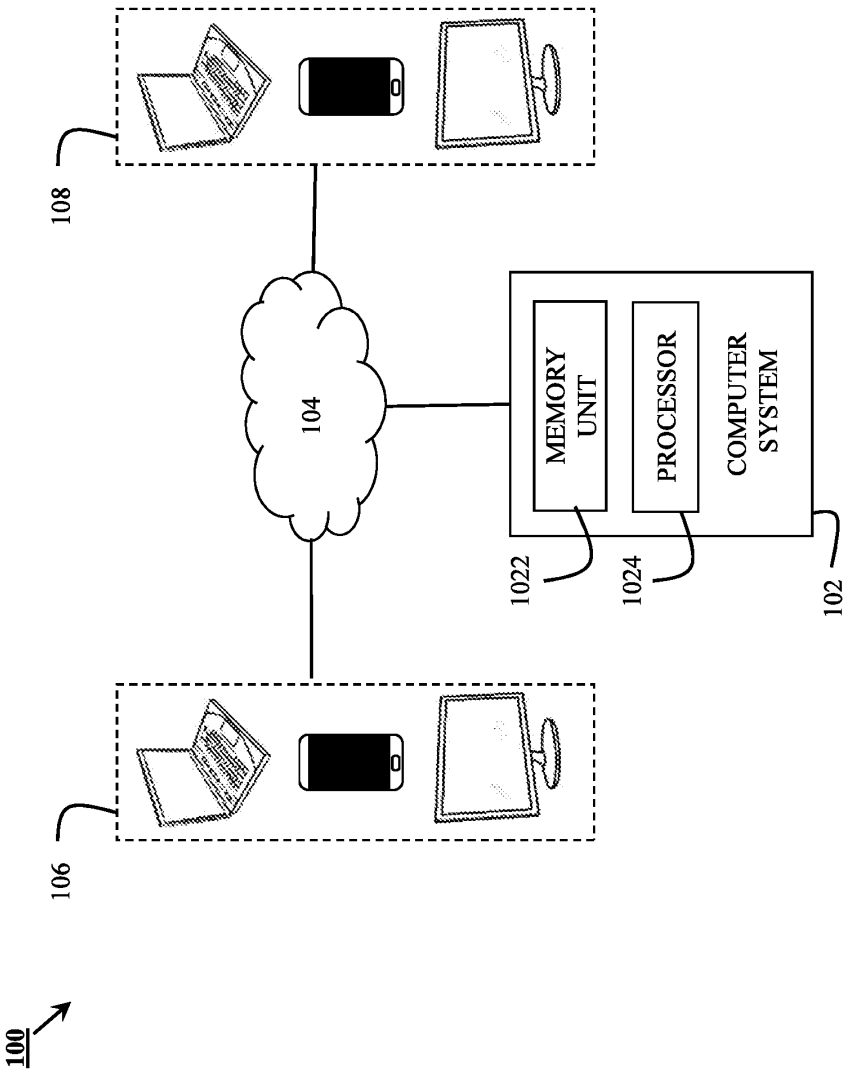

100
108
106
104
COMPUTER SYSTEM
MEMORY UNIT
PROCESSOR
1022
1024
102

FIG. 1

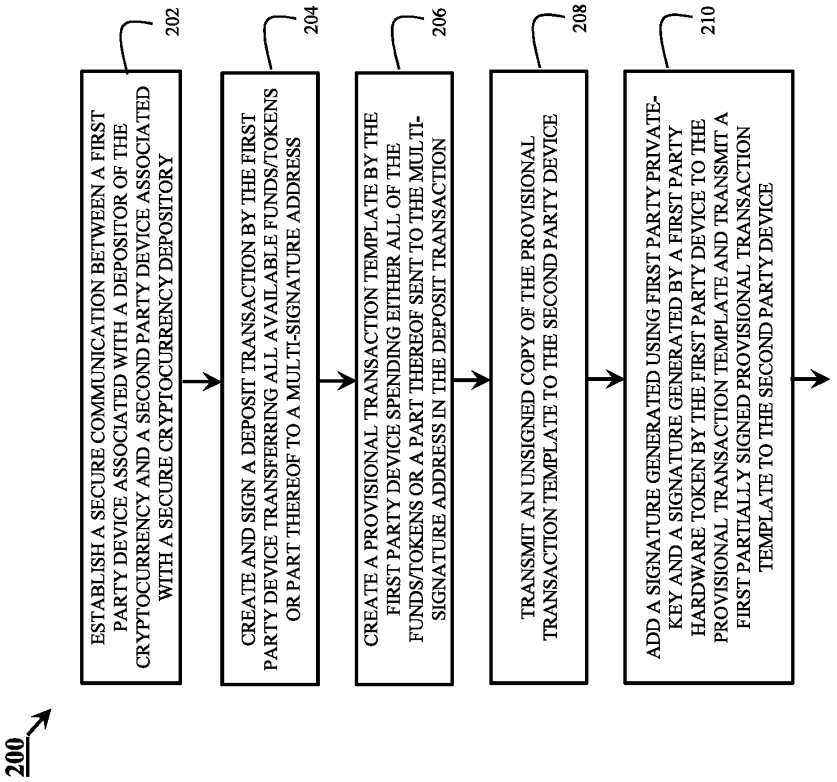

200
ESTABLISH A SECURE COMMUNICATION BETWEEN A FIRST PARTY DEVICE ASSOCIATED WITH A DEPOSITOR OF THE CRYPTOCURRENCY AND A SECOND PARTY DEVICE ASSOCIATED WITH A SECURE CRYPTOCURRENCY DEPOSITORY
202
CREATE AND SIGN A DEPOSIT TRANSACTION BY THE FIRST PARTY DEVICE TRANSFERRING ALL AVAILABLE FUNDS/TOKENS OR PART THEREOF TO A MULTI-SIGNATURE ADDRESS
204
CREATE A PROVISIONAL TRANSACTION TEMPLATE BY THE FIRST PARTY DEVICE SPENDING EITHER ALL OF THE FUNDS/TOKENS OR A PART THEREOF SENT TO THE MULTI-SIGNATURE ADDRESS IN THE DEPOSIT TRANSACTION
206
TRANSMIT AN UNSIGNED COPY OF THE PROVISIONAL TRANSACTION TEMPLATE TO THE SECOND PARTY DEVICE
208
ADD A SIGNATURE GENERATED USING FIRST PARTY PRIVATE-KEY AND A SIGNATURE GENERATED BY A FIRST PARTY HARDWARE TOKEN BY THE FIRST PARTY DEVICE TO THE PROVISIONAL TRANSACTION TEMPLATE AND TRANSMIT A FIRST PARTIALLY SIGNED PROVISIONAL TRANSACTION TEMPLATE TO THE SECOND PARTY DEVICE
210

FIG. 2

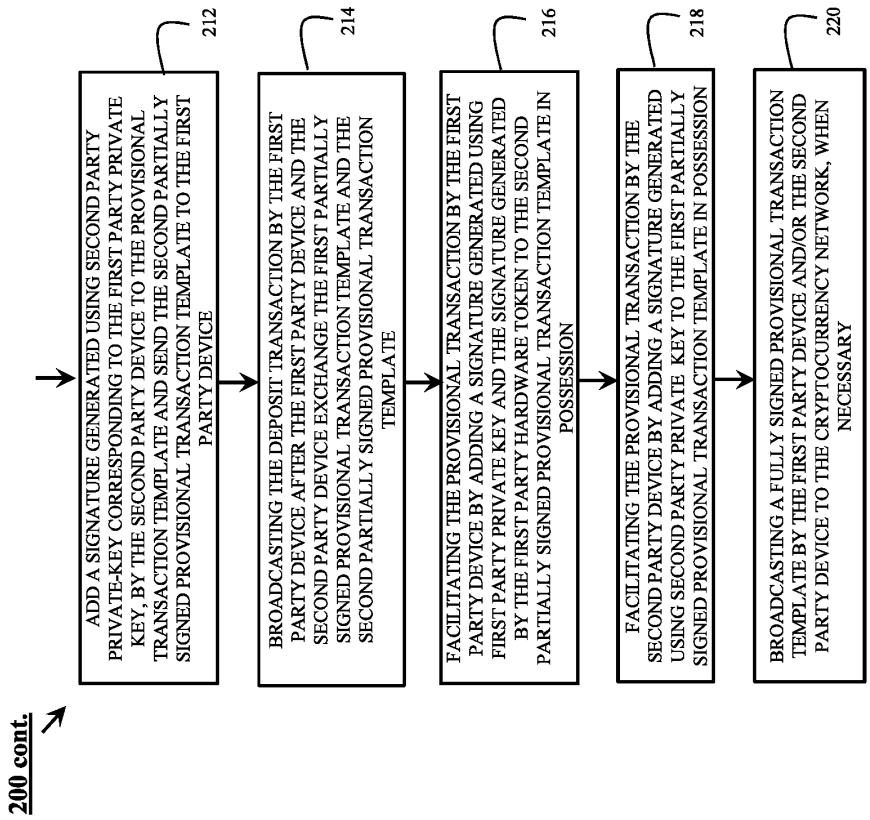

200 cont.
ADD A SIGNATURE GENERATED USING SECOND PARTY PRIVATE-KEY CORRESPONDING TO THE FIRST PARTY PRIVATE KEY, BY THE SECOND PARTY DEVICE TO THE PROVISIONAL TRANSACTION TEMPLATE AND SEND THE SECOND PARTIALLY SIGNED PROVISIONAL TRANSACTION TEMPLATE TO THE FIRST PARTY DEVICE
212
BROADCASTING THE DEPOSIT TRANSACTION BY THE FIRST PARTY DEVICE AFTER THE FIRST PARTY DEVICE AND THE SECOND PARTY DEVICE EXCHANGE THE FIRST PARTIALLY SIGNED PROVISIONAL TRANSACTION TEMPLATE AND THE SECOND PARTIALLY SIGNED PROVISIONAL TRANSACTION TEMPLATE
214
FACILITATING THE PROVISIONAL TRANSACTION BY THE FIRST PARTY DEVICE BY ADDING A SIGNATURE GENERATED USING FIRST PARTY PRIVATE KEY AND THE SIGNATURE GENERATED BY THE FIRST PARTY HARDWARE TOKEN TO THE SECOND PARTIALLY SIGNED PROVISIONAL TRANSACTION TEMPLATE IN POSSESSION
216
FACILITATING THE PROVISIONAL TRANSACTION BY THE SECOND PARTY DEVICE BY ADDING A SIGNATURE GENERATED USING SECOND PARTY PRIVATE KEY TO THE FIRST PARTIALLY SIGNED PROVISIONAL TRANSACTION TEMPLATE IN POSSESSION
218
BROADCASTING A FULLY SIGNED PROVISIONAL TRANSACTION TEMPLATE BY THE FIRST PARTY DEVICE AND/OR THE SECOND PARTY DEVICE TO THE CRYPTOCURRENCY NETWORK, WHEN NECESSARY
220

FIG. 2 cont.

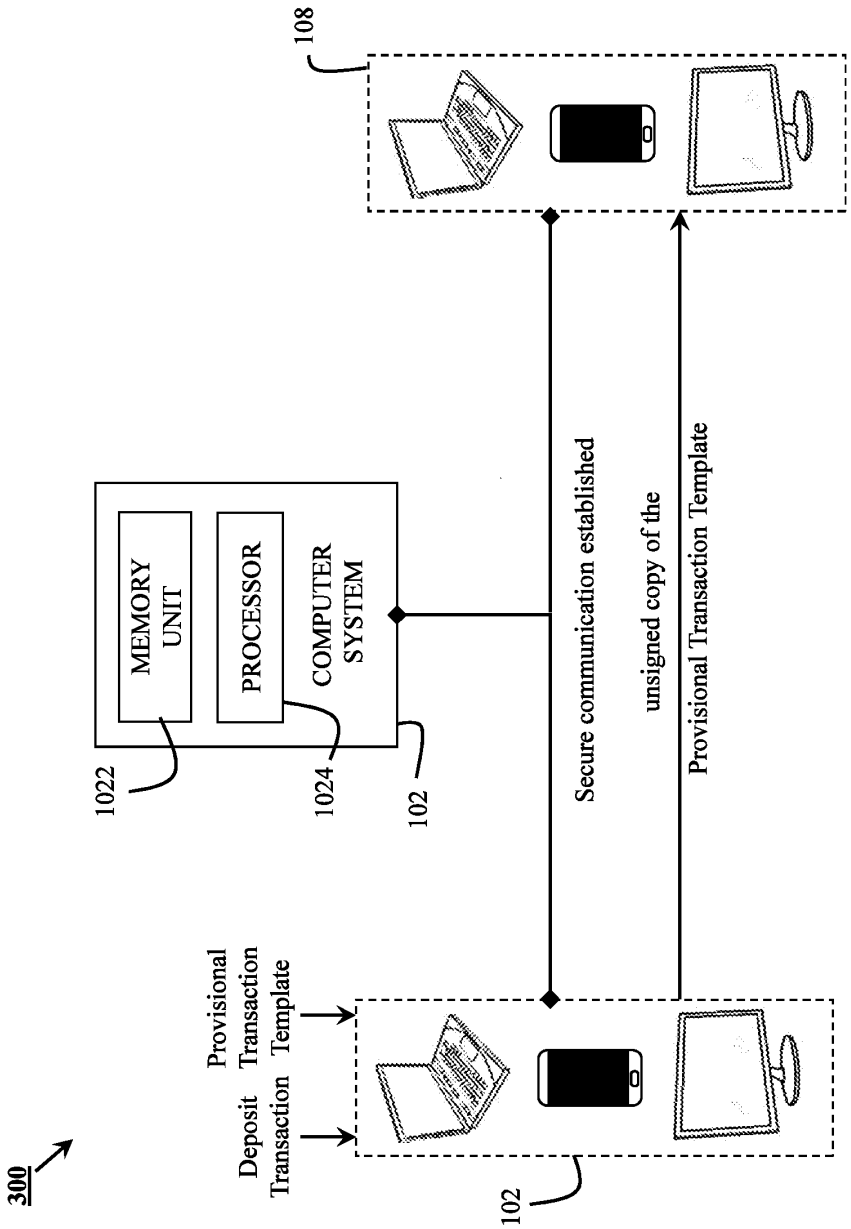

300
Provisional Transaction Template
Deposit Transaction Template
102
Secure communication established
unsigned copy of the
Provisional Transaction Template
108
COMPUTER SYSTEM
PROCESSOR
MEMORY UNIT
1022
1024
102

FIG. 3

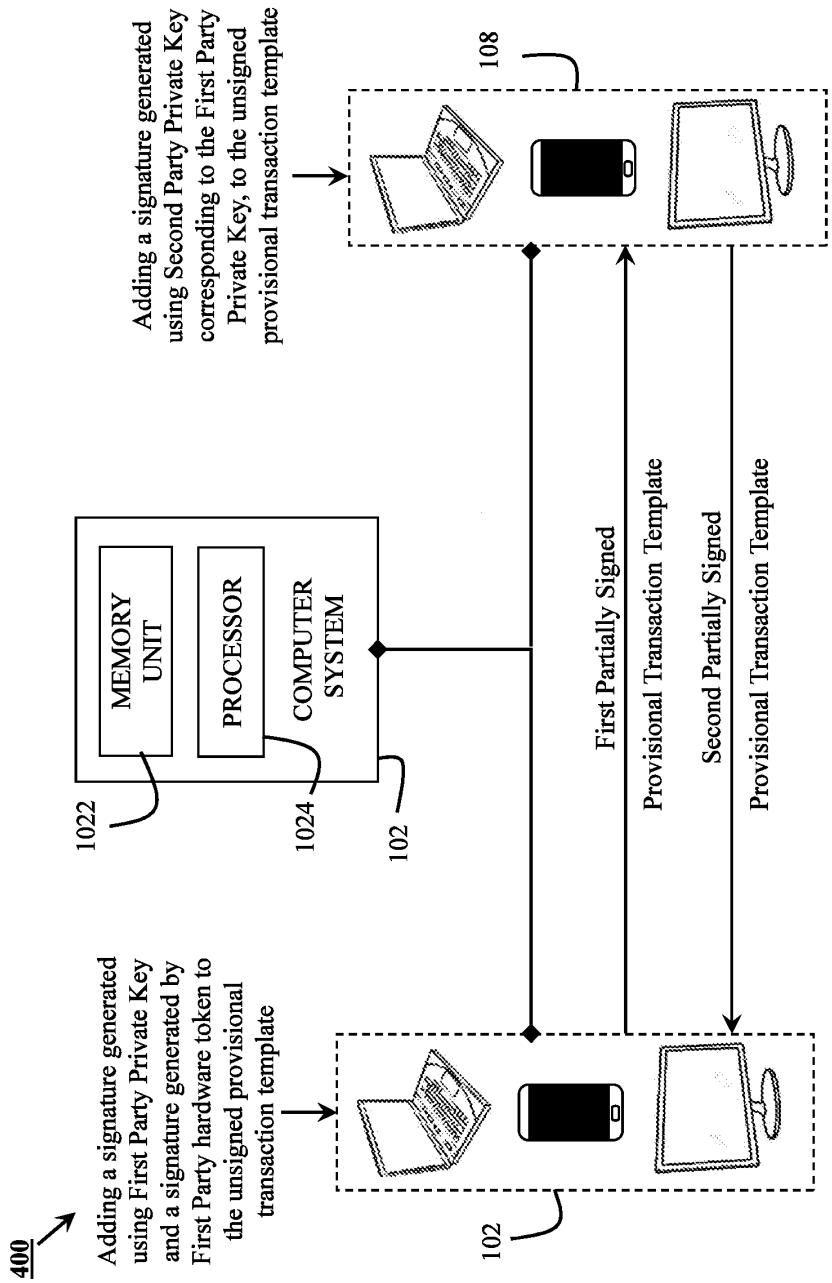

400
Adding a signature generated using First Party Private Key and a signature generated by First Party hardware token to the unsigned provisional transaction template
102
First Partially Signed Provisional Transaction Template
Second Partially Signed Provisional Transaction Template
108
Adding a signature generated using Second Party Private Key corresponding to the First Party Private Key, to the unsigned provisional transaction template
COMPUTER SYSTEM
MEMORY UNIT
PROCESSOR
1022
1024
102

FIG. 4

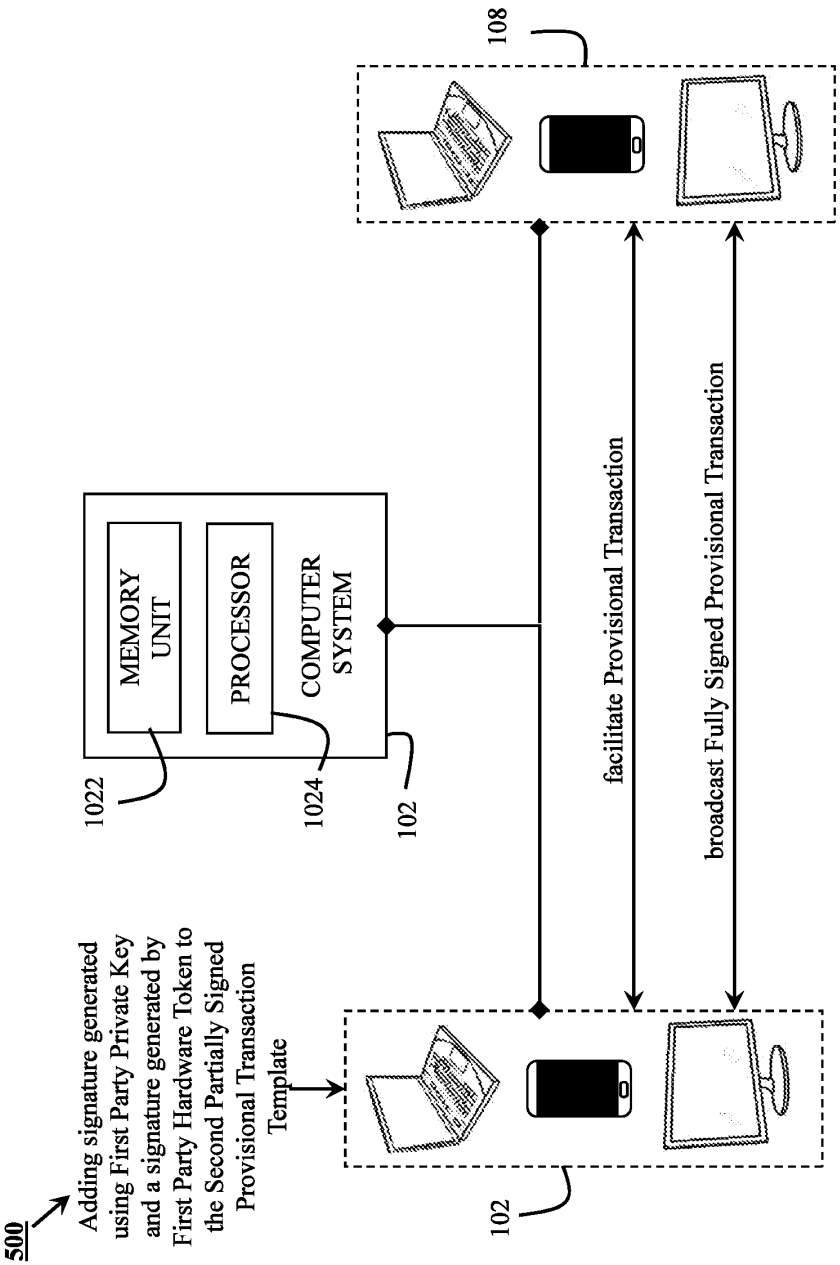

500
Adding signature generated using First Party Private Key and a signature generated by First Party Hardware Token to the Second Partially Signed Provisional Transaction Template
102
108
facilitate Provisional Transaction
broadcast Fully Signed Provisional Transaction
COMPUTER SYSTEM
PROCESSOR
MEMORY UNIT
1022
1024
102

FIG. 5

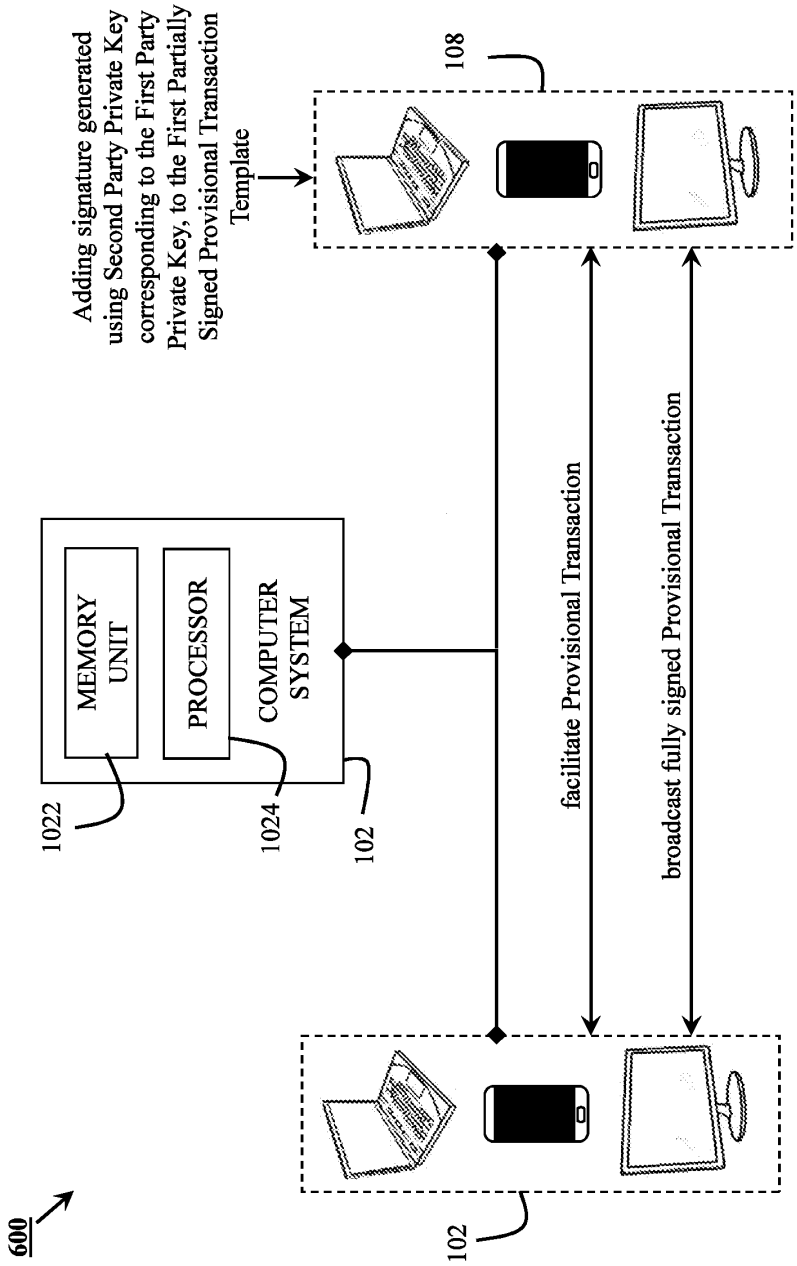

600
102
108
Adding signature generated using Second Party Private Key corresponding to the First Party Private Key, to the First Partially Signed Provisional Transaction Template
facilitate Provisional Transaction
broadcast fully signed Provisional Transaction
COMPUTER SYSTEM
PROCESSOR
MEMORY UNIT
1022
1024
102

FIG. 6

700

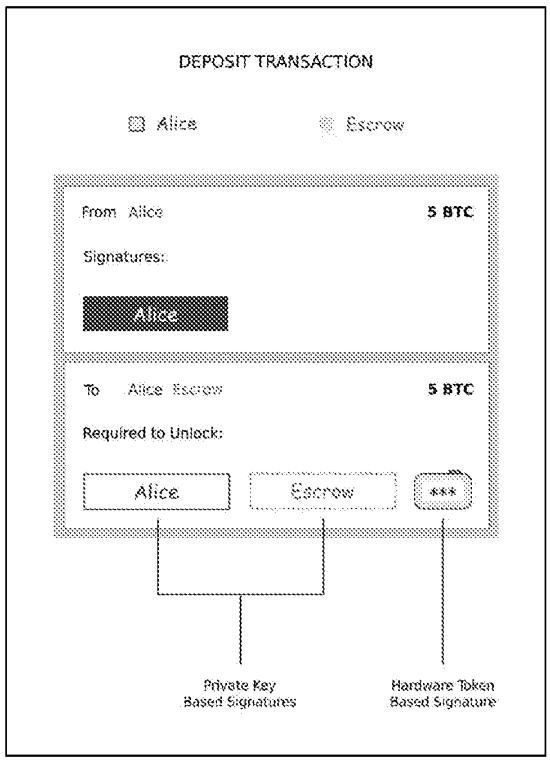

DEPOSIT TRANSACTION
Alice
Escrow
From Alice
5 BTC
Signatures:
Alice
To Alice Escrow
5 BTC
Required to Unlock:
Alice
Escrow
***
Private Key
Based Signatures
Hardware Token
Based Signature

FIG. 7

800

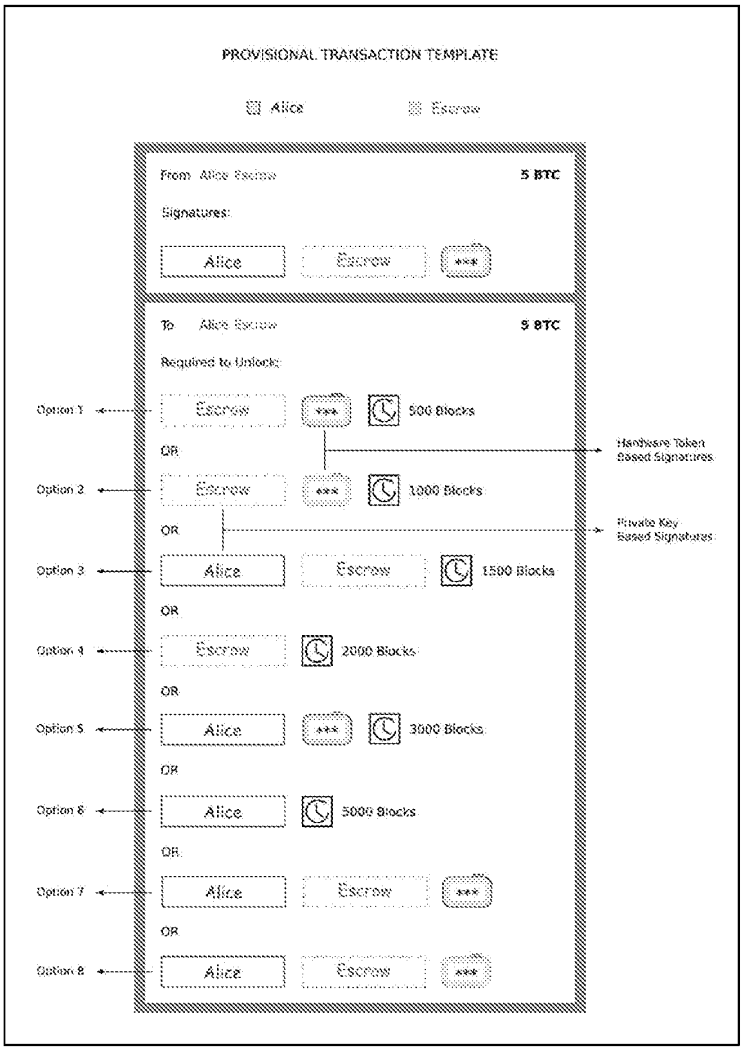

PROVISIONAL TRANSACTION TEMPLATE
Alice
Escrow
From Alice Escrow
5 BTC
Signatures:
Alice
Escrow
***
To Alice Escrow
5 BTC
Required to Unlock:
Option 1
Escrow
***
500 Blocks
OR
Option 2
Escrow
***
1000 Blocks
OR
Option 3
Alice
Escrow
1500 Blocks
OR
Option 4
Escrow
2000 Blocks
OR
Option 5
Alice
***
3000 Blocks
OR
Option 6
Alice
5000 Blocks
OR
Option 7
Alice
Escrow
***
OR
Option 8
Alice
Escrow
***
Hardware Token Based Signatures
Private Key Based Signatures

FIG. 8

900

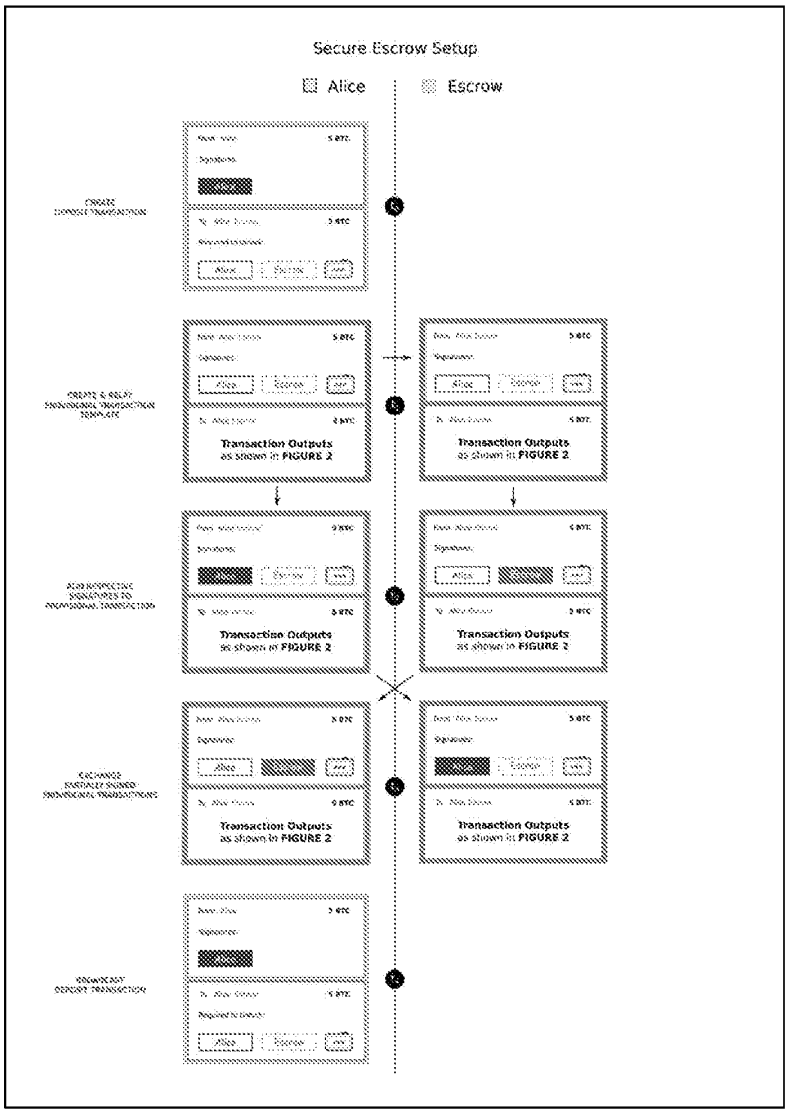

Secure Escrow Setup
Alice
Escrow
Transaction Outputs
as shown in FIGURE 2

FIG. 9

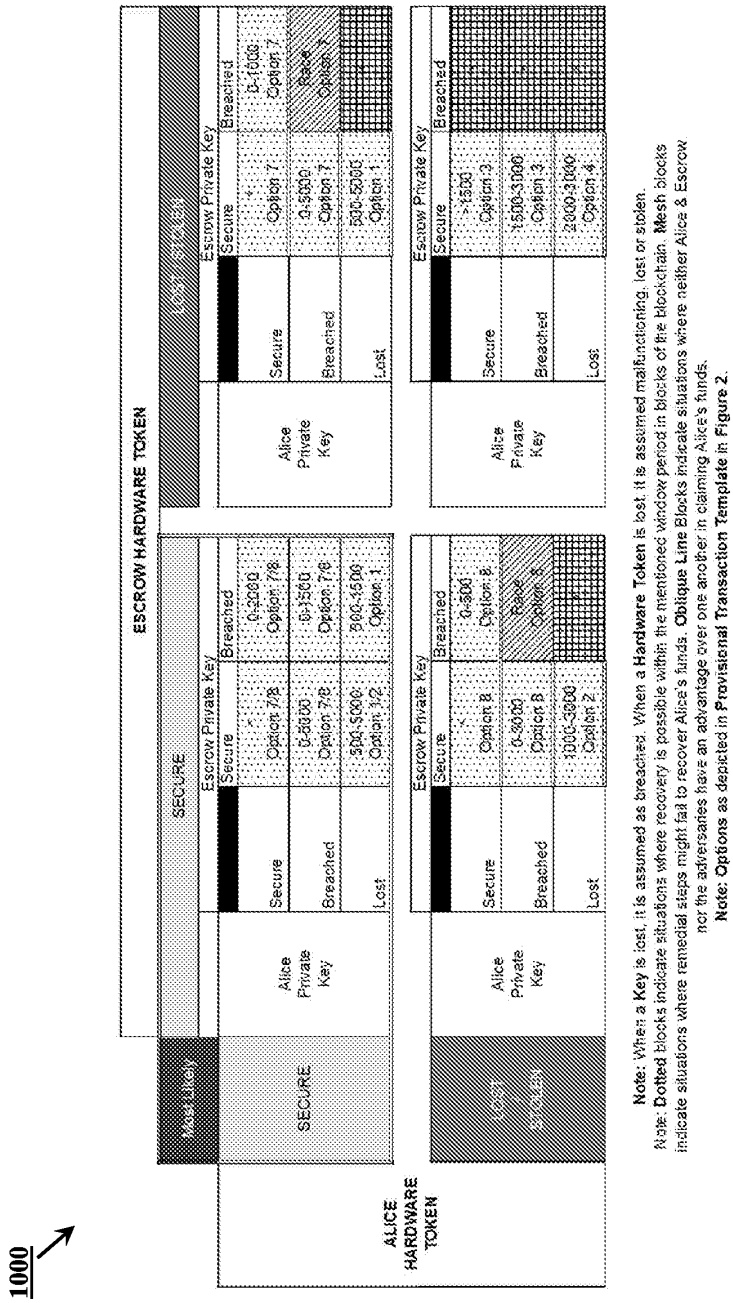

1000
ALICE HARDWARE TOKEN
Most Likely
SECURE
LOST
Alice Private Key
Secure
Breached
Lost
Escrow Private Key
Secure
Breached
Option 7/8
Option 1/2
Option 8
Option 2
Option 7
Option 1
Option 3
Option 4
ESCROW HARDWARE TOKEN
Note: When a Key is lost, it is assumed as breached. When a Hardware Token is lost it is assumed malfunctioning, lost or stolen.
Note: Dotted blocks indicate situations where recovery is possible within the mentioned window period in blocks of the blockchain. Mesh blocks indicate situations where remedial steps might fail to recover Alice's funds. Oblique Line Blocks indicate situations where neither Alice & Escrow nor the adversaries have an advantage over one another in claiming Alice's funds.
Note: Options as depicted in Provisional Transaction Template in Figure 2.

FIG. 10

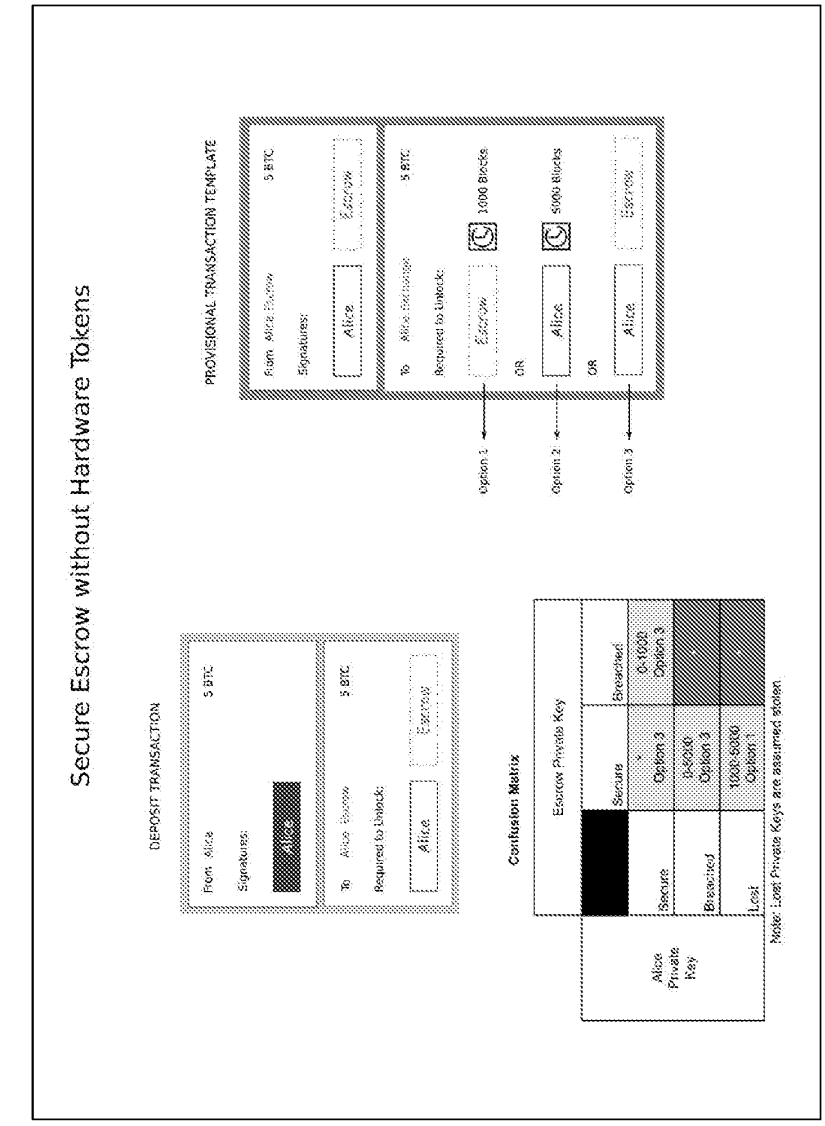

1100
Secure Escrow without Hardware Tokens
DEPOSIT TRANSACTION
From Alice
5 BTC
Signatures:
Alice
To Alice Escrow
5 BTC
Required to Unlock:
Alice
Escrow
PROVISIONAL TRANSACTION TEMPLATE
From Alice Escrow
5 BTC
Signatures:
Alice
Escrow
To Alice Recovery
5 BTC
Required to Unlock:
Escrow
1000 Blocks
OR
Alice
5000 Blocks
OR
Alice
Escrow
Option 1
Option 2
Option 3
Confusion Matrix
Escrow Private Key
Secure
Breached
Alice Private Key
Secure
Option 3
0-1000 Option 3
Breached
1001-5000 Option 3
Lost
1001-5000 Option 1
Note: Lost Private Keys are assumed stolen

FIG. 11

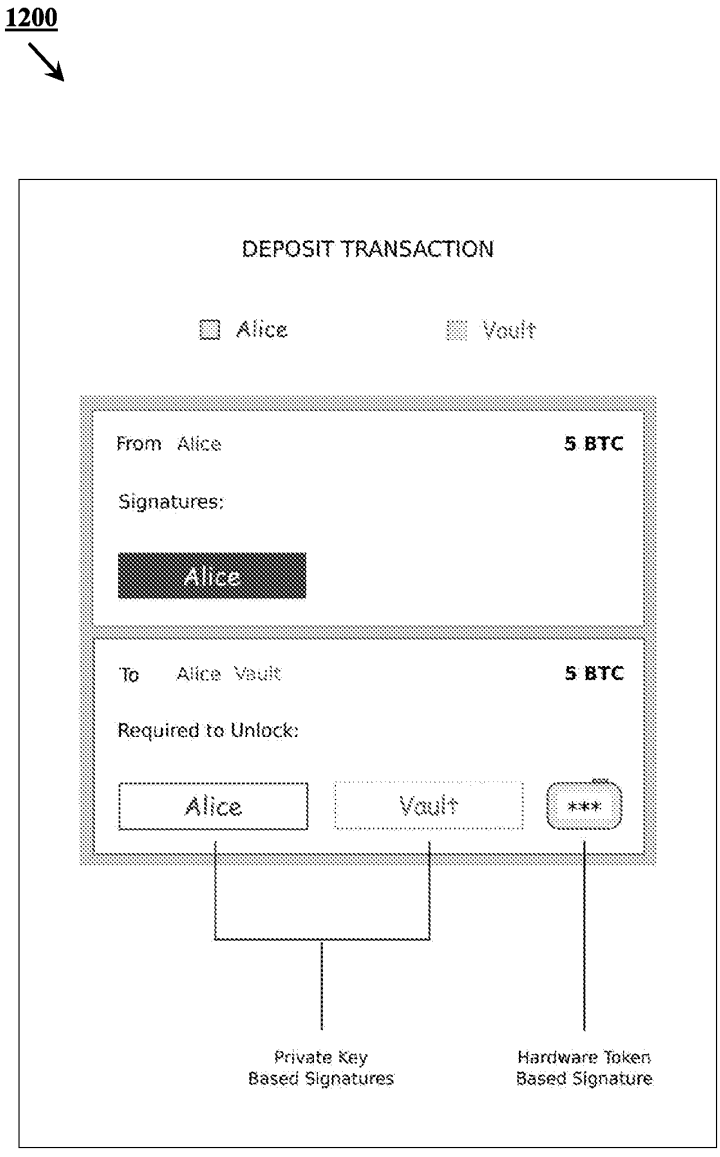

1200
DEPOSIT TRANSACTION
Alice
Vault
From Alice
5 BTC
Signatures:
Alice
To Alice Vault
5 BTC
Required to Unlock:
Alice
Vault
***
Private Key
Based Signatures
Hardware Token
Based Signature

FIG. 12

1300

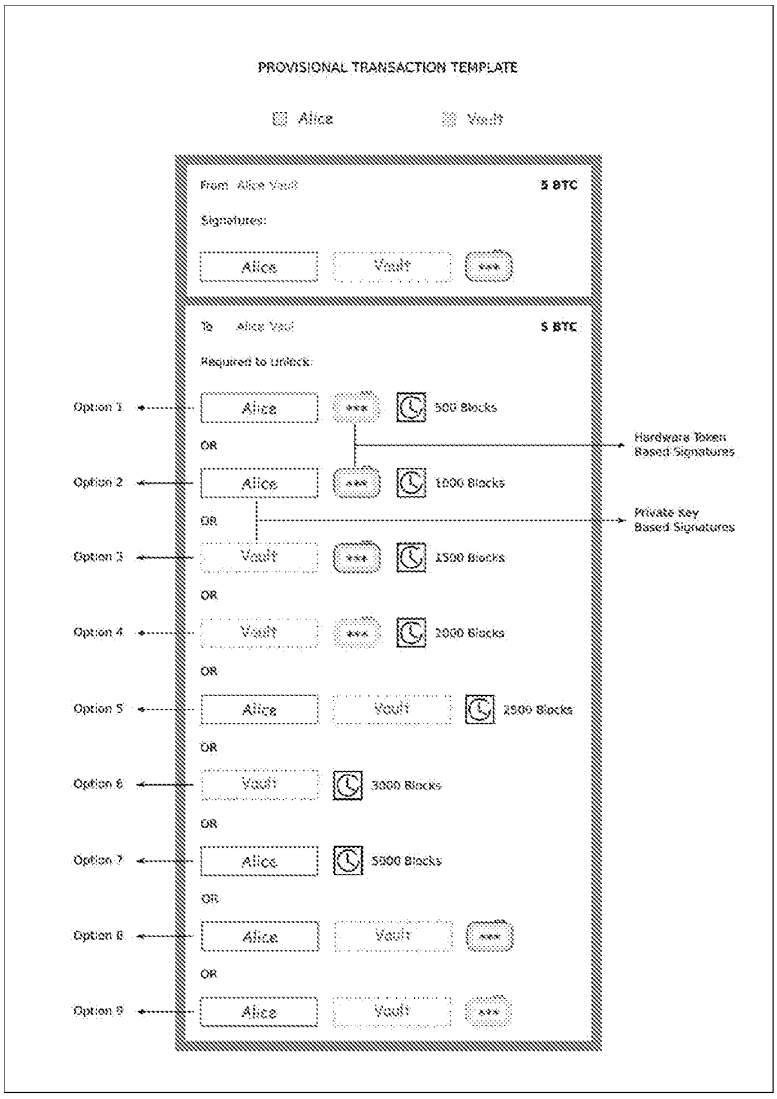

PROVISIONAL TRANSACTION TEMPLATE
Alice
Vault
From Alice Vault
5 BTC
Signatures:
Alice
Vault
To Alice Vault
5 BTC
Required to Unlock:
Option 1
Alice
500 Blocks
OR
Option 2
Alice
1000 Blocks
OR
Option 3
Vault
1500 Blocks
OR
Option 4
Vault
2000 Blocks
OR
Option 5
Alice
Vault
2500 Blocks
OR
Option 6
Vault
3000 Blocks
OR
Option 7
Alice
5000 Blocks
OR
Option 8
Alice
Vault
OR
Option 9
Alice
Vault
Hardware Token Based Signatures
Private Key Based Signatures

FIG. 13

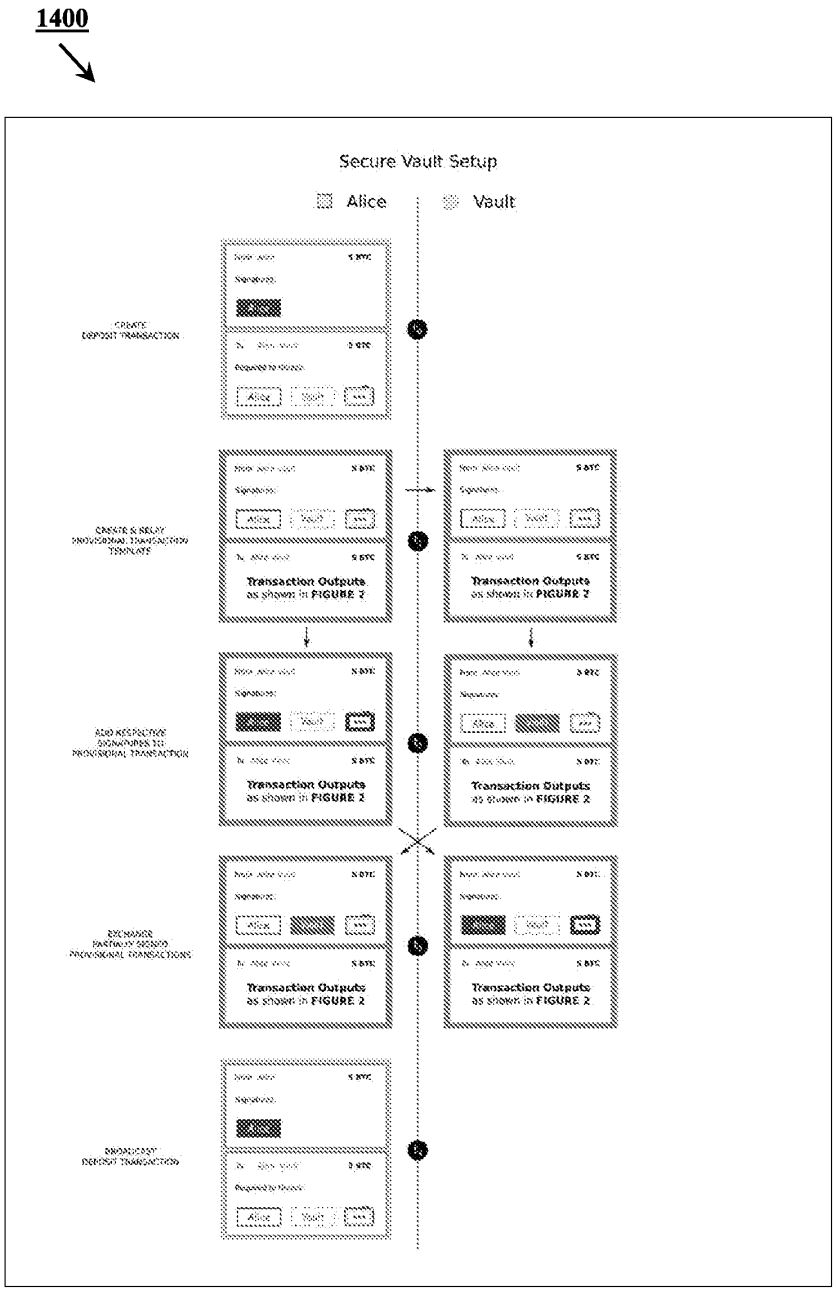

1400
Secure Vault Setup
Alice
Vault
Transaction Outputs
as shown in FIGURE 2

FIG. 14

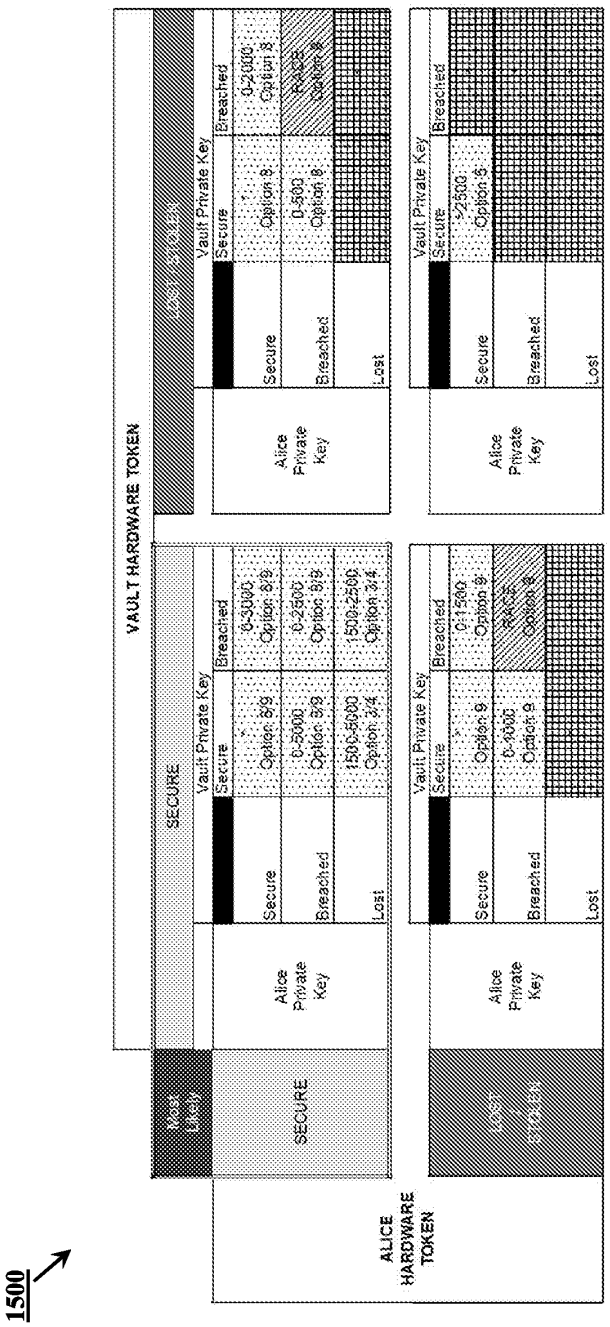
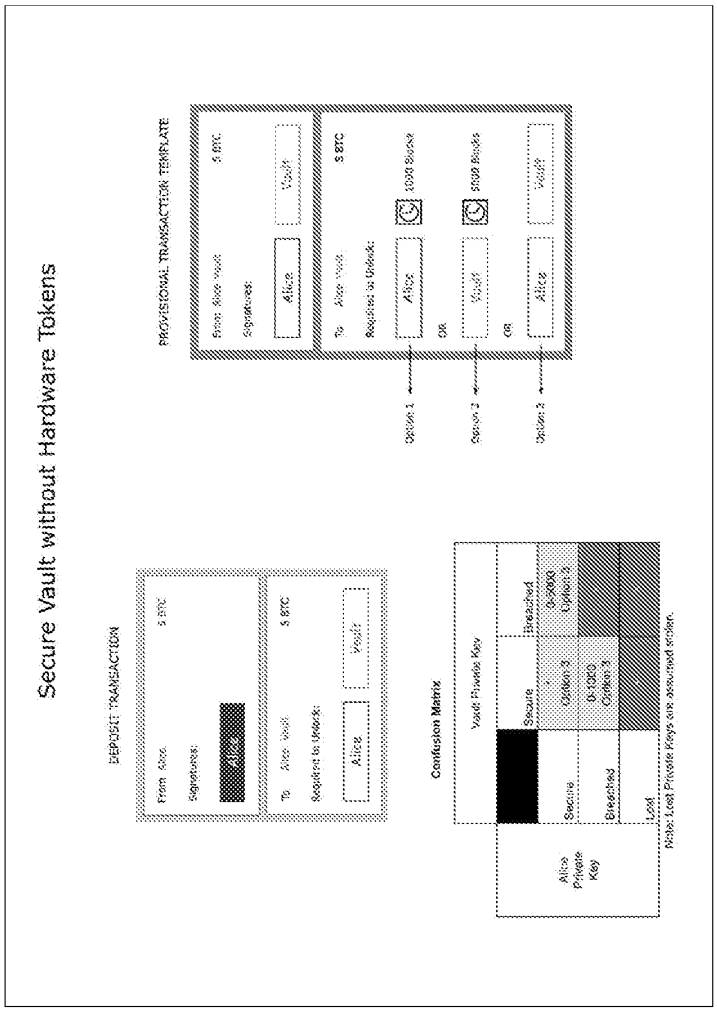

1500
ALICE HARDWARE TOKEN
Alice Key
SECURE
Alice Private Key
Vault Private Key
Secure
Breached
Option 8/9
Option 3/4
0-5000
0-2500
1500-5000
1500-2500
Lost
VAULT HARDWARE TOKEN
Vault Private Key
Secure
Breached
0-2000
0-500
Option 8
Option 9
Option 6
Note: When a Key is lost, it is assumed as breached. When a Hardware Token is lost, it is assumed malfunctioning, lost or stolen.
Note: Dotted blocks indicate situations where recovery is possible within the mentioned window period in blocks of the blockchain. Mesh blocks indicate situations where remedial steps might fail to recover Alice's funds. Oblique Line Blocks indicate situations where neither Alice+Vault nor the adversaries have an advantage over one another in claiming Alice's funds.
Note: Options as depicted in Provisional Transaction Template in Figure 2.

FIG. 15


Secure Vault without Hardware Tokens
DEPOSIT TRANSACTION
From Alice 5 BTC
Signatures:
Alice
To Alice Vault 5 BTC
Required to Unlock:
Alice
Vault
PROVISIONAL TRANSACTION TEMPLATE
From Alice Vault 5 BTC
Signatures:
Alice
Vault
To Alice Vault 5 BTC
Required to Unlock:
Alice
1008 Blocks
OR
Vault
5008 Blocks
OR
Alice
Vault
Option 1
Option 2
Option 3
Confusion Matrix
Vault Private Key
Secure
Breached
Alice Private Key
Secure
Option 3
8,000 Option 3
Breached
8,000 Option 3
Lost
Note: Lost Private Keys are assumed stolen.

1600

FIG. 16