August 2022

Digital Currency Policy and Accountability Technical Framework

William Drewry

DIGITAL CURRENCY POLICY AND ACCOUNTABILITY TECHNICAL FRAMEWORK

Introduction

Traditionally, transactions with a digital currency are verified by a digital currency provider's system, and in the event of a transaction failure or double spend, either party in the transaction are held liable for any losses, damages, or other implications of the transaction failure. However, there arises the possibility of accidental failed transactions or abuse of system protocols by bad actors such that someone is held liable for losses for which they have no actual responsibility. There remains a need for technologies to reduce or eliminate the ability to successfully double spend digital currency while simultaneously protecting end users from being held liable for losses for which they are not responsible.

Summary

The disclosed technology provides computer-implemented systems and methods for reducing eliminating double spending in digital currency wallets and transactions through responsible observers and transaction integrated applications. A digital wallet or other digital currency storage device may be associated with a responsible observer, wherein the responsible observer acts as a transaction guarantor for transactions proportional to the security guarantees made by the responsible observer to a given financial authority, amount of currency being handled, and the adherence to currency systems expectations. A responsible observer may be a digital wallet vendor or merchant acquirer who vouches for the transaction based on their own criteria. The responsible observer may vouch for any transactions executed within their defined criteria, such that if an error occurs, the responsible observer will be held liable for losses, damages, or any other implications resulting from a failed transaction. The addition of cryptographic signatures with known public keys from the responsible observer may be used to realize such an approach.

For transactions performed offline, such as where a merchant or customer may not have access to digital currency servers, a policy carrying data structure (hereinafter "gadget") may be attached to the transaction, or currency exchanged within the transaction such that the transaction may be verified once either party reestablishes a connection with the digital currency servers. The gadget may be queried during an offline transaction (or, in some instances, online transactions) to verify the identity of the digital currency storage device. If a double spend is attempted, the gadget notifies both parties and the transaction will fail.

Computer-implemented systems and methods for providing transaction guarantors and offline transaction verification with the disclosed technology can provide for reduced or eliminated double spending with digital currencies and end-user liability protection. When a transaction is executed using digital currency, a transaction guarantor may be provided in the form of a responsible observer. A verified observer may be a secure hardware manufacturer, merchant, third party observer service or other medium for insuring transactions using digital currencies. The verified observer may be held accountable for any losses, damages, or other issues resulting from a failed transaction, such that the transaction abides by the verified observer's criteria. To determine whether a transaction has a verified observer, the verified observer may provide cryptographic proof in a plurality of ways including, but not limited to, a privacy-aware remote attestation system, privacy-preserving attestation protocol, a remote server verification, or similar protected identity proofing system.

The verified observer's criteria may include any number of conditions (physical and/or) virtual that must be met for the observer to be held responsible for a given transaction. For example, a digital wallet manufacturer may adopt a verified observer policy such that transactions by users of their products are protected by the digital wallet manufacturer. The digital wallet manufacturer may require further criteria in order to be considered the verified observer such as, for example, transactions with a worth <$10,000, withdrawal transactions only, or similar criteria decided by the digital wallet manufacturer. In another example, a merchant may adopt a verified observer policy such that transactions performed with the merchant hold the merchant liable. Further still, in another example, a third party company may develop a business model whereby they serve as the verified observer for transactions using digital currency. The third party company may require common policies or technical standards that merchants, transaction systems, and digital wallet manufacturers must abide by in order for the third party company to serve as the verified observer.

A responsible verified observer may reduce double spending and end-user liability, but may require online-only digital currencies or may only be able to observe transactions where a connection to a verification server is established. To ensure protection of offline transactions, a gadget may be appended to transactions, coins, or digital wallets to prevent or eliminate double spending and end user liability. A gadget may be a verifiable data structure that, when queried, exposes protected data. This attribute of the gadget allows different services to be notified of the type of device or user that attempted to double spend. A gadget may be bound to a coin along with a randomized access data structure (e.g., binary tree, SHA-256 Merkle tree, graph, etc.). The gadget is created and verified by a central authority (e.g., currency issuer, bank, transaction system, etc.) and bound to the coin. When the gadget is bound to the coin, a secret key such as, for example, the device key may be decomposed and placed within the randomized access data structure. When a transaction is performed against the coin, the randomized access data structure may be queried to reveal pieces of the secret key. The revealed pieces act as a form of receipt for the coin. If a double spend is attempted against the coin, when the randomized access data structure is queried, there is a significant probability that different pieces of the secret key will be revealed. The transaction may then be cancelled and both parties' devices may store the error to be uploaded when a connection is established.

When a gadget is bound to a coin, additional restrictions and metadata may be incorporated with the gadget. The recipient (e.g., counter-party, merchant, or opposing party in a transaction) device may decide whether or not to accept a transaction based on the metadata associated with the gadget. In some instances, the gadget metadata may comprise a time limit or expiration on the gadget. As such, the coin the gadget is bound to may be unusable or inaccessible after the time limit is reached until the digital wallet storing the coin reestablishes a connection with a validation system. Further, the gadget metadata may comprise a settlement time limit. As such, the coin bound to the gadget is usable so long as the transaction may be settled within the settlement time limit. With each transaction completed with the coin, the settlement time limit may decrease to encourage reestablishing connection with the validation system.

In one embodiment, a coin is stored on a user computing device. When the coin is downloaded to the user computing device, a server computing system attaches a verified gadget to the coin. If a user attempts to complete a transaction with the user computing device, the gadget may be queried to prevent double spending of the coin and the transaction is uploaded and verified by the server computing system. In the event the user attempts to complete a transaction without connection to the server computing system, the gadget may be queried to prevent double spending and the coin is stored on the user computing device along with the gadget result. An expiration time and settlement time limit may be instantiated on the gadget such that reestablishing connection with the server computing system is required before the expiration time and any transaction that takes longer than the settlement time limit to settle is cancelled. In some instances, a separate server computing system may be queried with a private key to identify a verified observer responsible for a current transaction. If the private key identifies a verified observer and the current transaction satisfies the verified observer's criteria, the verified observer may be listed as the liable party for the transaction in the event of an attempted abuse of systems or the transaction fails. Any combination or order of the methods described herein can be executed on a user computing device, remote computing device, or similar. For example, all steps of binding a gadget to a coin, identifying a verified observer, and querying a gadget may be performed on a remote computing system or parts of the process can be performed on a user computing device and others on a remote computing system as previously described.

Detailed Description

Figure 1 depicts an example computing system 100 in which systems and methods in accordance with the present disclosure can be executed. The computing system comprises a user computing device 102 including one or more processors 112, memory 114 which may include data 116 and instructions 118 configured to carry out the methods disclosed herein, and a user input component 122. The user input component can be, for example, a touch display or physical buttons within the user computing device 102. The computing system 100 further comprises a network 180 and a server computing system 130. The server computing system 130 comprises one or more processors 132, and memory 134 which may contain data 136 and instruction 138 configured to carry out the methods disclosed herein.

Figure 2 depicts an example transaction 200 according to aspects of the present disclosure. A first digital currency storage medium 202, a second digital currency storage medium 204, and an observer validation server 206 are depicted. During the transaction 200, a digital currency 212 may be exchanged between the first digital currency storage medium 202 and the second digital currency storage medium 204 in exchange for goods or services 214. During the transaction 200, the first digital currency storage medium 202 may query the observer validation server 206 with a key 208. If the transaction 200 satisfies the necessary criteria outlined by the observer validation server 206, the observer validation server 206 will provide the signature 210 for the transaction and assign or assume the role of the responsible observer. The responsible observer will be held liable for any losses, damages, or other outcome resulting from the transaction 200 being abused or failing. In some instances, the manufacturer of the first digital currency storage medium 202 or the second digital currency storage medium 204 may certify their devices such that the manufacturer (not pictured) may provide signatures within their devices to sign transactions.

Referring now to Figure 3, an example transaction 300 is provided using a first digital currency storage medium 302, a second digital currency storage medium 304, and a transaction authentication server 306 according to aspects of the present disclosure. In the transaction 300, the first digital currency storage medium 302 and the second digital currency storage medium 304 may have failed connections 316 and 314 to the authentication server 306 respectively. Due to the failed connections 316 and 314, the first digital currency storage medium 302 may attach a gadget 310 to the digital currency 308 in the transaction 300 for goods or services 312. The gadget 310 may be responsible for preventing double spending of the digital currency 308 and may be bound to the digital currency 308 until either failed connection 316 or 314 is rectified.

The gadget 310 may operate by revealing a portion of a secret key at transaction time when queried. As such, if the first digital currency storage medium 302 attempts another transaction with the digital currency 308, the gadget 310 may reveal further pieces of the secret key, thus identifying a double spend. Since the second digital currency storage medium 304 is the recipient of the digital currency 308, it may choose to re-spend the digital currency 308. To do so, the second digital currency storage medium 304 must attach its own gadget (not pictured) to prevent double spending once again.

As the digital currency 308 is spent and re-spent with failed connections 316 and 314, the limitations encompassing the bound gadgets may become stricter and stricter to encourage rectification of the failed connections 316 and 314. The limitations encompassing the bound gadgets may comprise a plurality of parameters. The plurality of parameters may include, but is not limited to, gadget expiration time, or a settlement time limit. In the event any of the limitations are exceed, the digital currency 308 is no longer usable for transactions. In order to access the digital currency 308, the failed connection 314 or 316 must be rectified.

Figures

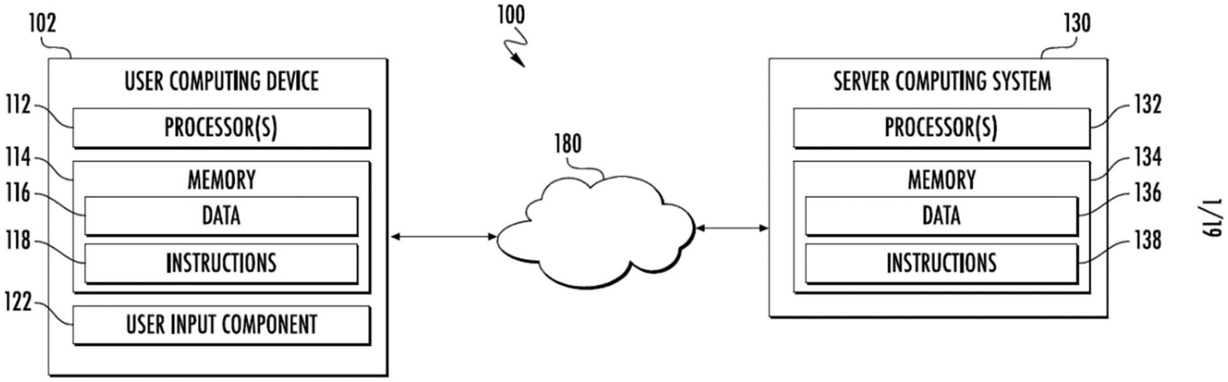

FIG. 1

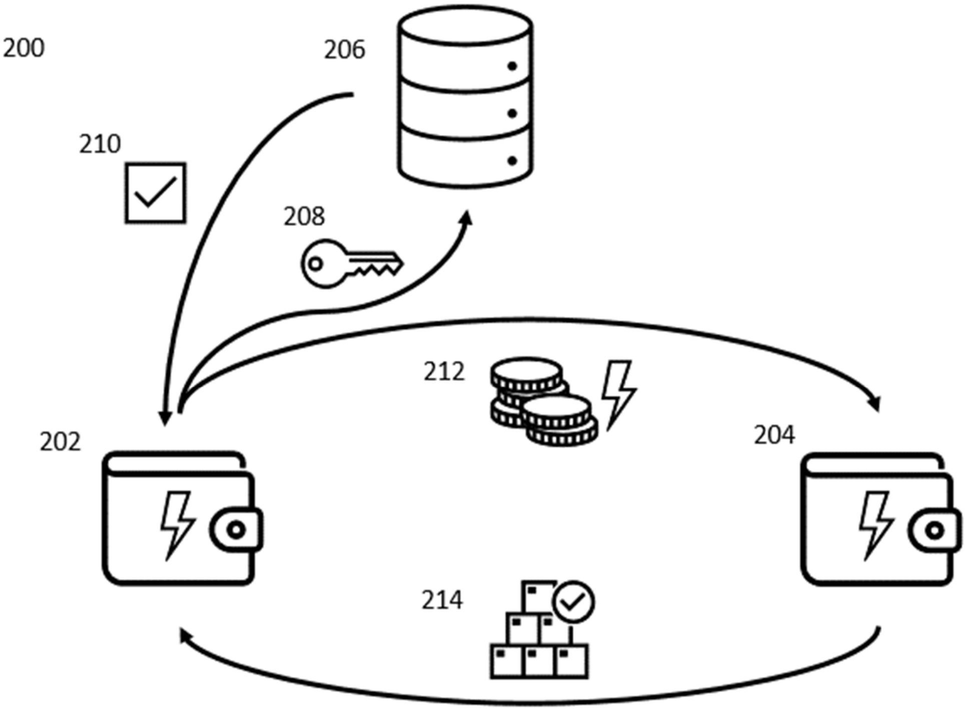

FIG. 2

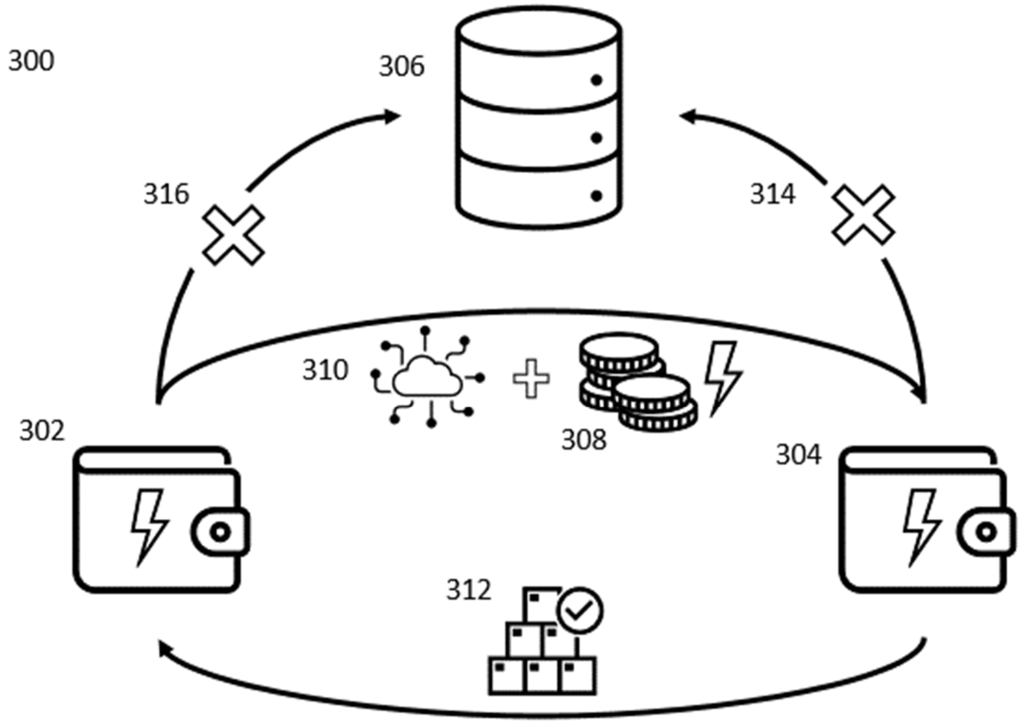

FIG. 3

Abstract

Computer-implemented systems and methods for digital currency transaction guarantors and double spending protection are described herein. A verified observer may be defined for a given transaction depending on certain criteria required by the verified observer such that any liability incurred for failure of the given transaction or an abuse of a system in the given transaction is the sole responsibility of the verified observer. When a coin is deposited to a digital currency storage device, a gadget may be bound to the coin by a verified authority or the digital currency storage device such that when the coin is used in a transaction the gadget generates an output to prevent double spending of the coin.