UN/CEFACT Blockchain Whitepaper

Chapter

Security and Authentication for Blockchain

Chapter Coordinator

Mr. Tahseen Ahmad Khan, Vice Chair, UN/CEFACT

Contributing Experts

Ms. Anita Patel

Mr. Anurag Bana

Mr. Kaushik Srinivasan

Mr. Ravi Jagannathan

Mr. Venkatraman V

Mr. Vijay Kumar

Mr. Yuvaraj Thanikachallam

Security and Authentication for Blockchain

- Key aspects covered
  - Identity
  - Identification and Authentication
  - Authorization and Non-repudiation/ Admissibility of Electronic Evidence
  - Time Stamping
  - Data Access, Sharing, Retention, Accuracy and Integrity
  - Liability Issues and Dispute Settlement
  - Mutual Recognition
  - Conclusion

Security and Authentication for Blockchain

- Key Points
  - Like other systems, Blockchain systems also have a need for establishing trust (to ensure participants are who they claim they are)
  - Relying parties or regulations often define the level of risk assurance and this drives the requirements identity proofing, authentication/authorization and non-repudiation for such transactions on a Blockchain system.
  - Definition of Standards, Transaction Rules, Technology Assurance and Audit Trails may be critical to cross border acceptance of contracts
  - Blockchain offers huge scope in creating a security and authentication framework that can reduce costs significantly and offer enhanced security. Intergovernmental framework may be required for enablement and mass adoption.

Security and Authentication for Blockchain

- Identity
  - There are several identifiers that exist today (Social ID, Private ID and Government Issued ID) for individuals/organizations with varying levels of identity proofing
  - Despite the move to digital transactions, we continue to largely rely on these physical identities and username-passwords authentication to prove identity in online transactions
  - While a number of countries have moved to an e-ID, it is also estimated that 1.1bn people live without an officially recognized identity therefore creating huge exclusion
  - Blockchain can transform this
    - Evolution of self-sovereign identities which nobody controls (For ex. Sovrin)
    - Can enable standardization and reliability for cross border acceptance of identity systems and documents

Security and Authentication for Blockchain

- Identification and Authentication
  - Refers to the process of identifying a person/organization through a process of creating/using credentials. Ranges from “What you know” to “What you have”
  - Several Blockchain systems have emerged which combine the decentralized Blockchain ledger with ID proofing to create electronic Ids to users
  - User interaction with Blockchain may be through Wallet Software or integration with other User Applications which may authenticate user
  - Ineffective security controls either in the Blockchain system (Storage of keys) or at User Application level could result in compromise of data
  - Aspects of governance, particularly accountability in case of breaches needs to be defined through intergovernmental framework

Security and Authentication for Blockchain

- Authorization and Non-Repudiation/Admissibility of Electronic Evidence
  - Authorization refers to process of giving user consent to transactions (for ex: Payment Transfer)
    - Click to Sign or Click to Agree most common. These are susceptible to man in the middle attacks
  - Blockchain uses cryptographic signatures and sequential cryptographic hashes ensuring tamper proofing.
  - Security of the system critical. Aspects to consider include
    - Identity of the person transacting
    - Storage media of Private Key
    - Key Management controls
  - In the context of Blockchain, while private keys are used to sign a transaction, non-repudiation will depend on
    - Security measures under which Data Integrity, Confidentiality, Privacy and Authenticity of transactions are established and agreed to between various parties in the contract
    - Compliance of such measures with respect to local laws and regulations
  - If any Blockchain system can satisfy non-repudiation criteria and provides for immutability, auditability and ability to verify identity, a Blockchain transaction can qualify as admissible electronic evidence

Security and Authentication for Blockchain

- Time Stamping
  - Standards and processes for time stamping are defined in RFC 3161
  - In Blockchain, signed data and timestamp can be stored on a distributed ledger where consensus on time can be established through rules without relying on a central authority
  - This way any timestamped data can be verified to ensure document wasn't backdated
  - cross-border recognition of Blockchain transactions

Security and Authentication for Blockchain

- Data Access, Sharing, Retention, Accuracy and Integrity
  - Data integrity is a design feature of Blockchain as it uses cryptographic keys as modification of data is nearly impossible
  - Based on the type of Blockchain (public or permissioned), data access and sharing can be effectively controlled through access control mechanisms. This is particularly important in the context of Privacy Laws globally
  - Data accuracy is determined by the ability of Blockchain to resolve conflicts quickly
  - Blockchain replicates data across all nodes. This is an important aspect to consider in terms of retention as different regulators could potentially have varying retention periods for data
  - As can be seen a lot of the above facets will need to be taken care at design stage of Blockchain as altering this could prove expensive at a later stage

Security and Authentication for Blockchain

- Liability Issues and Dispute Settlement
  - Smart Contracts in Blockchain are self-executing without human intervention
  - In such cases, interpretation and dispute settlement may prove to be a challenge
    - Interpreting reasonableness is difficult in Smart Contract
    - Liability attribution in case of failure of execution of Smart Contract or partial execution
    - Jurisdictional issues
    - Authority and ability to easily reverse transactions
  - But, there are certain benefits
    - Defined Outcomes and lesser ambiguity
    - Neutral third party enforcement through side chains
  - Key questions include when does a legally binding contract get formed, at what point does it perform, how is breach defined and definitions of the enforcement and remedies available in traditional law?
  - This requires evolution and some changes may be required in the existing legal framework, setup, interpretation, qualification of the interpreters to address the legal challenges in Blockchain

Security and Authentication for Blockchain

- Mutual Recognition
  - Cross-border trade using Blockchain will result in parties being in multiple jurisdictions
  - Currently mutual recognition efforts are largely region or domain specific.
  - Depending on law, mutual recognition frameworks may allow parties to the contract to decide what constitutes a valid Blockchain transaction
  - TTP Project of eGovernment focusses on mutual recognition mechanism for trusted trans-boundary electronic interaction and may provide a framework for cross-border recognition of Blockchain transactions

Security and Authentication for Blockchain

- In Conclusion
  - Information Security is a critical aspect of Blockchain
    - User roles and access rights need to be clearly defined and understood
    - Private keys must be stored securely
    - Change management process needs to be well defined
    - Designing Blockchain in compliance with global privacy laws
  - Suggested focus areas
    - Trusted Trans-boundary mutual recognition mechanism for cross border transactions to include Blockchain in scope
    - Recommendations on Governance, enforcement and dispute resolution structures
    - Understand the impact of Quantum computing for Blockchain

UNECE

UN / CEFACT

Security and Authentication for Blockchain

UNECE

UN / CEFACT

Thank you