NDAChain

WHITEPAPER

Empowering Vietnam's Digital Future with Hybrid Decentralized Identity (Hybrid DID) System

2025

Table of contents

NDAChain Whitepaper

Empowering Vietnam's Digital Future with Hybrid Decentralized Identity (Hybrid DID) System

Abstract

As Vietnam accelerates its digital transformation, the demand for a secure, scalable, and privacy-preserving digital identity system becomes paramount. The existing centralized identity infrastructure, while authoritative, faces limitations in privacy protection, scalability, and global interoperability. NDAChain introduces a Hybrid Decentralized Identity (DID) solution that leverages blockchain technology to enhance the national identity framework. By integrating a permissioned blockchain network with the National Database, NDAChain empowers citizens with control over their personal data, strengthens security, and enables seamless cross-border interactions. This whitepaper provides an in-depth technical overview of NDAChain, including formal protocol specifications, consensus mechanisms, performance benchmarks, and compliance with international standards.

1. Introduction

1.1. Background and motivation

Vietnam's rapid economic growth and digital transformation necessitate a robust digital identity infrastructure. The National Data Center (NDC) currently manages an identity system for over 100 million citizens, serving as the backbone for identity verification across various sectors. However, the centralized nature of this system presents challenges in cyber security, privacy, scalability, and interoperability.

1.2. The digital identity challenge

Key challenges include:

- Cyber security risks: Centralized storage creates a single point of failure, increasing vulnerability to data attacks and thefts.
- Scalability constraints: The existing centralized infrastructure may not be able to support the growing demand for digital services.
- Global interoperability limitations: Lack of alignment with international standards hinders cross-border interactions.
- Limited citizen control: Citizens have no tools to control their personal data and how it is shared.

1.3. Limitations of the existing solutions

While there are a couple of common identity solutions, they often fall short in balancing trust, privacy, scalability, and compliance:

- Centralized systems: Suffer from privacy and scalability issues.
- Federated systems: Depend on third-party providers, raising data sovereignty concerns.
- Self-sovereign identity (SSI): Offer user control but may lack authoritative verification and regulatory compliance.

1.4. The needs for NDAChain

NDAChain aims to:

- Combine the centralized identity system with the decentralized verification system.
- Enhance privacy through advanced cryptographic techniques.
- Scale efficiently to support national deployment.
- Align with global standards for interoperability.
- Empower citizens with control over their data.

---

2. Vision and Objectives

2.1. Enhancing security and privacy

- Advanced cryptography: Implement robust encryption and cryptographic protocols.
- Decentralized authentication: Mitigate risks associated with the centralized system.

2.2. Empowering citizens

- Data ownership: Citizens have full ownership and control over their identity data.
- Selective disclosure: The use of Zero-Knowledge Proofs (ZKPs) allows sharing only necessary information.

2.3. Achieving scalability and efficiency

- Efficient Consensus: Utilize Proof of Authority (PoA) for high throughput.
- Modular Architecture: Allow independent scaling of system components.

2.4. Enabling global interoperability

- Standards compliance: Adhere to W3C DID and Verifiable Credentials standards.
- Cross-border recognition: Facilitate international use of digital identities.

2.5. Ensuring regulatory compliance

- National regulations: Comply with Vietnamese laws on data protection.
- International regulations: Align with GDPR and other global standards.

---

3. The NDAChain Solution

3.1. Overview of the Hybrid DID System

NDAChain integrates a permissioned blockchain with the National Database to create a Hybrid DID system:

- Centralized identity: The National Database remains the authoritative source.
- Decentralized authentication management: Blockchain enables secure, distributed identity operations.
- User empowerment: Citizens manage their identities through DID wallets.

3.2 Key components

1. Permissioned blockchain network (Hyperledger Besu)
2. Validator nodes and governance
3. DID management layer and smart contracts
4. API gateway integration
5. Citizen DID wallets

---

4. Technical Architecture and Protocol Specifications

4.1. System architecture

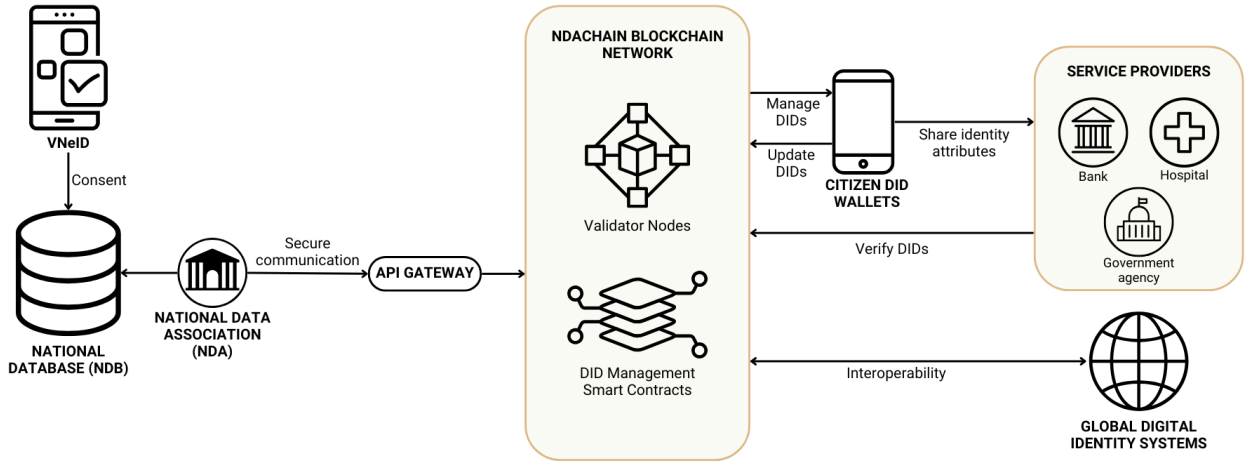

Figure 1: Detailed System Architecture of NDAChain

The system architecture comprises:

- VNeID: An authorized application that has access to the National Database and gets consent from citizens before using their data.
- National Database (NDB): A centralized repository of verified identity data.
- National Data Association (NDA): A government body managing data transmission from NDB and blockchain.
- API gateway (APIG): An interface between NDA and blockchain, ensuring secure communication.
- NDAChain blockchain network:
    - Validator nodes (VNs): Nodes that validate transactions.
    - DID management smart contracts (DIDSC): Contracts handling DID operations.
- Citizen DID wallets (CDW): Applications for citizens to manage identities.
- Service providers (SPs): Entities requiring identity verification.

4.2. Data structures and algorithms

4.2.1. Data structures

- Decentralized identifier (DID):

```
{
  "id": "did:pila:123456789abcdefghi",
  "publicKey": [ ... ],
  "authentication": [ ... ],
  "service": [ ... ],
  "created": "2023-01-01T00:00:00Z",
  "updated": "2023-01-01T00:00:00Z"
}
```

- Verifiable credentials (VC):

```
{
  "@context": [ "https://www.w3.org/2018/credentials/v1" ],
  "id": "credential-id",
  "type": [ "VerifiableCredential", "IdentityCredential" ],
  "issuer": "did:pila:issuer-id",
  "issuanceDate": "2023-01-01T00:00:00Z",
  "credentialSubject": {
    "id": "did:pila:subject-id",
```

```
    "attributes": { ... }
  },
  "proof": { ... }
}
```

4.2.2 Algorithms

- DID creation algorithm:
    1. Input: User registration data from NDB.
    2. Process:
        - Generate a unique DID using a cryptographic hash of the user's public key and other identifiers.
        - Store the DID Document on-chain via smart contracts.
    3. Output: DID assigned to the user.
- Zero-Knowledge Proof generation (using zk-SNARKs):
    1. Input: User's attribute to prove.
    2. Process:
        - Generate a zk-SNARK proof that verifies the attribute without revealing it.
    3. Output: ZKP sent to the verifier.

4.3. Consensus mechanism: Proof of authority (PoA)

4.3.1. Justification and comparison

- PoA advantages:
    - Efficiency: Lower latency and higher throughput compared to Proof of Work (PoW).
    - Energy consumption: Significantly less energy-intensive than PoW.
    - Control: Allows for a controlled set of validators, aligning with regulatory requirements.
- Comparison with other mechanisms:
    - Proof of stake (PoS): While PoS offers decentralization, it may not provide the necessary control for compliance.
    - Delegated PoS (DPoS): More complexities in governance and potential centralization risks.

4.3.2. Technical operation

- Validator selection:

    - Criteria: Compliance with security standards, trustworthiness, and operational capacity.
    - Onboarding process: Validators are added through a multi-signature smart contract requiring approval from existing validators.
- Block production:
    - Validators take turns producing blocks in a round-robin fashion.
    - Algorithm:

```
For each block height h:
    Validator V_i = V_h mod N
    V_i proposes block B_h
    Other validators validate B_h
    If B_h is valid, add to blockchain
```

- Consensus process:
    - Normal conditions: Validators follow the protocol, and blocks are confirmed quickly.
    - Byzantine conditions: If a validator behaves maliciously, the block is rejected by others.
- Fault tolerance:
    - The network can tolerate up to (N-1)/3 faulty validators.
    - Implements mechanisms for slashing or removing malicious validators.

4.4. DID management and smart contracts

- DID registry contract:
    - Functions:
        - `registerDID(didDocument)`
        - `updateDID(didDocument)`
        - `revokeDID(did)`
- Security measures:
    - Access control via role-based permissions.
    - Input validation to prevent injection attacks.

4.5. Zero-Knowledge Proof implementation

- ZKP protocol:
    1. Type: zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge)
    2. Properties:

        - Completeness: Honest proofs are always accepted.
        - Soundness: False proofs are rejected.
        - Zero-Knowledge: No information about the underlying data is revealed.
- Implementation steps:
    1. Setup: Generate public parameters (trusted setup).
    2. Proving: User generates a proof for a statement (e.g., age over 18).
    3. Verification: Verifier checks the proof using the public parameters.

4.6. Integration with existing systems

- API gateway specifications:
    - Protocol: RESTful API with TLS encryption.
    - Authentication: OAuth 2.0 with JWT tokens.
    - Endpoints:
        - `/register`: For registering new identities.
        - `/update`: For updating identity attributes.
        - `/revoke`: For revoking identities.
- Data synchronization:
    - Real-time updates via event-driven architecture.
    - Use of message queues for reliability.

4.7. Validator onboarding process

4.7.1. Overview

NDAChain is a national blockchain platform, requiring the selection and participation of validators to adhere to stringent criteria to ensure security, reliability, and data sovereignty. Validators are restricted to organizations with critical roles in the national ecosystem, including:

- National ministries and agencies, such as the Ministry of Information and Communications, the Ministry of Public Security, or the National Data Center (NDC).
- Representatives of key provinces and cities, such as Hanoi, Ho Chi Minh City, Da Nang, or provinces with significant economic roles.
- State-owned enterprises or major private corporations with national influence, such as Viettel, VNPT, or large banks, provided they meet security and operational capacity standards.

4.7.2. Validator selection criteria

To become a validator, organizations must meet the following criteria:

- Legality and Reputation: The organization must be officially recognized by a competent state authority, with a transparent operational history and compliance with legal regulations.
- Technical Capability: Possession of robust IT infrastructure, meeting hardware, software, and security requirements (e.g., use of Hardware Security Modules - HSM).
- Regulatory Compliance: Commitment to national and international security standards, including ISO/IEC 27001 and Vietnam's Cybersecurity Law.
- Strategic Contribution: Evidence of a strategic role in supporting national digital transformation or promoting public services.

4.7.3. Validator onboarding process

The onboarding process is designed to be rigorous, transparent, and managed by the National Data Association (NDA) or the National Data Center (NDC). The steps include:

1. Application:
    - Organizations submit applications through the official NDA/NDC portal, providing details on technical, legal, and strategic capabilities.
2. Evaluation and approval:
    - The committee assesses applications based on capability and alignment with national objectives. Approved organizations are added to a whitelist.
3. Authorization by the root validator:
    - The National Data Center (NDC), acting as the root validator, formally authorizes new validators through a multi-signature smart contract. This process requires approval from at least two-thirds of existing validators.
4. Configuration and activation:
    - The new validator deploys a node according to NDA-provided technical specifications, undergoes security and performance audits. Upon passing, the node is activated and joins the Proof of Authority (PoA) consensus mechanism.
5. Continuous monitoring and evaluation:
    - Validators are continuously monitored to ensure compliance and performance. Non-compliance may result in suspension or removal.

4.7.4. Role of the root validator

The National Data Center (NDC) serves as the root validator with the following responsibilities:

- Veto power: Holds 35% of the network's voting rights, enabling veto authority over critical decisions, such as validator onboarding or protocol updates.
- Validator authorization: Approves new validators through smart contracts, ensuring only qualified entities participate.
- Network Governance: Oversees network operations, coordinating with the NDA to maintain system integrity and security.

5. Security Analysis

5.1. Threat models

- External attackers: Attempt unauthorized access to data or disrupt network operations.
- Internal adversaries: Malicious validators or insiders compromising system integrity.
- Privacy threats: Unauthorized linkage of user identities or attribute disclosure.

5.2. Security properties

- Confidentiality: Ensured through encryption and ZKPs.
- Integrity: Protected by blockchain immutability and consensus mechanisms.
- Availability: Achieved via network redundancy and fault tolerance.
- Non-repudiation: Transactions are signed and verifiable.

5.3. Formal verification methods

- Smart contract verification:
    - Use of formal methods like TLA+ or Isabelle/HOL to verify contract correctness.
    - Model checking to detect logical errors.
- Protocol verification:
    - Security protocol analysis: Verify properties like secrecy and authentication using tools like ProVerif.
- Compliance verification:
    - Regular audits to ensure adherence to standards and regulations.

---

6. Performance Benchmarks

6.1. Transaction throughput and latency

- Test environment:
    - Validators: 5 nodes with recommended hardware specifications.
    - Full nodes: 5 nodes with recommended hardware specifications.
    - Network conditions: Simulated latency of 50ms between nodes.
- Results:
    - Throughput: Achieved an average of 1,200 transactions per second (TPS).
    - Latency: Average transaction confirmation time of 1.5 seconds.

6.2. Scalability tests

- Linear scaling:
    - Increased validator nodes from 10 to 50.
    - Observed proportional increase in network capacity.
- Stress testing:
    - Simulated peak loads with 10,000 concurrent transactions.
    - The system maintains 95% uptime with minor performance degradation.

6.3. Comparative analysis

- Compared to Ethereum (PoW):
    - Ethereum TPS: Approximately 15 TPS.
    - NDAChain TPS: ~1,200 TPS, significantly higher due to PoA and permissioned network.
- Compared to Hyperledger Fabric:
    - Hyperledger Fabric TPS: Up to 3,500 TPS under optimal conditions.
    - NDAChain TPS: Comparable, with potential for optimization.

---

7. Use Cases and Scenarios

7.1. Accessing government services

Scenario: Nguyen, a resident of Hanoi, needs to renew his driver's license online. Traditionally, this process requires multiple visits to government offices and extensive paperwork.

Process with NDAChain:

1. Authentication:
    - Nguyen logs into the VNeID app, which in this case also serves as his DID wallet, secured with biometric authentication.
2. Selective disclosure:
    - Through his DID wallet, he consents to share only the necessary attributes required for license renewal, such as proof of identity and current license details.
    - Generates a Zero-Knowledge Proof (ZKP) that validates his eligibility without exposing personal data.
3. Verification:
    - The government system verifies the ZKP via NDAChain, confirming Nguyen's identity and eligibility.

    - The verification process is recorded on the blockchain for audit purposes.
4. Application processing:
    - The application is automatically processed, and any necessary updates are made to Nguyen's DID document.
5. Notification:
    - Nguyen receives a digital notification of his renewed license, which is also reflected in his DID wallet.

Benefits:

- Efficiency: Reduces processing time from days to minutes.
- Privacy: Protects personal data through ZKPs.
- Auditability: Provides a tamper-proof record of the transaction.

7.2. Simplifying financial transactions

Scenario: Linh wants to apply for a loan from a bank to start her small business.

Process with NDAChain:

1. Initiation:
    - Linh accesses the bank's online loan application portal.
2. Identity verification:
    - Uses her DID wallet to share verifiable credentials required by the bank, such as identity proof and credit history.
3. ZKP utilization:
    - Generates ZKPs to prove her income level and creditworthiness without revealing detailed financial information.
4. Real-Time Verification:
    - The bank verifies the credentials and ZKPs via NDAChain, ensuring data integrity and authenticity.
5. Loan Approval:
    - Upon successful verification, the bank processes her loan application promptly.

Benefits:

- Speed: Accelerates the loan approval process.
- Data security: Sensitive financial details remain confidential.
- Trust: Builds confidence in the authenticity of the applicant's information.

7.3. Enhancing cross-border interactions

Scenario: Anh is an entrepreneur planning to expand his business internationally. He needs to establish his identity with foreign partners.

Process with NDAChain:

1. Credential presentation:
    - Anh shares his DID and relevant verifiable credentials with international partners.
2. Interoperability:
    - Because NDAChain adheres to W3C DID standards, foreign entities can verify his credentials using their systems.
3. Verification:
    - Partners verify the authenticity of Anh's credentials via compatible global identity networks.
4. Business transactions:
    - Anh can securely engage in contracts and transactions with international parties.

Benefits:

- Global recognition: Facilitates cross-border business activities.
- Security: Ensures secure and verifiable identity exchange.
- Efficiency: Reduces time and resources spent on identity verification.

7.4. Additional use cases

7.4.1. Healthcare services

Scenario: Minh, a patient, needs to share medical records with a specialist while maintaining privacy.

Process with NDAChain:

- Minh uses his DID wallet to generate ZKPs that confirm necessary medical conditions without exposing full medical history.
- The specialist verifies the information via NDAChain.

Benefits:

- Protects sensitive health data.
- Streamlines patient onboarding and consultation processes.

7.4.2. Academic credential verification

Scenario: Thao, a recent graduate, applies for a job and needs to verify her educational qualifications.

Process with NDAChain:

- Thao shares verifiable credentials of her degrees through her DID wallet.
- Employers verify the credentials via NDAChain, ensuring they are tamper-proof.

Benefits:

- Prevents credential fraud.
- Simplifies the hiring process for employers.

---

8. Implementation Plan

8.1. Phased deployment strategy

Phase 1: Pilot deployment

- Duration: Months 1-3
- Technical Activities:
    - Set up initial validator nodes with high-security standards.
    - Deploy smart contracts for DID management on the blockchain.
    - Develop and distribute beta versions of the DID wallet to a controlled group.
    - Integrate the API gateway with the National Database.
- Infrastructure setup:
    - Configure secure network environments.
    - Establish monitoring and logging systems.
- Expected outcomes:
    - Validate system functionality and security.
    - Gather initial performance data.

Phase 2: Regional rollout

- Duration: Months 4-6
- Technical activities:
    - Expand the validator network to include additional nodes.
    - Optimize smart contracts based on pilot feedback.
    - Enhance DID wallet features for better user experience.
- Node configuration:
    - Implement load balancing.
    - Ensure redundancy and high availability.
- Expected outcomes:
    - Demonstrate scalability.
    - Refine the system based on regional usage patterns.

Phase 3: National rollout

- Duration: Months 7-12
- Technical activities:
    - Onboard additional validators nationwide.
    - Fully integrate with government services and major private-sector partners.
    - Implement advanced security measures, such as HSMs across validator nodes.
- Network management:
    - Establish a national network operations center.
    - Implement comprehensive security incident response protocols.
- Expected outcomes:
    - Achieve nationwide adoption.
    - Establish sustainable governance structures.

8.2. Testing and quality assurance

8.2.1. Functional testing

- Scope:
    - Test all smart contract functions.
    - Validate API gateway operations.
- Tools:
    - Use testing frameworks like Truffle and Ganache for smart contracts.
    - Automated API testing tools like Postman.

8.2.2. Performance testing

- Scope:
    - Assess the system under various load conditions.
- Tools:
    - Load testing tools such as Apache JMeter.
- Metrics:
    - TPS, latency, resource utilization.

8.2.3. Security testing

- Scope:
    - Penetration testing on network and application layers.
    - Vulnerability scanning of smart contracts.

- Tools:
    - Use tools like Metasploit, Nessus, and MythX for smart contract analysis.

8.2.4. User acceptance testing (UAT)

- Scope:
    - Real-world testing with end-users.
- Activities:
    - Collect feedback on usability, performance, and functionality.
- Outcome:
    - Finalize user interfaces and workflows.

8.3. Public awareness and education programs

8.3.1. Citizen education campaigns

- Methods:
    - Create educational content explaining NDAChain and its benefits.
    - Host webinars and workshops.
    - Utilize social media platforms for wider reach.

8.3.2. Validator training programs

- Content:
    - Technical training on node operation and maintenance.
    - Security best practices.
    - Compliance and regulatory requirements.

8.3.3. Service provider workshops

- Objectives:
    - Facilitate integration with NDAChain.
    - Provide technical support and resources.
- Activities:
    - Hands-on workshops.
    - Development of integration toolkits and SDKs.

8.4. Stakeholder engagement and collaboration

- Government agencies:
    - Establish inter-departmental committees.
    - Align policies and regulations.

- Private sector partners:
    - Form strategic partnerships.
    - Co-develop solutions leveraging NDAChain.
- Regulatory bodies:
    - Regular consultations.
    - Ensure compliance with evolving regulations.
- International organizations:
    - Participate in global forums.
    - Align with international best practices.

---

9. Future Outlook and Roadmap

9.1. Expansion of the validator network

- Objective:
    - Increase network resilience and decentralization.
- Actions:
    - Onboard academic institutions, NGOs, and international organizations.
    - Implement geographic distribution of nodes.

9.2. Enhanced privacy and security features

- Advanced cryptography:
    - Implement zk-STARKs for more efficient ZKPs.
- Quantum-resistant algorithms:
    - Research and integrate cryptographic algorithms resistant to quantum computing threats.
- MFA and biometrics:
    - Enhance DID wallet security with multi-factor authentication and other advanced biometric options.

9.3. Integration with global digital identity standards

- Standards adoption:
    - Incorporate emerging standards like DIDComm for secure communication.
- International partnerships:
    - Collaborate with global identity initiatives like ID2020.

9.4. Enhancing user experience

- Accessibility:
    - Support multiple languages.
    - Design for users with disabilities.
- User feedback loop:
    - Establish channels for continuous user feedback and improvement.

9.5. Research and development for advanced use cases

- IoT integration:
    - Develop identity solutions for devices in smart cities.
- AI and machine learning:
    - Utilize AI for anomaly detection and fraud prevention.
- Decentralized autonomous organizations (DAOs):
    - Explore governance models utilizing DAOs for community-driven decision-making.

9.6. Continuous improvement of privacy and compliance standards

- Regulatory monitoring:
    - Stay abreast of changes in data protection laws.
- Ethical considerations:
    - Ensure ethical use of data and technology.

9.7. Sustainability and long-term vision

- Funding models:
    - Explore options like service fees, grants, and public-private partnerships.
- Global leadership:
    - Position NDAChain as a model for digital identity solutions worldwide.

---

10. Risk Analysis and Mitigation Strategies

10.1. Technical risks

10.1.1. Consensus mechanism attacks

- Risk: Malicious validators colluding to disrupt consensus.
- Mitigation:
    - Implement stringent validator selection criteria.

    - Incorporate slashing mechanisms to penalize misbehavior.

10.1.2. Cryptographic vulnerabilities

- Risk: Advances in computing rendering current cryptographic algorithms insecure.
- Mitigation:
    - Regularly update cryptographic protocols.
    - Research and adopt quantum-resistant algorithms.

10.2. Operational risks

10.2.1. Node failure

- Risk: Validator nodes going offline affecting network performance.
- Mitigation:
    - Ensure redundancy.
    - Implement automatic failover mechanisms.

10.2.2. Data synchronization issues

- Risk: Inconsistencies between the National Database and NDAChain.
- Mitigation:
    - Implement robust synchronization protocols.
    - Regular audits and consistency checks.

10.3. Adoption risks

10.3.1. User resistance

- Risk: Users reluctant to adopt new technologies.
- Mitigation:
    - Focus on user-friendly design.
    - Provide incentives and clear benefits.

10.3.2. Stakeholder misalignment

- Risk: Conflicting interests among stakeholders hindering progress.
- Mitigation:
    - Establish clear governance structures.
    - Foster transparent communication.

10.4. Compliance risks

10.4.1. Non-compliance with regulations

- Risk: Unintentional violations of data protection laws.

- Mitigation:
    - Engage legal experts.
    - Implement compliance monitoring tools.

10.4.2. International legal challenges

- Risk: Cross-border data sharing leading to legal disputes.
- Mitigation:
    - Establish clear international agreements.
    - Adhere to international data protection standards.

---

11. Compliance and Standards Alignment

11.1. International standards compliance

- W3C DID and VC standards:
    - Ensures interoperability with global identity systems.
- ISO/IEC 27001:
    - Adheres to international standards for information security management.
- ISO/TC 307:
    - Aligns with blockchain and distributed ledger technologies standards.

11.2. Regulatory compliance

- GDPR alignment:
    - Legal basis: Data is processed only with explicit consent from data subjects or based on legal obligations.
    - Data subject rights: Mechanisms are in place for individuals to access, rectify, or delete their data.
- Compliance with Vietnam's Cybersecurity Law and Personal Data Protection Decree, incorporating the following principles:
    - Transparent consent: Citizens must provide consent before their data is processed, facilitated through the VNeID application.
    - Data minimization: Only essential data is collected, leveraging Zero-Knowledge Proofs (zk-SNARKs) to verify information without exposing sensitive details.
    - Data subject rights: Citizens have the right to access, modify, or delete their personal data.

11.3. Privacy control mechanisms

- Anonymization: Temporary identifiers and Zero-Knowledge Proofs are used to prevent unauthorized linking of user identities.
- Auditing: Regular privacy audits are conducted to ensure compliance with data protection policies.

---

12. Conclusion and Call to Action

NDAChain represents a significant advancement in Vietnam's digital identity landscape. By combining centralized trust with decentralized technologies, it offers a secure, scalable, and user-centric solution. The successful implementation of NDAChain requires collaboration among government entities, private sector partners, and citizens.

We call upon all stakeholders to join us in this transformative journey towards a secure and efficient digital future. Together, we can make NDAChain a model for digital identity systems worldwide.

---

13. References

1. W3C Decentralized Identifiers (DID) v1.0
    - Link to Standard
2. W3C Verifiable Credentials Data Model v1.1
    - Link to Standard
3. General Data Protection Regulation (GDPR)
    - Link to Regulation
4. Vietnamese Law on Cybersecurity
    - Link to Law
5. Hyperledger Besu Documentation
    - Link to Documentation
6. Zero-Knowledge Proofs in Blockchain
    - Educational Resource
7. ISO/IEC 27001 Information Security Management
    - Link to Standard
8. NIST Cybersecurity Framework
    - Link to Framework
9. OWASP Top Ten Security Risks
    - Link to Resource

10. Blockchain Security Best Practices
    - Link to Resource

---

14. Appendix

A. Glossary

- Blockchain: A decentralized ledger of all transactions across a peer-to-peer network.
- Decentralized Identifier (DID): A globally unique identifier that does not require a centralized registration authority.
- Zero-Knowledge Proof (ZKP): A cryptographic method where one party can prove to another that a statement is true without revealing any information beyond the validity of the statement.
- Proof of Authority (PoA): A consensus mechanism where transactions are validated by approved accounts known as validators.
- Permissioned blockchain: A blockchain network where access and participation are controlled.
- Validator node: A node responsible for validating transactions and maintaining the blockchain ledger.
- Hyperledger Besu: An open-source Ethereum client designed for enterprise use.
- Verifiable credentials (VC): A tamper-evident credential that can be cryptographically verified.

B. Detailed protocol specifications

B.1. DID registry smart contract functions

- registerDID(address did, DIDDocument doc):
    - Registers a new DID and associates it with a DID Document.
    - Access Control: Only authorized entities can call this function.
- updateDID(address did, DIDDocument doc):
    - Updates the DID Document associated with an existing DID.
    - Validation: Ensures the caller has the authority to make changes.
- revokeDID(address did):
    - Revokes an existing DID, marking it as inactive.
    - Impact: Prevents future verifications using this DID.

B.2. Access control mechanisms

- Role-based access control (RBAC):
    - Defines roles such as 'Validator', 'Issuer', and 'User'.

- Assigns permissions based on roles.

C. Mathematical definitions and algorithms

C.1. Zero-Knowledge Proofs (zk-SNARKs)

- Definition:
  - A tuple `(G, P, V)` where:
    - $G(1^\lambda) \rightarrow (pp, vk)$: Generates public parameters and verification keys.
    - `P(pp, x, w) → π`: Prover uses public parameters, statement `x`, and witness `w` to generate proof `π`.
    - $V(vk, x, \pi) \rightarrow \{0,1\}$: Verifier uses verification key, statement, and proof to accept or reject.
- Properties:
  - Completeness: If `w` is a valid witness for `x`, then `V(vk, x, π) = 1`.
  - Soundness: If `V(vk, x, π) = 1`, then there exists a `w` such that `P` could have generated `π`.
  - Zero-Knowledge: `π` reveals no information about `w`.

C.2. Consensus algorithm formalization

- System model:
  1. A set of validators `V = {v1, v2, ..., vn}`.
  2. Each validator maintains a local copy of the blockchain `B`.
- Safety property:
  1. For any two honest validators `vi` and `vj`, their blockchains `Bi` and `Bj` agree on all blocks up to the latest confirmed block.
- Liveness property:
  1. Transactions submitted by honest clients are eventually included in `B`.
- Algorithm steps:
  1. Proposal:
     - Validator `v_p` proposes a block `B_h` at height `h`.
  2. Validation:
     - Other validators verify `B_h` for correctness.
  3. Commitment:
     - If valid, validators add `B_h` to their local blockchain.

D. Performance benchmark data

D.1. Transaction throughput graph

- Description:
    - Graph showing TPS over time under varying loads.
- Observation:
    - TPS remains stable up to 80% of maximum capacity.

D.2. Latency distribution chart

- Description:
    - Histogram of transaction confirmation times.
- Observation:
    - The majority of transactions are confirmed within 1-2 seconds.

D.3. Scalability test configurations

- Test parameters:
    - Number of validator nodes: 10, 20, 30, 40, 50.
    - Network latency: Simulated at 50ms, 100ms.
- Results summary:

Validators	TPS	Latency (Avg)
10	1,200	1.5s
20	1,800	1.7s
30	2,200	1.9s
40	2,500	2.1s
50	2,800	2.3s