CRYPTOCURRENCY TRANSACTIONAL SYSTEMS AND METHODS

BACKGROUND OF THE INVENTION

[0001] The proliferation of mobile devices with Internet capabilities (e.g., mobile phones, wearable devices) has made it increasingly easy for users to conduct electronic commerce and online purchases using merchant websites and mobile applications. This has also led to an increased shift away from paper-based monetary schemes (e.g., the exchange of physical or paper currency) to instead rely upon electronic systems for monetary exchange. Many electronic payment systems have been developed for exchanging money, including the use of electronic wallets and electronic funds transfer (EFT). EFT includes a direct debiting/crediting of a user's bank account at the instance of the user from a remote location.

[0002] In the context of gaming, such as casino gaming, ticketing systems and chips have replaced the use of physical currency for wagering purposes. Casino customers are not permitted to directly use credit cards and debit cards for gaming, such as by inserting credit cards in gaming machines, but rather trade money for credits or chips, either at a gaming table or at a gaming machine for example, which can then be redeemed as paper currency after play is completed.

[0003] Another type of electronic system for monetary exchange is commonly referred to as an electronic peer-to-peer payment system or digital currency system. Bitcoin is one example of a digital currency system that utilizes cryptographic techniques, and thus the digital currency is referred to as cryptocurrency. Although there are many such cryptocurrencies, Bitcoin (BTC) is one of the most well-known and thus will be discussed herein with reference to Bitcoin as encompassing other cryptocurrencies, as many other cryptocurrencies share similar features or derive from the same code base, such as Bitcoin Cash (BCH) and Bitcoin SV (BSV). Payments made using the Bitcoin system are recorded in a ledger (the "Block Chain", which is maintained in parallel by many different entities in the system) using its own unique monetary unit, which is also called a "bitcoin." The Bitcoin system has no central repository and no single administrator, and thus is viewed as a decentralized virtual currency.

[0004] One drawback of systems such as Bitcoin is that fraudsters and criminals may be able to rely upon the generally anonymous nature of the Bitcoin system to avoid detection. Thus, while a person engaging in transactions involving traditional payment forms, such as credit cards and US

dollars is normally identifiable, bitcoins are anonymous and do not typically require any identification (other than a randomly generated key address) of the party currently owning such bitcoins.

[0005] Thus, there is a need for new and enhanced cryptocurrency payment systems and methods to create a digital currency system that has greater efficiency and more security.

SUMMARY OF THE INVENTION

[0006] The invention addresses and resolves the aforementioned issues, among other things.

[0007] Some embodiments of the invention are directed to a method and system for enabling secure cryptocurrency transfers in transactions involving an electronic gaming machine and a user cryptocurrency wallet or "cryptowallet", the system comprising: a) memory configured to store an amount of credit, the credit being usable to actuate play of a game on the electronic gaming machine; b) a server in communication with the electronic gaming machine and a blockchain memory pool, the server being configured to detect a cryptocurrency transaction, the cryptocurrency transaction being defined by a transaction data communicated by the user cryptocurrency wallet to a blockchain memory pool, the transaction data comprising an amount of a cryptocurrency involved in the cryptocurrency transaction and a user public key, wherein responsive to detecting the transaction data, the server being further configured to communicate with the electronic gaming machine whereby an amount of credit is added to the credit stored in the memory, the amount of credit corresponding to the amount of cryptocurrency involved in the cryptocurrency transaction.

[0008] In some embodiments, the transaction data further comprises a unique identification associated with the electronic gaming machine, the server being further configured to communicate with the electronic gaming machine associated with the unique identification.

[0009] In some embodiments, the memory resides or is installed in the electronic gaming machine.

[0010] In some embodiments, the server is further configured to compare the user public key included in the transaction data with a user cryptocurrency wallet public key associated by the server with the electronic gaming machine, the amount of credit being added to the credit stored in the memory responsive to the user public key matching the user cryptocurrency wallet public key.

[0011] In some embodiments, the user and/or user cryptocurrency wallet public key is associated by the server with the electronic gaming machine responsive to a user interaction with the electronic gaming machine. The server may be further configured to receive the user cryptocurrency wallet public key and an identification of the electronic gaming machine responsive to the user interaction.

[0012] In some embodiments, the user interaction comprises communicating the user cryptocurrency wallet public key to the server. The user cryptocurrency wallet public key may comprise a user loyalty club membership identification. In some embodiments, the user interaction comprises communicating an identification of the electronic gaming machine to the server. The user interaction with the electronic gaming machine may be from a variety of sources such as a user device, wallet, input device on the gaming machine or software application. In some embodiments, the user interaction comprises communicating an identification of the electronic gaming machine to the server.

[0013] In some embodiments, the transaction data further comprises an input identification associated with the cryptocurrency involved in the cryptocurrency transaction and an output identification associated with the cryptocurrency, the server being further configured to use the output identification associated with the cryptocurrency as a subsequent input identification in a subsequent cryptocurrency transaction involving the cryptocurrency.

[0014] In some embodiments, the server is further configured to generate a subsequent cryptocurrency transaction responsive to a withdrawal request received from the user cryptocurrency wallet, the withdrawal request comprising instructions to deduct a withdrawn amount of credit from the memory and return the withdrawn amount of credit to the user cryptocurrency wallet in the form of cryptocurrency, the server communicating with the electronic gaming machine to cause the withdrawn amount of credit to be deducted from the credit stored in the memory, the subsequent cryptocurrency transaction being defined by a subsequent transaction data comprising a return amount of a cryptocurrency and a user cryptocurrency wallet public key associated with the user cryptocurrency wallet, wherein the return amount of cryptocurrency corresponds to the withdrawn amount of credit.

[0015] Some embodiments of the invention are directed to methods and systems for enabling secure cryptocurrency transfers involving an electronic gaming machine and a user cryptocurrency wallet, comprising: a) memory configured to store an amount of credit, the credit being usable to

actuate play of a game on the electronic gaming machine; b) a server in communication with the electronic gaming machine and a blockchain memory pool, the server being configured to detect a cryptocurrency transaction, the cryptocurrency transaction being defined by a transaction data communicated by the user cryptocurrency wallet to a blockchain memory pool, the transaction data comprising an amount of a cryptocurrency involved in the cryptocurrency transaction and a user public key, wherein responsive to detecting the transaction data, the server being further configured to compare the user public key included in the transaction data with a user cryptocurrency wallet public key associated by the server with the electronic gaming machine, and communicate a signal to the electronic gaming machine to add an amount of credit to the credit stored in the memory responsive to the user public key matching the user cryptocurrency wallet public key, wherein the amount of credit corresponding to the amount of cryptocurrency involved in the cryptocurrency transaction.

[0016] The cryptocurrency transaction may be cryptographically signed by the cryptocurrency wallet or cryptographic key pair.

[0017] In some embodiments, the transaction data further comprises an input identification associated with the cryptocurrency involved in the cryptocurrency transaction and an output identification associated with the cryptocurrency.

[0018] In some embodiments, the server is further configured to use the output identification associated with the cryptocurrency as a subsequent input identification in a subsequent cryptocurrency transaction involving the cryptocurrency.

[0019] In some embodiments, the systems and methods of the invention further comprise the server actuating a subsequent cryptocurrency transaction responsive to a withdrawal request received from the user cryptocurrency wallet, the server being configured to communicate a signal to the electronic gaming machine to deduct an amount of credit from the credit stored in the memory and add the amount of credit to the user cryptocurrency wallet associated with the user cryptocurrency wallet public key, wherein the amount of credit corresponds to the amount of cryptocurrency involved in the transaction data defining the subsequent cryptocurrency transaction. In some embodiments, the withdrawal request is received from the user cryptocurrency wallet.

[0020] Some embodiments of the invention are directed to a method and system for enabling secure cryptocurrency transfers in transactions involving gaming devices, comprising: an

electronic gaming machine, the electronic gaming machine including a memory configured to store an amount of credit, the credit being usable to actuate play of a game on the electronic gaming machine; a casino backend server in communication with a database and the electronic gaming machine, the database storing user data including a user cryptocurrency wallet public key; and a user device configured to actuate a cryptocurrency transaction, the cryptocurrency transaction being defined by transaction data communicated to a blockchain, the transaction data including an amount of a cryptocurrency involved in the cryptocurrency transaction and a user public key, wherein the casino backend server is configured to detect the transaction data communicated to the blockchain, and responsive to the user cryptocurrency wallet public key matching the user public key included in the transaction data, communicate a signal to the electronic gaming machine, the signal causing the addition of an amount of credit to the credit stored in the memory, the amount of credit corresponding to the amount of cryptocurrency involved in the cryptocurrency transaction.

[0021] In some embodiments, the transaction data further comprises an input identification associated with a source of the cryptocurrency involved in the cryptocurrency transaction and an output identification associated with the cryptocurrency transaction. The casino backend server may be further configured to use the output identification associated with the cryptocurrency as a subsequent input identification in a subsequent cryptocurrency transaction involving the cryptocurrency.

[0022] In some embodiments, the casino backend server actuates a subsequent cryptocurrency transaction responsive to a withdrawal request received from the user device, the withdrawal request comprising instructions to deduct a withdrawn amount of credit from the memory and return the withdrawn amount of credit to the user cryptocurrency wallet in the form of cryptocurrency, wherein the casino backend server communicates a signal to the electronic gaming machine to deduct the withdrawn amount of credit from the credit stored in the memory and generates a subsequent cryptocurrency transaction defined by a subsequent transaction data comprising a return amount of a cryptocurrency and the user cryptocurrency wallet public key, wherein the return amount of cryptocurrency corresponds to the withdrawn amount of credit.

[0023] In some embodiments, the casino backend server associates the user device with the electronic gaming machine. The association may involve the user device or an application, such as a cryptocurrency wallet, connecting with the electronic gaming machine, such as by Bluetooth

connection. The connection may be used to inform the casino backend server of the electronic gaming machine to be associated with the user having the user public key and user cryptocurrency wallet public key, and may further instruct the casino backend server to communicate the signal to such associated electronic gaming machine.

[0024] In some embodiments, the transaction data further comprises a unique identification of the electronic gaming machine. The user device may be further configured to communicate the unique identification to the casino backend server. The user cryptocurrency wallet public key may thereafter be associated by the casino backend server with the electronic gaming machine responsive to the casino backend server receiving the unique identification.

[0025] Some embodiments of the invention are directed to a method for enabling secure cryptocurrency transfers in transactions involving an electronic gaming machine, the electronic gaming machine including a memory configured to store an amount of credit, the credit being usable to actuate play of a game on the electronic gaming machine, wherein the electronic gaming machine, the method comprising the steps of: actuating a cryptocurrency transaction through a user device, the cryptocurrency transaction being defined by transaction data communicated to a blockchain, the transaction data including an amount of a cryptocurrency involved in the cryptocurrency transaction and a user public key; a casino backend server detecting the transaction data communicated to the blockchain, the casino backend server being in communication with a database and the electronic gaming machine, the database storing user data including a user cryptocurrency wallet public key; and responsive to the user cryptocurrency wallet public key matching the user public key included in the transaction data, the casino backend server communicating a signal to the electronic gaming machine, the signal causing an amount of credit to be added to the credit stored in the memory, the amount of credit corresponding to the amount of cryptocurrency involved in the cryptocurrency transaction.

[0026] In some embodiments, the method further comprises the step of the user device communicating with the electronic gaming machine, whereby the casino backend server associates with the user device with the electronic gaming machine. In some embodiments, the transaction data includes an identification of the electronic gaming machine, whereby the casino backend server associates the user or user cryptocurrency wallet public key with the identified electronic gaming machine.

[0027] Some embodiments of the invention are directed to a method for enabling and confirming transfers of cryptocurrency from player wallets to gaming wallets for use in a gaming application, the transfer of cryptocurrency being transmitted over a global communication network and temporarily stored in a memory pool prior to being recorded in a block on a blockchain, the gaming application being in communication with the memory pool, the method comprising the steps of: a) transmitting a first transaction to the memory pool, the first transaction executing the transfer of cryptocurrency from the player wallet to the gaming wallet, the first transaction including wager data relating to a wager to be placed in the gaming application, wherein the first transaction is stored in the memory pool in association with one or more first transaction input identifiers and a first transaction output identifier; and b) executing a second transaction involving a determination by the gaming application of a wager outcome, the second transaction being stored in the memory pool in association with one or more second transaction input identifiers and a second transaction output identifier, wherein the first transaction output identifier is the same as at least one of the one or more second transaction input identifiers.

DESCRIPTION OF THE DRAWINGS

[0028] Figure 1A and 1B provide flow charts illustrating player bet transactions, wherein a player sends a fraudulent transaction;

[0029] Figure 2 is a printout showing an exemplary BSV transaction; and

[0030] Figure 3 provides a high level flow chart illustrating movement of funds.

DETAILED DESCRIPTION OF THE INVENTION

[0031] All references to documents contained herein, including any links, incorporates those documents in this application by reference as if copied herein.

[0032] For purposes of this description, the term "digital currency" may refer to units of value that may be used as a form of payment for transactions, including financial transactions involving gaming operations, such as transferring digital currency electronically to an electronic gaming machine, mobile device, kiosk, gaming device, gaming terminal, fixed odds terminal, lottery machine, table game, gaming system, online or standalone computerized gaming platform or electromechanical gaming device (collectively referred to as an "EGM" or "electronic gaming machine" herein), applying the digital currency to a player account created in memory on the

electronic gaming machine in the form of credits for game play, initiating a game on the electronic gaming machine involving one or more wagers of credits, wherein the outcome of the game results in a loss of the wagered credits or a win in which an amount of credits are added to the credits in a player account.

[0033] Digital currency may be a currency that is electronically generated by and stored within one or more devices, such as a user device such as a computing device, mobile device or smartphone, a casino or central management system, or an electronic gaming machine. Digital currency may be purchased using conventional forms of currency (e.g., fiat currency) and generated with a specific value. Typically, the digital currency may not have a physical form of tender but may be accessible through a device such as those mentioned above using a software application such as a digital wallet or mobile application.

[0034] The term "cryptocurrency transactional system" may refer to one or more server computers that function to operate and maintain a cryptocurrency system. The cryptocurrency transactional system may function to facilitate the generation/issuance and distribution of digital currency between the one or more server computers within the cryptocurrency transactional system. The cryptocurrency transactional system may also function to enable the performance of transactions between the server computers for the transfer or wagers, credits, goods/services and/or the transfer of funds, for example, between a user's mobile device and an electronic gaming machine.

[0035] The term "node" may refer to a computing device within a cryptocurrency system. A node in a cryptocurrency system may be associated with and/or operated by a server computer of an operator or casino, or other provider. Each node may have particular rights and restrictions associated with the node. For example, an issuer node may have the right to generate and issue digital currency within a cryptocurrency payment network, while a distributor node may have the right to distribute digital currency, but not generate or issue digital currency. Other nodes in the cryptocurrency transactional system, such as operators, merchants and users (e.g., consumers or players), may have the right to transfer digital currency. In other embodiments, nodes may be permissionless and/or operated by others.

[0036] A blockchain is a type of distributed ledger technology (DLT) that consists of growing list of records, called *blocks*, that are securely linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree, where data nodes are represented by leaves). The timestamp proves

that the transaction data existed when the block was created. Since each block contains information about the previous block, they effectively form a chain (compare linked list data structure), with each additional block linking to the ones before it. Consequently, blockchain transactions are irreversible in that, once they are recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks. Blockchains are typically managed by a peer-to-peer (P2P) computer network for use as a public distributed ledger, where nodes collectively adhere to a consensus algorithm protocol to add and validate new transaction blocks.

[0037] The term "key" may refer to a piece of data or information used for an algorithm. A key may be a unique piece of data and is typically part of a key pair where a first key (*e.g.*, a public key) may be used to encrypt a message, while a second key (*e.g.*, a private key) may be used to decrypt that encrypted message. The key may be a numeric or alphanumeric value and may be generated using an algorithm. A system server computer in a cryptocurrency transactional system of the invention may generate and assign a unique key pair for each node in the system. In some embodiments, a key may refer to either a node verification key pair or a transaction key pair.

[0038] A transaction key pair may include a transaction public key and a transaction private key. The transaction key pair may be used by the nodes and/or payment entities to conduct transactions in the cryptocurrency transactional system. The transaction key pair may be generated by a system server computer or may be generated by an operator server computer for a customer or player when a player account with the operator server computer is created. Individual participants or players can also generate their own key pairs for the system. In this embodiment, the individual participant would keep their private key a secret and keep it from being revealed to others. The transaction public key of a node may be distributed throughout the system in order to allow for authentication of payment transaction messages signed using the private key of the node.

[0039] A node verification key pair may include a node verification public key and a node verification private key. The node verification key pair may be used by the nodes and the system of the invention to verify that a node is an issuer node or a distributor node. The node verification key pair may be generated by a system server computer in response to a request message from a node to be designated an issuer node or a distributor node in the system. In other embodiments, the node verification key pair may be generated by a node (e.g., an operator server computer) and sent to the system server computer. In some embodiments, a node verification public key may be functionally similar to a transaction public key. However, the node verification public key may

only be distributed to the node associated with the node verification public key. In such embodiments, the node verification public key may be encrypted prior to being sent to the appropriate node.

[0040] Embodiments of the invention may utilize one or more system server computers to determine and designate issuer nodes, which have the right to generate and issue digital currency, and distributor nodes, which have the right to distribute digital currency but not issue digital currency. Transactions performed through the cryptocurrency transactional system using the digital currency can be tracked and maintained in a ledger of transactions maintained by the issuer nodes and the distributor nodes. A cryptocurrency wallet in some embodiments may comprise a device, program or service configured to store cryptocurrency, and public and private keys used in transactions involving cryptocurrency, as well as provide other functionality, such as encrypting and signing information.

[0041] Embodiments of the cryptocurrency transactional system of the invention are directed to various general and specific enhancements and improved security features such as those discussed herein. For example, a feature can be implemented to prevent "double spend" on a blockchain.

Feature 1 - Preventing Double Spend on a Blockchain

Background And Definition of a Blockchain Transaction and Inputs and Outputs

[0042] A transaction of cryptocurrency, such as in the Bitcoin network as an example, describes the transfer of a specific amount of digital currency from one account to another. Transactions are represented as signed data structures that are broadcast into the blockchain and recorded by all nodes in the network. It is comprised of references to one or more previous transactions that funded the spending party and an assignment of a specific amount of digital currency to one or more addresses. A transaction is atomic in the sense that this digital currency from the previous transactions is inseparably linked to the transfer of this digital currency to the receiving account.

[0043] In a blockchain that supports the UTXO model, such as Bitcoin, a transaction consists of inputs and outputs. The references to previous transactions are referred to as inputs to the transaction, whereas the account and the amount of digital currency that it ought to receive are called outputs. After the transfer, the owner of the receiving account has new funds at her disposal to spend in future transactions. The balance of an account is the sum of the values of all unspent outputs owned by that account.

[0044] Other blockchains that are EVM (Ethereum virtual machine) compatible use an account-based model which represents assets as balances within accounts. Deploying a smart contract leads to the creation of a code-controlled account. Smart contracts can hold funds themselves, which they can redistribute according to the conditions defined in the contract logic. Every account in EVM compatible blockchain has a balance, storage, and code-space for calling other accounts or addresses.

Double Spending with a Cryptocurrency

[0045] Double spending is the risk that a digital currency can be spent twice. Double-spending is a potential problem unique to digital currencies because digital information can be reproduced relatively easily. Physical currencies do not have this issue because they cannot be easily replicated, and the parties involved in a transaction can immediately verify the bona fides of the physical currency. With digital currency, there is a risk that the holder could make a copy of the digital token and send it to a merchant or another party while retaining the original.

[0046] More specifically, double spending a cryptocurrency is accomplished by creating two transactions and broadcasting those two transactions to different nodes on the network at the same time. Both transactions have exactly the same inputs but the transactions have separate outputs. The output of the first transaction typically sends the crypto to a wallet owned by the double spender. The second transaction output typically sends the output to the party the double spender wishes to fool. The double spender is hoping that the receiving party he wishes to fool sees the transaction as valid and the double spender receives something back of value before the miners notify the targeted party the transaction was invalid.

Standard Protection Against Double Spending

[0047] Bitcoin has a mechanism that verifies all of the transactions going into a block to verify that the same digital token isn't being spent in other transactions. More specifically, each transaction input is checked against the entire blockchain to ensure that the same input has **NOT** already been used in a different transaction. Bitcoin therefore only guarantees confirmation of a transaction once it has been accepted by the majority of participating nodes and hashed into the blockchain.

[0048] Even after the transaction has been in 1 block there is a chance that a transaction containing the fraudulent double spend could be propagating around more of the blockchain nodes than the initial transaction (for example the one sent to a merchant), so it is common for a merchant to wait

for 4-6 blocks to be mined before trusting a payment, to verify that the transaction sent to their crypto wallet is valid and trusted. This can mean waiting for upwards of 1 hour before trusting the payment.

Prior Solutions

[0049] Three whitepapers for solutions to the double spending problem incorporated herein by reference include:

"Have a Snack, Pay with Bitcoins"

Summary: the proposal does not fully prevent a double spend. It requires that a merchant's software connect to a large random sample of nodes in the Bitcoin network and follow other specific rules to make it harder for the attacker to successfully submit their fraudulent transaction and have it trump the valid transaction being used to pay the merchant;

"Countering Double-Spend Attacks on Bitcoin Fast-Pay Transactions"

Summary: requires additional server software called "enhanced observers" to be running and to send alerts to the mining nodes. Requires updated blockchain node software that the miners must agree to run to react to these alerts; and

"Double-spending Prevention for Bitcoin zero-confirmation transactions"

Summary: requires changes to the Bitcoin protocol which would require all of the miners of that blockchain to agree to the change to update their blockchain node software

Drawbacks with Existing Solutions

[0050] The "out of the box" solution for most blockchains as mentioned above in the "Standard Protection Against Double Spending" section requires waiting for multiple transactions to be mined into a block. On average it takes a block 10 minutes to be mined, though the variance can be very high, ranging from ~1 second to 2 hours.

[0051] The inventors mentioned drawbacks for each of the whitepaper solutions in the above section. There are likely several other double spend solutions out there that I haven't found. Most of the solutions that we have seen discussed on the internet require waiting for some period of time before considering a transaction as being valid (however these solutions do not required waiting for a transaction to get mined into a block). The solutions require waiting for the transaction to propagate around to multiple Bitcoin nodes in the mempool, which is essentially an in-memory list of transactions waiting to be put into blocks. The longer that you wait, the more secure a

transaction is because it is being propagated to other nodes globally, and each mining node will ignore a transaction if it detects that the same input is being used for some other transaction.

[0052] Note: when you see reference to "zero confirmations" that means being able to consider a transaction valid once it reaches the Bitcoin nodes mempool, before the time it takes to actually mine it into a block.

Further Definition of the Bitcoin Mempool

[0053] Transactions are broadcast to nodes on the Bitcoin network. The transaction typically reaches the node that is closest to the sender and is included in a list of unconfirmed transactions called the mempool. Miners have the ability to include transactions in new blocks they are mining or to leave these transactions in the mempool. Typically transactions with higher included fees will be included first. Transactions with very low included fees can persist in the mempool and may not be processed for days or weeks. There are multiple ways that a transaction leaves the mempool on a Bitcoin node:

1. The transaction was included in a block

2. The transaction or one of its unconfirmed ancestors conflicts with a transaction that was included in a block

3. The transaction was replaced by a newer version (this is the "replace by fee" feature is only relevant to BTC)

4. The transaction expired by timeout

Exemplary Solutions Provided by the Invention

[0054] Embodiments of the invention provide a solution that guarantees the prevention of a double spend instantaneously. The exemplary embodiments discussed herein involve the placement of a bet in gaming, but that is just one application of the invention.

[0055] Referring to Figure 1A, which shows the various transactions that are involved in the gaming use case to place a bet, process the bet, and return the bet results and any winnings back to the player.

[0056] Transaction #1 is the player submitting a bet. Note that input 7282 for 0.5 BSV is combined with another input 8912, also for 0.5 BSV. These inputs originate from 2 unspent outputs from prior transactions that the player's wallet has received. These two inputs total 1 BSV, which is the amount that the player wants to bet. The two inputs are combined into a new single output 5555

to send to the blockchain. This new output also contains the data for what specific bet the player is making. The two inputs are noted, at least because the blockchain is a simple ledger without the power or logic to compute values. Hence there is no way the chain itself can add input 7282 (0.5 BSV) and input 8912 (0.5 BSV) together. The sender has to include both input balances in a transaction to create output 5555 (1.0 BSV).

[0057] The Game Server sees this bet transaction show up in the blockchain mempool and immediately processes it and determines if the player has won or lost the bet. This transaction uses the players bet output 5555 as a new input to send the player the bet results and payout (if the player won the bet). There may be other inputs included, especially if the player has won, since the player will get payouts in excess of whatever amount was bet. The player wallet and gaming app then sees this new blockchain transaction and shows the win or loss results in the game.

[0058] Transaction #3 is the player's fraudulent transaction during their double spend attack. The player is attempting to place a bet (and win) with the casino and at the same time is also sending that same 1 BSV cryptocurrency back to themselves, for example to another wallet address that they own. It should be noted that the player is trying to use the same inputs 7282 and 8912 to send a total of 1 BSV.

[0059] The blockchain nodes are eventually going to determine that either Transaction 1 or Transaction 3 is valid, but not both, since both transactions are using the same inputs. Exemplary unique features of the invention include using the players bet output (5555) as input when responding back to the player. This ensures that if the player were to attempt a double spend to send himself back the same crypto used to place the bet (*i.e.*, reusing inputs 7282 and 8912), and the fraudulent transaction (#4) were to be the one accepted by the blockchain, then the bet transaction would not be accepted by the miners.

[0060] This is because the miners would analyze the transaction's chain of outputs back to their associated inputs, back to their associated outputs, and so on, all the way back as far as that chain goes. It would be determined that one or more of the inputs were already used in another transaction. The miners would then drop the transaction from the mempool.

[0061] Subsequently the bet result transaction would also be seen as an invalid transaction and ignored by the miners. The player would not receive any payout. This prevents a double spend attack from being beneficial to the attacker/player and avoids any loss of revenue by the casino.

Other Uses Cases Other Than Placing a Bet

Buying a token with the blockchain's native currency.

[0062] For example, in other embodiments custom token protocols are used as a way to create tokens on the a blockchain. Tokens are similar to a casino chip in gaming. We can pin a token to a fiat currency to protect the casino from native cryptocurrency fluctuation, like the price in USD rising and falling for 1 BSV.

[0063] The Double Spend feature of the invention protects us for this use case in the same way as placing a bet. Assume that a user tries to purchase tokens from us or one of our casino partners and they attempt to double spend the BSV they send us and the fraudulent transaction is the one accepted by the Bitcoin network. For that case the tokens that they received from us will become invalid as soon as the miners invalidate the transaction that the user created to purchase our tokens. The transaction will be invalid because the player's output is used as an input in the transaction to send the user the tokens. The transaction will be invalid because the player's output is used as an input in the transaction to send the user tokens as shown in Figure 1B. The output of BSV to the player is 0.000001 BSV. It should be understood that this is an example, as the exact amount can be any negligible amount (that is, what is referred to as a "dust" transaction, which is so small to not matter financially but sufficient for miners to detect an issue).

Exemplary use case - BSV

[0064] BTC has a "replace by fee" feature (RBF) that allows an unconfirmed transaction to be replaced with another transaction that has a higher fee, and miners will prioritize transactions that have higher fees. Transactions can be marked as non-RBF, but then there's also the risk of transactions not being confirmed for days or weeks.

[0065] All three forks (BTC, BSV, BCH) also have the drawback in that there is a maximum of 25 (or 50, just for BSV) chained unconfirmed transactions. There is a plan to remove this limit in BSV; we're not sure about BCH or BTC. Until this restriction is removed for a particular blockchain, at times we may not be able to use our solution on that blockchain (set the players bet output transaction as an input to the bet response transaction) because it's already been chained too many times. It should be understood that twenty-five bets equals fifty transactions because if a bet involves a response from the casino.

[0066] The player could attempt the double spend after he receives a loss response in an attempt to undo the bet. However since this requires the bet to propagate through the network sufficiently for the game server to have received it and for the response to also have been sufficiently

propagated for the player to have seen it, it should be too late to successfully submit the double spend transaction.

BSV Transaction Example

[0067] The following real BSV transaction is a good visual on how inputs and outputs are used for sending someone crypto. See Figure 2 for example.

[0068] The wallet sending crypto only has a large input of 72.34 BSV to use to send someone 0.162836 BSV. The large input is used, and the specific amount being sent to the other party is the first output, and the second output is the change that gets returned back to the sender's wallet.

[0069] Another feature of the system of the invention relates to paying Blockchain transaction fees as discussed below.

Feature #2: Paying Blockchain Transaction Fees on Behalf of the Player

[0070] Embodiments of the invention can be configured to pay the BSV mining fees for the players gambling on using the transactional system.

[0071] An exemplary method of performing such an embodiment may generally comprise the following steps:

1. The player requests for and receives an output from a service sufficient to pay for the transaction;
2. The player adds his own outputs to create a transaction. The player signs the transaction with his private key and sends it back to the service; and
3. The service adds a signature for the original output with its private key to form a complete transaction and the service then transmits the transaction to the blockchain.

[0072] Another feature of the system of the invention relates to including bet data in a public blockchain transaction as discussed below.

[0073] The system will include game servers, for example a Baccarat game server that will monitor for new transactions being added to the blockchain. It will recognize transactions that are being sent to the game server's address and that there is bet data within the transaction. The game server will read the bet data and then produce RNG and determine if the bet is won or lost. It will then create a new transaction with bet results and any payout for the user and submit to the blockchain. The bet data will be thus added to a public blockchain.

[0074] Another feature of the system of the invention relates to connecting a crypto wallet to a player loyalty account as discussed herein and as depicted in Figure 3. While the invention is

discussed in connection gaming machines, it should be understood that the invention includes systems and methods for routing cryptocurrency in transactions at other platforms, including tables games, kiosks and terminals. For example, a device may be installed at a table game wherein the device receives cryptocurrency which is then converted to gaming chips. A dealer or casino staff may print a receipt of the transaction which can be used for accounting and reconciliation purposes, that is, the receipt shows the table as having received an amount in cryptocurrency in the same way fiat currency is collected. It should be understood that receiving currency, whether expressed as dollars, credit or cryptocurrency as used herein, may be interchanged, in that a transaction may be completed with an offsite wallet and notification of the transaction may be transmitted to an EGM or another communication device associated with a management system that is configured to effectuate the addition of credits to the EGM pursuant to the completed transaction. Thus, no cryptocurrency is ever transmitted to the EGM. The term receiving may therefore refer to the completion of a transaction involving a receiving party, rather than any particular device which houses or stores a wallet. For example, receiving cryptocurrency includes receiving cryptocurrency at a cryptocurrency wallet at the EGM or receiving notification of a cryptocurrency transaction being executed with a cryptocurrency wallet residing at a different location or different device or system which then results in credit for play of the EGM being added to the EGM.

[0075] In a separate embodiment the player sends the cryptocurrency to a casino wallet that is not located in or on the EGM. The cryptocurrency wallet involved in the transaction which receives the cryptocurrency may reside in a specially configured computer system inside or outside of a casino. The EGM may either monitor for transactions (such as by identifying a player or the player identifying the EGM) or otherwise be notified of a successful cryptocurrency transaction that was sent to the casino wallet, wherever the location, and add a corresponding amount of credit provided that the owner of the cryptocurrency who initiated the transactions has satisfied any identification requirements.

[0076] A player can connect the cryptocurrency wallet of the invention to their casino player loyalty account and then send and remove credits from an EGM. Although there may be other transactions a casino player may be involved in, the exemplary method described below is directed to cryptocurrency transactions that result in credits being sent, added and/or removed from an EGM.

[0077] Exemplary Solution:

1. Player downloads our crypto wallet to phone. Wallet is typical crypto type that uses public key encryption. The Player generates a public/private key pair.
2. Player associates the public key of their crypto wallet with their unique player loyalty ID in the operator or solution provider mobile app. The Casino could also make this association using their software. In either case the end result is that there is an association of player loyalty ID and player cryptocurrency wallet public key in the casino's backend database.
3. Player inserts loyalty card into EGM and the EGM ID is then associated to the player loyalty ID (and player public key) in the backend database. The EGM could also have a QR or barcode scanner that would scan a player's wallet's public key. The key could be represented with a QR code or barcode displayed on a mobile device, or alternatively, Bluetooth, NFC or facial recognition could be used.
4. Casino backend notifies the player wallet which EGM the player is located at
5. Player opens mobile app and is able to select deposit or withdraw from within the app
6. This player to EGM association or mapping may be stored on a server or blockchain.

[0078] Exemplary Deposit to EGM Method:

1. Player chooses the amount of credits they'd like to deposit in the app and clicks the send button
2. At this point the wallet creates a transaction and digitally signs it with the private key. The recipient of the transaction is the casino that owns the EGM.
3. Transaction is broadcast to the blockchain and casino wallet receives the credits
4. Note that the transaction includes the public key of the sender. The casino therefore matches the sender's public key to the player loyalty ID.
5. The casino backend identifies the EGM that the player is located at by looking up the EGM ID from the public key value of the player's wallet or the player's loyalty ID that made the deposit request.
6. Casino backend send amount of credits received to that particular EGM that the player is sitting at (for example via a SAS protocol network call)
7. The balance is updated on the EGM

[0079] Exemplary Withdraw from EGM Method:

1. Player uses the mobile app and chooses the amount of credits to cash out of the EGM that they are currently playing at. It can be all or just a portion of the current credits balance at the EGM, meaning that the player could leave some credits on the EGM and cash those credits out with a ticket if so desired. In some embodiments, the player can use the EGM or other communication means to send a message to the casino service to request a withdrawal transaction.

2. Player wallet creates and signs a transaction to request an amount of credits to withdraw. This transaction is a dust transaction with the minimum amount of cryptocurrency needed to have the blockchain accept the transaction. That transaction is broadcast to the blockchain. A service running with the casino datacenter is watching the blockchain. It then identifies the command sent to its public key. The blockchain is used as a messaging bus to send commands to other components in the system. In a separate embodiment, the player wallet can send a message to the casino service using standard communication protocols to request a withdrawal transaction from a particular EGM without the use of a message sent over a blockchain.
3. After receiving the withdrawal request, the casino service identifies the EGM that the player is located at by looking up the EGM ID from the public key value of the wallet that made the withdraw request.
4. The casino service then communicates or "calls" the software of the invention running on the EGM that the player is located at to invoke the withdraw action (for example via a SAS protocol network call)
5. The casino service creates and signs a transaction to send credits from the casino hot wallet to the player's wallet. This transaction is sent to the blockchain.
6. Player receives credits on the mobile wallet, removes player card and may walk away as the transaction is completed.

[0080] In some embodiments, the casino backend or central management system is actively maintaining a mapping of each loyalty card and the EGM that the loyalty card is inserted into.

[0081] In some embodiments, the invention replaces the player loyalty card with a cryptocurrency wallet public key as the player ID. In some embodiments, an additional piece of hardware is installed or repurposed on the EGM to be able to securely read the public key of the customer's mobile device. For example, in some embodiments an EGM card reader is replaced with a QR/bar code scanner. The scanner is able to securely read a QR code displayed by the crypto wallet via the mobile device display to establish a link the EGM to the customer's public key of his crypto wallet. In other embodiments, the association of cryptocurrency wallet to EGM is created via one or more of a QR code on the display device of the EGM, Bluetooth beacons, entering a code or password into the EGM, or identifying the EGM in the wallet through the customer's mobile device, or through NFC tags on the EGM used to identify the EGM.

[0082] The various participants and elements described herein may operate one or more computer apparatuses to facilitate the functions described herein. Any of the elements in the figures,

including any servers or databases, may use any suitable number of subsystems to facilitate the functions described herein.

[0083] Some embodiments also relate to an apparatus for performing the operations herein. Such an apparatus may be specially constructed for the purposes, e.g., a specific computer, or it may comprise a general-purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer-readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, application specific integrated circuits (ASICs), or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus. Memory can include any of the above and/or other devices that can store information/data/programs and can be a transient or non-transient medium, where a non-transient or non-transitory medium can include memory/storage that stores information for more than a minimal duration. Furthermore, the computers referred to in the specification may include a single processor or may be architectures employing multiple processor designs for increased computing capability.

[0084] Various general-purpose systems may also be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the method steps. The structure for a variety of these systems will appear from the description herein. In addition, the embodiments are not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the embodiments as described herein, and any references herein to specific languages are provided for the purposes of enablement and best mode.

[0085] Those skilled in the art will appreciate that the types of software and hardware used are not vital to the full implementation of the methods of the invention. The order of execution or performance of the operations in the embodiments of the invention illustrated and described herein is not essential, unless otherwise specified. That is, the operations described herein may be performed in any order, unless otherwise specified, and embodiments of the invention may include additional or fewer operations than those disclosed herein. For example, it is contemplated that executing or performing a particular operation before, contemporaneously with, or after another operation is within the scope of aspects of the invention.

[0086] While exemplary systems and methods, and applications of methods of the invention, have been described herein, it should also be understood that the foregoing is only illustrative of a few particular embodiments with exemplary and/or preferred features, as well as principles of the invention, and that various modifications can be made by those skilled in the art without departing from the scope and spirit of the invention. Additional information regarding exemplary embodiments of the invention is provided below.

Computer program

[0087] In some embodiments, the methods, systems, and media disclosed herein include at least one computer program, or use of the same. A computer program includes a sequence of instructions, executable in the digital processing device's CPU, written to perform a specified task. Computer readable instructions may be implemented as program modules, such as functions, objects, Application Programming Interfaces (APIs), data structures, and the like, that perform particular tasks or implement particular abstract data types. In light of the disclosure provided herein, those of skill in the art will recognize that a computer program may be written in various versions of various languages.

[0088] The functionality of the computer readable instructions may be combined or distributed as desired in various environments. In some embodiments, a computer program comprises one sequence of instructions. In some embodiments, a computer program comprises a plurality of sequences of instructions. In some embodiments, a computer program is provided from one location. In other embodiments, a computer program is provided from a plurality of locations. In various embodiments, a computer program includes one or more software modules. In various embodiments, a computer program includes, in part or in whole, one or more web applications, one or more mobile applications, one or more standalone applications, one or more web browser plug-ins, extensions, add-ins, or add-ons, or combinations thereof.

Web application

[0089] In some embodiments, a computer program includes a web application. In light of the disclosure provided herein, those of skill in the art will recognize that a web application, in various embodiments, utilizes one or more software frameworks and one or more database systems. In some embodiments, a web application is created upon a software framework such as Microsoft® .NET or Ruby on Rails (RoR). In some embodiments, a web application utilizes one or more database systems including, by way of non-limiting examples, relational, non-relational, object

oriented, associative, and XML database systems. In further embodiments, suitable relational database systems include, by way of non-limiting examples, Microsoft® SQL Server, mySQL™, and Oracle®. Those of skill in the art will also recognize that a web application, in various embodiments, is written in one or more versions of one or more languages. A web application may be written in one or more markup languages, presentation definition languages, client-side scripting languages, server-side coding languages, database query languages, or combinations thereof. In some embodiments, a web application is written to some extent in a markup language such as Hypertext Markup Language (HTML), Extensible Hypertext Markup Language (XHTML), or eXtensible Markup Language (XML). In some embodiments, a web application is written to some extent in a presentation definition language such as Cascading Style Sheets (CSS). In some embodiments, a web application is written to some extent in a client-side scripting language such as Asynchronous Javascript and XML (AJAX), Flash® Actionscript, Javascript, or Silverlight®. In some embodiments, a web application is written to some extent in a server-side coding language such as Active Server Pages (ASP), ColdFusion®, Perl, Java™, JavaServer Pages (JSP), Hypertext Preprocessor (PHP), Python™, Ruby, Tcl, Smalltalk, WebDNA®, or Groovy. In some embodiments, a web application is written to some extent in a database query language such as Structured Query Language (SQL). In some embodiments, a web application integrates enterprise server products such as IBM® Lotus Domino®. In some embodiments, a web application includes a media player element. In various further embodiments, a media player element utilizes one or more of many suitable multimedia technologies including, by way of non-limiting examples, Adobe® Flash®, HTML 5, Apple® QuickTime®, Microsoft® Silverlight®, Java™, and Unity®.

Mobile application

[0090] In some embodiments, a computer program includes a mobile application provided to a mobile digital processing device. In some embodiments, the mobile application is provided to a mobile digital processing device at the time it is manufactured. In other embodiments, the mobile application is provided to a mobile digital processing device via the computer network described herein.

[0091] In view of the disclosure provided herein, a mobile application is created by techniques known to those of skill in the art using hardware, languages, and development environments known to the art. Those of skill in the art will recognize that mobile applications are written in

several languages. Suitable programming languages include, by way of non-limiting examples, C, C++, C#, Objective-C, Java™, Javascript, Pascal, Object Pascal, Python™, Ruby, VB.NET, WML, and XHTML/HTML with or without CSS, or combinations thereof.

[0092] Suitable mobile application development environments are available from several sources. Commercially available development environments include, by way of non-limiting examples, AirplaySDK, alcheMo, Appcelerator®, Celsius, Bedrock, Flash Lite, .NET Compact Framework, Rhomobile, and WorkLight Mobile Platform. Other development environments are available without cost including, by way of non-limiting examples, Lazarus, MobiFlex, MoSync, and Phonegap. Also, mobile device manufacturers distribute software developer kits including, by way of non-limiting examples, iPhone and iPad (iOS) SDK, Android™ SDK, BlackBerry® SDK, BREW SDK, Palm® OS SDK, Symbian SDK, webOS SDK, and Windows® Mobile SDK.

[0093] Those of skill in the art will recognize that several commercial forums are available for distribution of mobile applications including, by way of non-limiting examples, Apple® App Store, Android™ Market, BlackBerry® App World, App Store for Palm devices, App Catalog for webOS, Windows® Marketplace for Mobile, Ovi Store for Nokia® devices, Samsung® Apps, and Nintendo® DSi Shop.

Standalone application

[0094] In some embodiments, a computer program includes a standalone application, which is a program that is run as an independent computer process, not an add-on to an existing process, e.g., not a plug-in. Those of skill in the art will recognize that standalone applications are often compiled. A compiler is a computer program(s) that transforms source code written in a programming language into binary object code such as assembly language or machine code. Suitable compiled programming languages include, by way of non-limiting examples, C, C++, Objective-C, COBOL, Delphi, Eiffel, Java™, Lisp, Python™, Visual Basic, and VB .NET, or combinations thereof. Compilation is often performed, at least in part, to create an executable program. In some embodiments, a computer program includes one or more executable complied applications.

Software modules

[0095] In some embodiments, the methods, systems, and media disclosed herein include software, server, and/or database modules, or use of the same. In view of the disclosure provided herein, software modules are created by techniques known to those of skill in the art using machines,

software, and languages known to the art. The software modules disclosed herein are implemented in a multitude of ways. In various embodiments, a software module comprises a file, a section of code, a programming object, a programming structure, or combinations thereof. In further various embodiments, a software module comprises a plurality of files, a plurality of sections of code, a plurality of programming objects, a plurality of programming structures, or combinations thereof. In various embodiments, the one or more software modules comprise, by way of non-limiting examples, a web application, a mobile application, and a standalone application. In some embodiments, software modules are in one computer program or application. In other embodiments, software modules are in more than one computer program or application. In some embodiments, software modules are hosted on one machine. In other embodiments, software modules are hosted on more than one machine. In further embodiments, software modules are hosted on cloud computing platforms. In some embodiments, software modules are hosted on one or more machines in one location. In other embodiments, software modules are hosted on one or more machines in more than one location.

Databases

[0096] In some embodiments, the methods, systems, and media disclosed herein include one or more databases, or use of the same. In view of the disclosure provided herein, those of skill in the art will recognize that many databases are suitable for storage and retrieval of player and game information. In various embodiments, suitable databases include, by way of non-limiting examples, relational databases, non-relational databases, object oriented databases, object databases, entity-relationship model databases, associative databases, and XML databases. In some embodiments, a database is internet-based. In further embodiments, a database is web-based.

[0097] In still further embodiments, a database is cloud computing-based. In other embodiments, a database is based on one or more local computer storage devices.

General information relating to various embodiments of the invention

[0098] A controller, computing device, or computer, such as described herein, may include at least one or more processors or processing units and a system memory. The controller typically also includes at least some form of computer readable media. By way of example and not limitation, computer readable media may include computer storage media and communication media. Computer storage media may include volatile and nonvolatile, removable and non-removable media implemented in any method or technology that enables storage of information, such as

computer readable instructions, data structures, program modules, or other data. Communication media typically embody computer readable instructions, data structures, program modules, or other data in a modulated data signal such as a carrier wave or other transport mechanism and include any information delivery media. Those skilled in the art should be familiar with the modulated data signal, which has one or more of its characteristics set or changed in such a manner as to encode information in the signal. Combinations of any of the above are also included within the scope of computer readable media.

[0099] In some embodiments, a controller may include a processor, which as described herein, includes any programmable system including systems and microcontrollers, reduced instruction set circuits (RISC), application specific integrated circuits (ASIC), programmable logic circuits (PLC), and any other circuit or processor capable of executing the functions described herein. The above examples are exemplary only, and thus are not intended to limit in any way the definition and/or meaning of the term processor.

[00100] The order of execution or performance of the operations in the embodiments of the invention illustrated and described herein is not essential, unless otherwise specified. That is, the operations described herein may be performed in any order, unless otherwise specified, and embodiments of the invention may include additional or fewer operations than those disclosed herein. For example, it is contemplated that executing or performing a particular operation before, contemporaneously with, or after another operation is within the scope of aspects of the invention.

[00101] This written description uses examples to disclose the invention and also to enable any person skilled in the art to practice the invention, including making and using any devices or systems and performing any incorporated methods. The patentable scope of the invention is defined by the claims, and may include other examples that occur to those skilled in the art. Other aspects and features of the invention can be obtained from a study of the drawings, the disclosure, and the appended claims. The invention may be practiced otherwise than as specifically described within the scope of the appended claims. It should also be noted, that the steps and/or functions listed within the appended claims, notwithstanding the order of which steps and/or functions are listed therein, are not limited to any specific order of operation.

[00102] Those skilled in the art will readily appreciate that the systems and methods described herein may be a standalone system, gaming device, gaming machine or incorporated in an existing gaming system or machine. The gaming machine of the invention may include various

computer and network related software and hardware, such as programs, operating systems, memory storage devices, data input/output devices, data processors, servers with links to data communication systems, wireless or otherwise, and data transceiving terminals. It should also be understood that any method steps discussed herein, such as for example, steps involving the receiving or displaying of data, may further include or involve the transmission, receipt and processing of data through conventional hardware and/or software technology to effectuate the steps as described herein. Those skilled in the art will further appreciate that the precise types of software and hardware used are not vital to the full implementation of the methods of the invention so long as players and operators thereof are provided with useful access thereto, either through a mobile device, gaming platform, or other computing platform via a local network or global telecommunication network.

[00103] Although specific features of various embodiments of the invention may be shown in some drawings and not in others, this is for convenience only. In accordance with the principles of the invention, any feature of a drawing may be referenced and/or claimed in combination with any feature of any other drawing.

[00104] Those skilled in the art will readily appreciate that the apparatus described herein may include various computer and network related software and hardware, such as programs, operating systems, memory storage devices, data input/output devices, data processors, servers with links to data communication systems, wireless or otherwise, and data transceiving terminals. Those skilled in the art will further appreciate that the precise types of software and hardware used are not vital to the full implementation of the apparatus of the invention so long as it performs as described in at least one of the embodiments herein.

[00105] While exemplary apparatus, systems and methods of the invention have been described herein, it should also be understood that the foregoing is only illustrative of a few particular embodiments with exemplary and/or preferred features, as well as principles of the invention, and that various modifications can be made by those skilled in the art without departing from the scope and spirit of the invention. Therefore, the described embodiments should not be considered as limiting of the scope of the invention in any way. Accordingly, the invention embraces alternatives, modifications and variations which fall within the spirit and scope of the invention as set forth herein, in the claims and any equivalents thereto.

CLAIMS:

1. A system for enabling secure cryptocurrency transfers in transactions involving an electronic gaming machine and a user cryptocurrency wallet, the system comprising:

a) memory configured to store an amount of credit, the credit being usable to actuate play of a game on the electronic gaming machine;

b) a server in communication with the electronic gaming machine and a blockchain memory pool, the server being configured to detect a cryptocurrency transaction, the cryptocurrency transaction being defined by a transaction data communicated by the user cryptocurrency wallet to a blockchain memory pool, the transaction data comprising an amount of a cryptocurrency involved in the cryptocurrency transaction and a user public key,

wherein responsive to detecting the transaction data, the server being further configured to communicate with the electronic gaming machine whereby an amount of credit is added to the credit stored in the memory, the amount of credit corresponding to the amount of cryptocurrency involved in the cryptocurrency transaction.

2. The system as recited in claim 1, wherein the transaction data further comprises a unique identification associated with the electronic gaming machine, the server being further configured to communicate with the electronic gaming machine associated with the unique identification.

3. The system as recited in claim 1, wherein the memory resides in the electronic gaming machine.

4. The system as recited in claim 1, further comprising the server being configured to compare the user public key included in the transaction data with a user cryptocurrency wallet public key associated by the server with the electronic gaming machine, the amount of credit being added to the credit stored in the memory responsive to the user public key matching the user cryptocurrency wallet public key.

5. The system as recited in claim 4, wherein the user cryptocurrency wallet public key is associated by the server with the electronic gaming machine responsive to a user interaction with the electronic gaming machine.

6. The system as recited in claim 5, wherein the user interaction comprises communicating the user cryptocurrency wallet public key to the server.

7. The system as recited in claim 5, wherein the user interaction comprises communicating an identification of the electronic gaming machine to the server.

8. The system as recited in claim 1, wherein the transaction data further comprises an input identification associated with the cryptocurrency involved in the cryptocurrency transaction and an output identification associated with the cryptocurrency, the server being further configured to use the output identification associated with the cryptocurrency as a subsequent input identification in a subsequent cryptocurrency transaction involving the cryptocurrency.

9. The system as recited in claim 1, further comprising the server being configured to generate a subsequent cryptocurrency transaction responsive to a withdrawal request received from the user cryptocurrency wallet, the withdrawal request comprising instructions to deduct a withdrawn amount of credit from the memory and return the withdrawn amount of credit to the user cryptocurrency wallet in the form of cryptocurrency, the server communicating with the electronic gaming machine to cause the withdrawn amount of credit to be deducted from the credit stored in the memory, the subsequent cryptocurrency transaction being defined by a subsequent transaction data comprising a return amount of a cryptocurrency and a user cryptocurrency wallet public key associated with the user cryptocurrency wallet, wherein the return amount of cryptocurrency corresponds to the withdrawn amount of credit.

10. A system for enabling secure cryptocurrency transfers in transactions involving gaming devices, the system comprising:

an electronic gaming machine, the electronic gaming machine including a memory configured to store an amount of credit, the credit being usable to actuate play of a game on the electronic gaming machine;

a casino backend server in communication with a database and the electronic gaming machine, the database storing user data including a user cryptocurrency wallet public key; and

a user device configured to actuate a cryptocurrency transaction, the cryptocurrency transaction being defined by transaction data communicated to a blockchain, the transaction data including an amount of a cryptocurrency involved in the cryptocurrency transaction and a user public key,

wherein the casino backend server is configured to detect the transaction data communicated to the blockchain, and responsive to the user cryptocurrency wallet public key matching the user public key included in the transaction data, communicate a signal to the electronic gaming machine, the signal causing the addition of an amount of credit to the credit stored in the memory, the amount of credit corresponding to the amount of cryptocurrency involved in the cryptocurrency transaction.

11. The system as recited in claim 10, wherein the transaction data further comprises an input identification associated with a source of the cryptocurrency involved in the cryptocurrency transaction and an output identification associated with the cryptocurrency transaction.

12. The system as recited in claim 11, wherein the casino backend server is further configured to use the output identification associated with the cryptocurrency as a subsequent input identification in a subsequent cryptocurrency transaction involving the cryptocurrency.

13. The system as recited in claim 10, further comprising the casino backend server actuating a subsequent cryptocurrency transaction responsive to a withdrawal request received from the user device, the withdrawal request comprising instructions to deduct a withdrawn amount of credit from the memory and return the withdrawn amount of credit to the user cryptocurrency wallet in the form of cryptocurrency, wherein the casino backend server communicates a signal to the electronic gaming machine to deduct the withdrawn amount of credit from the credit stored in the memory and generates a subsequent cryptocurrency transaction defined by a subsequent

transaction data comprising a return amount of a cryptocurrency and the user cryptocurrency wallet public key, wherein the return amount of cryptocurrency corresponds to the withdrawn amount of credit.

14. The system as recited in claim 13, wherein the withdrawal request is received from the user device.

15. The system as recited in claim 10, wherein the casino backend server associates the user device with the electronic gaming machine.

16. A system as recited in claim 10, wherein the transaction data further comprises a unique identification of the electronic gaming machine.

17. The system as recited in claim 16, wherein the user device is further configured to communicate the unique identification to the casino backend server.

18. The system as recited in claim 17, wherein the user cryptocurrency wallet public key is associated by the casino backend server with the electronic gaming machine responsive to the casino backend server receiving the unique identification.

19. A method for enabling secure cryptocurrency transfers in transactions involving an electronic gaming machine, the electronic gaming machine including a memory configured to store an amount of credit, the credit being usable to actuate play of a game on the electronic gaming machine, wherein the electronic gaming machine, the method comprising the steps of:

actuating a cryptocurrency transaction through a user device, the cryptocurrency transaction being defined by transaction data communicated to a blockchain, the transaction data including an amount of a cryptocurrency involved in the cryptocurrency transaction and a user public key;

a casino backend server detecting the transaction data communicated to the blockchain, the casino backend server being in communication with a database and the electronic gaming machine, the database storing user data including a user cryptocurrency wallet public key; and

responsive to the user cryptocurrency wallet public key matching the user public key included in the transaction data, the casino backend server communicating a signal to the electronic gaming machine, the signal causing an amount of credit to be added to the credit stored in the memory, the amount of credit corresponding to the amount of cryptocurrency involved in the cryptocurrency transaction.

20. The method as recited in claim 18, further comprising the step of the user device communicating with the electronic gaming machine, whereby the casino backend server associates with the user device with the electronic gaming machine.