

Keychain

Blockchain Based Public Key Infrastructure

Claims

What is claimed is:

1. A method for storing public keys on a blockchain ledger, the method comprising: generating a private and public key using a public-key cryptosystem that may be independent of the cryptosystems used by the blockchain ledger; generating a blockchain-ledger transaction by embedding the generated public key in the transaction's payload space; broadcasting the generated transaction onto the blockchain ledger using the blockchain protocol.
2. The method of claim 1, wherein the blockchain ledger transaction contains no data identifying the transaction sender other than the public key.
3. The method of claim 1, embedding a hash or reference of the public key in the transaction payload space.
4. The method of claim 1, the generated transaction comprising: a transaction input that is the output from a previously signed transaction that was also signed by the sender of the generated transaction.
5. A method for retrieving public keys from a blockchain ledger, the method comprising: looking up the transaction containing the public key by its blockchain address; decoding the public key from the transaction output payload space.
6. The method of claim 5, retrieving the hash or reference of the public key and looking up the public key from a data store external to the blockchain ledger.
7. A method for verifying whether a public key is cryptographically linked to another public key on the blockchain ledger, the method comprising: retrieving the input transactions of the transaction containing the public key or hash or reference thereof; verifying whether the payload of either input transaction contains the other public key (respectively, hash or reference thereof); recursively retrieving and examining the payloads of the inputs of those inputs transactions until the other public key (respectively, hash or reference thereof) is reached or until a transaction that is beforehand known as the root of a chain of public keys is reached.
8. A method defining the time-based acceptability of data that is encrypted or signed using a public key that is stored on the blockchain ledger, the method comprising: storing the public key in the blockchain ledger; as a consumer of data that will be encrypted or signed with the public key, waiting for a predetermined number of confirmations on a block containing the transaction that holds the public key or hash or reference thereof; as the producer, waiting an additional predetermined number of blockchain confirmations on that block, encrypting or signing the data with the public key, and sending the data to the consumer independently of the blockchain ledger; as a consumer, decrypting or verifying the received encrypted or signed data using the public key and verifying the number of confirmations on the block exceeds the number of confirmations in the first wait time.
9. The method of claim 1, wherein the stored public key is specified using an extensible data format, the format comprising: the name of the public-key cryptosystem that was used to

produce the public key; the timestamp of the approximate time the public key was created; the public key.

10. The method of claim 1, wherein data that is encrypted using the public key is encapsulated in an extensible data format, the format comprising: the cipher text of the data as encrypted by a symmetric cipher; the cipher text of the symmetric key as encrypted using the public key and the public-key cryptosystem; the public key; the name of the public-key cryptosystem.
11. The method of claim 10, further specifying the public key by the address and transaction output index of a blockchain-ledger transaction that contains the public key or a hash or reference thereof in its output payload space, thereby reducing the size of the encapsulation of the encrypted data and public key while allowing the blockchain ledger to be used as a historical reference for the public key of the recipient of the data.
12. The method of claim 10, further specifying a plurality of pairs of symmetric key cipher texts and public keys, wherein each symmetric key cipher text is the result of encrypting the symmetric key using the corresponding public key, thereby allowing multiple recipients to decrypt the data from the same cipher text while using the blockchain ledger as a historical reference for their respective public keys.
13. The method of claim 1, wherein data that is signed using the public key is encapsulated in an extensible data format, the format comprising: the data; the digital signature as produced using a public-key digital signature algorithm and the public key; the public key; the name of the public-key digital signature algorithm.
14. The method of claim 13, wherein the public key is specified by the address and transaction output index of a blockchain-ledger transaction which contains the public key or a hash or reference of the public key in its output payload space, thereby reducing the size of the encapsulation of the signed data and the signature public keys and allowing verifiers of the digital signature to use the blockchain ledger as a historical reference for the public key of the signer of the data.
15. The method of claim 13, further specifying a plurality of digital signatures and corresponding public keys, wherein each digital signature is the result of signing the data with the corresponding public key, thereby allowing multiple signers to sign the same data and allowing recipients to verify the digital signatures and their cryptographic links with known chain-root public keys on the blockchain ledger.