provide these essential functions, transaction information upon registration, the updating of this information and the revoking of public keys are posted to the blockchain. Meanwhile, the blockchain also stores new and old user certificates in the form of a library.

- Certification generation:

The user creates a self-signed certificate that contains a certificate ID, public key, signature, proof version, certificate version, timestamp and metadata. The certificate ID is defined as a hash of the certificate content, which can be used to ensure the integrity of certificate data. Key pairs (*PK*, *SK*) and signature values are generated locally by the user. The metadata contain information needed for the security functions, such as key usage or a signature algorithm identifier. Users can also add additional information according to their own needs to increase the functions expressed by the certificate. Meanwhile, users derive a verifiable presentation from verifiable credentials in a cryptographically verifiable format as proof of identity. An example of a self-signed certificate and proof are provided in Figure 2.

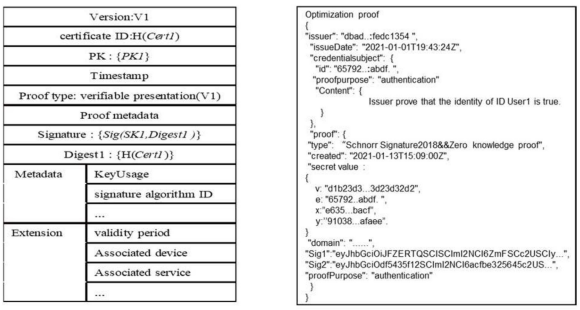

Figure 2. An example of a self-signed certificate and proof.

When a user registers a public key certificate on the blockchain, the self-signed certificate is passed along with an identity proof for verification by miners. The verification process is described in Figure 3. Once the certificates have been verified, they will be stored on the blockchain.

- Updating and revoking:

When users update or revoke the public key certificate, a claim, in the form of a new certificate, is passed along with the identity proof for verification. Examples of updating and revoking claims are shown in Figure 4. The red elements are unique to the updating process. Miners verify the signature using the old public key (PK1) of the certificate. After the verification of the old version of the signature is complete, the verification is performed with the new public key (PK2). Then, the miners verify the proof of identity as before. The new certificate is added to the distributed ledger after the verification. The verification process is described in Figure 5.

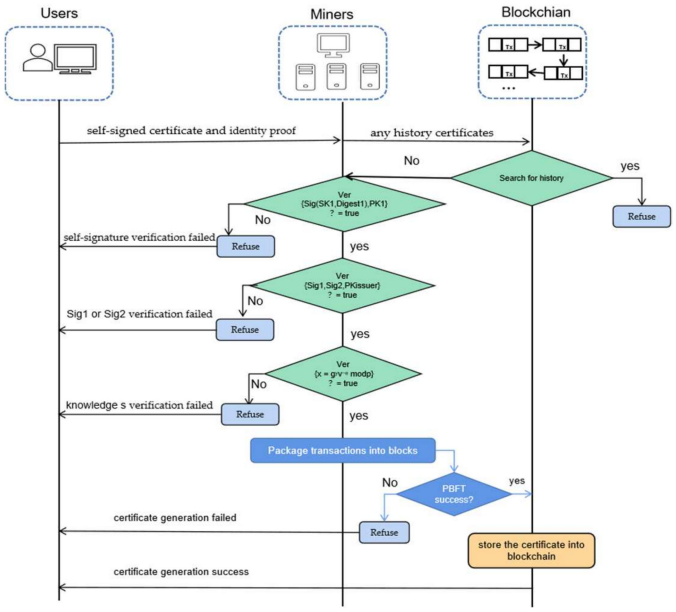

Figure 3. The verification process for certification generation.

- Secure communication:

Version:V2	
certificate ID:H(*Cert1*)	
Type : Updating/Revoking	
Proof type: verifiable presentation(V1)	
Proof metadata	
PK : {*PK1, PK2*}	
Timestamp	
Signature : {*SigSK1*|*SigSK2(SK2,Digest)*}	
Digest2: {H(Cert1)|H(Cert2)}	
Metadata	KeyUsage
	signature algorithm ID
	...
Extension	validity period
	Associated device
	Associated service
	...

Figure 4. An example of updating and revoking claims.

The secure communication process is illustrated in Figure 6. To be clear, our communication model is based on the architecture of standalone name resolution system [44–46], which is suitable for prototype systems such as DONA, Netlnf, etc. The designed ICN communication mode is a single handshake mode, so there is no three-handshake process of ACK before certificate exchange. In order to ensure security, after obtaining the network address through naming resolution, user A first queries and checks the certificate of user B according to the certificate ID in the decentralized PKI based on the blockchain. When the certificate is verified as correct, user A makes a communication request, encrypts and sends their certificate ID to the user B. Because the SNR system will not check the correctness of ID-NA registration, that is, if there are malicious users, it is not guaranteed that the ID-NA registered for content resources is a valid content link, and the certificate verification in advance can ensure that it will not be linked to the phishing address and be attacked. At the same time, the certificate ID needs to be registered with the user ID in the SNR system to provide anchoring and query services for the user ID and the corresponding certificate ID.

During the initial interaction, there is no public key certificate between the communication parties. If the certificate ID is sent in clear text, the security of the information cannot be guaranteed. Therefore, SNR is responsible for issuing the certificate ID during the initial interaction. Here, user A represents the subscriber and user B represents the provider of services, which may be publishing or caching.

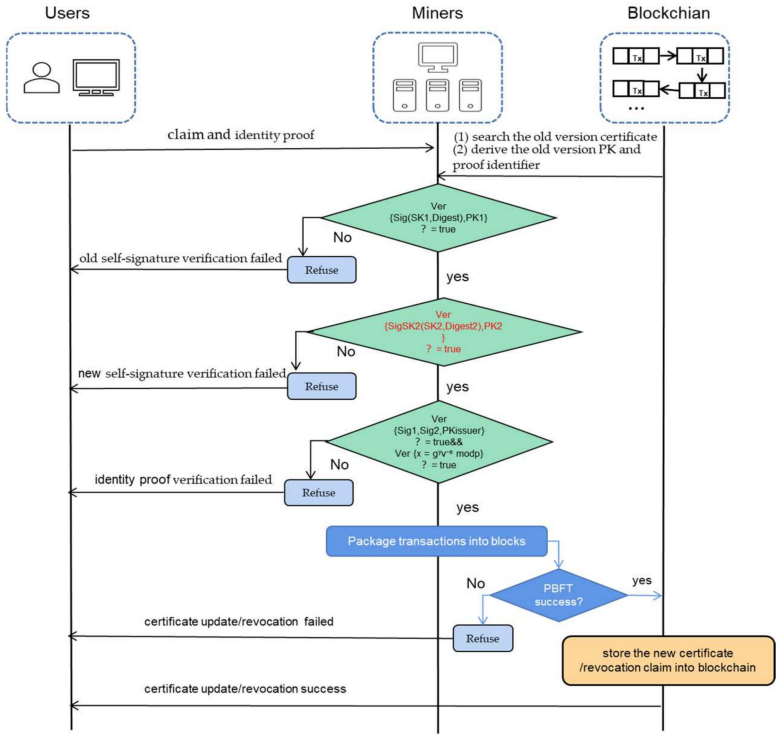

Figure 5. The verification process of updating and revoking claims.

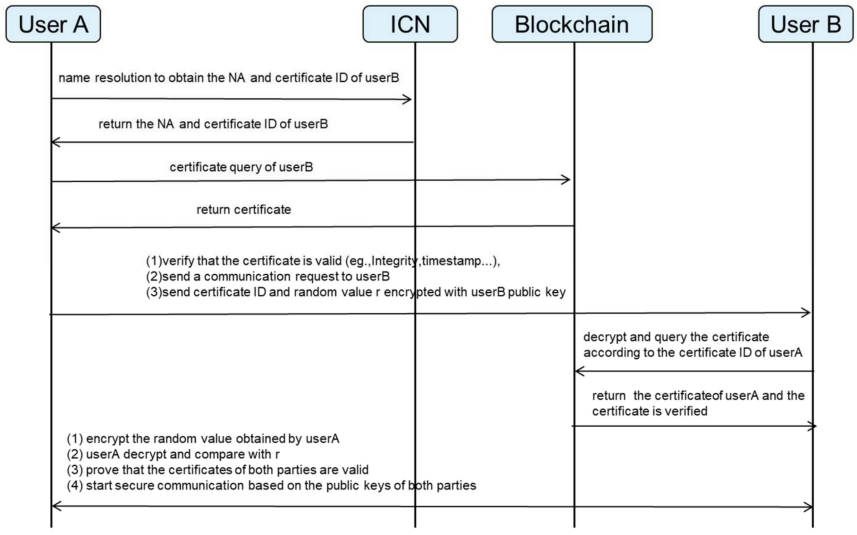

Figure 6. The process of the secure communication.

5. Security Analysis

According to the adversary model we proposed in Section 3.2, the security analysis is mainly interpreted according the following three perspectives: proof security, certificate security and communication security.

5.1. Proof Security

Since the consensus nodes are semi-trusted nodes and malicious adversaries may steal the proof P of legitimate users to fake the identity in the process of certificate registration, we discuss the security of our proof in three parts: zero-knowledge, to ensure the protection of privacy, completeness, to prove the rationality of the verifiable presentation of the proof and soundness, to explain the unforgeability of the proof, all of which are the security properties of zero-knowledge proof.

Completeness: As the secret value s is not disclosed, and the honest prover follows our protocol, the proof $\pi = \{x, Sig1, Sig2\}$ can be accepted by the honest verifier in the following checking list as Section 4.1. The verifier checks the issuer signature $Sig1$ and $Sig2$ according to the rules $(Sig2)Q = (k+ H (v||K||credential)^* SK_{issuer})Q = kQ + H(v||K||credential)^* (SK_{issuer}Q) = Sig1 + Hash(v||K||credential)^* PK_{issuer}$ and verifies the computed value of the x according to the rules $g^y v^{-e} = g^{+se} v^{-e} = g^{r+se} (g^s)^{-e} \ mod\ p = g^r mod\ p = x$. If the proof π passes successfully, s must be the shared secret value to calculate parameter v, and the verifier believes the prover knows the secret value s, which proves the identity of the prover.

Soundness: Based on the difficulty of solving discrete logarithm problems (DLPs), adversaries rarely forge the parameters x, $Sig1$, $Sig2$ without the secret s, private random k and SK_{issuer}, according to the rules in Section 4.1. Therefore, the proof π remains secret and hidden, which means that after the prover publishes the proof π, the probability of changing the secret and generating the same proof is negligible. In addition, if the adversaries do not know the secret value s and the SK_{issuer}, they have little chance of guessing the proof π. Even if they steal the proof π of a legal prover, the timestamp ensures that they cannot launch replay attacks. Meanwhile, due to the rules that $P_i(n) \neq P_i(n + 1)$, provers can generate different proofs given at random r, which ensures that they can regenerate new proof and timestamps when a proof is stolen. These rules prevent adversaries from using an old proof to impersonate legal identities. Therefore, our protocol provides the property of soundness.

Zero-knowledge: During the whole protocol, the verifier does not have any further information other than proof π. The secret value s and other unnecessary private data are not revealed. The prover does not interact with the verifier and the prover can convince the verifier that they knows s without revealing knowledge of s according to the verification rules, which proves the zero-knowledge of our scheme.

Therefore, the authentication presentation using zero-knowledge proof is secure as an identity proof and also provides further security for the following certificate generation and management process.

5.2. Certificate Security

In the previous sub-section, we proved the security and unforgeability of the verifiable presentation as identity proof. Additionally, malicious adversaries will attempt to steal the certificates or the private keys of legitimate users to forge the identity of legitimate users in the process of data exchange. Since the identity proof is unforgeable, even if a user's private key is lost or stolen, an old certificate can be revoked and regenerated with the identity proof. Therefore, adversaries cannot forge a user's self-signed certificate by stealing and replaying, which ensures the security of the certificate in the process of data exchange. In the revocation and update phase, we designed two guarantees: identity and old version ownership verification, which makes it difficult for the adversaries to tamper with the user certificate on the blockchain.

5.3. Communication Security

In order to ensure the security of communication, we register the certificate ID in the SNR system along with the network address, because the hash name of the certificate ID must be reliable as the validation proof to prove the integrity of the certificate. After that, users can conduct further certificate interaction and prove their ownership of the private key through the nonce challenge. Asymmetric encryption guarantees the security

of the remaining steps. If one party is a fake user, they cannot pass the nonce challenge of authentication, which ensures the security of communication security in our scheme.

6. Experiments and Performance

The experiments of our scheme are deployed based on an open-source blockchain platform called FISCO BCOS [47,48]. This platform includes many features, such as security, reliability and scalability. Our implementation consists of two parts. One is smart contract algorithms based on the blockchain. The smart contracts should implement basic functions consisting of registering transactions and retrieving data on the blockchain. The other is the implementation of verification functions for cryptography calculations which do not include smart contracts, such as proof and signature verification. The blockchain we chose features Java SDK, offering APIs for developers to program through the Java SDK, providing parameters for the smart contract and the calling of the functions implemented by smart contracts, which is shown as Figure 7. Therefore, we first used register and query smart contracts to implement the basic functions with respect to the blockchain and then wrote a Java application to complete the entire experiment as required.

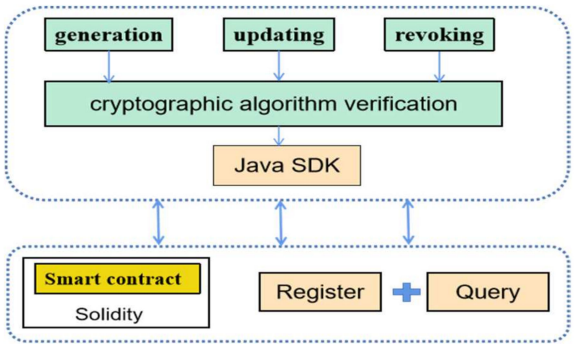

Figure 7. The experimental scheme.

Because it is possible to deploy several different nodes on the same server for a test chain, we used a Linux server to deploy nodes. The CPU of this server possesses a dual physics core and eight logical cores with an Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz on each core. The memory was 64 GB. We ran 10 test cases for every experiment to obtain average results. The communication link delay was set as 100ms. The consensus algorithm employed in our experiments was PBFT.

We first investigated the delay of the registration phase under the CL signature and our proposal. As presented in Figure 8, it is obvious that the verification of the CL signature takes longer, which delays the certificate registration. With an increase in the number of credential claims that need to be verified in verifiable presentations, the advantages of the Schnorr signature become clearer. On average, the proposed scheme saves about 20% in terms of the registration delay compared to the Cl signature in the context of multiple claim verification.

Then we counted the delay of the registration phase under different numbers of consensus nodes. The results are presented in Figure 9, in which it is possible to see how the delay increases along with the blockchain height and more consensus nodes, which is because more time is required to ensure consistency and reach a consensus.

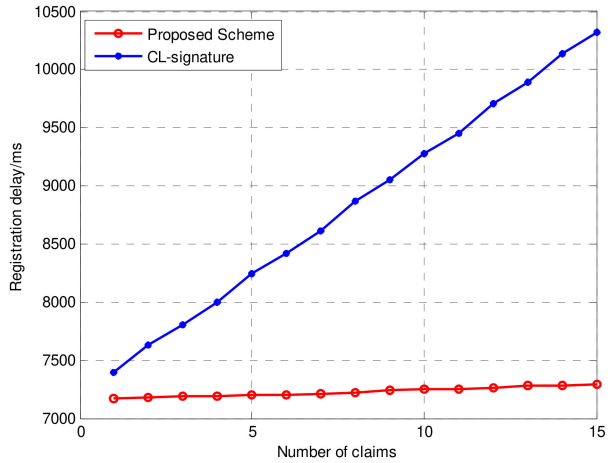

Figure 8. The delay in certificate registration for multiple claims.

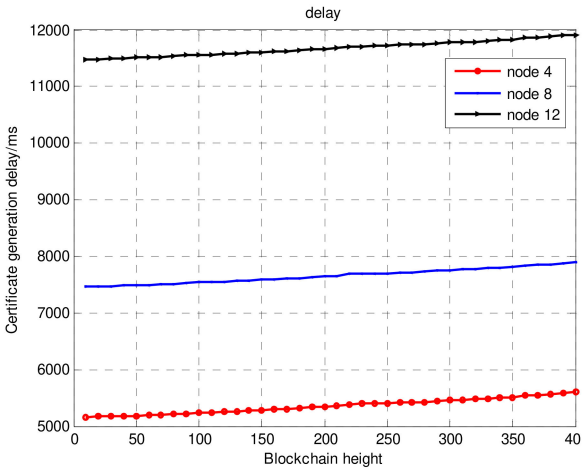

Figure 9. The registration phase delay under different numbers of nodes.

Finally, we focused on the query delay, updating delay and revoking delay of certificates. The number of consensus nodes was eight. Meanwhile, since the certificate query was based on the blockchain distributed database and the query will not have been concentrated on one node, we assumed that there would be no waiting delay by default. As shown in Figure 10, the query time for certificates increase rapidly along with the blockchain height. This is because the increase in data size of distributed ledger slows down the query traversal time, which may be a challenge faced by all blockchain-based decentralized PKIs. Therefore, the optimization of the certificate query delay will be discussed in detail in future research by our groups. Figure 11 shows the updating and revoking delays for certificates. Due to the influence of the query delay, the delays in terms of update and revocation were also longer.

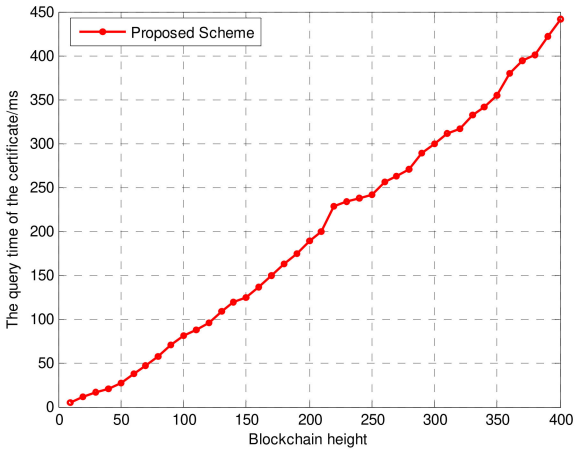

Figure 10. The query time for certificates.

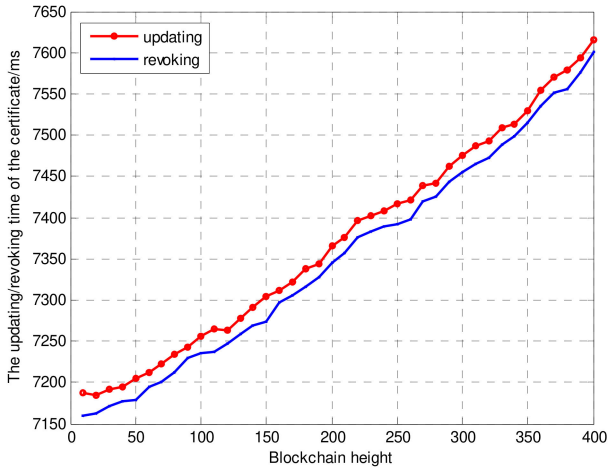

Figure 11. The updating and revoking delays for certificates.

7. Conclusions

In this paper, a complete decentralized PKI scheme was presented by combining the DID, verifiable credentials project and blockchain. We designed an optimized zero-knowledge proof verifiable representation scheme, so that users can prove their real-world identities without undermining their privacy. We complete the binding of the identity with the public key certificates and realize the certificate generation and certificate management through the blockchain. Meanwhile, we also provided the application of the decentralized certificates in ICN secure communication and discussed the security and basic performance of the whole scheme.

Meanwhile, there are still some limitations of current work in terms of in-depth research on the integration of ICN and DPKI. Using the characteristics of the ICN, the blockchain can sink various technologies into the network. In addition, the query time for certificates increased rapidly along with the blockchain height, which may be a challenge faced by DPKI. Therefore, in future work, we hope to apply the scheme to a practical project and, on this basis, we will optimize our scheme in terms of certificate efficiency, storage and queries by using additional characteristics of ICN networks, such as caching, routing, etc. The discovery and certificate revocation of malicious nodes, as well as blacklist synchronization, will also be discussed by our groups in future work.

Author Contributions: Conceptualization, J.S. and R.H.; data curation, J.S.; formal analysis, J.S.; funding acquisition, R.H. and X.Z.; investigation, J.S.; methodology, J.S., R.H. and X.Z.; software, J.S.; supervision, X.Z.; validation, J.S.; writing—original draft, J.S.; writing—review and editing, R.H. and X.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by SEANET Technology Standardization Research System Development (Project No. XDC02070100).

Data Availability Statement: Not applicable, as the study does not report any data.

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

References

1. Proof-of-Concept for Data Service Using Information Centric Networking in IMT-2020. Available online: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13655 (accessed on 20 May 2020).
2. Xylomenos, G.; Ververidis, C.N.; Siris, V.A.; Fotiou, N.; Tsilopoulos, C.; Vasilakos, X.; Katsaros, K.V.; Polyzos, C.G. A survey of information-centric networking research. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 1024–1049. [CrossRef]
3. Koponen, T.; Chawla, M.; Chun, B.-G.; Ermolinskiy, A.; Kim, K.H.; Shenker, S.; Stoica, I. A data-oriented (and beyond) network architecture. In Proceedings of the ACM SIGCOMM 2007 Conference, Kyoto, Japan, 27–31 August 2007.
4. Jacobson, V.; Smetters, D.K.; Thornton, J.D.; Plass, M.F.; Briggs, N.H.; Braynard, R.L. Networking Named Content. In Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies, Rome, Italy, 1–4 December 2009; pp. 1–12.
5. Zhang, L.; Afanasyev, A.; Burke, J.; Jacobson, V.; Claffy, K.; Crowley, P.; Papadopoulos, C.; Wang, L.; Zhang, B. Named data networking. *ACM SIGCOMM Comput. Commun. Rev.* **2014**, *44*, 66–73. [CrossRef]
6. Ohlman, B.; Karl, H.; Ahlgren, B.; Farrell, S.; Dannewitz, C.; Kutscher, D. Network of Information (NetInf)—An information-centric networking architecture. *Comput. Commun.* **2013**, *36*, 721–735.
7. Wang, J.; Cheng, G.; You, J.; Sun, P. SEANet: Architecture and Technologies of an On-site, Elastic, Autonomous Network. *J. Netw. New Media Technol.* **2020**, *9*, 1–8. (In Chinese)
8. Chen, Z.; Meng, H.W.; Guan, Z. Research on intrinsic security in future internet architecture. *J. Cyber Secur.* **2016**, *1*, 10–13.
9. Housely, R. Public key infrastructure (PKI). In *The Internet Encyclopedia*; John Wiley & Sons: Hoboken, NJ, USA, 2004.
10. Wu, J.; Dong, M.; Ota, K.; Li, J.; Yang, W.; Wang, M. Fog-Computing-Enabled Cognitive Network Function Virtualization for an Information-Centric Future Internet. *IEEE Commun. Mag.* **2019**, *57*, 48–54. [CrossRef]
11. Fayazbakhsh, S.K.; Lin, Y.; Tootoonchian, A. Less Pain, Most of the Gain: Incrementally Deployable ICN. *ACM SIGCOMM Comput. Commun. Rev.* **2013**, *43*, 147–158. [CrossRef]
12. Burke, J.; Horn, A.; Marianantoni, A. *Authenticated Lighting Control Using Named Data Network*; NDN Technical Report NDN-0011; UCLA: Los Angeles, CA, USA, 2012.
13. Ahlgren, B.; D'Ambrosio, M.; Marchisio, M.; Marsh, I.; Dannewitz, C.; Ohlman, B.; Pentikousis, K.; Strandberg, O.; Rembarz, R.; Vercellone, V. Design considerations for a network of information. In Proceedings of the 2008 ACM CoNEXT Conference, Madrid, Spain, 9 December 2008; pp. 1–66.
14. Abidi, A.; Gammar, B.; Kamoun, W. Memory Management Optimization for Content Routers in DONA. In Proceedings of the 2015 IEEE 14th International Symposium on Network Computing and Applications, Cambridge, MA, USA, 28–30 September 2015; pp. 85–89.
15. Sporny, M.; Noble, G.; Longley, D.; Zundel, B. Verifiable Credentials Data Model 1.1. W3C Rec. Available online: https://www.w3.org/TR/vc-data-model/#presentations (accessed on 9 November 2021).
16. Yu, Y. *Public Key Management in Named Data Networking*; Technical Report; UCLA: Los Angeles, CA, USA, 2015.
17. Mauri, G.; Verticale, G. Up-to-date key retrieval for information centric networking. *Comput. Netw.* **2017**, *112*, 1–11. [CrossRef]
18. Li, R.D.; Asaeda, H.; Li, J. A distributed authentication and authorization scheme for in-network big data sharing. *Digit. Commun. Netw.* **2017**, *3*, 226–235. [CrossRef]
19. Hamdane, B.; Serhrouchni, A.; Fadlallah, A.; Fatmi, S.G.E. Named-Data security scheme for Named Data Networking. In Proceedings of the 2012 Third International Conference on The Network of the Future (NOF), Tunis, Tunisia, 21–23 November 2012; pp. 1–6.
20. Yu, Y.; Afanasyev, A.; Zhu, Z. *An Endorsement-Based Key Management System for Decentralized NDN Chat Application*; Technical Report NDN-0023; UCLA: Los Angeles, CA, USA, 2014; Available online: https://named-data.net/publications/techreports/ndn-tr-23-chronochat-security/ (accessed on 22 July 2014).
21. Lou, J.; Zhang, Q.; Qi, Z. A Blockchain-based key Management Scheme for Named Data Networking. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018; pp. 141–146.
22. Schutze, B.; Kammerer, M.; Klos, G.; Mildenberger, P. The public-key-infrastructure of the radiological society of Germany. *Eur. J. Radiol.* **2006**, *57*, 323–328. [CrossRef] [PubMed]

23. Papageorgiou, A.; Loupos, K.; Mygiakis, A.; Krousarlis, T. DPKI: A Blockchain-Based Decentralized Public Key Infrastructure System. In Proceedings of the 2020 Global Internet of Things Summit (GIOTS), Dublin, Ireland, 3–5 June 2020.
24. Chu, Y.; Kim, J.M.; Lee, Y.; Shim, S.; Huh, J. SS-DPKI: Self-Signed Certificate Based Decentralized Public Key Infrastructure for Secure Communication. In Proceedings of the 2020 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 4–6 January 2020.
25. Liu, Y.; Lu, Q.; Paik, H.-Y.; Xu, X.; Chen, S.; Zhu, L. Design pattern as a service for blockchain-based self-sovereign identity. *IEEE Softw.* **2020**, *37*, 30–36. [CrossRef]
26. Ferdous, M.S.; Chowdhury, F.; Alassafi, M.O. In search of selfsovereign identity leveraging blockchain technology. *IEEE Access* **2019**, *7*, 103059–103079. [CrossRef]
27. Reed, D.; Sporny, M.; Longley, D.; Sabadello, M.; Steele, O.; Allen, C. Decentralized Identifiers (DIDs) v1.0. W3C Working Draft. Available online: https://www.w3.org/TR/did--core/ (accessed on 25 August 2021).
28. Sporny, M.; Longley, D. Verifiable Claims Data Model and Representations 1.0. Available online: https://www.w3.org/2017/05/vc-data-model/CGFR/2017-05-01/ (accessed on 1 May 2017).
29. Maram, D.; Malvai, H.; Zhang, F.; Jean-Louis, N.; Frolov, A.; Kell, T.; Lobban, T.; Moy, C.; Juels, A.; Miller, A. CanDID: Can–Do Decentralized Identity with Legacy Compatibility, Sybil–Resistance, and Accountability. In Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 24–27 May 2021; pp. 1348–1366.
30. Yoon, D.; Moon, S.; Park, K.; Noh, S. Blockchain–based Personal Data Trading System using Decentralized Identifiers and Verifiable Credentials. In Proceedings of the 2021 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, 20–22 October 2021; pp. 150–154.
31. Wang, X.; Qiu, W.; Zeng, L.; Wang, H.; Yao, Y.; He, D. A credible transfer method of cross–chain assets based on DID and VC. In Proceedings of the 2021 IEEE 4th International Conference on Information Systems and Computer Aided Education (ICISCAE), Dalian, China, 24–26 September 2021; pp. 238–242.
32. Alzahrani, B. An information-centric networking based registry for decentralized identifiers and verifiable credentials. *IEEE Access* **2020**, *8*, 137198–137208. [CrossRef]
33. Alzahrani, B.A. Self–protected content for information–centric networking architectures using verifiable credentials. *Telecommun. Syst.* **2022**, *79*, 387–396. [CrossRef]
34. Otto, N.; Lee, S.; Sletten, B.; Burnett, D.; Sporny, M.; Ebert, K. Verifiable Credentials Use Cases. W3C Working Group Note. Available online: https://www.w3.org/TR/vcuse--cases/ (accessed on 19 September 2019).
35. Chadwick, D.; Longley, D.; Sporny, M.; Terbu, O.; Zagidulin, D.; Zundel, B. Verifiable Credentials Implementation Guidelines 1.0. W3C Working Group Note. Available online: https://www.w3.org/TR/vc--imp--guide/ (accessed on 19 September 2019).
36. Brunner, C.; Gallersdörfer, U.; Knirsch, F.; Engel, D.; Matthes, F. DID and VC: Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust. In Proceedings of the 2020 the 3rd International Conference on Blockchain Technology and Applications, Xi'an, China, 14–16 December 2020.
37. Sporny, M.; Longley, D.; Chadwick, D. Verifiable Credentials Data Model 1.1. W3C Rec. Available online: https://www.w3.org/TR/vc--data--model/ (accessed on 9 November 2021).
38. Blum, M.; Feldman, P.; Micali, S. Non–interactive zeroknowledge and its applications. In Proceedings of the 20th Annual ACM symposium on Theory of computing (STOC '88), Chicago, IL, USA, 2–4 May 1988; pp. 103–112.
39. Sporny, M.; Longley, D.; Chadwick, D. Verifiable Credentials Data Model 1.1. W3C Rec. Available online: https://www.w3.org/TR/vc--data--model/#zero--knowledge--proofs (accessed on 9 November 2021).
40. Camenisch, J.; Lysyanskaya, A. A Signature Scheme with Efficient Protocols. IBM Research. Peer Reviewed Paper. Available online: https://www.researchgate.net/publication/220922101_A_Signature_Scheme_with_Efficient_Protocols (accessed on 19 March 2022).
41. W3C Credentials Community Group. BBS+ Signatures 2020. 2020. Available online: https://w3c--ccg.github.io/ldp--bbs2020/ (accessed on 19 March 2022).
42. Schnorr, C.P. Efficient identification and signatures for smart cards. In *Advances in Cryptology—Crypto '89*; Lecture Notes in Computer Science; Brassard, G., Ed.; Springer: New York, NY, USA, 1990; pp. 239–252.
43. Schnorr, C.P. Efficient signature generation by smart cards. *J. Cryptol.* **1991**, *4*, 161–174. [CrossRef]
44. Barakabitze, A.A.; Tan, X.; Tan, G. A survey on naming, name resolution and data routing in information centric networking (ICN). *Int. J. Adv. Res. Comput. Commun. Eng.* **2014**, *3*, 8322–8330. [CrossRef]
45. Sevilla, S.; Mahadevan, P.; Garcia-Luna-Aceves, J.J. FERN: A unifying framework for name resolution across heterogeneous architectures. *Comput. Commun.* **2015**, *56*, 14–24. [CrossRef]
46. Liao, Y.; Sheng, Y.; Wang, J. A deterministic latency name resolution framework using network partitioning for 5G–ICN integration. *Int. J. Innov. Comput. Inf. Control.* **2019**, *15*, 1865–1880.
47. FISCO BCOS, A Consortium Blockchain Platform. Available online: https://fisco--bcosdocumentation.readthedocs.io/en/latest/ (accessed on 19 March 2022).
48. FISCO BCOS Whitepaper. Available online: https://github.com/FISCO--BCOS/whitepaper/blob/master/README(EN).md (accessed on 19 March 2022).