



A Decentralized Public Key Infrastructure Based on Verifiable Random Function-Leader Election and Proof of Context and History over Solana Blockchain

Dena S. Alani^{1*}, Ali M Sagheer²

¹ College of Education for Women, University of Anbar, Ramadi 31001, Iraq

² Department of Computer Networks Systems, College of Computer Science and Information Technology, University of Anbar, Ramadi 31001, Iraq

Corresponding Author Email: edw.denasalim83@uoanbar.edu.iq

Copyright: ©2026 The authors. This article is published by IIETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijssse.160801>

ABSTRACT

Received: 29 April 2026

Revised: 23 July 2026

Accepted: 31 July 2026

Available online: 31 August 2026

Keywords:

certification authority, decentralized public key infrastructure, proof of history, proof of context and history, proof of stake, Solana, verifiable random function

Traditional public key infrastructure (PKI) is the cornerstone of internet communications, as the design of these infrastructures depends on centralized certification authorities (CAs) to manage digital certificates, despite the great role played by these authorities. It still represents a single point of trust. In this research, a new decentralized PKI system was proposed based on the Solana blockchain. The proposed system utilized a new mechanism for leader election based on a verifiable random function (VRF). The leader is treated as a temporary CA for managing the digital certificate lifecycle. Also, a new hash-controlled log for proof of context and history (PoCH) was proposed. Finally, a data warehouse was hired outside the chain to store the entire certificate while keeping its hash imprint on the chain. The results of the tests showed an improvement in the level of decentralization compared to the original leader selection mechanism in Solana, where the value of the Herfindahl-Hirschman Index (HHI) decreased from 0.1422 to 0.1115, while the value of Shannon Entropy increased from 3.0272 to 3.2393, indicating a more balanced distribution of opportunities for choosing leaders among validators. In addition, the comparison results showed that the ECC-based key generation mechanism using the P-256 curve achieved an average time of 0.000105 seconds compared to 0.077686 seconds in RSA-2048. The proposed system has also achieved high performance in terms of transaction productivity compared to other systems while maintaining a low latency, which enhances its ability to manage the certification process efficiently in large-scale environments.

1. INTRODUCTION

Public key infrastructure (PKI) is one of the basic pillars of electronic communications security, as it deals with identity verification mechanisms, non-repudiation, and data integrity through the use of digital certificates [1, 2]. However, the traditional PKI system is based on the employment of centralized certification authorities (CAs) representing a single central point of trust that takes over the task of issuing and revoking certificates [3]. Practical experiments have proven that this system suffers from structural problems, the most important of which are the transformability of CAs into a single point of failure, as well as the risks of abuse or penetration, in addition to the lack of transparency in the management of the certificate lifecycle, reports have also shown multiple incidents of unauthorized issuance of certificates by CAs trusted globally [4, 5].

Recently, the concept of blockchain has emerged as an alternative means of trust management in distributed systems due to its characteristics: transparency, decentralized consensus, and non-manipulability [6, 7]. This has led to the emergence of the concept of decentralized public key infrastructure (DPKI) based on blockchain technology, which

seeks to decrease or eliminate dependence on centralized CAs, replacing them with a distributed publicly auditable ledger for managing electronic identities and certificates [8, 9]. Many blockchain-based PKI systems have managed to eliminate the central point of failure, but they still depend on a specific group of nodes responsible for issuing or verifying certificates, which leads to a concentration of leadership among a specific number of nodes and limits the fairness of the distribution of responsibilities, as well as increases the risk of targeting and complicity. Also, some systems focus on recording the issuance and cancellation process without focusing on the entire certificate lifecycle, including issuance, cancellation, and renewal, in addition to not providing the possibility of tracking all events in an interconnected and verifiable manner. To address this research gap, this paper presents a new design DPKI system based on the Solana architecture that employ the selection of a dynamic leader using verifiable random function (VRF) with non-linear stake to distribute the temporary authority between the validators temporarily and fairly and also propose a new ledger for recording events that are not amenable to manipulation to record all events related to the certificate life cycle for maintaining an integrated historical record.

The research contributions of this paper can be summarized as follows:

- (1) Introducing a new integrated design for a DPKI system to address many of the limitations inherent in the traditional PKI structure.
- (2) Employing an improved mechanism for dynamic selection of authority based on VRF mechanism and non-linear stakes to ensure fairness of choice and distribution of authority.
- (3) Present a new ledger for Proof Context and History (PoCH) to document all events related to the life cycle of the digital certificate in a non-manipulable way.
- (4) Enhance system security and reduce network load by storing the certificate in an off-chain data warehouse while the certificate hash is stored on-chain.

The structure of this paper is organized as follows: Section 2 presents related work, while Section 3 explains PKI. Section 4 explains the concept of the blockchain Solana. The VRF mechanism was introduced in Section 5. Section 6 describes the proposed method in detail. Then, Section 7 is dedicated to presenting and discussing the results. The final Section of the paper was the conclusion.

2. RELATED WORKS

The traditional PKI architecture mainly relies on a CA, which creates concerns related to centralized trust, transparency, and digital certificate management. To improve certificate accountability, the Certificate Transparency (CT) system introduced auditable and traceable public logs for detecting unauthorized certificates [10]. Although CT improves transparency, it does not fundamentally remove dependence on centralized trust, which has motivated the development of blockchain-based DPKI approaches.

One direction replaces the CA with distributed blockchain-based identity and key management. A Hyperledger Fabric-based architecture stores device identities and public keys on a distributed ledger and manages identity-related operations through smart contracts [11]. Transaction validation is supported by ECDSA on the P-256 curve, while a multi-signature mechanism allows operations to be verified collectively rather than by a single entity. This architecture enables devices in an IoT network to verify identities without directly relying on a CA and provides an immutable record of identity-related operations. However, its consortium-based verification mechanism still depends on a limited set of trusted entities, resulting in a partially centralized form of identity management.

Blockchain has also been combined with the Web of Trust (WoT) to support decentralized public key management [12]. In this approach, public keys can be registered, updated, and revoked through consensus among trusted network nodes using PBFT. A dynamic cryptographic complex is further employed to improve public key validation efficiency and reduce the need to scan the entire blockchain. Although the framework provides an alternative to traditional PKI in distributed environments, its dependence on a group of trusted nodes means that complete decentralization is not achieved.

Another approach applies Ethereum to decentralized public key management in Information-centric networking (ICN) [13]. Public keys and related operations are stored on the blockchain through smart contracts, while an optimized zero-

knowledge proof and the decentralized identifier (DID) project are incorporated to improve transparency, privacy, and resistance to tampering. Users can directly validate data using public keys recorded on the blockchain, thereby reducing reliance on a CA. Nevertheless, the use of Ethereum introduces limitations related to block-generation time, consensus overhead, scalability, and the cost of executing smart contracts.

A more specialized decentralized public key management architecture, PKChain, replaces the CA with a distributed group of validators responsible for verifying, updating, and revoking public keys [14]. Public key records are stored on the blockchain to provide transparency, verifiability, and non-repudiation. Its Threshold Block Validation (TBV) mechanism requires a majority of validators to approve a key-registration request before it is added to the blockchain, while Aggregate Commitment Signature (ACS) is used to collectively sign and validate these operations. PKChain also adopts a PBFT-derived consensus mechanism to reduce communication overhead and improve efficiency. Despite these improvements, the system still relies on a limited validator group, which may introduce another form of centralized trust.

A blockchain- and WoT-based DPKI model further develops this distributed trust concept through a trusted network called Key-Ring [15]. Instead of depending on a single CA, certificate requests are verified by a group of trusted members, while certificate information and related operations are recorded on the blockchain. Ethereum Smart Contracts are used to demonstrate the feasibility of the proposed architecture. Although this design improves transparency and resistance to tampering, it remains affected by transaction delays, fees, scalability constraints, and relatively high computational costs compared with some modern high-performance blockchains.

More recent work has extended blockchain-based identity management to IoT environments by combining DIDs, verifiable credentials, and ZKP [16]. To improve energy efficiency and performance, the system adopts PoS and PBFT instead of PoW. Simulation results indicate an authentication time of approximately 250 milliseconds and a transmission rate of approximately 200 messages per second, while maintaining relatively low hardware power consumption. However, the framework does not provide sufficiently dynamic mechanisms for identity management and revocation when device states change or when devices move between networks.

As summarized in Table 1, existing blockchain-based PKI and DPKI studies demonstrate that distributed ledgers can reduce dependence on conventional CA-based architectures, but several limitations remain. Some approaches still rely on specific authoritative entities or restricted validator groups, creating new forms of centralization. Others depend heavily on smart contracts and therefore face transaction-cost and scalability constraints. In addition, large-scale performance, dynamic identity revocation, and efficient lifecycle management have not been adequately addressed in many existing solutions. These limitations indicate the need for a more decentralized and scalable DPKI architecture with secure verification mechanisms, lower operational overhead, and stronger support for dynamic certificate and identity lifecycle management.

Table 1. Comparison of the proposed system with the previous related works

Ref.	Consensus Mechanism	Type of Blockchain	CA Model	Smart Contracts Depend	Storage Model	Decentralization	Limitations of the Systems
[11]	PBFT	Hyperledger Fabric	Consortium	Medium	On-chain	Low	Relying on a specific group of trusted entities
[12]	PBFT	Blockchain and WoT	Distributed Trust	Low	On-chain	Medium	Needs a high connection load between nodes.
[13]	PoS	Ethereum	DID	High	On-chain	High	Poor scalability.
[14]	PBFT	Not specified	Threshold Validators	Medium	On-chain	Medium	High cost of smart contract
[15]	PoS	Ethereum	WoT	High	On-chain	High	Concentration of trust among a specific group
[16]	PoS and PBFT	Blockchain	DID	Medium	Hybrid	High	High transaction time, fees, and poor scalability
Proposed system	PoH, PoS, Tower PFT	Modified Solana	Dynamic Leader as CA	No	Hybrid	High	Not provide an effective dynamic mechanism for managing and revoking IDs and certificates.
							Improve decentralization.
							Using PoH reduce to a high connection load between nodes and improves fairness.

Note: proof of history (PoH); certification authority (CA); proof of stake (PoS); Practical Byzantine Fault Tolerance (PBFT); Web of Trust (WoT); decentralized identifier (DID)

3. BACKGROUND AND TECHNICAL FOUNDATIONS

The PKI has become an essential element of cybersecurity necessary for securing and transmitting information and communications over the internet [17, 18]. The main function of PKI is to link the digital identity of an entity to its public key through a digital certificate signed by a trusted central CA, which ensures the confidentiality and integrity of data and verifies the identity of the communicating parties [19]. Despite PKI's effective role in many applications, its reliance on a centralized architecture has made it vulnerable to many risks related to single points of failure and abuse of centralized trust, which has spurred a trend towards more decentralized models to address these challenges.

Solana is one of the public blockchain high-performance platforms [20, 21]. It is distinguished from the rest of the platforms by its engineering design, which relies on the use of a new consensus mechanism called the proof of history (PoH) mechanism, in addition to PoS, to provide a chronological order of events within the network, verifiable by the rest of the validators [22]. Despite this, some studies have pointed out that there are some of the challenges faced by Solana, including the possibility of concentration of authority among validators with large stakes due to reliance on stakes in choosing the leaders' schedule [23]. Moreover, the leader table is predefined for time periods, which reduces the level of randomness in the leader selection mechanism compared to selection methods based on VRF, which affects the decentralization of the network [24].

VRF is one of the important modern encryption tools that seeks to achieve a secure, reliable, and achievable random selection in decentralized systems [25, 26]. The basic concept of this function is using the private key to generate a random value associated with a specific input, with the production of proof verifiable by any party using the public key without the need to disclose the private key [27, 28]. These functions were characterized by important security features, most notably ensuring a single output for each input and the unpredictability of outputs before calculating them. The possibility of public verification makes them the most suitable for applications that require transparency and resistance to manipulation [29].

Many blockchain networks utilize VRF in the methods of selecting leaders or committees, achieving a balance in the choice between randomness and fairness, because it provides a reduction in the likelihood of bias or centralized control compared to mechanisms of traditional selection [30, 31].

4. THE PROPOSED DECENTRALIZED PUBLIC KEY INFRASTRUCTURE SYSTEM

The proposed system is a construction of an integrated DPKI system based on Solana blockchain technology, with fundamental improvements aimed at addressing the limitations associated with centralization, performance efficiency, and scalability. Figure 1 shows the architecture of the proposed system; it consists of four functional layers. In the first layer, the user generates his/her keys Public (PU) and Private (PR) keys utilizing the ECC algorithm on the National Institute of Standards and Technology (NIST) P-256 curve, so that this pair consists of a random PR key with a length of 256 bits and PU derived from it. Later, the PR is utilized with the ECDSA algorithm to sign CSR. While PU is included in the CSR.

Then, creates the transaction of one of these certification functions: issue, renew, or revocation of a certificate. and send to the system. The second layer (services layer of DPKI) receives the transactions of users to verify the PoP and CSR of users and puts the request in the memory pool. In the third layer, the proposed system designs a combination of four main components: VRF-Based Leader Election mechanism, PoH mechanism, Validators, as well as a contextual documentation mechanism, PoCH log. In the VRF-Based Leader Election, to reduce the impact of large stakes and achieve distributive justice, the VRF-based selection mechanism and non-linear stakes are used as a leader selection mechanism instead of Solana's leader schedule. In this mechanism, each validators generates a verifiable random value using its own key, the current slot ID and the hash value of the previous block, then the result is compared with a threshold derived from applying the probability of the non-linear stake to the validators using square root, and as a result of this comparison produces a set

of candidates, among these candidates the candidate with the smallest random value was selected as leader. It ensures randomness and inability to predict, with the ability to ensure the correctness of the choice. The elected leader of this slot represents the temporary CA.

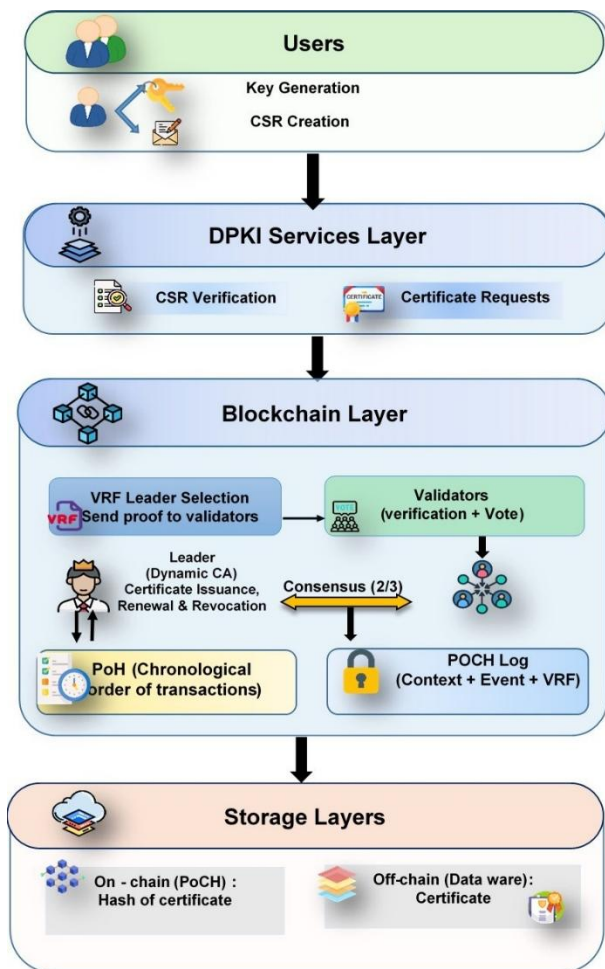


Figure 1. The architecture of the proposed decentralized public key infrastructure (DPKI) system

The tasks of each temporary CA are listed as follows:

- (1) Collecting the transactions of users.
- (2) Arranging transactions chronologically using PoH.
- (3) Verifying the validity of transactions.
- (4) Broadcasting the block to validators.
- (5) Issues, revokes, or renews the certificate after receiving a vote of 2/3 from the validators.

The second component of this layer is PoH, where the proposed system employs Solana's original PoH, which is a hash algorithm used as an encrypted time clock in the network that provides a chronological order of transactions; issue, revokes, or renews the certificate, verifiable by generating a sequential hash chain. So that each output depends on the previous one in such a way as to prevent arrangement manipulation or speed up time. This mechanism also allows network validators to check the chronological order of transactions without the need for intensive communication between the validators. The other essential component of the third layer is the validators, where the validators play a major role in verifying the validity of transactions and maintaining the integrity of the record. After completing the selection process, the leader (Dynamic CA) performs its main tasks, which are to compile transactions and arrange them

chronologically using PoH and then send them to validators, after which the validators take over the process of verifying the authenticity of transactions at several stages, including:

verifying the digital signature of the transaction and verifying the authenticity of CSR in addition to verifying PoP. After the verification process, the validators conduct a collective vote according to the principle of a supermajority (2/3) to add or reject the block. This approach seeks to strengthen trust and its distribution among a large number of validators in the network, which contributes to strengthening the system's resistance to attacks. At the end of the third layer, a new contextual record called PoCH was introduced, which is like an extension of the traditional PoH mechanism.

The PoH mechanism is a cryptographic synchronization mechanism used in the Solana blockchain to determine the order of transactions before reaching consensus. It works by generating a continuous chain of hashes, where each hash builds upon the previous one, creating a verifiable timeline. Transactions are inserted into this hash chain, allowing validators to verify when and in what order events occurred. This reduces the amount of communication required between validators and significantly improves the network's speed and scalability. The PoH mechanism works in conjunction with the PoS mechanism, helping Solana achieve high transaction throughput and low latency.

But it is worth noting that PoH is limited to arranging transactions chronologically, while PoCH added a documented contextual record of all events in the network, including the identity of the leader and proof of the correct choice of transaction type; issue, revoke, renew, and verify, as well as linking it to the hash of the previous record to ensure that the record could not be manipulated. It also allows the rest of the nodes in the network to fully verify the context and sequence of events. Thus, this new type of integration turned the registry into a reliable source within the system for supporting administrative processes. The last layer of the proposed system is the storage layer; in order to achieve a balance between performance and storage and reduce the burden on the network, the system adopts a hybrid storage model that combines on-chain and off-chain storage. The hash of the certificate is stored only on the blockchain to ensure its integrity, while the full certificate is kept in an external data warehouse. This design contributes to reducing the volume of data on the chain and improving overall performance, while maintaining the possibility of validating certificates by comparing hashes.

Therefore, these parts are integrated among themselves to work harmoniously, forming a decentralized infrastructure system that aims to achieve a balance between the main requirements: decentralization, security, and speed of performance by distributing trust among validators without the need for a specific central authority while ensuring complete transparency and auditability. Moreover, the proposed system combined modern encryption algorithms with Solana's high-performance blockchain, which made it suitable for practical application in systems requiring reliable and scalable management of digital identities.

4.1 Verifiable Function-based leader election mechanism

In this research, the leader selection mechanism was developed by replacing the leader schedule in Solana with a VRF-based dynamic selection method to assign the role of the winning leader for each slot in the next stage to the Dynamic

CA. The proposed method is based on combining the concept of VRF with nonlinear normalization of the stake using the square root in order to achieve a more equitable distribution of leadership opportunities and reduce the effect of centralization associated with a large share among validators. The stages of the proposed method were carried out as follows:

(1) Key Generation

Let to be the set of validators $V = \{v_1, v_2, \dots, v_m\}$, where each v_i has:

The Stake (s_i).

VRF key pairs are generated using the ECVRF on the SECP256k1 curve with SHA-256 as follows:

$$(sk_i, pk_i) \leftarrow ECC.GenerateKey \quad (1)$$

where,

sk_i : represents validator secret key (kept secret).

pk_i : represents the validator's public key (it is published in the network so that others can verify VRF results).

After which, the following steps are performed by each validator in each slot.

(2) Derivation of the slot

At the beginning of each slot, the VRF seed is re-derived from the hash of the previous block and the index of the slot to ensure unpredictability and temporal independence for the slots.

$$Seed_t = H(B_{t-1} \parallel t) \quad (2)$$

where,

$Seed_t$: Seed of slot t .

B_{t-1} : Hash of previous block.

t : Index of current slot.

(3) Computation of non-linear weight of the stake

To decrease the excessive impact of large stakes, the square root function was utilized to process the original stake of each validator as follows:

$$w_i = \sqrt{s_i} \quad (3)$$

where, w_i : represents the nonlinear weight of the stake; s_i : represents the original stake of v_i .

Such processing helps to reduce the large gap between large and small validators while maintaining the correlation of selection with the stake factor. Then the sum for the nonlinear weights of all the validators is computed as follows:

$$W = \sum_{i=1}^m w_i \quad (4)$$

where,

W : represents the summation of the nonlinear weight of the stake.

(4) Computing the probability distribution with non-linear stake

After computing the nonlinear weights, they are normalized to obtain a valid probability distribution for the leader selection:

$$P_i = w_i / W \quad (5)$$

where,

P_i : represents the probability of selecting v_i as leader.

(5) Computation of Verifiable Function output

Each v_i computes VRF output locally utilizing $seed, sk, index\ of\ slot\ (t)$ as follows:

$$VRF_{ski}(seed_t) \rightarrow (y_i, \pi_i) \quad (6)$$

where,

y_i : represent as semi random output. π_i : a proof represents an actual result of applying VRF on S_i utilizing sk_i .

(6) Converting output of Verifiable Function to the standard value

To eliminate dominance and achieve stakes-related justice, the VRF output is converted to a standard value r_i [0,1) as the following:

$$r_i = \text{int}(H(y_i)) / 2^\lambda \quad (7)$$

where,

r_i : represents a real value $\in [0,1)$. λ : represents the length of the hash output in bits.

(7) Eligibility test

Then, for each node, the driving eligibility threshold is defined according to a basic probability: The v_i is qualified if: $P_i > r_i$; this test results in a set of candidates C as follows:

$$C_t = \{v_i \in V : P_i > r_i\} \quad (8)$$

where,

C_t : represents a set of candidates.

(8) Rules of the leader selection

In case the candidates' set is not empty, the leader(L) is selected as the owner of the smallest r_i inside the candidate list.

$$L = \text{MIN}arg_i(r_i) \quad (9)$$

This mechanism is adopted to ensure that the selection process for each slot is a random process that is not predictable in advance and, at the same time, publicly verifiable by all participants. Algorithm 1 outlines the procedures used to obtain the VRF-Based Leader Election Mechanism.

Algorithm 1: VRF-based leader election mechanism

Inputs: $V = \{v_1, v_2, \dots, v_m\}$, $S = \{s_1, s_2, \dots, s_m\}$, t , B_{t-1} .

Output: The selected validator as leader.

Step 1: Compute seed

$Seed_t = H(B_{t-1} \parallel t)$

Step 2: Compute the non-linear weight of the stake

Loop $i = 1$ to m *do*

$w_i = \text{sqrt}(s_i)$

Step 3: Compute the sum of nonlinear weights

$W \leftarrow \sum w_i$

Step 4: Compute probability distribution with non-linear stake

4.1: For $i=1$ to m *do*

4.2: Compute non-linear stake weight

$P_i = w_i / W$

4.3: Compute VRF output and proof

$VRF_{ski}(seed_t) \leftarrow (y_i, \pi_i)$

4.4: Converting the output of VRF

$r_i \leftarrow \text{int}(H(y_i)) / 2^\lambda$

4.5: Test eligibility

IF $r_i < P_i$

$\text{Candidate_set} \leftarrow \text{Candidate_set} \cup \{(v_i, r_i, \pi_i)\}$

Step 5: Leader selection

IF $\text{Candidate_set} = \{\}$ *then*

Else
Slected Leader $\leftarrow$ full back rule

Selected Leader $\leftarrow \min \arg_i(r_i)$

Step 6: *Selected leader broadcast:* (seed, pk_L , y_L , π_L)

Step 7: Network Verification

True $\leftarrow \text{Verify } pk_i(\text{seed}, y_i, \pi_i)$

Step 8: Return: Accept selected leader for slot.

4.2 Dynamic certification authorities trust chain

The traditional PKI and several blockchain-based PKI systems are based on a single CA or a specific group of validators which management the systems and affect the concept of decentralization. In the proposed system, there is no fixed CA. The system suggests that the dynamically elected slot leader assumes the role of CA for the duration of the slot. The slot leader is selected using a selection mechanism based on VRF and non-linear stakes of validators, as this mechanism ensures the fairness of the choice and the possibility of verification by all participants. After the election and assuming the role of CA, the leader has the authority to manage the digital certificate and sign it after the vote and approval of the vast majority of validators, where all certificate management processes are subject from issuance, cancellation and renewal to the approval of the super majority, the leader plays the role of the executive CA within the current slot, while trust remains distributed among all auditors, which eliminates the individual point of failure and reliance on one centralization CA and contributes to achieving a higher level of transparency and decentralization.

After the leader selection process is completed, the public key and its CA certificate are published in the Leader_Public Key_Registry to be available to all participants in the network. Then the leader authorization event is registered in the PoCH log through the leader_Authorized event, which includes: leader (Leader-ID, the slot number, the hash of the leader's public key, and the VRF output& proof, where the selected leader information becomes part of the PoCH ledger. The selected leader performs his tasks of collecting transactions and arranging them chronologically using PoH and sending them to the auditors, and after the approval of the auditors, the certificate is issued, where the leader signs the certificate using his private key, as in the following formula. Then the identity of the leader and the time slot number from which the certificate was issued are included inside the certificate X.509.

To verify the reliability of the certificate issued by the commander to the client, the client performs the following actions:

Comparison of the certificate hash value with the hash value stored on the network.

Checking that the Certificate Status Record matches the last registered event in PoCH.

Verification of the authenticity of the signature of the certificate using the public key published on the network belonging to the issuing leader.

In the event of a mismatch of any of the previous steps, the certificate is considered incorrect and unreliable. In this system, trust is not granted to the leader himself, but is based on a series of successive encryption operations. In the event of a malicious leader issuing an incorrect certificate, a mismatch between any of the verification steps mentioned will lead to a certificate refusal. The malicious leader responsible for issuing fake certificates can be identified through the L_i registrar in PoCH and excluded from future leader selection processes.

4.3 Integrating proof of context and history into Solana

In this step, PoCH was presented as the second style of modifications of the architecture of the blockchain Solana, after replacing the leader schedule mechanism with the proposed VRF-based leader election mechanism. It is worth noting that PoH's work in the original Solana is limited to generating an encrypted chronological order of events and transactions in the form of a sequential hash chain. So, Solana lacks a contextual log that documents the context of the administrative events carried out by the leader. To address this shortcoming and create a suitable work environment for DPKI, PoCH has been proposed as an additional log layer that seeks to document the entire context of the events. It can be described as a non-manipulable historical record that is proposed and designed specifically to document and manage the entire life cycle of a digital certificate within the proposed system, as it contributes to recording all events related to the digital certificate, such as issuance, verification, cancellation, and rotation in the form of a series of interrelated events whose integrity can be checked later. The historical record provides the possibility of tracking all events of the certificate life cycle in an interconnected and verifiable way while maintaining the integrity of the record with the possibility of detecting any manipulation or change in its content. The PoCH acts as a supplementary record documenting who performed the event, under what authority, and within any time frame; thereby, it provides a non-manipulable, verifiable record that contributes to documenting contextual events related to the role of the leader and the events related to certificates. Algorithm 2 outlines the procedures of PoCH Ledger. PoCH Ledger adds a security layer that goes beyond what traditional blockchain logs or Certificate Transparency Logs provide, as it not only records the result of the work, but also records the entire context in which the operation took place.

Algorithm 2: PoCH record generation and validation

Input: Transaction (T_x), SL_i , L_i , y_i , π_i , $H(\text{PoCH}_{i-1})$, PoH, validator-votes (vv), Total Number of validators (m).

Output: PoCH_Record, Status.

Step 1: $T_x_H \leftarrow H(T_x)$

Step 2: For each validator do

2.1: Verify leader election

IF Verify (L_i , Pk_i , y_i , π_i) = True Then

2.2: Verify PoH ordering

IF Verify_PoH (PoH_H , T_x_H) = True Then

2.3: Transaction validation

IF Verify_Signature (T_x) = True Then

2.4: IF Verify_CSR_PoP (T_x) = True Then

2.5: vv $\leftarrow$ vv+1

Else Return Rejected

End For

Step 3: Check voting

IF vv < CEIL ($2/3 \times m$) Then

Return Rejected

Else Accept T_x .

Step 4: Create PoCH Commitment

Commitment $\leftarrow H(T_x \parallel T_x_H \parallel \text{PoH} \parallel SL_i \parallel L_i \parallel y_i \parallel \pi_i \parallel (\text{Commitment}_{i-1}))$.

Step 5: Create PoCH Record

PoH_Record $\leftarrow \{\text{Seq}, T_x, T_x_H, \text{PoH}, SL_i, L_i, y_i, \text{Previous_Commitment},$

Commitment, Status = Finalized}

Step 6: Append record to ledger

Append (PoCH_Ledger, PoCH_Record)

End.

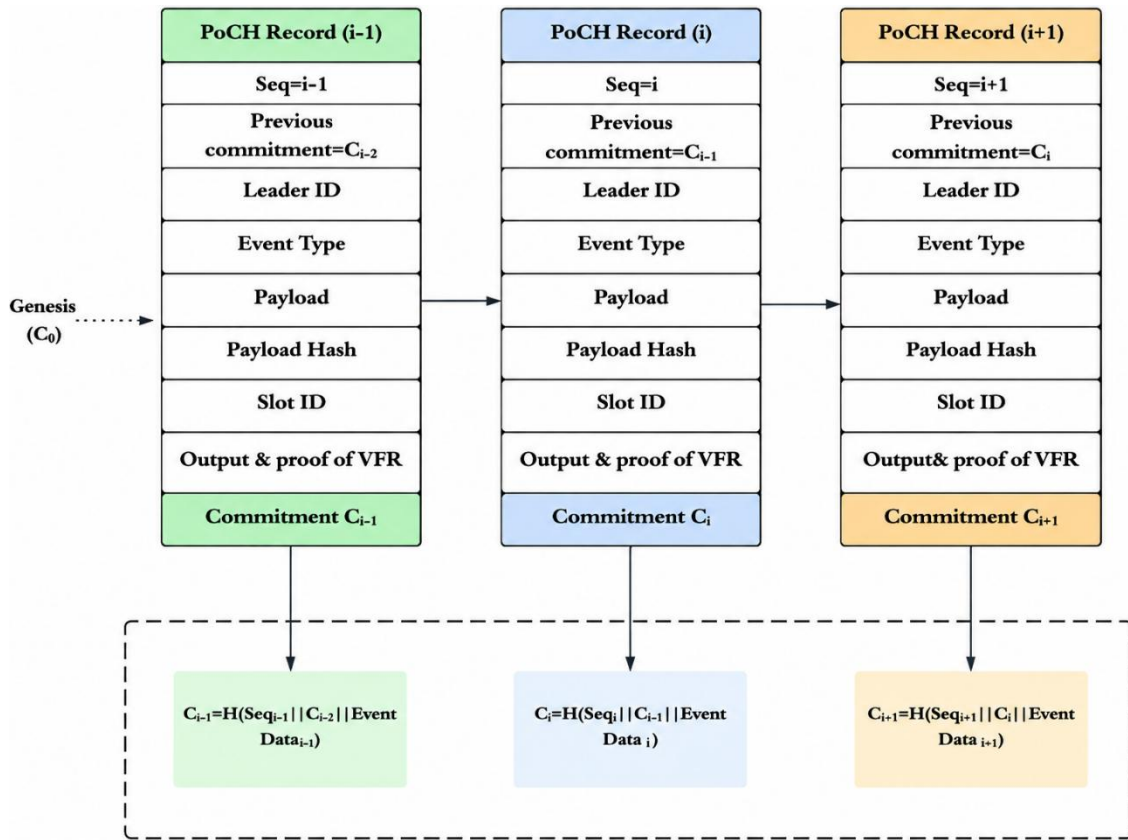


Figure 2. The structure of proof of context and history (PoCH) ledger

The difference between PoCH ledger and PoH is that PoH's main function is to provide a chronological order of transactions within the network by creating a series of verifiable hashes. While the work of the PoCH ledger is not limited to providing only a chronology, it adds the context associated with each event. Figure 2 shows the structure of the PoCH Ledger.

It includes information about the leader choice, the voting results, and the status of the certificate. PoCH ledger provides a log that allows auditing of administrative and security events related to the PKI. The PoCH ledger also features from a traditional Audit ledger, that the traditional Audit ledger can be modified by a central entity, while the PoCH record provides a series of commitments (hashes) that link each record with the previous record, so that it providing a high security layer that makes any attempt to modify the contents of a record or delete it immediately detectable by breaking the chain of obligations. PoCH ledger is also distinguished from other registers such as the CT log, which was employed to publish issued certificates, allowing checking the absence of forged or unauthorized certificates, while the PoCH ledger is employed to record the entire certificate life cycle and all events related to the certificate. To ensure the non-tampering and integrity of the PoCH records, a series of cryptographic commitments are created, where the commitment value (hash) is calculated using SHA-256 for each record using the commitment of the previous record along with the data of the current event, as this mechanism provides high protection, as any change in the information of the previous record leads to a mismatch with the values of previous commitments, therefore, any attempt to delete or modify is detected during the verification process. The PoCH ledger can be checked by recalculating the hash of the event and the commitment of the data stored inside the log, then comparing them with the previously recorded values, and

also checking the correlation between the logs by calculating the commitment of the previous log and matching it with the previous commitment recorded in the current log, which allows detecting any attempted manipulation or modification in the log. Any illegal modification of the identity of the leader, the status of the certificate or the sequence of events becomes detectable due to the interruption of the encrypted chain. It also enhances the auditability by enabling validators to know what happened, who carried out the audit, and under what context the consensus and accreditation were carried out.

The PoCH ledger contributes to enhancing transparency and accountability in the blockchain, and enables the integration of identity applications and DPKI. The PoCH consists of chain of connected records and each record includes a set of fields that document each event related to the life cycle of the digital certificate, where a separate log is created for each process such as issuance, revocation, etc. After this, the log is added to the end sequentially. Each record consists of the basic data of the event and information linking with the previous record to preserve the chronology of events, with the possibility of verifying the integrity of the historical records in full. Each PoCH record includes the following components:

Sequence Number (Seq)

Indicates the serial number of the record.

Slot Identifier (SL_i)

Indicates the slot index in which the event occurs.

Leader Identifier (L_i)

Denotes the selected leader utilizing the VRF mechanism for this slot.

Event Type (E)

Represents the contextual event type related to the certificate (issuance, renewal, revocation).

Payload (P_y)

Represents details of this event.

Hash of P_y

Represents the cryptographic hash function of the event.

VRF output (y_i)

VRF output providing leader eligibility.

VRF Proof (π_i)

VRF Proof providing leader eligibility.

Hash of previous record (Commitment $_{i-1}$)

The hash value of the previous record, which is utilized for connecting the records in a non-manipulable chain.

Commitment $_i$ The hash of the current record computed as the following:

$$H(PoCH)_i = H \left((Seq \| SL_i \| L_i \| P_y \| H(P) \| VRF y_i \| VRF \pi_i \| H(PoCH)_{i-1}) \right)$$

and the general structure of the record is arranged in the following form:

$$PoCH_i = \{Seq, SL_i, L_i, P_y, E, H(P_y), y_i, \pi_i, H(PoCH)_{i-1}\}$$

4.4 The certificate state record

In order to quickly access and verify the current status of the certificate without having to search through all the PoCH records, the proposed system employs a quick reference that maintains a separate status record for each digital certificate known as the Certificate State Record. This leg includes the basic and important information associated with the certificate, as shown in Figure 3, such as the user ID, the certificate hash, the current status of the certificate, the hash of PUU, as well as indicators linking the record to the last event registered in PoCH and the location of the encrypted certificate in DW. After each associated operation with the certificate, such as issuance, revocation, renewal, ...). The status log is updated automatically as it always stores the latest Certified status of the certificate. This record plays a major role in reducing search and verification time, as the system starts querying the certificate status record using cert_hash to verify the existence of the certificate and its current status, then moves to check the record PoCH or retrieve the full certificate from off-chain DW, thereby contributing to improving performance while maintaining data integrity with the possibility of auditing all operations recorded on the PoCH. Algorithm 3 outlines the procedures for querying the status of the certificate.

CERTIFICATE STATE RECORD	
cert_hash (Primary Key)	Unique identifier of the certificate
user_id	Owner (user) of the certificate
status	Current status (ISSUED / RENEWED / REVOKED / ROTATED)
current_public_key_hash	Hash of the current public key
last_event	Type of the last event
poch_seq	PoCH sequence number
poch_commitment	PoCH commitment hash
DW_pointer	Pointer to the Data Warehouse entry (metadata reference)

Figure 3. The structure of certificate state record

Algorithm 3: Querying the status of the certificate

Input: Cert_hash

Output: Status of Certificate (Active, Revoke, Renewal) or Not_MATCH (not found).

Step 1: Start

Step 2: User sends cert_hash to system.

Step 3: System receives cert_hash and implements the following:

3.1: Search in Certificate State Record utilizing cert_hash.

3.2: IF not found, matching record Return NOT_FOUND

3.3: Else get poch_seq and retrieve corresponding PoCH entry.

3.4: Compute hash of corresponding PoCH entry.

3.5: Compare the computed hash with record. poch_commitment.

3.6: IF two values do not match, return NOT_MATCH.

3.7: Else return the current status of the certificate stored in Certificate State Record.

Step 4: End.

4.5 The certificate lifecycle management

The digital certificate management is the main function of the proposed system, so the system means managing all the processes related to the certificate from issuing, canceling, verifying, renewing and recording all these events inside a tamper-proof record. The system is concerned with maintaining the current status of the certificate in a certificate status record, which contributes to speeding up the search and verification processes.

Its life cycle begins with the issuing process. After the user registration process is completed and the login process is successful, the user starts sending a certificate issuance request, which is signed with his own PR and sent to the system. Then the leader receives the request and verifies the transaction locally and inserts it into PoH, and then sends it to the auditors to verify the user's identity, the authenticity of the digital signature, the integrity of the data and the conformity of the public key documented in the request with the pre-registered in its account, after approval the majority of the validators, temporary CA issues the certificate X.509 and digitally signed it using his private key. After the certificate is issued, the issue event and the certificate hash are recorded in the PoCH ledger, while the certificate status and the PoCH serial number (PoCH_Seq) are saved in the Certificate Status Record to speed up the process of accessing it during the search process without having to search all the PoCH records. The certificate is encrypted using an AES-256 algorithm and is saved in off-chain DW.

The second important stage of the certificate life cycle is revocation, which is the stage when the certificate holder resorts to revoking the certificate before it expires as a result of a leak of the private key. In this case, the certificate revocation transaction is sent to the system. When the system receives the transaction, it does not execute the cancellation process directly, but starts the following procedures:

(1) Verification of the identity of the request.

(2) Check the status of the certificate by searching the Certificate Status Record of the certificate and make sure whether the certificate is valid or it was revoked; in case the certificate is revoked, the transaction is rejected.

(3) Matching the status record to the last event recorded in PoCH.

The validators repeat the same validation process in the

steps (1,2,3), and if they are approved by the majority of the validators, the certificate is revoked. The revocation event is recorded in PoCH, while certificate status is updated to “REVOKE” and a PoCH record number (PoCH_ Seq) is recorded in the Certificate Status Record.

Upon receipt of a digital certificate from one of the users of the system, the other party executes a series of verification operations on the receiver (client) to confirm the authenticity and integrity of the certificate before trusting it and using it in the authentication process or establishing a secure connection.

The verification process for the certificate starts when the user sends a verification request to the system containing the certificate hash. When the system receives the request, the commander and the validators perform the following verification operations:

(1) Utilize the Certificate Status Record for direct access to the last Certificate event linked in PoCH.

(2) Use the PoCH_ seq installed in the status log to access the corresponding log and match the certificate hash with the hash installed on the network.

(3) Retrieve the encrypted certificate from DW, decrypt it, and compare its hash with the hash recorded on the chain.

(4) Verify the signature of the certificate using the temporary CA Key located on the network.

The certificate is accepted if all the previous tests are correct; otherwise, the certificate will not be rejected.

4.6 Off-chain data warehouse security

In order to reduce the storage cost on the network, an off-chain storage layer was employed, using DW to store certificates, and in order to enhance the security of this layer, a set of mechanisms were assigned that ensure the

confidentiality and availability of digital certificates. Where the certificate is stored in encrypted format on DW using an AES-256-GCM algorithm with key management; the certificate hash and its status are saved on the network, which contributes to reducing the amount of data stored on the network. The system can detect any attempted data manipulation by recalculating the certificate hash and matching it with the hash stored on the network. Other protection mechanisms have also been employed, such as Object Lock mechanism and the automatic backup mechanism, this contributes to the protection of backup copies of certificates from deletion and manipulation because it depends on the principle of Writing Once Reading Many times(WORM), which prevents any modification or deletion of data, and in the event of any malfunction or damage to the data warehouse, the backup copy of certificates stored in another warehouse can be used to ensure business continuity and data integrity. To ensure that data is not manipulated and its availability, and to preserve the full content of the certificate when restoring the repository, which enhances the reliability of the system and its resistance to malfunctions and tampering attempts.

4.7 Proposed decentralized public key infrastructure system based on modified Solana

In the previous section, the layers of the proposed system were comprehensively reviewed with a detailed explanation of each of its components. To achieve a deeper understanding of how these layers are integrated during operation, in this section, the operational stages of the system are presented sequentially as shown in Figure 4.

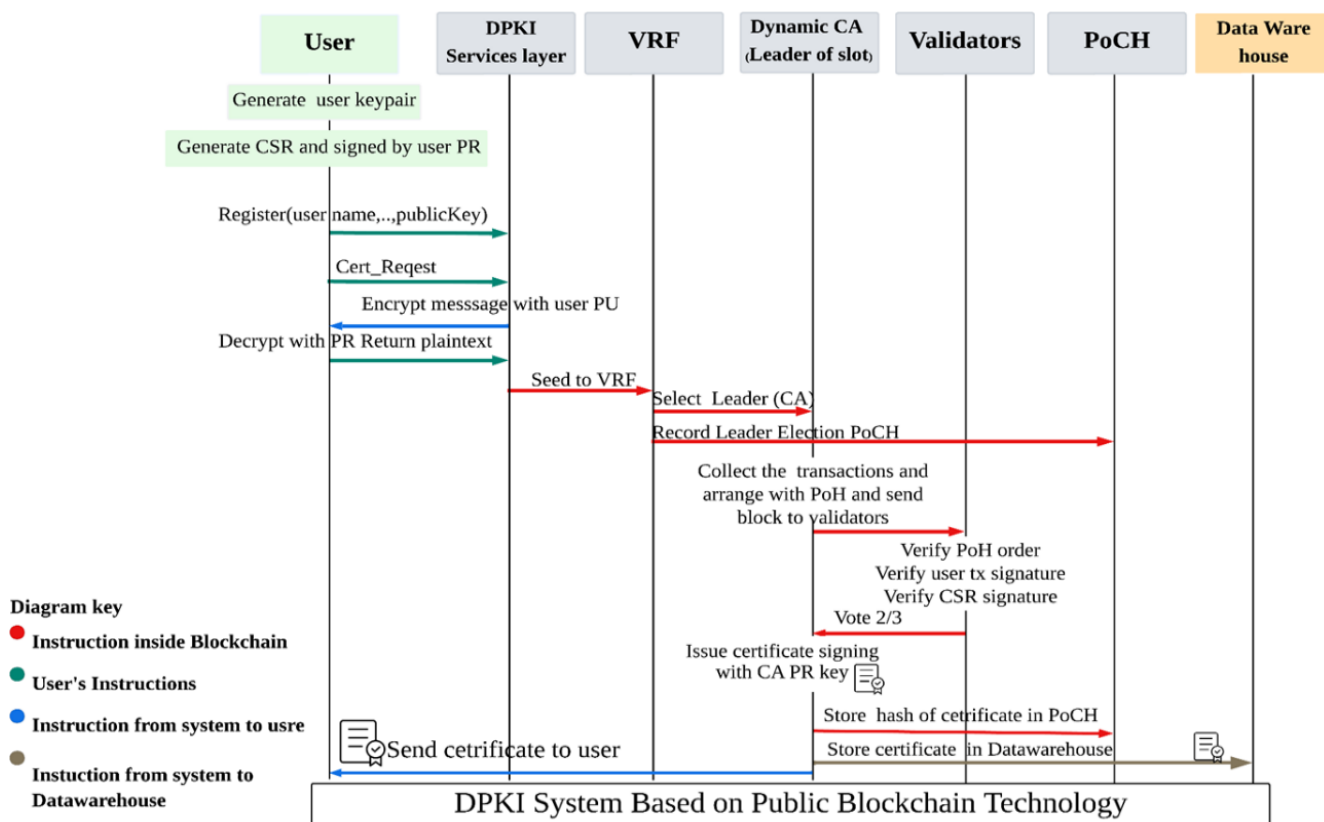


Figure 4. The decentralized public key infrastructure (DPKI) system based on public blockchain technology

(1) The new user can generate his keys (PU and PR) using ECDSA, then create a CSR and sign it with his PR key.

(2) In the registration stage of the system, a new user can enter his information, such as name, email, public key, and password. In case of login, the system encrypts the message using the user's public key and sends it to the user's e-mail to prove ownership of the user's private key.

(3) Sending a CERT_REQUEST transaction to the DPKE Services layer, which is signed by the user's private key.

(4) Selection of the leader (CA) for the slot based on the VRF mechanism.

(5) The leader (CA) receives slot transactions and implements the following tasks:

- Collects the transactions and arranged chronologically within PoH.

- Checks the authenticity of transactions locally, then broadcasts them to the validators.

(6) The validators conduct the following:

- Check the PoH and the authenticity of transactions.

- Verify the user's signature on the request and the signature on the CSR.

- Vote / confirm.

(7) The validators conduct the following:

- Check the PoH and the authenticity of transactions.

- Verify the user's signature on the request and the signature on the CSR.

- Vote / confirm.

(8) The validators conduct the following:

- Check the PoH and the authenticity of transactions.

- Verify the user's signature on the request and the signature on the CSR.

- Vote / Confirm.

(9) When voting on the validity of transactions by the overwhelming majority (2/3 supermajority), the application is approved.

(10) The CA issues the certificate and signs it with his PR key, then cert_hash stores it on the chain and sends the certificate to the user.

(11) Event registration, such as leader election, type of the request, and hash of the certificate inside PoCH.

(12) The encrypted certificate is stored in the Data Warehouse (DW).

4.8 The proposed system application scenarios

In this paper, the proposed system is designed as a general framework for the management of the digital certificate course based on the X.509 standard in DPKE, in an environment without specifying a specific application area. Considering that the system's main function is to manage the certificate life cycle from issuance, verification, cancellation and renewal, which is a common function between various PKI applications, therefore, the public system has flexibility that allows it to be used in many fields and applications such as digital academic certificate management, digital identity of institutions, critical structures, industrial systems and other applications that depend on the standard X.509 in the digital identity Department. These areas have been mentioned as potential application examples. All experiments were conducted within a simulation environment in order to evaluate the performance of the basic functions of the system in managing the certificate life cycle independently of any specific application area. The results reflect the efficiency of the basic mechanisms of the system and the possibility of its

application in various environments that depend on the management of the digital certificate.

4.9 Limitations of the proposed system

The proposed system is designed to work on a decentralized blockchain environment, but the evaluation of this system was limited to a prototype in a simulated environment on a single computer to verify the protocol performance and evaluate the performance of managing the life cycle of the digital certificate within a controllable environment. Therefore, the experiments were focused on evaluating the basic functions of the system, such as issuing, verifying, and revoking certificates, as well as analyzing security features within a simulated environment without relying on a physical network. However, the simulation results showed the efficiency of the proposed system, and evaluating the system on an actual blockchain network is an extension of future work to verify its performance in realistic operating environments.

5. RESULTS AND DISCUSSION

The proposed system was implemented and tested using a software simulation environment designed and developed specifically for this system using the Python language and the Streamlit framework, because it is not possible to make any direct modifications to the Solana network or its internal mechanisms. The system was implemented and tested on a computer with the following specifications: Windows 11 Pro 64-bit, Intel(R) Core (TM) i7-8665U CPU, and 16.0 GB of RAM. The Python language version 3.11 was also used. To implement the functions of the proposed system and simulate operations, several software libraries were employed, including the cryptography library to implement cryptographic operations for key generation using ECC, signing, and verification using ECDSA. Also, hashlib was used to implement the hash functions used within PoH / PoCH; the python-ecvrf mechanism was used to implement the leader selection process; in addition to the time and datetime libraries for time simulation and performance measurement. Table 2 shows the parameters of the simulator.

Table 2. The parameters of the simulator

Parameter	Type/Value
Language	Python
Framework	Streamlit
The number of validators	10
Time of slot	0.4 sec
Blockchain	Modified Solana
Hash function	Hashlib
Leader election mechanism	VRF & $\sqrt{stake}$
Number of execution times of user key generation	1000

Note: verifiable random function (VRF)

5.1 Execution time

Table 3 shows that the ECC-P256 algorithm significantly outperformed the RSA-2048 algorithm in Key Generation time, where the average Key Generation time in ECC was about 0.000105 seconds compared to 0.077686 seconds in RSA-2048. Each test was performed 1000 times to ensure

improved reliability of results and reduce random oscillation in execution times. This superiority is due to the dependence of ECC on elliptic curves with high computational efficiency and smaller keys, while RSA requires more complex calculations associated with the generation of large primes. The results also showed that ECC provides less execution time and lower computational consumption, which makes it more suitable for decentralized systems and blockchain environments that require high efficiency and speed in the creation of digital identities and key management.

$$\begin{aligned} \text{Propabilty of the proposed system} \\ = \sqrt{S_i} / \sum \sqrt{S_j} \end{aligned} \quad (10)$$

Table 3. The comparison of the execution time of ECDSA used in the proposed system with RSA used in traditional public key infrastructure (PKI)

Algorithm	Avg-Sec	Std-Sec	Min-Sec	Max-Sec
RSA-2048	0.077686	0.054821	0.007713	0.482922
ECC-P 256	0.000105	0.000107	0.000053	0.001112

5.2 Security strength

The recommendations of the NIST indicated that ECC algorithms can achieve an equivalent level of security when using much smaller encryption keys. For example, the RSA algorithm using a 2048-bit key can provide a security level of approximately 112 bits, while the ECDSA algorithm using a 256-bit key achieves a security level of 128 bits [32]. It was thus concluded that the key length is not directly proportional to the security strength and that encryption algorithms based on elliptic curves can achieve higher levels of security using much shorter keys compared to traditional algorithms based on integer analysis, such as RSA. Reducing the key size in ECDSA algorithms reduces memory consumption and the time required to generate keys and perform signature and verification operations. Therefore, the ECDSA algorithm has become the preferred choice in many modern security systems, including secure communication protocols and blockchain applications, which require a balance between a high level of security and computational efficiency.

5.3 The probability of leader selection

In the Solana blockchain, the leaders are selected via the Leader schedule mechanism, which schedules leaders at the epoch level based on this mechanism. Leadership opportunities are distributed in a linear manner directly proportional to the amount of stake belonging to each validator, which gives the validator with the largest stake control over the highest number of slots. Where the probability of the selection for validator i is calculated according to the following equation:

$$\text{ropabilty of Solana} = S_i / \sum S_j \quad (11)$$

While the proposed system is based on the dynamic selection of a leader utilizing the VRF mechanism with non-linear stake, so that the probability of validator election i is calculated according to the following equation:

Suppose 10 validators(v) with the following stakes(S):

$$\begin{aligned} V &= [v1, v2 \dots \dots \dots, v10] \\ S &= [40,60,80,100,120,150,200,250,300,400] \\ \text{Sum}(S) &= \sum S_i \\ \text{Sum} &= 400 + 300 + 250 + 200 + 150 + 120 + 100 + \\ &80 + 60 + 40 \\ \text{Sum} &= 1700 \end{aligned}$$

$$\begin{aligned} \text{As for the proposed system based on the non-linear stake} \\ (\sqrt{S_i}) \\ \text{Sum}(\sqrt{S_i}) &= \sqrt{400} + \sqrt{300} + \sqrt{250} + \sqrt{200} + \sqrt{150} + \\ &\sqrt{120} + \sqrt{100} + \sqrt{80} + \sqrt{60} + \sqrt{40} \\ \text{Sum}(\sqrt{S_i}) &\approx 123.4907 \end{aligned}$$

An experimental distribution consisting of 10 validators was adopted within the simulation environment as a mini-model aimed at studying the behavior of the VRF-based leader selection mechanism and the nonlinear pattern of stakes in a clear and analyzable way to analyze the indicators of decentralization and the impact of different distributions of stakes on the probability of choosing a leader in a way that can be tracked and measured. Table 4 shows the comparison of the probability of the leader election for the proposed system with the probability of the leader election used in original Solana. In the linear selection mechanism of Solana, the direct proportionality of the leader's choice is adopted with the stake, which leads to the dominance of holders' high stakes over the leadership. In the original Solana, the V1, which holds the highest stake, got an election probability surpassing the V10, which holds the least stake, by almost ten times, while the V2 got eight times the V10, and so on. While the proposed system contributed to reducing this gap between the validators significantly, so that the use of the square root function led to a redistribution of the probability of leadership, as leadership opportunities were reduced for owners of high stakes (V1-V4) while leadership opportunities were increased for owners of small stakes (V6-V10). This has reduced the difference between the highest and lowest probability of selection to only about three times. Thus, the proposed system does not completely eliminate the impact of the stake, but redistributes the probability in such a way as to achieve a more efficient balance between fairness, distribution of leadership opportunities, and the requirements of the security of the blockchain network.

Table 4. Comparison of the probability of the leader selection in the proposed system with Solana

The Validators	The Stakes of the Validators	The Probability of Solana Leader	Probability Proposed System
V1	400	0.2353	0.1620
V2	300	0.1765	0.1403
V3	250	0.1471	0.1280
V4	200	0.1176	0.1145
V5	150	0.0882	0.0992
V6	120	0.0706	0.0887
V7	100	0.0588	0.0810
V8	80	0.0471	0.0724
V9	60	0.0353	0.0627
V10	40	0.0235	0.0512

5.4 Herfindahl-Hirschman Index

It is an important and widely used measure of concentration degree in blockchain and networks based on PoS; it is used as an indicator to measure the degree of concentration of stakes and authority among a number of validators. Let P_i be the leader selection probability. The Herfindahl-Hirschman Index (HHI) is defined as [23]:

$$HHI = \sum_{i=1}^N P_i^2 \quad (12)$$

It ranges from 0–1; when the value is close to zero, the system is closer to a decentralized state, while higher values mean a greater concentration of power. The comparative results in Table 5 show that the value of the centering factor HHI in the original Solana system amounted to 0.1422, while in the proposed system it decreased to 0.1115. The decrease in the value of the index indicates a more balanced distribution of stakes among validators in the proposed system compared to the Solana blockchain. Since in the proposed system, the HHI indicator is dependent on the distribution of leader election probabilities derived from the square root weighting among validators rather than raw stakes, smaller values indicate a lower degree of concentration and a decrease in the likelihood that a limited number of validators will control the block production process. In the Solana blockchain, the determination of the leader depends heavily on the stake (stake weight), which may lead to the concentration of the ability to produce blocks among validators with large stakes. Whereas the proposed system is based on the employment of a VRF mechanism with a non-linear distribution of the stake (square root stake) for the selection of the leader, which reduces the impact of large stakes and increases the chances of a larger number of validators participating in the leadership process. Thus, this adjustment led to an improvement in the level of decentralization in the choice of the leader, which is clearly evidenced by the decrease in the value of the HHI index from 0.1422 to 0.1115. This means that the proposed system has reduced the likelihood of monopolization of the block production process among a limited number of participants, which enhances equity in participation and increases the system's resistance to the risks of centralization.

Table 5. The comparison Herfindahl-Hirschman Index (HHI) factor of the proposed system with original Solana

No.	The Systems	HHI Factor
1	Original Solana	0.1422
2	Proposed system	0.1115

5.5 Entropy

In 1948, the scientist Shannon proposed the entropy scale in information theory to determine the amount (uncertainty) of randomness in a probability distribution. Recently, this metric has been adopted to analyze decentralization of networks and the risk of a small group of validators controlling the network. High values indicate a more balanced distribution among the participants, while low values reflect a higher degree of centrality. The equation of Shannon's entropy is [33]:

$$H(x) = \sum_{i=1}^N -P_i \log P_i \quad (13)$$

and the maximum entropy of the system is calculated as follows [34]:

$$Max(H) = \log_2(N) \quad (14)$$

Table 6 values were adopted to measure entropy; the results in the table show that the proposed system achieved an entropy of 3.2393, which is approximately 98% of the maximum. While the original Solana achieved an entropy of 3.0272. The results indicate that the distribution of leadership opportunities in the proposed system more random and it is closer to the ideal distribution, which mean that the probability of choosing leaders is not highly concentrated among a specific group of validators, and this superiority in results is due to the VRF mechanism with a non-linear distribution of the stakes, This has reduced the excessive influence of holders of large stakes and increases the likelihood of the participation of the largest number of validators in the process of generating blocks in the chain.

Table 6. Comparison of the entropy of the proposed system with the original Solana

Systems	Entropy	Proximity to the Maximum Entropy
The Proposed System	3.2393	98%
Original Solana	3.0272	91 %
Maximum Entropy	3.3219	100%

5.6 The security model and thread

The security architecture of the proposed system is designed to withstand threat situations, since this section includes scenarios descript multi types of attackers and protection mechanisms used within the system. The first scenario assumes the occurrence of a breach for the leader (temporary CA); the leader selected via VAR and non-linear stakes does not have the authority to issue certificates individually, since all issuance requests are subject to mass verification by validators, where CSR, DS, and PoP of the key are verified, requiring a collective vote by the vast majority of validators before any process. The second scenario concerns the penetration and collusion of validators, where the system assumes that all validators are active and qualified participate in the process of managing the certificate life cycle and no process is approved without the consent of the vast majority(2/3) of qualified auditors, as this contributes to preventing one validator or a group of complicit validators from adopting unauthorized operations, as this is based on the standard assumption in the Byzantine fault tolerance protocol, which requires the number of malicious auditors to be less than the limit (1/3) that allows influencing the consensus mechanism.

Under this assumption, the system maintains the integrity of the data, but if this assumption is violated and the number of malicious auditors exceeds the minimum, this may affect the security features of the protocol. This principle is shared by all Byzantine fault-tolerant protocols. Also one of the attack scenarios is DoS: this scenario assumes that an attacker is trying to target some of the system components, such as the current leader or auditors, or DW to affect the availability of the service and slow down the processes associated with the certificate lifecycle, the system counteracts this type of attack by relying on group verification by a group of validators with the election of a new leader periodically using VRF, which

reduces the impact of targeting one node or the continuation of the attack on the same leader. Also, the PoCH and certificate state record and automatic backup allow certificate status verification even in case of temporary inaccessibility to DW. The system also resists Sybil attacks through the stake-weighted VRF-based selection mechanism, which reduces the influence of dummy nodes and limits centralized dominance. As for hacking the DW, the system relies on hybrid storage, where it stores the hash value of certificates inside the blockchain, which allows detecting any illegal modification to certificates stored off-chain.

Rollback and Equivocation attacks are limited by using the immutability feature of the blockchain and the PoH

mechanism, which imposes a non-manipulable chronological order of transactions, allowing any conflict to be detected or an attempt to create contradictory blocks. The handling of Revocation Race Conditions is also clarified by relying on the chronological order of transactions to determine the final cases of the certificate. Finally, the protection against Certificate Mis-Issuance was strengthened by imposing CSR verification, digital signature, and PoP of the key before issuing any certificate, in addition to the adoption of a collective vote of validators before approving the final issuance of the certificate. Table 7 summarizes different types of attacks and the security mechanisms in the proposed system.

Table 7. Threat scenarios analysis and response mechanisms in the proposed system

No.	The Scenario of Attack	The Circumstance of the Attack	The Response of the Proposed System	The Security Mechanisms in the Proposed System
1	Malicious Leader	Attempting to carry out an unauthorized operation or issuing a false certificate	No process is carried out without the approval of the vast majority of the validators. And all events are recorded in PoCH	Approval of the vast majority & immutable record in PoCH
2	Validators Collusion	A group of validators agreed to approve an incorrect process	The system requires the approval of the majority of the validators, with the possibility of scrutinizing all recorded events	Supermajority Consensus& PoCH
3	DoS Attack	The attacker is trying to flood the system with heavy requests to delay the processes associated with the certificate	The attacker may try to increase the response time, but he cannot modify or forge certificates, as the certificate remains verifiable through the PoCH and Certificate Status Record.	VRF-based leader election, distributed validators, PoCH and Certificate State Record
4	Sybil Attacks	Creating a large number of fake nodes to control the network	The system requires a valid Stake and passing the requirements to join the network	$VRF \& \sqrt{stake}$
5	Certificate Forgery	Modify or create a fake certificate	The system rejects the certificate when the hash mismatch or signature verification fails	Certificate hashing stored in PoCH and Signature Verification
6	Off-chain DW manipulation	Modify the certificate stored in DW	The system recalculates the hash, detects tampering, and then restores the original Object Lock when needed	Hashing Verification & Object Lock
7	Off-chain DW Failure	DW unavailable during verification	Certificate status verification continues based on blockchain and PoCH, and data is later recovered	Certificate State Record& PoCH & Auto Backup
8	Delayed Revocation	Try to use a newly revoked certificate	The decision is based on the most recent status registered with Certificate State Record prior to the certification is accepted	Certificate State Record& PoCH

Note: verifiable random function (VRF); proof of context and history (PoCH)

5.7 Security analysis

Table 8 shows that there are fundamental differences between traditional architectures and decentralized systems for managing PKI. The CT system relies mainly on centralized trust, which has led to the existence of an individual point of failure that may affect the reliability of the entire system in the event of a breach by the central authority or improper certification. Although the CT system has improved transparency and audit capability, the system still relies on a central authority to manage certificates. Blockchain-based PKI systems, such as Ethereum-based DPKI and WoT-based PKI, and Threshold PKM, are characterized by a higher level of decentralization and better resistance to manipulation due to their dependence on non-modifiable storage and distributed verification mechanisms. These systems differ in terms of the trust model and verification mechanism, where Ethereum-based DPKI relies on smart contracts in the verification process, while WoT-based PKI relies on trust between participants in the verification process, and Threshold PKM relies on a collective threshold verification mechanism to reduce dependence on one entity. Despite these features, these systems still suffer from limitations such as scalability or

limited direct support for X.509 certificates. Finally, Solana-native, which is based on PoH and Tower BFT, is characterized by high performance and low processing time, but this platform does not inherently provide a specialized layer for managing the lifecycle of X.509 certificates due to the nature of its main design for money transfers, which makes it inadequate as an integrated DPKI system. While the proposed system achieves a lower level of centralization by integrating the VRF mechanism with the leader-as-CA model and distributed verification by validators, which reduces the likelihood of an individual point of failure and enhances the resistance to manipulation of records. The system provides a high level of transparency and auditability as a result of the PoCH distributed time record function. The system also features full dynamic support for X.509 certificates via a hybrid model that combines the series and an external Data Warehouse. Based on what has been presented, the results of the security analysis indicate that the proposed system achieves a balance between performance, centralization, and digital certificate management compared to other reference systems while improving resistance to centralization and reducing the concentration of trust without sacrificing performance efficiency and security auditability.

Table 8. Comparison of the proposed system with other systems of public key infrastructure (PKI)

Security Metric	Conventional CA/CT	Ethereum based-PKI	WoT Based-PKI	Threshold PKM	Native Solana	The Proposed System
Centralization of trust	High	Low	Low	Moderate	Moderate	Very Low
One point of failure	Present	Reduce	Reduce	Reduce	Reduce	Significatereduce
Resistance to the manipulation	Limited	High	Moderate	High	High	Very High
Transparency of certification	Moderate	High	Moderate	High	Moderate	Very High
Resistance to internal attacks	Moderate	High	Moderate	High	High	High
Auditability	Moderate	High	Moderate	High	High	High
Validation model	CA- based	Smart contract validation	Trust based validation	Threshold validation	Validators& Tower BFT	Validators & Tower BFT
X.509 certificate support	Full support	Limited/custom	Limited	Partial	No support	Fully Dynamic support
Type of storage	Off-chain	On-chain	On-chain	On-chain	On-chain	Hybrid

5.8 Throughput

In the proposed system, Throughput (TPS) is calculated by measuring the number of certificate transactions that have been successfully processed and confirmed during a specific period and time. The productivity measure is one of the most important indicators of the performance of decentralized blockchain systems, because it reflects the extent of the network's ability to handle high loads without affecting the stability of the network. TPS can be calculated as in the following equation:

$$TPS = (N \text{ of } Tx) / (Total \text{ time}) \quad (15)$$

where,

$N \text{ of } Tx$: The total number of accepted and documented transactions within the network.

$Total \text{ time}$: The total time it takes to process these transactions.

The TPS values of the proposed system were calculated, where the values in the figure show the increase in TPS with an increase in the number of transactions from 100 to 1000 transactions. The results show an increase in productivity from 727.81 TPS at 100 transactions to 916.23 at 1000 transactions. As can be seen from the figure, the increase is not completely linear; it appeared after oscillations at certain loads. Productivity decreased from 907.96 TPS at 300 transactions to 870.20 TPS at 400 transactions, and also decreased from 919.59 TPS at 500 transactions to 892.09 TPS at 600 transactions. The reason for this fluctuation is the increased competition for computational resources, the different distribution of transactions between blocks, and the effects of scheduling and verification mechanisms within the simulation. As can be seen from Figure 5, the increase is not completely linear; it appeared after oscillations at certain loads. Productivity decreased from 907.96 TPS at 300 transactions to 870.20 TPS at 400 transactions, and also decreased from 919.59 TPS at 500 transactions to 892.09 TPS at 600 transactions. The reason for this fluctuation is the increased competition for computational resources, the different distribution of transactions between blocks, and the effects of scheduling and verification mechanisms within simulation.

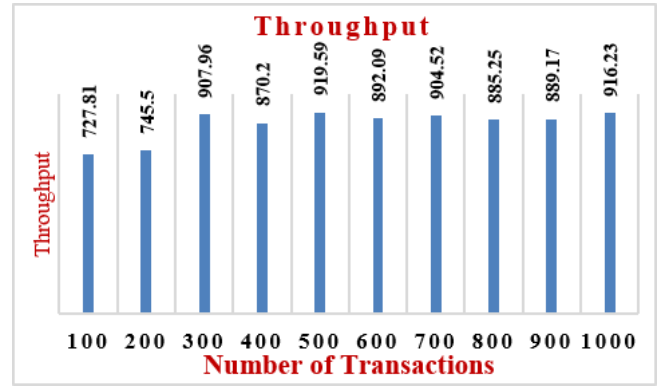
To calculate the average of TPS, the following equation is used:

$$Average \text{ of } TPS = \sum TPS/n \quad (16)$$

where, n is number of experiments.

These results indicate the ability of the system to maintain

a high level of productivity with an average of 865.83TPS, which demonstrates the ability of the system to process large numbers of transactions with high efficiency and stability.

**Figure 5.** Throughput (TPS) of the proposed system

5.9 Latency

It is an important indicator for measuring the efficiency of blockchain systems and DPKI. Latency represents the time required to process a transaction from the start of its execution until the verification process is completed within a system. DPKI, this measure affects the speed of issuing and verifying a digital certificate. The system was tested at different load levels using a varying number of coefficients ranging from 100 to 1000 in order to analyze the behavior of the system and evaluate scalability under different conditions. The latency is calculated according to the following equation:

$$Latency = B_{endtime} - Tx_{submit \text{ time}} \quad (17)$$

where,

$B_{endtime}$: Block execution end time.

$Tx_{submit \text{ time}}$: Processing time of the transaction within the slot.

Figure 6 shows the Latency value gradually increasing as the number of transactions increases from 100 to 1000 transactions. It increased from 0.1374 seconds at 100 transactions to 1.0914 seconds at 1000 transactions. This increase is due to the increased burden on the nodes involved in the processing and verification of transactions.

Despite this rise, the rise was regular and semi-linear, which indicates the stability of the system's performance and its lack of saturation. The results also indicate that the system maintained a relatively low latency even at the highest test load, if the value remains less than 1.1 seconds, this ratio

reflects the reliability of the verification mechanism used in the system and also confirms the ability of the system to handle increasing numbers of transactions while maintaining an acceptable level of response time, which makes the system suitable for decentralized infrastructure applications that require efficient processing of certificates and associated verification processes.

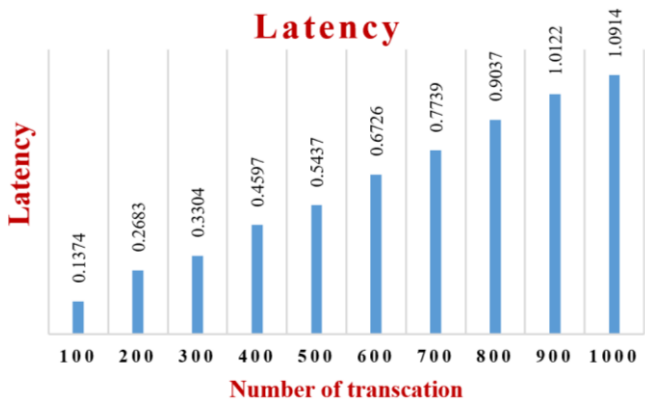


Figure 6. Latency of the proposed system

5.10 Evaluates system performance in terms of Throughput

In order to evaluate the proposed system and determine its efficiency, the TPS rate was calculated and compared with the system BPKI [35] and the system in the study [16]. TPS is an important metric that reflects the system's ability to process transactions per unit of time. Figure 7 shows a comparison of the TPS rate between the proposed system and two previous studies, namely BPKI and the blockchain-based decentralized identity management system.

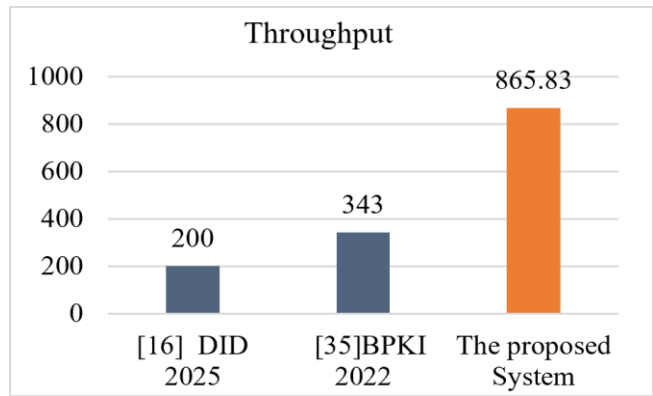


Figure 7. The comparison between the proposed system with other systems

The results show the proposed system achieved a productivity with an average of 865.83 TPS, while both the previous two studies achieved BPKI 343TPS and the other 200 TPS. The adoption of the proposed system on the PoH mechanism contributed significantly to reducing the burden of communication between nodes and also contributed to increasing the number of transactions that the system can process per second. While the BPKI system has adopted the DPBFT mechanism, which provides good performance compared to many other traditional systems, the multiple

stages of verification and voting among validators lead to an increase in the communication load and lower productivity compared to the proposed system. While the study [16] focused mainly on Decentralized Identity Management in IoT environments using ZKP & DID, the focus was more on security and Privacy than achieving high productivity. Although the current evaluation environment of the proposed system was based on a prototype implemented on a single computer, the current results reflect the efficiency of the proposed system under approved test conditions, while verifying the scalability of the system and its performance requires conducting future experiments on a real blockchain network.

6. CONCLUSION

This paper dealt with the design of a new integrated DPKI system based on the Solana blockchain with many fundamental improvements. The proposed system focused mainly on addressing the vulnerabilities of traditional PKI systems, most notably the problem of centralized trust, lack of transparency, and mainly the problem of leadership concentration in betting-based Solana blockchain systems. In order to achieve this and provide a suitable framework for building a DPKI system and managing the digital certificate in a decentralized manner, the Solana blockchain was developed by re-engineering and redesigning the block production path and the mechanism for selecting leaders to reduce the possible motives for centralization in the consensus layer. The proposed system was based on four main pillars representing the essence of the work and its innovation, where a new mechanism for electing a leader was proposed based on the nonlinear stake pattern. The nonlinear pattern contributed to reducing the excessive impact of the large stakes, which was reflected by reducing the stake gap between validators. While the VRF mechanism allowed random and unpredictable selection, resulting in a balance of leadership opportunities. The results showed that the proposed mechanism contributed significantly to improving the level of decentralization compared to the linear pattern in the original Solana, while retaining the process of linking to the stake. The dynamic CA model was also introduced, where the elected leader for each slot is assigned as a temporary CA. It abolished the principle of assigning trust to the fixed CA that exists in traditional systems, which contributed to the system's adaptation and flexibility significantly. Moreover, the system relied on PoCH, employing a new extended time record to document events and arrange them chronologically within the network, thereby achieving a higher level of transparency and auditability. Finally, the system adopted a hybrid storage model that combined on-chain and off-chain storage. The hash of the certificate is stored only on the chain to ensure its integrity, while the full certificate is kept in an external data warehouse. This contributed to achieving a balance between performance and storage and reducing the burden on the network. From a practical and experimental point of view, the results of the evaluation of approved cryptographic algorithms in the proposed system showed efficiency in generating keys in terms of speed and security compared to the algorithms used in traditional systems. In addition, achieving a random and fair selection of leaders.

REFERENCES

- [1] Fernando, W.K.B.A.K. (2020). An alternative to certificate authorities using blockchain-based decentralized PKI. <https://dl.ucsc.cmb.ac.lk/jspui/handle/123456789/4628>.
- [2] Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: A state of the art review. *EURASIP Journal on Wireless Communications and Networking*, 2020(1): 56. <https://doi.org/10.1186/s13638-020-01665-w>
- [3] Talamo, M., Arcieri, F., Dimitri, A., Schunck, C.H. (2020). A blockchain-based PKI validation system based on rare events management. *Future Internet*, 12(2): 40. <https://doi.org/10.3390/fi12020040>
- [4] Kfoury, E.F., Khoury, D., AlSabeh, A., Gomez, J., Crichigno, J., Bou-Harb, E. (2020). A blockchain-based method for decentralizing the ACME protocol to enhance trust in PKI. In 2020 43rd International Conference on Telecommunications and Signal Processing (TSP), Milan, Italy, pp. 461-465. <https://doi.org/10.1109/tsp49548.2020.9163555>
- [5] Ali, F.S., Kupcu, A. (2020). Improving PKI, BGP, and DNS using blockchain: A systematic review. *arXiv preprint* arXiv:2001.00747. <https://doi.org/10.48550/arXiv.2001.00747>
- [6] Guo, H., Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: Research and Applications*, 3(2): 100067. <https://doi.org/10.1016/j.bcr.2022.100067>
- [7] Brunner, C., Knirsch, F., Unterweger, A., Engel, D. (2020). A comparison of blockchain-based PKI implementations. In *Proceedings of the 6th International Conference on Information Systems Security and Privacy*, Valletta, Malta, pp. 333-340. <https://doi.org/10.5220/0008914503330340>
- [8] Zhu, C., Li, J., Zhong, Z., Yue, C., Zhang, M. (2023). A survey on the integration of blockchains and databases. *Data Science and Engineering*, 8(2): 196-219. <https://doi.org/10.1007/s41019-023-00212-z>
- [9] Alani, D.S., Sagheer, A.M. (2024). Public key infrastructure approaches based on blockchain. In 2024 21st International Multi-Conference on Systems, Signals & Devices (SSD), Erbil, Iraq, pp. 369-375. <https://doi.org/10.1109/ssd61670.2024.10549485>
- [10] Pletinckx, S., Nguyen, T.D., Fiebig, T., Kruegel, C., Vigna, G. (2023). Certifiably vulnerable: Using certificate transparency logs for target reconnaissance. 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P), 817-831. <https://doi.org/10.1109/EuroSP57164.2023.00053>
- [11] Papageorgiou, A., Mygiakis, A., Loupos, K., Krousarlis, T. (2020). DPKI: A blockchain-based decentralized public key infrastructure system. In 2020 Global Internet of Things Summit (GloTS), Dublin, Ireland, pp. 1-5. <https://doi.org/10.1109/giots49054.2020.9119673>
- [12] Toorani, M., Gehrmann, C. (2021). A decentralized dynamic PKI based on blockchain. In *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, Virtual Event, Republic of Korea, pp. 1646-1655. <https://doi.org/10.1145/3412841.3442038>
- [13] Shi, J., Zeng, X., Han, R. (2022). A blockchain-based decentralized public key infrastructure for information-centric networks. *Information*, 13(5): 264. <https://doi.org/10.3390/info13050264>
- [14] Mosakheil, J., Yang, K. (2023). Decentralized compromise-tolerant public key management ecosystem with threshold validation. *Cryptology ePrint Archive, Report 2023/1791*. <https://eprint.iacr.org/2023/1791>
- [15] Halder, R., Das Roy, D., Shin, D. (2024). A blockchain-based decentralized public key infrastructure using the web of trust. *Journal of Cybersecurity and Privacy*, 4(2): 196-222. <https://doi.org/10.3390/jcp4020010>
- [16] Patidar, K., Jain, S., Husain, M., et al. (2025). Blockchain based decentralized identity management system for authentication and authorization in IoT networks. *Informatica*, 49(34): 131-146. <https://doi.org/10.31449/inf.v49i34.9164>
- [17] Dulia, O., Minochkin, D. (2023). An exploration of public key infrastructure applications across diverse domains: A comparative analysis. *Information Technology and Security*, 11(2): 137-148. <https://doi.org/10.20535/2411-1031.2023.11.2.293496>
- [18] Stapleton, J., Epstein, W.C. (2024). *Security Without Obscurity*. CRC Press. <https://doi.org/10.1201/9781003425298>
- [19] Patil, V.T., Shyamasundar, R.K. (2022). Evolving role of PKI in facilitating trust. In 2022 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA), Bangalore, India, pp. 1-7. <https://doi.org/10.1109/PKIA56009.2022.9952249>
- [20] Yakovenko, A. (2018). Solana: A new architecture for a high performance blockchain v0.8.13. Whitepaper. 2018. <https://solana.com/solana-whitepaper.pdf>
- [21] Wijaya, M., Melvyn, F., Setiawan, R., Rumagit, R.Y. (2025). Ethereum vs Solana: A comparative study of blockchain architecture on performance, security, and ecosystem development. *Procedia Computer Science*, 269: 200-217. <https://doi.org/10.1016/j.procs.2025.08.273>
- [22] Alizadeh, S., Khabbazi, M. (2025). Solana's transaction network: Analysis, insights, and comparison. *EPJ Data Science*, 14(1): 48. <https://doi.org/10.1140/epjds/s13688-025-00561-x>
- [23] Pierro, G.A., Tonelli, R. (2022). Can Solana be the solution to the blockchain scalability problem? In 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), Honolulu, HI, USA, pp. 1219-1226. <https://doi.org/10.1109/saner53432.2022.00144>
- [24] Song, H., Wei, Y., Qu, Z., Wang, W. (2024). Unveiling decentralization: A comprehensive review of technologies, comparison, challenges in Bitcoin, Ethereum, and Solana blockchain. In 2024 IEEE 6th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Chongqing, China, pp. 1896-1901. <https://doi.org/10.1109/IMCEC59810.2024.10575445>
- [25] Ashraf, M., Heavey, C. (2023). A prototype of supply chain traceability using Solana as blockchain and IoT. *Procedia Computer Science*, 217: 948-959. <https://doi.org/10.1016/j.procs.2022.12.292>
- [26] Zheng, X., Wan, Z., Lo, D., Xie, D., Yang, X. (2025). Why does my transaction fail? A first look at failed transactions on the Solana blockchain. *Proceedings of the ACM on Software Engineering*, 2(ISSTA): 1489-1512. <https://doi.org/10.1145/3728943>

- [27] Burdges, J., Kılınç Alper, H., Stewart, A., Vasilyev, S. (2023). Sassafras and semi-anonymous single leader election. Cryptology ePrint Archive, Report 2023/031. <https://eprint.iacr.org/2023/031>
- [28] Mishra, D.P., Behera, S.R., Behera, S.S., Patro, A.R., Salkuti, S.R. (2024). Solana blockchain technology: A review. *International Journal of Informatics and Communication Technology*, 13(2): 197-205. <https://doi.org/10.11591/ijict.v13i2.pp197-205>
- [29] Catalano, D., Fiore, D., Giunta, E. (2023). Efficient and universally composable single secret leader election from pairings. In *26th IACR International Conference on Practice and Theory of Public-Key Cryptography*, Atlanta, GA, USA, pp. 471-499. https://doi.org/10.1007/978-3-031-31368-4_17
- [30] Li, Z., Tan, T.G., Szalachowski, P., Sharma, V., Zhou, J. (2021). Post-quantum VRF and its applications in future-proof blockchain system. *arXiv preprint arXiv:2109.02012*. <https://doi.org/10.48550/arXiv.2109.02012>
- [31] Boneh, D., Eskandarian, S., Hanzlik, L., Greco, N. (2020). Single secret leader election. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, New York, NY, USA, pp. 12-24. <https://doi.org/10.1145/3419614.3423258>
- [32] Barker, E. (2020). Recommendation for key management: Part 1 - General, NIST Special Publication 800-57 Part 1 Revision 5. National Institute of Standards and Technology, Gaithersburg, MD. <https://doi.org/10.6028/nist.sp.800-57pt1r5>
- [33] Esgin, M.F., Ersoy, O., Kuchta, V., et al. (2023). A new look at blockchain leader election: Simple, efficient, sustainable and post-quantum. In *Proceedings of the ACM Asia Conference on Computer and Communications Security*, Melbourne, Australia, pp. 623-637. <https://doi.org/10.1145/3579856.3595792>
- [34] Gochhayat, S.P., Shetty, S., Mukkamala, R., Foytik, P., Kamhoua, G.A., Njilla, L. (2020). Measuring decentrality in blockchain-based systems. *IEEE Access*, 8: 178372-178390. <https://doi.org/10.1109/access.2020.3026577>
- [35] Zhai, Z., Shen, S., Mao, Y. (2022). BPKI: A secure and scalable blockchain-based public key infrastructure system for web services. *Journal of Information Security and Applications*, 68: 103226. <https://doi.org/10.1016/j.jisa.2022.103226>