OPEN ACCESS CASES

Vol 1. Issue 3, Q3 2024 (July-September)
Section: Commentaries & Reviews
Category: Public Administration, Policy, and Governance

Review of Bhutan NDI & ToIP Digital Trust Ecosystems

Tshering Wangdi[1]

Introduction

The Bhutan National Digital Identity (NDI) case study, authored by Pallavi Sharma, a key figure in the Bhutan National Digital Identity Project at Druk Holding & Investments, and Eric Drury, Director of Forthco.io, highlights an ambitious and forward-looking initiative undertaken by Bhutan. Their expertise and experience in digital identity and governance lend credibility to the insights presented in this case study. This project represents the Kingdom's strategic efforts to establish a robust national digital trust ecosystem seamlessly integrating citizens, governmental institutions, and private organisations. By adopting the transformative principles of Self-Sovereign Identity (SSI), the NDI system prioritizes secure, privacy-centric, and inclusive digital interactions. This approach safeguards user data and empowers individuals with greater control over their personal information, setting the stage for a digitally empowered society.

The initiative aligns with Bhutan's broader vision of leveraging digital transformation to foster national progress and lay the groundwork for a thriving digital economy. It reflects the country's strategic foresight in embracing cutting-edge technologies to enhance the efficiency of public services strengthen governance, and catalyse economic growth.

The case study provides a detailed and holistic perspective on Bhutan's unique circumstances, including its challenging geographical terrain, dispersed rural population, and economic structure largely centred around agriculture. These factors have historically posed barriers to equitable access to public services and digital inclusion. By embracing SSI principles, Bhutan has effectively addressed these challenges through a decentralised framework emphasising privacy preservation, security, and adaptability.

This decentralised approach aligns with Bhutan's commitment to safeguarding individual privacy and ensures inclusivity, particularly for remote and underserved communities. By overcoming infrastructure limitations and reducing dependency on traditional centralised systems, the Bhutan NDI initiative demonstrates the potential of technology to bridge divides

[1] Tshering Wangdi is a research fellow at Gedu College of Business Studies, Bhutan, specializing in digital transformation, sustainable development, and public policy.

OPEN ACCESS CASES

Vol 1. Issue 3, Q3 2024 (July-September)
Section: Commentaries & Reviews
Category: Public Administration, Policy, and Governance

and foster nationwide digital connectivity. This ambitious endeavour serves as a shining example for other nations and instils optimism about the future of digital governance.

Key Components

Ecosystem Parties

The Bhutan NDI ecosystem revolves around three primary participants: the government, individuals, and organisations. Each party plays a crucial role in the ecosystem, ensuring that digital interactions are secure, trustworthy, and efficient. Through a robust authentication process, all parties receive unique Decentralized Identifiers (DIDs), which are fundamental to enabling seamless and reliable digital transactions within the ecosystem.

Government

The government is the central authority and ultimate trusted entity within the Bhutan NDI ecosystem. It oversees the issuance of foundational IDs and manages key governance aspects, ensuring that all processes align with national priorities such as privacy, security, and inclusivity. Various governmental departments, such as the Department of Civil Registration and Census (DCRC) and the Department of Immigration, are actively involved in issuing verifiable credentials for citizens and non-residents, including academic records, employment credentials, and visas.

Individuals

Citizens, non-resident workers, students, and even tourists are all integral parts of the ecosystem. By undergoing biometric verification and receiving DIDs, individuals are empowered to access a range of digital services. This approach ensures that even those in remote areas can benefit from the ecosystem's inclusivity. Self-attested credentials further enhance user autonomy by allowing individuals to manage and share specific data without external validation.

Organizations

Private and public sector organizations participate as ecosystem parties, gaining organizational DIDs to authenticate their interactions. Banks, educational institutions, telecommunications companies, and others that issue or verify credentials. Trust within the ecosystem is strengthened through these organizations' adherence to the governance framework and their presence in the NDI Trust Registry.

Strengths

- The structured onboarding process for all participants ensures transparency and instils trust within the ecosystem. The system exhibits flexibility and scalability by accommodating diverse categories, including tourists and non-nationals.

Challenges

- Scaling the onboarding process for non-national entities, such as foreign workers or international students, presents logistical and operational challenges. Similarly, achieving seamless interoperability with external systems for cross-border recognition of credentials remains a critical area for development.

Verifiable Data

At the core of the Bhutan NDI system lies its ability to manage and exchange verifiable data securely. The system employs W3C-compliant Verifiable Credentials (VCs), cryptographically signed digital information representations. These credentials cover a wide range of data types, including foundational IDs, academic records, employment credentials, and even self-attested information like allergies or email addresses. The inclusion of self-attested credentials empowers users to have greater control over their personal data, fostering autonomy and a user-centric approach.

Highlights

- Privacy is a cornerstone of the system, achieved through advanced techniques such as zero-knowledge proofs and selective data disclosure. These allow individuals to share only the necessary information without revealing their complete identity.

- VCs enhance trust by ensuring that data integrity is maintained during exchanges between parties, reducing the risks of tampering or fraud.

Potential Risks

- The system's reliance on specific underlying technologies, such as the Hyperledger Indy blockchain, could pose challenges during system updates or migrations. Any disruptions in these foundational technologies might impact the ecosystem's reliability and user experience.

Governance Framework

The governance of the Bhutan NDI ecosystem is meticulously structured to balance innovation, security, and inclusivity. Anchored by the National Digital Identity Act of Bhutan (2023), the

framework defines all ecosystem participants' roles, responsibilities, and operational standards. Governance is divided between two main bodies:

1. **The Governing Body:** This independent body oversees the ecosystem's strategic direction, ensuring alignment with the NDI Act and Bhutan's broader national goals. It approves regulations for onboarding participants and supervises cross-border interoperability.

2. **The Administrative Body:** Operated by the Bhutan NDI company, this entity manages the ecosystem's day-to-day operations, including onboarding, infrastructure development, and participant certification.

Observations

The governance framework's alignment with Bhutan's sustainability and governance goals reflects its holistic approach to development. However, continuous evaluation and updates will be necessary to adapt to rapid technological advancements and emerging threats, ensuring the system's adaptability and future-proof nature.

Trust Registries and Enabling Systems

Trust registries form the backbone of the Bhutan NDI ecosystem's technical infrastructure. The two primary registries are:

1. **NDI Trust Registry:** This registry contains a list of trusted organizational DIDs, which are essential for authentication and verification processes.

2. **Verifiable Data Registry:** Built on the Hyperledger Indy blockchain and set to migrate to Polygon, this registry stores public keys, DID documents, and cryptographic metadata, ensuring the integrity of data exchanges.

The ecosystem also relies on various enabling systems and technologies, such as decentralized identifiers, cryptographic protocols, and distributed ledger technology. These elements collectively enhance trust and ensure secure, privacy-preserving interactions. For example, zero-knowledge proof protocols allow parties to verify information without revealing sensitive data.

Strengths

- The use of blockchain technology ensures transparency and immutability, creating a strong foundation for trust.

Challenges

- Limited internet connectivity in remote areas hinders real-time data access. Developing offline solutions or hybrid systems could mitigate this issue.

Trust Tasks

Trust tasks represent the tangible actions performed within the ecosystem, where trust is built and maintained. These tasks are facilitated through the NDI wallet, a user-friendly interface that integrates critical onboarding, credential issuance, and verification workflows. By minimising manual intervention, these processes enhance user experience and build confidence in the system's reliability.

Examples of Trust Tasks

1. **Onboarding:** Individuals and organisations are onboarded into the ecosystem through biometric verification and credential issuance. For individuals, this involves receiving a foundational ID, while organisations gain public DIDs.

2. **Credential Exchange:** Parties within the ecosystem can issue, receive, and verify credentials securely. For instance, a university may issue a student ID VC, which the student can use to access academic portals.

3. **Passwordless Login:** The NDI wallet supports passwordless login, simplifying authentication for users. For example, users of the Bank of Bhutan's mobile banking app can log in using their NDI credentials instead of traditional usernames and passwords.

Use Case

- The integration of the NDI system with banking apps like mBOB demonstrates its practical utility. By leveraging the NDI wallet, users can securely log in without sharing sensitive information, streamlining access to financial services.

Impact on User Experience

- The NDI wallet's seamless workflows not only simplify digital interactions but also foster trust by ensuring that all participants in the ecosystem are authenticated and verified.

OPEN ACCESS CASES

Vol 1. Issue 3, Q3 2024 (July-September)
Section: Commentaries & Reviews
Category: Public Administration, Policy, and Governance

Recommendations

Technology Dependency

To address the challenges of over-reliance on specific technologies, organisations can take strategic measures to ensure resilience and adaptability. Establishing a **Technology Oversight Committee** comprised of experts can guide decision-making, manage dependencies, and oversee timely updates. Diversifying technology partnerships reduces the risks of relying on a single provider, promoting flexibility and minimising potential disruptions. Open standards, such as open-source platforms, enhance adaptability and prevent vendor lock-in. Regular **scenario-based testing** can help evaluate system resilience under various failure conditions and improve contingency planning. A Technology Reserve Fund should also be established to finance emergency updates, upgrades, or transitions, safeguarding operations during critical technological shifts.

Interoperability

Promoting seamless integration and collaboration between digital systems requires robust interoperability measures. A **National Interoperability Policy** aligned with international standards is essential for ensuring compatibility across Bhutan's digital identity ecosystem. Active participation in **international workshops** and forums can keep stakeholders informed about global advancements and best practices. Regional collaboration with neighbouring countries can establish shared goals and mutual recognition of digital credentials, leveraging trade agreements. Smart contracts powered by blockchain can automate interoperability protocols while ensuring compliance. Additionally, **interoperability hackathons** can foster innovation, engaging tech communities to develop and test cross-border solutions.

Awareness and Training

Awareness and training are critical for the widespread adoption and effective use of digital identity systems. Incorporating **digital identity education into school curricula** ensures that younger generations are well-versed in its benefits and safe usage. Multilingual educational materials in Bhutan's official languages and local dialects enhance inclusivity and understanding across diverse communities. Gamified training programs create interactive learning experiences, making the subject more engaging for all users. Providing certifications and incentives for workshop participants, especially rural leaders, encourages broader participation. Finally, tracking adoption rates can identify underserved regions or groups, enabling targeted outreach and resource allocation to ensure equitable access.

OPEN ACCESS CASES

Vol 1. Issue 3, Q3 2024 (July-September)
Section: Commentaries & Reviews
Category: Public Administration, Policy, and Governance

Infrastructure Limitations

Overcoming infrastructure challenges requires innovative solutions to extend connectivity and service delivery to remote areas. Satellite connectivity can be leveraged to provide internet access to mountainous and underserved regions. Public-private partnerships can co-fund and co-develop telecommunications projects, bridging the urban-rural divide. Deploying **mobile digital identity units** equipped with offline tools can deliver services to areas with limited connectivity. Renewable energy, such as solar-powered communication hubs, offers sustainable and reliable connectivity options for off-grid regions. Establishing a **community support network**, with trained local technicians maintaining digital infrastructure, ensures continuity and localised troubleshooting.

Data Security and Privacy

Ensuring robust data security and privacy is vital for building trust in digital systems. A **National Cybersecurity Task Force** can provide centralised oversight for monitoring, managing, and responding to cybersecurity threats. Continuous training for government officials and ecosystem partners ensures familiarity with emerging security practices and tools. Investments in **privacy-enhancing technologies**, such as homomorphic encryption, bolster data protection. Updating legal frameworks to align with international standards, such as GDPR, strengthens regulatory compliance. Public awareness campaigns can cultivate a security culture, empowering users with knowledge about safe practices. Advanced AI-driven threat detection systems can proactively identify and mitigate potential breaches, enhancing overall resilience.

References

Sharma, P., Druk Holding & Investments, Drury, E., ToIP Ecosystem Foundry Working Group members, & Druk Holdings & Investments NDI project team. (2024). Bhutan NDI (National Digital Identity) & TOIP Digital Trust Ecosystems. In *Bhutan NDI (National Digital Identity) & ToIP Digital Trust Ecosystems* [Case Study]. https://trustoverip.org/wp-content/uploads/Case-Study-Bhutan-NDI-National-Digital-Identity-ToIP-Digital-Trust-Ecosystems-V1.0-2024-05-21.ext_.pdf

Sharma, P. (2023). Bhutan NDI applications in digital governance and Economy. In *The Druk Journal* (Vols. 10–10, Issue 1, pp. 40–43). http://drukjournal.bt/wp-content/uploads/2024/06/Bhutan-NDI-Applications.pdf

https://parliament.bt. (n.d.). *National Digital Identity Act of Bhutan 2023*. Parliament of Bhutan. https://parliament.bt/national-digital-identity-act-of-bhutan-2023

OPEN ACCESS CASES

Vol 1. Issue 3, Q3 2024 (July-September)
Section: Commentaries & Reviews
Category: Public Administration, Policy, and Governance

DISCLAIMER: *This commentary/review has been independently researched and written, without any external influence or bias. The content presented is based solely on objective analysis, facts, and available data. There is no conflict of interest between the author(s) and the subject or the company featured in this commentary/review. Furthermore, this study has not been commissioned, sponsored, or compensated by the subject, the company, or any related party. All views and conclusions expressed in this commentary/review are those of the author(s) and are not influenced by any external stakeholders. The purpose of this commentary/review is to provide informative and unbiased insights for educational and research purposes.*