BIX Ledger™

Security, Privacy, and Anonymity Services for Blockchain Transactions

---

Identity Management System based on Public Identities Ledger

PKI based on Public Certificates Ledger

Secure Notary System based on Public Documents Ledger

BIX™ System Corporation

BIX™ System Corporation

Secure Blockchain Technologies and Infrastructures

Identity Management System based on Public Identities Ledger

BIX™ Identity Management System is based on the concept of peer-to-peer protocols and the public identities ledger. The system manages digital identities, which are digital objects that contain attributes used for the identification of persons and other entities in an IT system and for making identity claims.

The identity objects are encoded and cryptographically encapsulated.

Identity management protocols include the creation of identities, the validation of their binding to real-world entities, and their secure and reliable storage, protection, distribution, verification, updates, and use. The identities are included in a specially constructed global, distributed, append-only public identities ledger. They are forward- and backward-linked using the mechanism of digital signatures. The linking of objects and their chaining in the ledger is based on and reflect their mutual validation relationships.

The identities of individual members are organized in the form of linked structures called the personal identities chains. Identities of groups of users that validated identities of other users in a group are organized in community identities chains.

The ledger and its chains support accurate and reliable validation of identities by other members of the system and by application services providers without the assistance of third parties.

The ledger in the BIX™ Identity Management System may be either permissioned or unpermissioned. Permissioned ledgers have special entities, called BIX™ Security Policy Providers, which validate the binding of digital identities to real-world entities based on the rules of a given security policy. In unpermissioned ledgers, community members mutually validate their identities.

The BIX™ Identity Management System provides security, privacy, and anonymity for digital identities and satisfies the requirements for decentralized, secure, and anonymous public ledger.

BIX™ System Corporation

Secure Blockchain Technologies and Infrastructures

Public Key Infrastructure based on Public Certificates Ledger

BIX™ Public Key Infrastructure comprises the global, distributed architecture, components, and protocols based on the concept of a public certificates ledger.

The functions of the infrastructure are to manage public key certificates and support users when using them for various security services.

The certificates are cryptographically encapsulated objects that bind the identities of their owners to their public keys and provide digital signature mechanism for other users to verify that binding and correctness of other attributes of the certificate. Specially designed certificates contain double links that reflect their validation and position in the public certificates ledger. This solution prevents insertion or removal of certificates in the ledger.

Certificate protocols of the infrastructure include requesting issuance of certificates, issuing and returning certificates to their requesting users, storing certificates in the certificates ledger, requesting and distributing certificates to transaction partners, verification of certificates by transaction partners, and revoking certificates by their owners. These protocols are performed as direct peer-to-peer transactions between the members of the system.

The public certificates ledger is a linear, double-linked list of certificates. If the infrastructure is unpermissioned, any person may join the community, obtain, and then use certificates for secure, private and anonymous transactions. In permissioned infrastructures some members of the system have the role to enforce registration policies, so that only previously approved and registered persons may join certification infrastructure.

After their exchange and validation, certificates may be used to support various security services for users, applications, and transactions based on public transactions ledger.

The distinctive and very significant feature of the system is that private keys, that correspond to public keys stored in certificates, do not exist anywhere in the system. Therefore, the system is not vulnerable to theft of private keys and impersonation of regular users.

BIX™ System Corporation

Secure Blockchain Technologies and Infrastructures

Secure Applications supported by the BIX Ledger™
"Triple Helix" Secure Ledger

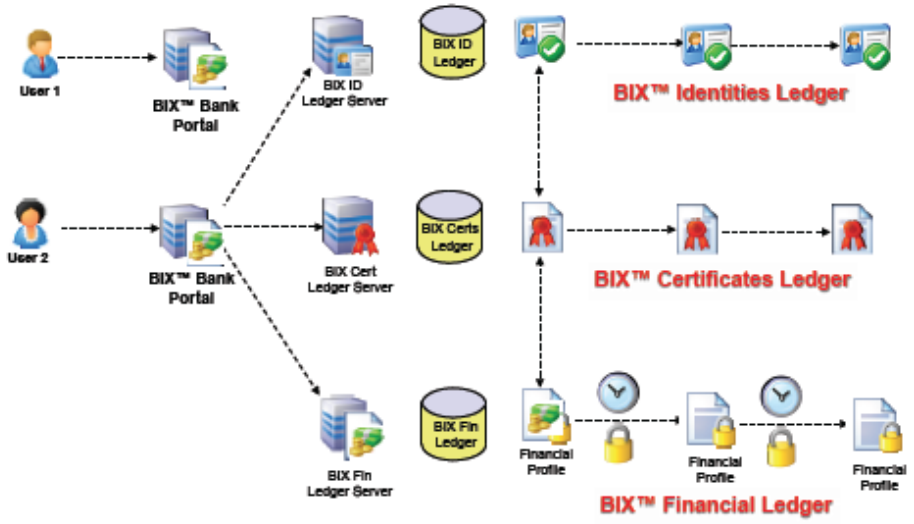

Figure 1: Secure Financial Transactions over Financial Transactions Ledger

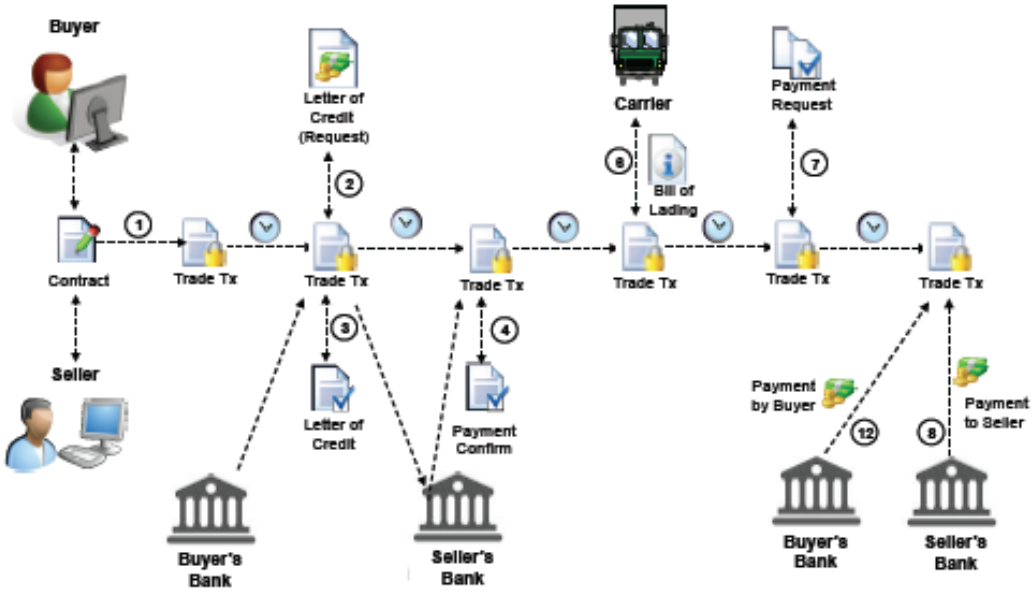

Figure 2: Secure Trading System