BIX System

White Paper

BIX Ledger

Security, Privacy, and Anonymity Services for Blockchain Transactions

This White Paper describes the architecture and the design of the BIX Ledger - a secure, peer-to-peer, hybrid (permissioned/unpermissioned) distributed ledger for blockchain applications

- **Identity Management System**
  (Public Identities Ledger)
- **Public Key Infrastructure**
  (Public Certificates Ledger)
- **Secure Financial Transactions**
  (Financial Transactions Ledger)

1. The Concept of Secure BIX Ledger

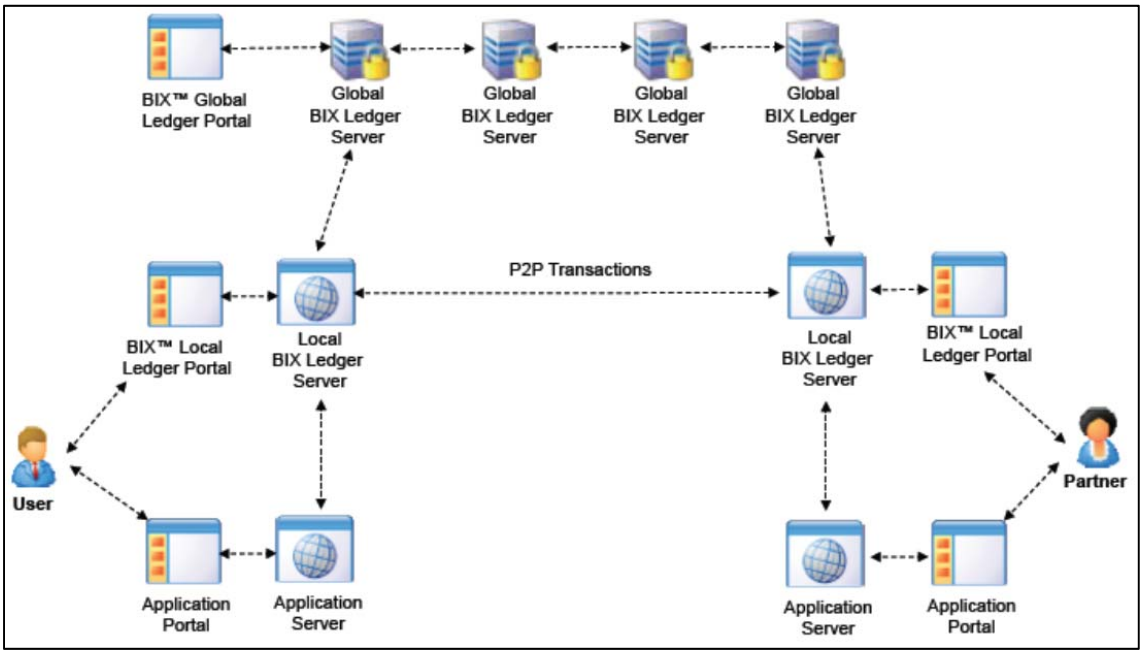
1.1 BIX Ledger - Infrastructure

BIX™ Ledger Infrastructure is a collection of cloud servers mutually linked by special ledger protocols. Each global ledger server manages and distributes special ledger objects – simple records and complex BIX™ Ledger chains. Each BIX™ Ledger Server is an IT container, comprising of

a. special ledger software modules, and
b. data storage capabilities.

Software modules perform BIX™ Ledger protocols maintain simple ledger objects and complex BIX™ Ledger chains stored in data storage areas. Contrary to the concept behind the original Bitcoin ledger (and followed by other ledgers) BIX™ Ledger Infrastructure is designed with different principles. It contains two types of BIX™ Ledger Servers, organized as a two–layered infrastructure: Global BIX™ Ledger Servers and Local BIX™ Ledger Servers. Global servers represent the "backbone" servers of the BIX™ Ledger Infrastructure. Individual Local BIX™ Ledger Servers are associated with instances of applications that use the Ledger. They communicate

a. with local applications that they support,
b. with Global BIX™ Ledger Servers, and
c. with their peer Local BIX™ Ledger Servers when assisting in execution and protection of peer–to–peer application transactions.



1.2 BIX Ledger – Services and Protocols

BIX™ Ledger System is a server infrastructure which enables security and privacy of users and execution, validation, and protection of applications, transactions, and data. BIX™ Ledger is itself an application which provides four types of services managed with different types of protocols.

a) **BIX Ledger as a Broadcast System** accepts objects from one BIX Member and distributes them (broadcast) to all other members of the BIX Community. These are public objects accessible to all members of BIX Community. Security services applied to these objects during their upload into the BIX Ledger are *Creator's authenticity* and *BIX Ledger notarization*.

b) **BIX Ledger as an Immutable and Reliable Archive** accepts objects from one BIX Member, permanently stores them, and distributes them to BIX Members authorized by the owner of the record, document or transaction. This service handles both public and private objects accessible to all (public) or only to the members of the BIX Community authorized by the owner / creator (private). Security services applied are: *Creator's authenticity*, *BIX Ledger notarization* (for public objects) and *Receiver's authorization* (for private objects).

c) **BIX Ledger as Security Infrastructure** manages security credentials (BIX Identities and BIX Certificates) of the members of the BIX Community, distributes certificates of individual members to all other BIX Members and distributes BIX Identities only to members authorized by their owner. BIX Identities are private objects and BIX Certificates are public objects. BIX Ledger provides the following services to these security objects: for BIX Certificates – *Issuer's authenticity*, *Certificate integrity* (name – key binding), and *Verification of certificate's validity*; for BIX Identities – *Owner's privacy and authenticity*, *BIX Ledger notarization*, and *Receiver's authorization*.

d) **BIX Ledger as Transactions Infrastructure** supports complex, multi-party, multi-documents, and multi-step applications with automated execution of "business chained" transactions and protocols for resolution of business conflicts ("smart contracts"). These services handle only private objects accessible only to a group of authorized BIX Community members registered in a group and authorized to perform certain actions and to handle objects within the complex transaction. Security services applied to each object are *Creator's authenticity*, *BIX Ledger notarization*, and *Receiver's (group) authorization*.

1.3 BIX Ledger – Cryptographic and Ledger Chains

BIX Leger Chains are collections of BIX Ledger objects organized in a specially linked structures – chains. Objects chaining is achieved by including certain cryptographic credentials of the logically previous object as attributes in the next object in the chain. This organization of objects prevents post-factum modification of individual objects or insertion of objects into the chain. Therefore, each chain is append-only data structure.

BIX Ledger chains, depending on the nature of the application that they belong to, may be linear or forked. Linear chains have all objects organized in a linear sequence. Forked chains have multiple instances of sub-chains ("forks"), each sub-chain originates with an object belonging to possibly another sub-chain or to the main chain. In case of forked chains, the main chain is called "backbone" chain for an application. It contains object describing the essential / core elements of an application, while sub-chains describe their additional features, properties and characteristics. These forked sub-chains should not be interpreted as soft-forked chains in ledgers that have parallel, simultaneous and distributed updates. In those ledgers such forks are redundant and must be synchronized with the main ledger using so called "consensus" protocol. In BIX Ledger these forked sub-chains are not redundant, as they contain objects that are relevant and used by an application. So, in that sense, they might be interpreted as hard forks used with other ledgers. But, even that interpretation is not completely accurate, for two reasons:

a) With other ledgers ("blockchains") forks completely replace the main chain and in fact substitute it as the new main chain. In the BIX Ledger System forked chains are complementary to the main – backbone chain.

b) Contrary to the common concept that the objects entered into the ledger are permanent, in the BIX Ledger some sub-chains may be removed from the chain, if or when they are not needed any longer. An example may be bids for an auction; they become redundant after the auction is completed.

1.4 BIX Ledger – Objects

BIX Ledger objects are specially constructed data structures. Each of them contains three segments: header segment, body segment, and security credentials.

Header segment contains references to the object owner and its authorized user. Body segment contains data of an object – the attributes of the object. Security credentials are parameters or results of crypto operations performed with the object in order either to create its security "encapsulation" or to create its cryptographic linking in the chain. Header and security credentials are mandatory segments – they are present in every objects, while body is an optional segment – it may be or may not be present in an object.

There may be certain exceptions to this object structure. Within the exceptions there are three types of BIX Ledger objects: (a) data objects, (b) reference (pointer) objects, and (c) validator objects.

Data objects are BIX Ledger objects that contain all three segments: header, body, and security credentials. Body segment with these objects contains the attributes that describe the related application entity. Examples may be an Identity objects, that contains identification attributes, or a document object, that contains the full text of a document.

Reference (pointer) objects in the data segment do not contain data but pointers to storage locations where the data of an object are physically stored. This type of storing ledger objects is called "off-chain", as data of actual entities that an object represent are not actually stored inside the ledger chain. An example of such objects could be chain objects related to a document which is stored in some cloud or in some shared documents server.

Validator objects are objects that in their data segment contain cryptographic credentials that are needed to validate cryptographic protection of an object. Objects may be stored off-chain or handled internally by an application. An example may be signed E-mail letter, where the letter itself is handled by the Mail System, but certificate of the sender is included in the validator object in the ledger chain. In this example, header segment contain(possible among other) sender's E-mail and receiver's E-mail attributes, while data segment contains sender's certificate.

1.5 BIX Ledger – Applications

The purpose of BIX Ledger – its components, objects and protocols, is to support execution and validation of peer–to–peer transactions. Peer–to–peer transactions are performed directly between two (or more) BIX members participating in the transaction. Usually, one BIX member is the initiator / creator of the transactions and one or more or all other members of the BIX system are receivers/responders. In order to support execution of such transactions in an open environment, BIX Ledger provides information needed for connection between two BIX members and their application instances. For that purpose, BIX Ledger distributes BIX Identities and BIX Certificates, acting as the security infrastructure.

These two security objects (security credentials) are also used to support validation of peer–to–peer transactions. BIX Identity is used by both parties to verify that the correct (intended) BIX member is participating in a transaction and executing only authorized actions. BIX Certificate is used to extract partner's and BIX Ledger Server's public key and verify digital signatures created by these entities. Public keys from BIX Certificates are also used by recipients to open digital envelopes of objects which they are authorized to use.

When used as broadcast infrastructure, BIX Ledger distributes objects to all members of the BIX Community or only to selected users, if that is the requirement of an application, and in that way enables application to perform their specific transactions using those objects. The same is when the BIX Ledger is used as an archive of reliable and immutable records: in this case applications may access objects stored in the Ledger, validate their correctness, integrity, time of creation, authorship and other properties and use these validated objects for transactions performed by these applications. Finally, when supporting complex transactions, BIX Ledger services help to resolve business conflicts and functional dependencies between objects and actions of an application.

Each application, used in a global, distributed and open environment, is configured as a collection of its individual instances. One instance of an application comprises Application Portal and Application Server. Application Portal is front-end, i.e. it provides user interface to the functions of an application. It is designed in the form of a complex Web server. The server comprises web pages, plus local software modules for interactions and communications with back–end functional software modules. These back-end modules are packaged in the form of a functional server called Application Server.

In addition to the two Servers of an application, each local instance of the application is also associated with an instance of the Local BIX™ Ledger Server.

That Server also comprises two functional servers – the front–end Portal and the back–end Server. Portal provides access to the Local BIX Ledger services – managing users' BIX™ Identities and BIX™ Certificates. The back–end Server executes functions with these objects using local cryptographic and ledger functional engines It also connects to its associated Global BIX™ Ledger Server and to its peer Local BIX™ Ledger Server which is supporting another instance of the application used to perform specific peer-to–peer transaction.

2. 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.

3. PKI 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.

4. Secure Applications supported by the BIX Ledger™ “Triple Helix” Secure Ledger

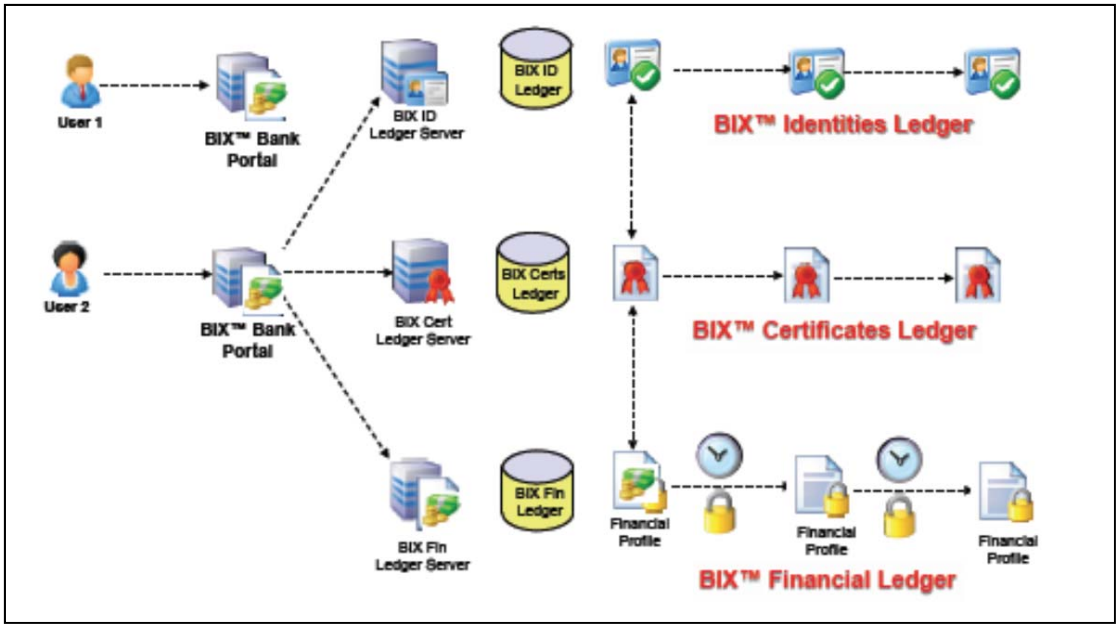


Figure 1: Secure Financial Transactions over Financial Transactions Ledger

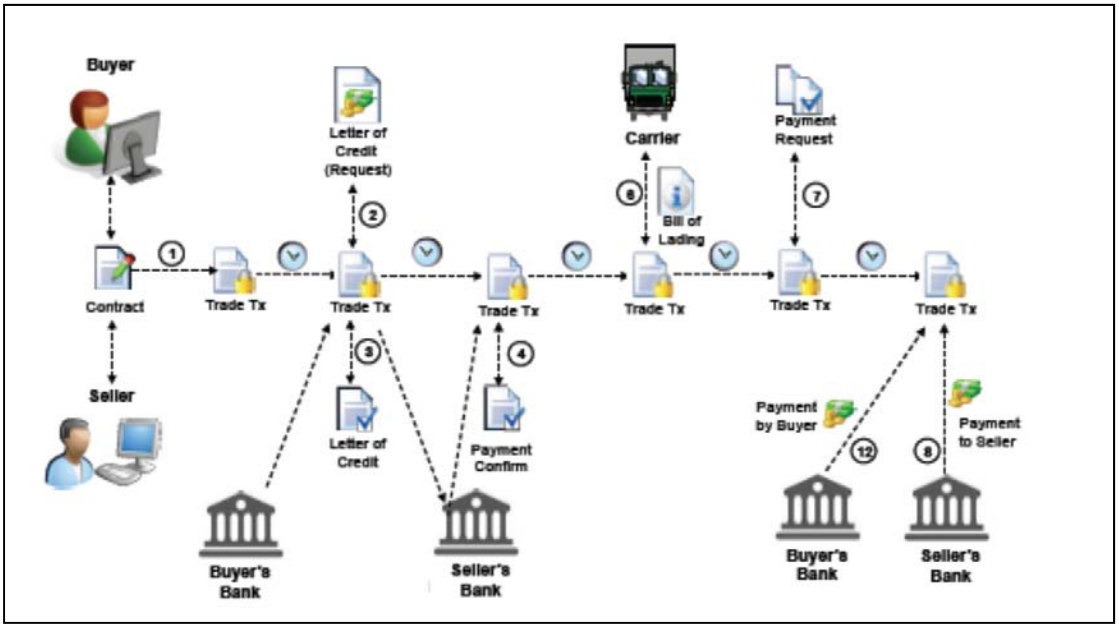


Figure 2: Secure Trading System with BIX Ledger Infrastructure

BIX SYSTEM CORP, BLOCKCHAIN EXPERTS

BIX System Corp, the company behind BIX Ledger, assembled a team of foremost experts in the areas of computer security and distributed networks. Decades of academic research and practical network security implementations led the BIX System team to design and architect the world's most secure and most capable blockchain platform, BIX Ledger.

BIX Ledger's architecture and design is protected by several US patents by the company's founder, Dr. Sead Muftic.

Dr. Sead Muftic, Founder & CEO

Dr. Muftic is an entrepreneur and an internationally-recognized expert in the area of IT security. He has been full professor at The Royal Institute of Technology in Stockholm, Sweden and a visiting professor at the George Washington University in Washington, DC. Dr. Muftic is registered as an International Expert for security of blockchain technologies and virtual currencies by the European Commission and as the visiting scientist by the CSIR Institute in South Africa.

A leading expert in the fields of computer security and blockchain, Sead worked with the World Bank and the European Commission on charting the vision & the future of secure digital and virtual currencies. Dr. Muftic currently serves as a project coordinator for blockchain and smart contracts at BAFT international trade organization.

Dr. Muftic is the author of five U.S. patents in the area of Blockchain, Identity Management, and Secure Financial transactions. He is the author more than 50 research papers, expert reports, and three books.

sales@bixsystem.com

www.bisxsystem.com

www.bixledger.com

BIX System