LEDGER
ledgerjournal.org

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

RESEARCH ARTICLE

BIX Certificates: Cryptographic Tokens for Anonymous Transactions Based on Certificates Public Ledger

Sead Muftic[†]*

Abstract. With the widespread use of Internet, Web, and mobile technologies, a new category of applications and transactions that requires anonymity is gaining increased interest and importance. Examples of such new applications are innovative payment systems, digital notaries, electronic voting, documents sharing, electronic auctions, medical applications, and many others. In addition to anonymity, these applications and transactions also require standard security services: identification, authentication, and authorization of users and protection of their transactions. Providing those services in combination with anonymity is an especially challenging issue, because all security services require explicit user identification and authentication. To solve this issue and enable applications with security and also anonymity we introduce a new type of cryptographically encapsulated objects called BIX certificates. "BIX" is an abbreviation for "Blockchain Information Exchange." Their purpose is equivalent to X.509 certificates: to support security services for users and transactions, but also enhanced with anonymity. This paper describes the structure and attributes of BIX certificate objects and all related protocols for their creation, distribution, and use. The BIX Certification Infrastructure (BCI) as a distributed public ledger is also briefly described.

1. Introduction

Internet, Web, and mobile applications that provide security, but also anonymity of users, are gaining increasing interest and importance. Examples of such new applications are various innovative payment systems, digital notaries, electronic voting, sharing of sensitive documents, electronic auctions, medical applications, and many others. The common characteristic of these applications is that they all require *anonymity* of users and their transactions.

In addition to their anonymity, user identifiers, data, and transactions handled by those applications also require standard security services, such as identification, authentication, and authorization of users, data confidentiality, data integrity, sender's/receiver's authenticity, and non-repudiation of transactions. Providing these security services in combination with anonymity is especially challenging, because all of them require explicit user identification and authentication.

[†]S. Muftic, Ph.D. (sead.muftic@setecs.com) SETECS Corporation, Washington DC, USA.
*15Dvv5QxpcJ4LDz38GQXkg5aKfMLUGgm7f

To solve this challenging problem, we introduce a new type of cryptographically encapsulated object, called a *BIX certificate*. Its purpose is equivalent to X.509 certificates, *i.e*., to support security services for users and transactions, but enhanced with anonymity. "BIX" is an abbreviation for "*Blockchain Information Exchange.*" BIX certificates enable applications and transactions whose main purpose is to exchange sensitive personal and business information and data to provide full security and also anonymity.[1]

Another problem when providing security services in combination with anonymity using current standards and technologies is that most of them, if not all, today are provided by or need the assistance of (*trusted*) *third parties*. Such concept, obviously, has no anonymity, as third parties learn everything about users participating in transactions, including sometimes even sharing their personal sensitive data, such as crypto keys, bankcard numbers, *etc*. We emphasize, contrary to the popular impression, that even Bitcoin is not a peer-to-peer protocol, as it depends on two types of third parties: (a) *the Bitcoin network,* for controlling mining difficulty level, charging fees for transactions, and time-stamping of blocks, and (b) *miners,* to generate hashes of transaction blocks.

The solutions for all these problems described in this paper are based on use of the concept called *Certificates Public Ledger (CPL)*. The general concept of the ledger is a collection of public user attributes and transactions, linked in a time, cryptographic, and functionality chain. General ledger has the property that its blocks and transactions are available to all users who use some application that requires verification of parameters and data, but with anonymity of users. Contrary to the concept of Bitcoin, our CPL and all of its protocols are truly *community based*, without requiring the assistance of any third party.

Yet another problem with most of the current Internet applications and transactions is that they are often performed with the assistance of various *application services providers*. Examples are banks for financial transactions, Web service providers for social Web sites, various Web sites for searching and information distribution, and others. In the course of providing their services, such service providers all require access to users' sensitive personal data and they all track and profile users by collecting their transactions data. This practice clearly violates users' privacy and anonymity.

In our research, we have solved these problems using the new concept of so-called *community transactions*. The community is a group of anonymous users who have agreed to participate in some application(s) or to support security and anonymity services provided by the Certificates Public Ledger. An example may be a community for sharing files[2,3] or to provide proof of existence of documents[4]. Users join the community only for the reason of participating in some of community–based transactions. Example, for instance, may be charities and donations. It is important to emphasize that users do not have to trust the members of the community, as validation of their identities and certificates is exactly one of the main purposes of the BCI. Even if there may be malicious users as members of a community, the case when they try to damage the BCI, its certificate, and protocols is discussed in Section 6.

In summary, our research results reported in this paper address and solve three important problems for users, applications, and transactions that need both security and anonymity: (a) provision of security services that require identification, authentication, and authorization of users while at the same time ensuring their anonymity, (b) provision of security and anonymity services by the community of users without the assistance of any third party, and (c) secure and anonymous peer-to-peer applications and transactions without centralized application providers.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

Our results resolve the conflict between, on one hand, the requirement for explicit sharing of identities and credentials for security services and, on the other hand, prevention of that sharing to ensure privacy and anonymity. The cryptographic objects and protocols described in this paper can be used with all of the applications mentioned earlier that require privacy and anonymity of validated users. We expect that the BIX certificates, the protocols for their management and use, and an infrastructure for their distribution and validation, based on the new concept of the Certificates Public Ledger, will provide the supporting technology and infrastructure for a new category of applications that will provide both security and anonymity to users. In that sense, we hope that the system described in this paper will become the enabling infrastructure for secure and anonymous transactions equivalent to what X.509 certificates and PKI represent for users, applications, and transactions that require only security.

2. Related Concepts and Associated Literature

The ideas described in this paper are an innovation. This means that we do not know of any publication or source where the same or even equivalent ideas are described. For instance, the concept of BitID[5] is just a simplified use of complex Bitcoin addresses without any additional security services or features of these addresses. Bamert[6] suggests the use of hardware devices to protect private keys. Goldfeder[7] created a comprehensive scheme based on the use of threshold signatures compatible with Bitcoin's ECDSA signatures that can be used to enforce complex security policies that provide: (1) shared control and use of Bitcoin wallets, (2) secure bookkeeping, a Bitcoin-specific form of accountability, (3) secure delegation of authority, and (4) two-factor authentication when using personal wallets.

Most of the current suggestions for any aspect of security for the Bitcoin system are focused on protection of local data used by wallets. During our research activities, we could not find any scheme or any protocol for secure, reliable, and verifiable distribution of public addresses, keys, and identities even for the Bitcoin system. We also could not find any ideas or concepts of the blockchain as the public ledger to support applications, other than Bitcoin payments and proof-of-existence, with security and anonymity. Therefore, in this section we review certain concepts that can be used only as an analogy for our solutions and that have only some resemblance to ideas and solutions presented in this paper.

2.1. X.509 Certificates and PKI—One of the purposes of BIX certificates is to distribute anonymous identities and public keys of users and to enable their verification for correctness and ownership. This is also one of the purposes of X.509 certificates. Therefore, it may be assumed that BIX certificates are analogous to X.509 certificates. The core differences are that (a) user credentials contained in BIX certificates are anonymous and (b) BIX certificates are not issued by any third party.

The X.509 certificate profile is described in the IETF standard.[8] The `version` attribute is used to denote various versions of X.509 certificates. We also use the `version` attribute in BIX certificates, but it is used to denote the type of the certificate, as explained in Section 3. It is equivalent to the `keyUsage` attribute in X.509 certificates. The current `Version` is *one* (1), denoting a certificate that can be used for security services: anonymous identification, authentication, and exchange of secret session keys.

The `Serial Number` attribute is used as the reference for the specific X.509 certificate within those issued by some Certification Authority (CA). It is also used to locate the certificate in the Certificate Revocation Lists (CRLs). BIX certificates are issued by the

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

members of the BIX community and "chained" in the certificates ledger, so serial number as the reference to the specific issuer is not needed. However, for easier referencing and for some other purposes, BIX certificates contain the `Sequence Number` attribute. This attribute's content and its use are explained in subsequent sections. X.509 certificates have the component `Subject`. This is the collection of identifying attributes organized in the form of a Distinguished Name (DN). BIX certificates also have the component `Subject`, but instead of a DN for explicit identification of the certificate's owner, this component contains as one of its attributes a `Personal Identification Number` (called *BIX Identifier*). Personal IDs are *random numbers, publicly available, globally unique*, and *anonymous* in the BIX system. They are used as a convenient reference to individuals, equivalent to mobile numbers. They are unique and permanently assigned to BIX members, while BIX certificates may be renewed and several of them belonging to the same member may exist at the same time. Personal ID in the BIX system is equivalent to the Social Security Number, issued in the US, which is issued to a person once in his/her lifetime, which is permanent, and unique.

X.509 certificates have a `Validity` component comprising two *Date/Time* attributes: one is an *Issuing Date/Time* and the other is an *Expiration Date/Time*. BIX certificates do not automatically expire, so they do not need an expiration date/time. The `Subject` segment of the BIX certificate contains a `Date/Time` attribute designating the time of its creation, *i.e.*, the generation of the crypto keys pair. Locating certificates in the Certificates Public Ledger and verification of their time validity is based on the special certificates protocol. BIX certificates are "chained" in the BIX Certificates Public Ledger using personal BIX Identifiers and cross-signatures and organized in a time sequence using the certificate's `Issuing Date/Time`.

Equivalent to X.509 certificates, BIX certificates in the `Subject` segment contain a public key and the associated algorithm identifier in the `Subject Public Key Info` and `Algorithm Identifier` attributes.

Four attributes comprising the `Subject` segment: `Personal ID Number`, `Date/Time`, `Algorithm Identifier` and `Subject Public Key Info`, are *signed*. Because BIX certificates are created by their owners, the `SubjectSignature` attribute is created using a private key that corresponds to the public key in the `Subject` segment. This means that the `Subject` segment is *self-signed*.

X.509 certificates have an `Issuer` segment. This segment represents the DN of the Certification Authority (CA) that issued the certificate. In the BIX Certification Infrastructure (BCI), the issuer is one of the other members of the BIX community. The structure of the segment `Issuer` in BIX certificates is equivalent to the structure of the segment `Subject`.

Finally, X.509 certificates have extensions. The purpose of these extensions is to enhance and more precisely designate the types and purposes of certificates (authentication certificates, signature certificates, certificate signing certificates, key exchange certificates, *etc*.), to identify supporting components of the PKI (such as repositories of revoked certificates, directories where certificates are stored, *etc*.), and certificate polices under which certificates should be used. BIX certificates also have extensions. But, at the moment specific extensions are not specified since all different aspects of their management and use are not known. So, in the current concept, indicated extensions are simply a "placeholder" for such extended and additional aspects, which will be definitely established in the near future.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

The main drawbacks and inconveniences of the current concept of the PKIs is that they represents very complex infrastructures, they heavily depend on trust in third parties, and they use very complicated procedures to distribute and validate certificates. Another major inconvenience is their scaling and federation, which may be solved either by issuing all certificates under one and the same Root Certification Authority or by establishing federated PKIs. Both approaches are very complicated and current lack of both clearly indicates that all these complexities are an obstacle for establishment and use of large–scale PKIs. The concept of a public ledger has one of general advantages over such large and complex infrastructures, built and dependent on third parties: it does not depend on and does not use any third parties. This makes it very convenient for many purposes and applications and one of them is certification infrastructure, described in this paper.

2.2. Bitcoin System and Blockchain—Bitcoin is an anonymous payment system that uses the concept of the public ledger—called blockchain—to perform and verify payment transactions.[9, 10] Its blockchain has a specific structure and protocols for its creation, distribution, and use, and is suitable primarily for payment transactions. There are some innovative ideas to use the same concept and the existing operational infrastructure to perform other types of community-based and anonymous transactions. Some examples are shared file storage,[3,2] a secure files sharing system,[11] a documents management system with digital notary services[12] or proof-of-existence for documents.[4]

Although the concept of the Bitcoin system is appropriate for anonymous payments and its current implementation is operational, the system has many conceptual and operational problems.[13,14,15] Many other problems have been reported by Sparkes[16] and Shibli.[17] In addition, to provide the full scope of security and anonymity services for various new applications, the system also needs certain conceptual extensions.

BIX certificates designed in this paper support both public key and secret key cryptographic protocols and services. This is their first important distinction compared to Bitcoin addresses. Bitcoin transactions, based on addresses that in essence represent a recipient's public key, can be received only by a single recipient. BIX certificates support transactions with multiple targets / recipients and also group transactions.

2.3 Peer-to-Peer Applications with Anonymity—After introduction of the concept of the blockchain by the Bitcoin system, many creative ideas emerged for new and innovative applications based on the concept of the blockchain.[18, 16, 19] But, for most of them, the current concept of the blockchain is not sufficient. First, there are certain problems with protection, integrity, and availability of Bitcoin credentials. Public addresses cannot be verified and protection of private credentials is not adequate. Second, the current concept of the blockchain contains only financial and other similar transactions that require "linear" ordering and dependencies of transactions data. This structure and relationships of transactions are not adequate for many new applications. Examples of such applications are all applications mentioned in the abstract and in general all others that require security, privacy, and anonymity. Furthermore, while anonymity may be an advantage for certain types of transactions, for some others it may present great problems.[20, 21]

Several improvements and extensions have already been suggested in documents reporting our current research.[22,23] BIX certificates and the generalized public ledger described in this paper represent enabling crypto objects and an infrastructure for security and anonymity of these new applications.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

2.4. Summary—Based on the examples in this section, it is obvious that the current concept of Bitcoin payment transactions and the blockchain for their validation are not adequate to support new and innovative applications, transactions, and services enhanced with security and anonymity.

In the Bitcoin protocol the address of the user who will receive payment must be available to the partner making payment. The address represents a "Bitcoin account." In addition, all of the partner's previous transactions must be available to the person receiving payment to verify the correctness and validity of the payment transaction.

There is no formal protocol to distribute and validate Bitcoin accounts (addresses) to partners. At the moment they are mainly distributed out-of-band or in the QR form, over-the-counter or over-the-Web. This approach is not satisfactory for serious business transactions that need verified, correct and legitimate personal parameters. Distribution over the network is vulnerable to man-in-the-middle attacks.

Verification of Bitcoin payments is performed by verifying that the sender (a) has a sufficient balance in his/her account to make the payment and (b) that he/she did not make "double" payments. Both verifications are performed by "tracing" the sequence of all transactions in the blockchain starting from the trusted "coinbase" transaction up to the latest transaction received by the partner who is making payment.

But, for many applications that support peer-to-peer transactions and require validation of personal credentials and/or transactions, this concept is not appropriate. For instance, in a voting application, there is no starting trusted "coinbase" transaction. "Double spending" is possible, as voting may be simultaneous at city, regional, and state levels. However, the validity of the voter, the correctness of the vote, and the controlled "use" of voting rights must all be verified and validated. The most important characteristics—the identity and other personal credentials—of each voter must be validated, but with full anonymity.

All of these examples, current problems, trends, innovative ideas, new applications, and possibilities for new services were motives for the research reported in this paper. Based on two examples, Bitcoin payments and the voting application, the conclusion is that personal credentials must be separated from specific transactions. Personal credentials are needed to verify the validity and the status of each participant in the BIX system. Once that is accomplished, valid and regular users may perform different types of transactions, and each of them requires and uses its own data and credentials.

3. Design and Implementation of the BIX Certification Infrastructure: The Structure and Attributes of BIX Certificates

BIX certificates, equivalent to X.509 certificates, are cryptographically encapsulated objects used to distribute identities and crypto keys to transaction partners with the possibility for their verification, but with full anonymity of all partners. The structure, attributes, and protocols for creation, distribution, and validation of BIX certificates must support their three main purposes: (1) reliable distribution and use of correct and legal identities, (2) their validation, and (3) their binding to public keys used for various applications and transactions. These three requirements may be specified in the form of the following six properties of BIX certificates:

(1) They must provide a method to verify that data structure representing the public key contained in the certificate is correct;

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

(2) The recipient of the certificate must be able to verify that there exists a private key that corresponds to the public key contained in the certificate;
(3) They must provide a method to validate that the anonymous identifier of the owner of the certificate is correct and globally unique;
(4) It should be possible to verify that the binding of the public key to the anonymous identifier of the owner of the certificate is correct;
(5) There must be a method to validate that the issuing date/time is correct;
(6) The user, when using certificate of his/her transaction partner, must be able to verify the validity of the certificate, *i.e.*, that it is not revoked.

All of these requirements simply mean that public keys must be distributed without accidental or intentional modifications, illegal insertions of fake certificates or unauthorized substitution of correct certificates must be detected, and certificate validity and correctness must be verifiable.

In addition to distributing anonymous identities and crypto keys, BIX certificates may be extended with additional data, suitable for different applications with anonymity and other properties. To satisfy these requirements, the attributes and the structure of BIX certificates are as follows:

Header: The header is a group of three attributes:

Sequence number: This attribute contains the sequence number of the certificate and reflects its relative position within an instance of the BCL with respect to certificates of other BIX members.

Version: This attribute contains the code that designates the type of the BIX certificate.

Date/time: This attribute indicates the date and time of issuance of the certificate. It represents the start of the validity period for the current certificate.

Subject: This is a group of four attributes:

Subject BIX ID: This is the unique global identifier of the user who owns the certificate.

Date/time: This attribute indicates the date and time of creation of the public/private key pair.

Algorithm identifier: This attribute designates the crypto algorithm with which the public key can be used.

Public key: This is the cryptographic public key of the owner of the certificate.

Subject signature: This attribute contains the signature over the four *Subject* attributes using the private key that corresponds to the public key in the *Subject* group. Therefore, the *Subject* structure is self-signed.

Issuer: This is the same group of four attributes as in the *Subject*, but they belong to the BIX member who issued this certificate.

Issuer signature: This is a self-signed signature over the four *Issuer* attributes created by the Issuer.

Backward cross-signature: This attribute contains a pair of signatures, one created by the Issuer and the other created by the Subject, over three *Header* attributes concatenated with the hash of the *Subject* and the hash of the *Issuer*. This attribute guarantees validity of the *Header* and binding between the *Subject* and the *Issuer*.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

Next Subject: This is the same group of four attributes as in the *Subject*, but belongs to the BIX member who was certified by this BIX member, *i.e.*, it contains the *Subject* attributes of the next member in an instance of the BCL.

Next Subject signature: This is the same attribute as *Subject signature,* except it is created by the Issuer of the current certificate over the *Next Subject* data.

Forward cross-signature: This attribute contains a pair of signatures, one created by the Issuer and the other created by the *Next Subject*, over three *Header* attributes concatenated with the hash of the *Issuer* and the hash of the *Next Subject*. This attribute guarantees binding between current user as the *Issuer* and the next user to whom the certificate is issued

Extensions: This attribute contains *objectID*, the value, and criticality flag of some additional attributes that may be needed for specific purposes of the BIX certificate.

The precise structure of the BIX certificate is given in the Appendix using ASN.1 notation.

4. Design and Implementation of the BIX Certification Infrastructure: BIX Certification Infrastructure (BCI)

The *BIX Certification Infrastructure (BCI)* is the collection of all BIX certificates issued to BIX members (users and applications) and corresponding protocols for their creation, distribution, and validation. Because there are no third parties involved, the entities managing certificates are BIX members themselves. This means that members have two roles: as users of the infrastructure and also as certification and validation authorities.

The main component of the BCI is a *BIX Certificates Ledger (BCL)*. It is a double-linked linear list of certificates without branches. This means that certificates in the ledger are linked to one another in a linear sequence. In instance of the BCL in fact represents the certificates chain. The certificate of each user points to the previous certificate ("backward" link) that belongs to the user that issued the certificate of the user and also points to the next certificate ("forward" link), the certificate that was issued by this user. The backward link is represented by the `Issuer` segment of the certificate and the forward link is represented by the `nextSubject` segment (see the Appendix).

An instance of the BCL starts with the *Root Certificate*. It is self-signed, *i.e.*, the `Subject` segment and the `Issuer` segment in that certificate are the same. To initiate one specific instance of the BCL, the Root Certificate must be issued by an entity that will initiate and manage the specific instance of the BCL (equivalent to the genesis transaction in the Bitcoin system).

When the Root Certificate is generated, the first user may be registered and his/her certificate will be issued by the BCI's initiating entity. The details of all BCI certification protocols are described in the next section, so at this point we will just mention that when the new certificate is issued by some user to another user:

- the `nextSubject` segment of the new certificate is left unpopulated, and
- the `nextSubject` segment of the issuing user's certificate is populated with the `Subject` segment of the new certificate.

This means that the last BIX member who joined the system is added to the "tail" of an instance of the BCL and he/she will be the issuer of the next certificate.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

An instance of the BCL can be traversed backwards (to reach the Root Certificate) and forward to find the "tail" / the end of an instance of the BCL, *i.e.*, the user who is the Issuer for the next certificate.

The BCI requires as the operational prerequisite a *broadcast messaging system* with *instantaneous* delivery of messages. That system is not a third party, as it only passively distributes BIX certificates and (for addressing purposes) verifies that the BIX Identifier of the new user is unique. The same system is needed for distributed file storage.[2,3] In our implementation of the BCI, we use the secure IM protocol for this purpose.[24]

5. Design and Implementation of the BIX Certification Infrastructure: BCI Certificate Protocols

BCI certificate protocols are performed as either peer-to-peer or group transactions between the members of the BIX system. Their purpose is to manage BIX certificates, what includes protocols for issuing, distribution, validation, and renewal of BIX certificates. All protocols are executed by the *BIX BCI Agent*—a PC or smart phone application. The application must be preconfigured only with the URLs of several of the broadcast distribution system servers, so it can communicate with that system to send and receive instant messages.

The *BCI Instant Messaging System* must also support user registration and distribution of reliable time. Most of the IM protocols, especially the XMPP protocol that we use, provide a user registration service.[25] Before executing the BCI certification protocol, each user must first register himself/herself in the BIX system. This is performed by registering in the BIX Instant Messaging System. Data provided by the user in this step are dependent on the IM system, but with our modifications, the system confirms a unique number that will be used as a BIX Identifier for the new BIX member.

We emphasize that one of the distinguishing features of the BCI, compared with the X.509 PKI, is that all protocol messages have only one object—the BIX certificate itself. Different messages are distinguished by different contents of the certificate. This simplifies parsing and processing of messages, as each step includes only handling values of certificate attributes.

5.1. Certification Request/Response Protocol—This protocol is executed by the person who wants to join the BIX system. The purpose of this protocol is to issue a BIX certificate to the new user. This certificate must be issued by the user who joined the BIX system last and therefore his/her certificate is at the "tail" of an instance of the BCL. Before initiating the protocol, the new user should have been registered in the BIX IM System and should have obtained his/her BIX Identifier and accurate date/time. For this purpose standard IM servers must be extended with the functionality to keep Register of issued identifiers, so that duplicate identifiers are not issued.

The procedure is illustrated in Fig. 1. Top level represents an instance of the BCL and the bottom level shows users and their BCI Agents. Only relevant segments of BIX certificates are shown. The convention is that when the segment is populated it is shown in bold; otherwise normal font is used.

As mentioned in the Section 4, an instance of the BCL is initiated by the BCI Authority generating Root Certificate. Its *Issuer* segment is the same as its Subject segment, *i.e.*, the certificate is self–issued. After generation by the BCI Agent, the `backwardCrossSignature`, `nextSubject` and `forwardCrossSignature` attribute are not populated.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

The protocol is initiated by the new member who creates a *Certification Request* message and sends it to the BIX IM system. The message is an instance of the BIX certificate with the `Header` partially populated, the `Subject` segment completely populated, and the `subjectSignature` created as follows:

- `version` is set to *one* (1) — this denotes the *Security Services Certificate*
- `subjectBIXID` is set to the value of the BIX Identifier returned by the BIX IM system
- `subjectDateTime` is set to the date/time returned by the BIX IM system
- `signatureAlg` is set to the ObjectID of the crypto algorithm used with asymmetric keys
- `subjectPublicKey` is the public key generated by the user using local BIX BCI Agent
- `subjectSignature` is the signature over the complete `Subject` structure using the private key that corresponds to the `subjectPublicKey`

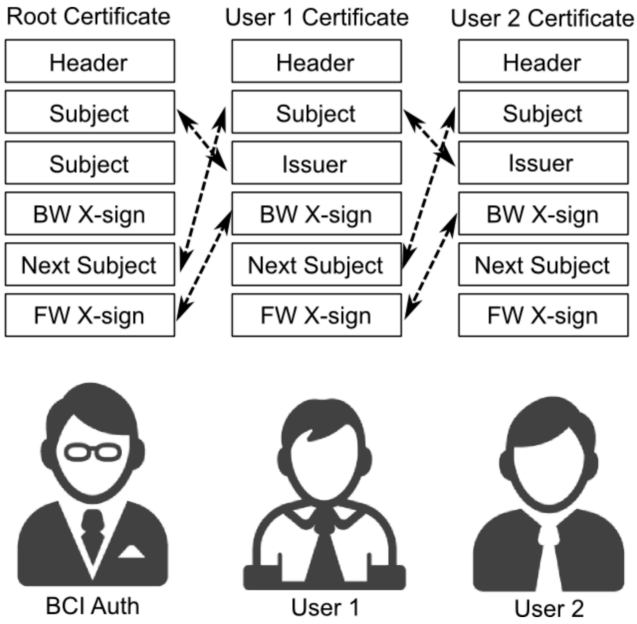

Fig. 1. Issuing of Certificates and Building an Instance of the BCL.

Because the new user is completely "detached" from the BIX system, he/she does not know which user has joined last the BIX system, *i.e.*, who should be the Issuer of the new certificate. Therefore, the new user broadcasts the certificate as a *Certificate Request* message to all current users in the BIX system. All users whose certificates have the `nextSubject` segment populated will disregard the request. Only one user will accept and process the request: the user whose certificate does not have the segment `nextSubject` populated. In Fig. 1 for User 1 that is BCI Authority and for User 2 that is User 1.

That user will be the *Issuer* of the new certificate, issued by the following procedure:

- `serialNumber` is populated with the value one higher than the value of the serial number in the issuer's certificate
- `issuingDateTime` is set by the Issuer to the current date and time

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

- `Issuer` segment and `issuerSignature` are the `Subject` segment and the `subjectSignature` from the issuer's certificate; therefore, they are copied into the new certificate

After populating the `Header` and `Issuer` segments, the Issuer recovers the hashes from the `subjectSignature` and `issuerSignature`, combines them with attributes from the now completed `Header` and signs that data combination using the Issuer's private key, creating an intermediate (single signature) version of the `backwardCrossSignature` attribute. In that way, the Issuer binds the `Subject` segment from his/her own certificate with the `Subject` segment from the certificate of the new user and creates a sequential relationship between the issuing user and the new BIX member. This relationship is also enforced by the values of the `serialNumber` attribute of the two certificates, as the new certificate is created with the value of the `serialNumber` attribute one larger than the value of the `serialNumber` attribute of the Issuer's certificate.

At the same time, the Issuer updates the segment `nextSubject` of his/her own certificate with the `Subject` segment of the new certificate. Then, he/she creates an intermediate (single signature) version of the `forwardCrossSignature` attribute over the `Header` and two hashes extracted from the `subjectSignature` attribute and the `nextSubjectSignature` attribute of his/her certificate. This is shown in Fig. 1 as relationships between certificates of User 1 and User 2.

After completing the certificate of the new user and extending his/her own certificate, as described, the Issuer returns three certificates to the new user by submitting them to the BIX IM System as a *Certification Reply* message: Root Certificate, its own certificate, and the certificate of the new user.

5.2. Verification of New Certificates—After receiving three certificates, the new user performs verification of the new certificate using two procedures:

Completion of the Issuer's certificate: The new user signs the `forwardCrossSignature` attribute of the Issuer's certificate and returns that certificate to the Issuer. In that way the relationship between the Issuer and the new member as his/her successor in an instance of the BCL is enforced. The purpose of this action is to prevent the Issuer from eventually being able to cheat by removing the `nextSubject` segment from his/her certificates and issuing the certificate to another user. That would "detach" the complete section of an instance of the BCL located beyond the cheating member. With the `forwardCrossSignature` attribute containing a pair of signatures in the Issuer's certificate, the new user is "tightly" linked into the BIX BCL, as he/she has the proof who is the Issuer of the new certificate.

Verification of the new certificate: The new user signs the `backwardCrossSignature` attribute in his/her own certificate and in that way links it to the certificate of the Issuer. After that, the user verifies the Issuer's certificate by traversing the complete instance of the BCL either forward, starting with the Root Certificate and following the `nextSubject` references, or backward, starting from his/her certificate and following the Issuer references.

During the verification process, the new user accumulates all certificates from an instance of the BCL, what is equivalent to the building of the blockchain in the Bitcoin payment system. Each certificate is validated and stored in the local storage of verified, therefore trusted, certificates for future use. It may be emphasized that this certificate verification procedure does not use and does not depend upon any third party. The user does not need to

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

trust any other component in the system and the main purpose of the BCL is utilized by a pure peer-to-peer protocol.

5.3. Certificate Request/Response Protocol—When a user wants to establish a secure session or to perform some secure transaction with another user, the two users must first exchange their BIX certificates. For that, after establishing a communication connection and, eventually, an application context, each user sends his/her own BIX certificate to another user. Because one user usually initiates the transaction, these two exchange messages may be considered as the *Certificate Request* and the *Certificate Reply* messages.

After receiving the partner's BIX certificate, the receiver must first verify the certificate before using its attributes. Verification comprises two steps: verification of the attributes included in the partner's certificate and verification of the membership of the partner in the BIX system. The first verification is performed by verifying `subjectSignature`, `issuerSignature` and `backwardCrossSignature` attributes. Both public keys for this verification are already available in the received partner's certificate. The membership of the partner in the BIX system is checked by verifying that the partner's certificate is included in an instance of the BCL. This procedure is equivalent to the verification of the user's own certificate after issuance, *i.e.*, by traversing an instance of the BCL from the partner's certificate backwards to the already verified certificate. For that, the *Issuer* segment of each certificate being verified is used as the reference.

Referring to Fig. 2, assume that users with Certificates 51 and 99 have just exchanged certificates and they want to verify each other's certificate. This procedure starts with the partner's certificate and may have three versions:

(1) If the partner's certificate is located "backwards" in an instance of the BCL from the user's own certificate (the partner was registered before the current user), then the partner's certificate is already in the local user's database of validated certificates. This is the case when User 99 validates certificate of the User 51.

(2) If the partner's certificate is located "forward" in an instance of the BCL from the user's own certificate (the partner was registered after the current user), and no other "forward" partners have been validated before, then the procedure will terminate when reaching own certificate. This is the case when User 51 validates certificate of User 99.

(3) If the partner's certificate is located "forward" in an instance of the BCL and some other "forward" partners have already been validated, then the procedure will terminate (a) immediately, if the partner's certificate is before some already validated certificate. This is the case when User 51 validates certificate of User 99, but he has already earlier validated certificate of User 100, (b) otherwise, when reaching the first already validated certificate of some other partner. This is the case when User 51 validates certificate of User 99, but he has already earlier validated certificate of User 52.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

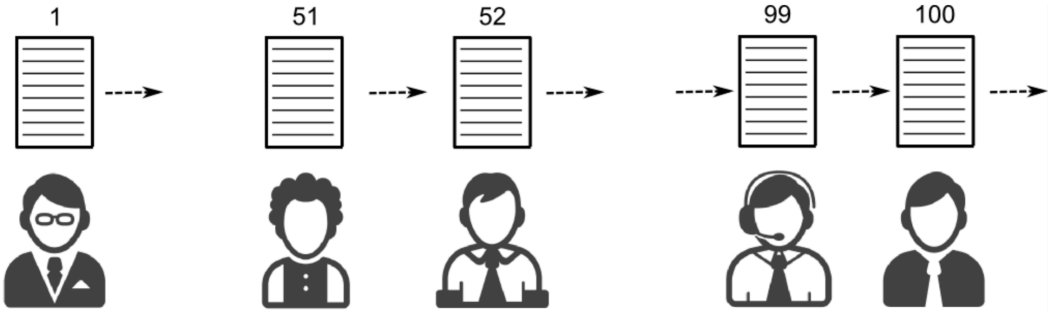

Fig. 2. Different Cases of Validation of Certificates.

During the validation procedure, if the partner's certificate is located "forward" and beyond all currently validated certificates, the user adds some additional certificates in his/her local certificates chain—all those located between the last validated and the new partner's certificate. This is the case (3b) above, when User 51, during validation of the certificate of the User 99 adds to his certificate chain certificates of Users 53 up to 99. This means that, by establishing secure connections with new partners, the users extend their local chain of validated certificates. The longer the local copy of the BCL is, the more efficient is the validation procedure of new certificates.

5.4. Certificates Ledger Request/Response—During the procedure of validation of partners' certificates, users extend their local database of validated certificates. The longer the local copy of the BCL is, more efficient the validation procedure of certificates of new partners is, as their certificates may be located between the user's certificate and the last validated certificate in the user's local chain. In that case, validation is simple, as the target certificate has already been validated, although the user never had a direct relationship with that partner.

This leads to the obvious conclusion that it is beneficial for a user to have all certificates currently in an instance of the BCL in his/her trusted (verified) local certificates chain. In particular, that means all certificates between the last validated certificate in the user's local chain and the current top of an instance of the BCL. But, as described earlier, the user who is at the top of the Ledger is the current Issuer of the next certificate. It is clear from the description of the validation procedure of the new certificate (Section 5.2) that the Issuer is certainly the member of the BIX system who is in possession of all certificates currently in the BIX Certificates Ledger. Therefore, that user is in the situation to distribute the full BIX BCL to other users. This step may be performed automatically after completion of the registration procedure for new BIX members. But, in order not to overload the system, this distribution is performed upon request sent by other users.

When some user wants to receive all certificates currently in an instance of the BCL, that user will send to the BIX IM system his/her own certificate. This message is a *Certificate Ledger Request* and it will be distributed to all users, equivalent to the *Certificate Request* message. Just as with that message, this *Request* is received out of the communications and applications context, so it will be disregarded by all users except the current Issuer.

The Issuer will collect all validated certificates from his/her local chain, starting with the certificate in the *Request* message and up to his/her own certificate, build a *Certificate Ledger Reply* message, and return it to the requesting user. The user will perform validation of each

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

new certificate, starting with his/her own and moving "forward" to the "tail" of the Ledger, and will store all new certificates in the local database.

This procedure overloads the Issuer, at least for some period of time, but it makes validation of partners' certificates for all other users in the system much more efficient. This is an example of the community-based procedure, where one protocol is not optimal for one, particular user in the system, but it is optimal for the overall community.

5.5 Renewal of the Certificates—The procedure to renew certificate is exactly the same as the procedure to request certificate the first time. This means that the new certificate of a user will be added to the tail of an instance of the BCL. Therefore, there will be two certificates in an instance of the BCL, both belonging to the same user. Therefore, other users will always use the certificate which is closer to the tail of an instance of the BCL.

This approach has two advantages compared to the standard concept of a PKI: (a) the same procedure is used to request an original version of the certificate and to request a renewed certificate, and (b) the same storage of certificates—BCL is used to store valid and also revoked certificates.

6. Optimization and Elimination of Threats

6.1. Optimization—One of the minor, but important operational issues, is that an instance of the BCL may grow very large with large number of users registered in the BIX system. As the consequence, the procedure for distribution and validation of certificates may become a bottleneck.

This problem may be solved by establishing multiple trusted certificates in an instance of the BCL, but without their verification using the protocol in the Section 5.2. That protocol has only one trusted certificate—Root Certificate, received by each member out-of-band.

The concept of multiple certificates that are also trusted, but without verification based on traversing the full instance of the BCL, means that such certificates are received from trusted partners, who are already the members of the BIX system. Those members of the BIX system can distribute their BIX certificates to new users using, for instance, secure E-mail. In our implementation we use S/MIME formatted E-mail letters with BIX certificates as their attachments. These E-mail letters provide sender's authenticity using digital signatures, receiver's authenticity using digital enveloping, confidentiality and integrity of E–mail letters. So, recipients may validate such E-mail letters and accept the attached certificate as trusted without traversing the full instance of the BCL

The disadvantages of this procedure are that it violates anonymity of the sending member and depends on the third party (Certificate Authorities to manage certificates used for S/MIME encapsulation). Its improvements to eliminate these disadvantages are one of the topics of our future research.

6.2. Threat: Breaking the Forward Link—One of the important threats to the consistency and correctness of the protocol, and therefore an instance of the BCL itself, is the case that malicious user may interrupt the Certificate Request/Response protocol by "breaking the forward link." In this analysis we assume that BCI Agent performs its functions correctly, so that illegal manipulation with the BCL can be done only by manipulating the certificates.

Malicious user, who is in the middle of an instance of the BCL, first removes `nextSubject` segment from his/her certificate, including `nextSubjectSignature` and `forwardCrossSignature`. With this manipulation malicious user (a) "detaches" all users that were certified after the malicious user from the BCL and (b) declares him/herself as

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

Issuer of the new certificate. When the new user sends Certification Request, the request will be processed by the BCI Agents of two users—malicious user and legitimate user, who is at the end of an instance of the BCL. Based on specific timing, the new user may receive certificate issued by malicious user before the correct certificate, issued by the legitimate Issuer.

Because of this problem, BCI Agent of the new user must accept certificate with some delay. If two Certification Responses are received, then illegal certificate may easily be recognized by the larger sequence number. If this case is detected, validation of an instance of the BCL must be performed backwards, as the `Issuer` segment of the first certificate in an instance of the BCL after the certificate of the malicious user will still point to the certificate of that user, so traversing of an instance of the BCL backwards will not be affected.

6.3. Threat: Breaking the Backward Link—Malicious user, in order to disrupt an instance of the BCL, may also remove `Issuer` segment from his/her certificate, thus breaking the backward link. In this case, validation of an instance of the BCL in the backward direction may be disrupted. But, forward traversing of an instance of the BCL would still work.

6.4. Threat: Breaking the BIX Certificates Ledger—Finally, malicious user may decide to remove both segment from his/her certificate and in that way disconnecting the two sections of an instance of the BCL. In that case, if the new user is traversing an instance of the BCL backwards, he/she will not be able to detect the Issuer of the damaged certificate. If traversing is forward, the new user will not be able to detect the next certificate after the damaged certificate. To resolve the issue and detect whether a certificate in an instance of the BCL without `NextSubject` segment is a legitimate certificate of the current Issuer or modified certificate, when traversing forward and reaching such certificate, the user should always request one more certificate, with the value of the `sequenceNumber` attribute one higher than the value of the same attribute in the certificate without `NextSubject` segment. If traversing backwards, the user should request one more certificate with the value of the `sequenceNumber` attribute one less than the value of the same attribute in the certificate without `NextSubject` segment. Requesting this extra certificate represents a "jump" when traversing an instance of the BCL over the damaged certificate.

6.5. Threat: Blocking the Progress of a BCL—A user whose certificate is at the tail of an instance of the BCL may intentionally turn-off its BCL Client or may decide to stop participating in the BCI before certifying the next user. Upon detecting this case, based on time-out of the request (the parameter of the BCI Policy), the certificate of the requesting user will be issued by the Root Authority. This means that in such certificate, the `Issuer` segment would designate be Root Authority and the value of the `sequenceNumber` attribute in the new certificate would indicate its position in the BCL.

This situation also means that there will be two (or more) certificates in an instance of the BCL without `NextSubject` segment populated. `NextSubject` segment determines the issuer of the next certificate. But since the owner of the previous certificate without `NextSubject` populated is passive, the user certified by the Root Authority, will issue the certificate based on the new request.

7. Contributions, Challenges and Open Issues

We hope and expect that the innovative concept of a new infrastructure represents significant contribution to the area of secure, private and anonymous applications and transactions based

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

on the concept of secure block ledger. One particular important contribution is the new structure of certificates. They are quite different from the structure of the current X.509 certificates, which are appropriate for hierarchical PKIs with trusted third parties. The structure of BIX certificates is suitable for peer–to–peer, community–based transactions and applications. Another innovative contribution is all certification protocols. They are very specific, applicable to the structure of BIX certificates and also providing validation of certificates without third parties. Finally, significant contribution is certificates extensions and application interfaces for use of BIX certificates.

There are three important challenges. One is formal and rigorous validation of the infrastructure and its protocols. The second are issues mentioned in Section 4, which require further studies. And, finally, as always with large IT infrastructures, the issue will be potential operational overheads, throughputs and distribution of certificates. However, in spite of these challenges, our on–going research and initial development/testing indicate that the concept of the infrastructure is correct and that operation issues are not too serious.

8. Conclusion

We hope and expect that the innovative concept of a new infrastructure will enable secure and reliable creation, distribution, verification, and use of anonymous user identities and public keys. The power of the infrastructure is to be the enabling technology for a new category of applications with anonymity of users, their data, and transactions. The profile of the BIX certificate specified in the Appendix and all BCI certification protocols provide all features listed in Section 3.

It is important to emphasize that BIX certificates, BCI for their management and all its protocols do not require or depend on the trust in any party other than the Root Certificate. Even that certificate can be verified using public posting, out-of-band distribution and/or confirmations by many members of the community. All other steps and all BIX certificates are validated by the user himself/herself. Security, privacy and anonymity of user data and transactions are fully under user control and consent.

It is also important to note that BIX certificates can be extended with additional attributes and in that way can support certain applications that, in addition to anonymity, have also some additional requirements. For instance, a *Electronic Voting* application requires anonymity for voting "transactions," but also requires explicit identification of voters. A *Digital Notary* application requires anonymity of customers, but requires explicit authorization to perform notary functions. *Digital Auctions* require anonymity for bidding, as well as anonymity for payments, but also require explicit identification for delivery of digital or tangible goods.

All of these new applications that require anonymity can easily be supported by BIX certificates with appropriate extensions, combined with application-specific protocols.

Our further research is focused on optimization of BCI protocols, extensions of BIX certificates, and a new category of applications that provide anonymity based on the use of BCI certificates and services. Another important topic is to design the concept of the trust in the members of the community in order to authorize them to perform correctly all specified protocols and steps. One of the solutions for that is to ensure correctness and integrity of BIX BCI Agents as software modules.

Several on-going projects in the US, EU, Brazil and South Africa will serve as the proof of concept, as the first validation and as the first examples of applications that use the services of the BCI.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

Future versions of the BIX certificates will include in their extensions attributes that are specific for and required by various applications with anonymity, as well as some additional requirements and/or services. For instance, for payments based on virtual currencies, the extensions will include Bank Routing and Account Numbers for conversion of virtual into real currency. For Electronic Voting, the extension will include real identities of voters that will be used to validate their eligibility to vote.

Acknowledgement

The author would like to thank Prof. Kostas Lambrinoudakis, University of Pireus (Greece), Prof. Ahmed Patel, Universiti Kebangsaan Malaysia (UKM), and the research team from the Department of Mathematics, University of Trento (Italy) for their very valuable comments and suggestions that greatly improved the clarity of the paper. We also acknowledge excellent comments and suggestions by the anonymous reviewers.

Appendix: BIX Certificate (ASN.1)

```
BIX Certificate ::= SEQUENCE {

    Header ::= SEQUENCE {
       sequenceNumber INTEGER
       version        INTEGER
       issuingDateTime   CHOICE {
          UTCTime,
          generalizedTime
       }
    }

    Subject ::= SIGNED SEQUENCE {
        subjectBIXID     INTEGER,
        subjectDateTime  CHOICE {
          UTCTime,
          GeneralizedTime
       }
       signatureAlg   AlgorithmIdentifier,
       subjectPublicKey  OCTET STRING
    }
    SubjectSignature ::= BIT STRING

    Issuer ::= SIGNED SEQUENCE {
       issuerBIXID    INTEGER,
       issuerDateTime CHOICE {
          UTCTime,
          GeneralizedTime
       }
       signatureAlg   AlgorithmIdentifier,
       issuerPublicKeyOCTET STRING
    }
    IssuerSignature ::=  BIT STRING

    BackwardCrossSignature::= BIT STRING

    NextSubject ::= SIGNED SEQUENCE {
       nextSubjectBIXID     INTEGER,
       nextSubjectDateTime  CHOICE {
         UTCTime,
         GeneralizedTime
       }
       signatureAlg      AlgorithmIdentifier,
```


ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

```
      nextSubjectPublicKey OCTET STRING
   }
   NextSubjectSignature::=  BIT STRING

   ForwardCrossSignature::= BIT STRING

   Extensions ::= SEQUENCE {
      extnID         objectIdentifier
      critical       BOOLEAN
      extnValue      OCTET STRING
   }
}
```

Notes and References

[1] Muftic, S., bin Abbdullah, N., Kounelis, I. "Business Information Exchange System with Security, Privacy, and Anonymity." *Journal of Electrical and Computer Engineering* **2016** 1-10 (2016) doi:10.1155/2016/7093642

[2] Buterin, V., "Secret Sharing and Erasure Coding: A Guide for the Aspiring Dropbox Decentralizer." *Ethereum Blog* (16 August 2014) https://blog.ethereum.org/2014/08/16/secret-sharing-erasure-coding-guide-aspiring-dropbox-decentralizer/

[3] Wilkinson, S. "Storj: A Peer-to-Peer Cloud Storage Network." No Publisher (15 December 2014) http://storj.io/storj.pdf

[4] See for example the following website offering proof-of-existence services: https://proofofexistence.com/

[5] Larcheveque, E. "Bitcoin address authentication protocol (BitID)." No Publisher (2014) https://github.com/bitid/bitid/blob/master/BIP_draft.md

[6] Bamert, T., Decker, C., Wattenhofer, R., Welten, S. "BlueWallet: The Secure Bitcoin Wallet." In *Security and Trust Management*. Springer 65–80 (2014)

[7] Goldfeder, S., Gennaro, R., Kalodner, H., Bonneau, J., Kroll, J. A., Felten, E. W., Narayanan, A. "Securing Bitcoin Wallets via Threshold Signatures." No Publisher (2014) http://www.cs.princeton.edu/~stevenag/bitcoin_threshold_signatures.pdf

[8] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., Polk, W. "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", *IETF* RFC 5280 (2008)

[9] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System." No Publisher https://bitcoin.com/bitcoin.pdf

[10] Pedro, F., *Understanding Bitcoin: Cryptography, Engineering and Economics*. Wiley Finance Series (2014) ISBN: 978-1-119-01916-9

[11] Svensson, D. *SecuRES: Secure Resource Sharing System*. M.Sc. thesis ICT/KTH (June 2015)

[12] Ratnayake, Y. *SDMS: Secure Documents Management System*. M.Sc. thesis ICT/KTH (November 2015)

[13] See for example "Mt. Gox shuts down: Leaked document states 744,408 Bitcoins lost" (CNN Money) http://finance.fortune.cnn.com/2014/02/25/mt-gox-shutdown/

[14] Pseudonymous (MysteryMiner). "Easywallet.org wallets compromised – Uninstall Google Chrome spyware right now!" *Bitcoin Forum* (10 April 2013) https://bitcointalk.org/index.php?topic=172527.0

[15] See for example https://en.bitcoin.it/wiki/Weaknesses#Sybil_attack

[16] Sparkes, M., "The coming digital anarchy," In *The Telegraph* (June 2014) http://www.telegraph.co.uk/technology/news/10881213/The-coming-digital-anarchy.html

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27

[17] Shibli, A., et al. "Security Analysis of Bitcoin System (Vulnerabilities, Threats and Defense Techniques)." Unpublished manuscript

[18] Andreesen, M. "Why Bitcoin Matters", *The New York Times* (2014)

[19] Kounelis, J. *Secure and Trusted Mobile Commerce System based on Virtual Currencies.* Ph.D. dissertation ICT/KTH (November 2015)

[20] "Cyber-Extortionists Targeting the Financial Sector Are Demanding Bitcoin Ransoms." *Bloomberg Business* (September 2015)

[21] "Bitcoin revealed: a Ponzi scheme for redistributing wealth from one libertarian to another." *Washington Post* (January 2015)

[22] bin Abdullah, N. *Security Architecture and Protocols for Protection, Privacy, and Anonymity of Users and Transactions*. Licentiate Thesis ICT/KTH (November 2015)

[23] Muftic, S. "Security, Privacy, and Anonymity of Peer–to–Peer Transactions." Lecture notes EIT Digital, University of Trento (November 2015)

[24] "Extensible Messaging and Presence Protocol." *XMPP Standards Foundation* `www.xmpp.org`

[25] "XEP–0080: User Location." *XMPP Standards Foundation* `www.xmpp.org/extensions/xep-0080.html`

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.27