CUSTOMIZED VIEW OF RESTRICTED INFORMATION RECORDED INTO A BLOCKCHAIN

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 62/639,393 filed March 6, 2018, entitled "Customized View of Restricted Transactions Recorded into a Blockchain," and U.S. Provisional Patent Application No. 62/701,947 filed July 23, 2018, entitled "Customized View of Restricted Information Recorded into a Blockchain," which are both incorporated herein by reference in their entirety for all purposes.

TECHNICAL FIELD

[0002] Aspects of the disclosure are related to computing hardware and software technology, and in particular to generate a customized view of restricted transactions recorded into a blockchain.

TECHNICAL BACKGROUND

[0003] Blockchains allow a network of users to make a digital ledger of data and share the data among the other users in the network. Unlike previous database structures, the blockchain database is maintained by a multitude of independent nodes spread across a large distributed network. When a transaction is recorded into the blockchain database, it is very difficult, if not impossible, to change or remove that data from the database since the data is stored in more than one node in the distributed network. Therefore, data is added into the blockchain database by multiple users and changing the recorded data would require each of these users (or a majority of the users) to agree to the change. This distribution of control to add, edit, and remove data from the blockchain database creates trust amongst users in the network, especially when users are not familiar with one another.

OVERVIEW

[0004] An enhanced system, method, and software application are disclosed herein to generate a customized view of a blockchain transaction. A blockchain of block entries requested by a plurality of users from user devices is maintained in a distributed network of nodes. The block entries each comprise a plurality of data portions that are each associated with an access level. A request to view one or more data portions of a block entry is received which includes an access code associated with at least one access level. The access code in the

request is evaluated with the blockchain of block entries to identify one or more data portions associated with the access level. A customized view of the block entry is generated which includes the one or more data portions associated with the access level.

[0005] Various embodiments provide techniques to store and provide access to information an owner intends to keep private but in public ledger that can be seen and audited by authorized entities or individuals. There are privacy laws world-wide that require information to be kept private. Various embodiments can ensure compliance with those privacy laws by ensuring the data is stored in correct formats and only accessible in compliant manners. As another example, there are businesses and governments that do not want their private information, knowledge or trade secrets to become known. While these groups do not have anything to hide, having all of their information in an open forum where anyone has viewability or knowledge of how people, businesses, governments, or the like operate will bring on loss, theft and increased competition.

[0006] For example, in the gaming industry, customers social security numbers, biometrics, addresses, photos, driver's license, prior game play, IRS tax notices, win/loss, comps, loyalty card/player card number information, birth dates, known associates, spouse/girlfriend, favorite teams, liked/disliked activities, tipping amounts, ATM use while on property, known electronic wallets, credit/debit cards used, cryptocurrency wallets used and the like can all be kept on a blockchain with other customer information. The customer would not want any of this information viewable in a public format and public access may create legal liabilities for the casinos. Various embodiments use various encryption and hashing techniques to securely store the data on the blockchain and only allow authorized user to view the data. As an example, the customer may enter into a tournament and his name or player number may be used to identify him in a public forum but none of the other private information would be available for anyone to see other than users with the correct access which would include the user, proper casino staff, auditors, regulators, or the like.

[0007] Logistics provides another direct application of the technology. For example, tracking of packages or cargo, movement of commodities from one place to another is important. All information can be included in what is being transported from where the cargo came from and is going to. At various points, the cargo may be scanned so the precise location is known for the cargo at specific times. This can be entered into the blockchain record. In addition, the cargo can be associated with specific vessels, trucks, vans, or other delivery

mechanisms (e.g., delivery drones) and the GPS location of that delivery mechanism can be tracked in real-time, upon request, or at certain time intervals. Additional information, such as the buyer, the seller, the owner insurance information, and the like can be reported as well as demurrage tied to GPS recorded on a blockchain. Companies and/or governments do not want everyone to know their business for a variety of reasons but need the ability to audit and prove to inspectors, controllers or regulators what they are or were doing at a certain time/place. The ability of keeping things private is mandatory. As such, various embodiments can use a combination of private, public, and hybrid blockchains to store the information. Moreover, various encryption schemes and access levels can be associated with individual portions of the data to ensure privacy where needed or wanted while granting access when necessary.

[0008] In some embodiments, the technology can provide specific applications to the defense industry. For example, the US government needs the ability to audit and control purchasing, logistics, supply, troop movement, and the like. This information if it falls into the wrong hands could have deadly consequences. Obfuscation of certain aspects of information in keeping them private is imperative to the success of a mission. Having the ability to classify the data and allow access is imperative to make sure only the people required have the ability to access the data (e.g., to see, monitor, work on, or audit, etc.) while anyone that does not have access is not able to see the data portions. In some embodiments, the system may automatically review documents relevant to a query and automatically apply one or more redaction filters based on the user's clearance status.

[0009] Some embodiments allow a data platform to connect to electronic voting machines. These machines can directly report information about voters, the ballots, and cast votes to the data platform for storage in a blockchain. The data platform can encrypt and set access levels for access to the voting records. For example, the voting machines may collect a person's information, social security number, address, party, biometrics, driver's license number, photo, or the like. As such, keeping much of this information used in an election there needs to be kept private from the public, some information may be public (e.g., that a person did vote in a particular election, their party affiliation, or the like). Moreover, some embodiments provide for the use of automated techniques for identifying and/or eliminating voter fraud. For example, some embodiments, may use an artificial intelligence or machine learning engine to review the voter data stored in the blockchain and identify voters voting twice, illegal voters, or the like.

[0010] In addition, the examples provided above, the technology may be used in banking, jury voting, court proceedings, healthcare, fire arm sales, retail sales, pharmaceuticals, pensions, financial transactions, insurance, and many other applications where auditing, public viewing of data, private viewing of data, and the like are needed.

[0011] Some embodiments of the present technology may use optional markers under the hybrid format. For example, in some embodiment the system may have the ability of setting things to private (not viewable by people without access), public (viewable by everyone), or a hybrid of the two (some information is public and some information is private). There are circumstances that a public blockchain should be used and can be totally transparent for everyone to see. There are also some cases where some privacy from some of the information is required in order to meet privacy laws or fore the mere fact that people do not want others to know that they are the person or organization who is responsible for doing something which would be the hybrid format. The ability to obfuscate or keep private certain information is imperative for the above industries.

[0012] In accordance with various embodiments that use the private or hybrid format, there are at least two option for securing the data. For example, in some embodiments, a total obfuscation of information can be done by applying encryption to unlock. Some embodiments may use multiple layers of encryption so that portions of the data can be limited and accessible to various individuals. In a hybrid mode of operation, some of the information can be public or transparently seen while other information will be kept obfuscated or private. In some cases, a marker can be used to designate the data access level. A marker could be something which shows who the user is to an auditor, election official, controller, or the like and could be a number like citizen 1, or customer 200. In some embodiments, a codex may be used which could be controlled by the system which would scramble the identity of the user so no one would know who the user is thus keeping the identity private. Only the persons responsible for the auditing or administering the blockchain would be able to figure out who the accountable party is. In some embodiments, the codex would never provide this information unless it needed to be audited and accounted for.

[0013] In some embodiments, an auditing functionality can be integrated into a user interface that would give a user (e.g., the with the click of a virtual button) the ability to allow all information or some information (e.g., column, format, section, etc.) private, public, and limited access. Some embodiments provide for real-time monitoring/auditing function which

will show and allow a user to double or triple check what is kept private. In some embodiments, a password, password with two-party authenticator, three-party authenticator, multiple signature, or the like would be a part of a decentralized application (DApp) powered by the blockchain that would enable a user to submit, add or attach information going into a blockchain. In some embodiments, this information can be set up in a decentralized manner so information can automatically be inserted and tested and monitored on a decentralized network in real-time so that information is not leaked out or hacked or seen by parties that are not permitted.

[0014] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter. Additional aspects, features, and/or advantages of examples will be set forth in part in the description which follows and, in part, will be apparent from the description, or may be learned by practice of the disclosure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] Many aspects of the disclosure can be better understood with reference to the following drawings. While several implementations are described in connection with these drawings, the disclosure is not limited to the implementations disclosed herein. On the contrary, the intent is to cover all alternatives, modifications, and equivalents.

[0016] Figure 1 illustrates an operational architecture for implementing an enhanced application to generate a customized view of restricted transactions recorded into a blockchain.

[0017] Figure 2 illustrates a view customization process employed in implementations of an enhanced application to generate a customized view of restricted transactions recorded into a blockchain.

[0018] Figure 3 illustrates various components of the distributed ledger architecture in an implementation to generate a customized view of restricted transactions recorded into a blockchain.

[0019] Figure 4 illustrates a block diagram in an implementation of an enhanced application to generate a customized view of restricted transactions recorded into a blockchain.

[0020] Figure 5 illustrates a flow diagram in an implementation of an enhanced application to generate a customized view of restricted transactions recorded into a blockchain.

[0021] Figure 6 illustrates a block diagram in an implementation of an enhanced application to generate a customized view of restricted transactions recorded into a blockchain.

[0022] Figure 7 illustrates a flow diagram in an implementation of an enhanced application to generate a customized view of restricted transactions recorded into a blockchain.

[0023] Figure 8 illustrates a block diagram in an implementation of an enhanced application to generate a customized view of restricted transactions recorded into a blockchain.

[0024] Figure 9 illustrates a flow diagram in an implementation of an enhanced application to generate a customized view of restricted transactions recorded into a blockchain.

[0025] Figure 10 illustrates an exemplary operational architecture in an implementation of a financial auditing scenario to generate a customized view of restricted transactions recorded into a blockchain.

[0026] Figure 11 illustrates an alternative operational architecture in an implementation of a gaming regulation scenario to generate a customized view of restricted transactions recorded into a blockchain.

[0027] Figure 12 illustrates an alternative operational architecture in an implementation of an inventory tracking scenario to generate a customized view of restricted transactions recorded into a blockchain.

[0028] Figure 13 illustrates an exemplary customized view of restricted transaction recorded into a blockchain.

[0029] Figure 14 illustrates an alternative exemplary customized view of restricted transaction recorded into a blockchain.

[0030] Figure 15 illustrates an alternative operational architecture in an implementation of an data access system capable of providing a customized view of restricted or sensitive data recorded into a blockchain.

[0031] Figure 16 illustrates a computing system suitable for implementing the technology disclosed herein, including any of the architectures, processes, operational scenarios, and operational sequences illustrated in the Figures and discussed below in the Technical Description.

DETAILED DESCRIPTION

[0032] Blockchains have become a commonplace in generating a blockchain of data and sharing the data among users in a distributed network. Unlike previous database structures, the blockchain database is maintained by a multitude of independent nodes spread across a large distributed network of nodes. A public blockchain is a digital ledger that is open to any user to enter and record data (also referred to herein as transactions or block entries) into a block of the blockchain. When a transaction is recorded into the blockchain database, it is very difficult, if not impossible, to change or remove the transaction data from the database since the data is stored in more than one node in the distributed network. Therefore, data is added into the blockchain database by multiple users and changing the recorded data by adding, editing, or removing data would require a majority of the users or a master controller supervising changes and a cosigner (e.g., manager and employee, auditor and pit boss, etc.) to agree to the change.

[0033] Additionally, each block contains the data, the hash of the current block, and the hash of the previous block. The blockchain may also store additional details about the transaction in the block, such as the username initiating the transaction, other usernames of parties associated with the transaction, a timestamp, executable code, among other information that relates to the transaction. The hash identifies the block and the transaction data stored within the block. The hash is unique from all other hashes and changes whenever a change is made to the block. Since each block contains the hash of the previous block, the blocks form what is known as a blockchain. Any tampering with a block will cause a change in the hash of that block. Therefore, all other blocks in the blockchain will become invalid since they no longer contain a valid hash of the previous block.

[0034] While it may be possible to change the hash of each subsequent block in the blockchain, it would be nearly impossible to change each blockchain stored on each node in the distributed network, for both private and public networks. This combination of storing previous hashes to form the blockchain and distributing a full copy of the blockchain to each node in the distributed network (private, permissive, and public) creates a system of trust amongst users and the stored transactions in the network, especially when users are not familiar with one another (i.e., public network).

[0035] Examples of the present disclosure describe a system, process, and application for generating a customized view of a blockchain transaction. A blockchain of block entries

requested by a plurality of users from user devices is maintained in a distributed network of nodes. The block entries each comprise a plurality of data portions that are each associated with an access level. A request to view one or more data portions of a block entry is received which includes an access code (e.g., hash, private key, biometric, password, PIN, etc.) associated with at least one access level. The access code in the request is evaluated with the blockchain of block entries to identify one or more data portions associated with the access level. A customized view of the block entry is generated which includes the one or more data portions associated with the access level. In some embodiments, the portions of the data stored in the block chain may be individually encrypted. As such, depending on the level of access associated with the access code, decryption of only a portion of the data may be authorized or available while other portions would remain secure.

[0036] A technical effect that may be appreciated from the present discussion is the increased efficiency in identifying entry data that a user is authorized to access (e.g., financial records in a banking institution, a customer/supplier tracking inventory, compliance data for a gaming regulation committee, classified documents from a governmental or semi-governmental agency, health records for a medical institution, Protected Critical Infrastructure Information (PCII), data needed for a government auditor/inspector, and the like) and providing a customized view of the data that was recorded in the blockchain transaction. Some of the embodiments described herein also improve security by only allowing access to the user if the user has authorization to access the portion of data from the blockchain entry. In addition, some embodiments can provide an immutable log showing when and who accessed various data. In addition, in some embodiments, automatic review (e.g., by an artificial intelligence or machine learning engine) can occur to detect specific events (e.g., insider trading, money laundering, cheating, voter fraud, etc.).

[0037] More specifically, one implementation may provide a non-routine process of generating a customized view of a banking transaction that limits user sensitive information (e.g., Anti-Money Laundering (AML) or Know Your Customer (KYC) policy documents, (ADD) account numbers, account balances, account statements), but allows an external banking institution or user to verify that an account has available funds for a transaction. Another scenario provides a non-routine process of auditing a transaction in the blockchain while not enabling an auditor to view a full version of the transaction. For example, the Internal Revenue Service (IRS) may require an audit of all monetary transactions performed within the previous tax year. However, the company being audited may not be required to provide a full

list of customer names and addresses for each transaction. By providing a customized view of the transaction, the IRS may have confidence in the accuracy of the transaction amounts and the company may maintain anonymity of its customers.

[0038] An additional technical effect of the present discussion may be appreciated in the gaming regulation industry. For example, one implementation described herein provides a non-routine process of viewing the outcome of a gaming bet while concealing a betting amount. This may be useful when monitoring a gaming community for advantage players (e.g., card counters, etc.) while allowing the players to maintain privacy of their money pot. In another example, a gaming committee may require a customized view of a transaction to view some personal information about each player (e.g., verification that each player is of a legal age to gamble, verification that each player has not been blacklisted, player handles/nicknames) but not enable other personal information to be viewable (e.g., credit card numbers used to buy into the game, legal names of each player, etc.).

[0039] Another example may include the Nevada Gaming Commission requiring disclosure documents of previous business relationships, employment history, criminal records, and financial stability from an applicant seeking a license for a gaming establishment. However, the applicant may not be required to provide expunged records of criminal behavior. Therefore, the view of the documents would be customized to display only those portions of the documents required by the Nevada Gaming Commission and omit, redact, or otherwise obfuscate data that is not deemed relevant or needed for seeking the license.

[0040] In some embodiments, the system may ingest the private information and generate a publicly viewable score, rating, or other indicator that may be used in making a decision without disclosing the underlying confidential information. In some embodiments, the system can connect to additional public and private data sources to collected additional information. For example, public information like FBI reports, credit reports, background reports, and the like. This additional information can be stored in the blockchain as part of the record or profile of an individual. This could be done off of a social security number, driver's license, facial recognition or fingerprint as a second factor for verification. As such, once a person enters the casino and registers a card to play it is possible that big data would be collected on who the person really is and that information would only be available to the casino, auditor and regulator to make sure the person is who the person says he is, is legal and allowed on property or able to play.

[0041] In yet another embodiment, a technical effect may be recognized for a non-routine process of tracking package deliveries and inventory transit. For example, one or more packages may be scanned at origin, then once again as the packages begin transit in one cargo unit. The transit company may want to allow a recipient of one of the packages to view data associated with their box but not allow the recipient to view all other data stored in the transaction associated with the other packages in the cargo unit. Therefore, a customized view of the transaction for the recipient user describing the location, departure time, and estimated arrival time for their package only would be enabled. Additional information associated with the product may also be collected and stored in a blockchain detailing product logistics, such as manufacturer, vendor, checkpoint location, checkpoint employee, quality control manager, testing center, as well as a chain of custody through the shipping process as well as individuals that accessed the cargo unit during its shipment. At any time or upon receipt, the receiving party may be enabled to see parts of this information but not all depending on the status of the recipient. For example, a gambling establishment or regulator may be able to view selective product information regarding manufactured dice along with a chain of custody to verify that the dice have not been tainted with while routed from the trusted dice manufacturer. This data may be displayed in a customized view.

[0042] Further, examples herein describe that the access code in the request with the blockchain of block entries may be evaluated by processing an encryption code to validate access to view the one or more data portions associated with the access level. In other examples, a pointer is also maintained for each of the plurality of data portions in the block entries indicating at least one published location for each of the plurality of data portions in the block entries. Further in this example, the customized view is generated by retrieving the one or more data portions associated with the access level using the pointer for each of the plurality of data portions in the block entries. The access of the portions of data require the use of a pin code, password, fingerprint, barcode, retinal scan, token, questionnaire, or any other type of access determination method including two-factor, multi-factor, or additional security authenticators.

[0043] In a further example, the blockchain of block entries requested by the plurality of users from the user devices is maintained by maintaining a separate block entry for the one or more data portions associated with each of the access levels. Further in this scenario, the access code in the request is validated to view the one or more block entry for the more or more data portions associated with each of the access levels. In some implementations, the

blockchain of block entries requested by the plurality of users from the user devices is maintained by maintaining a separate blockchain for the one or more data portions associated with each of the access levels. Further in this implementation, the access code in the request is validated to view the one or more block entry for the more or more data portions associated with each of the access levels.

[0044] In some examples, the received request to view the one or more data portions of the block entry comprises an inventory tracking request. In other examples, the received request to view the one or more data portions of the block entry comprises a financial auditing request. In some scenarios, the received request to view the one or more data portions of the block entry comprises a gaming regulation request. In other scenarios, the access level associated with the one or more data portions of the block entry comprises at least one of a private access level, a permissive access level, and a public access level. However, in even further examples, the access level associated with the block entry comprises at least one of a private access level, a permissive access level, and a public access level.

[0045] While the present disclosure describes various embodiments, it should be appreciated that additional examples may be included for technical improvement in additional industries. Example industries may include defense and security, finance and insurance, retail (e.g., firearms), sales and licensing, medical records, accounting, shipping and logistics, drugs and pharmaceuticals, cannabis, oil and gas, energy and commodities, national security, and the like.

[0046] Referring to the drawings, Figure 1 illustrates an exemplary operational architecture 100 related to processing operations for management of an exemplary enhanced system with which aspects of the present disclosure may be practiced. Operational environment 100 includes blockchain network 101. Blockchain network 101 employs a view customization process 200 in the context of authorizing a user to view a portion of data in a blockchain entry based on the user's approved access level. Blockchain network 101 may include various hardware and software elements in a supporting architecture suitable for performing view customization process 200. One such representative architecture is illustrated in Figure 16 with respect to controller 1600.

[0047] Server nodes 110-112 comprise one or more servers and devices capable of running a blockchain application. User devices interacting with server nodes 110-112 may include, but are not limited to, personal computers, mobile phones, handheld device, tablet

computers, desktop computers, laptop computers, wearable computing devices, voting machines, gaming machines, electronic financial exchanges, security systems, or any other form factor, including any combination of computers or variations thereof.

[0048] More particularly, Figure 2 illustrates view customization process 200 which, as mentioned, may be employed by blockchain network 101 to generate a customized view of restricted transactions recorded into a blockchain as described herein. Some or all of the steps of view customization process 200 may be implemented in program instructions in the context of a component or components of the application used to carry out the customized view feature. The program instructions direct blockchain network 101 to operate as follows, referring parenthetically to the steps in Figure 2 in the context of Figure 1.

[0049] In operation, blockchain network 101 maintains blockchain 120 of block entries requested by a plurality of users from user devices, wherein the block entries each comprise a plurality of portions that are each associated with an access level (step 201). The blockchain database is maintained by a multitude of independent users spread across blockchain network 101 of server nodes 110-112. Blockchain 120 is a digital ledger that is open to any user (e.g., a public blockchain), a specific set of users (e.g., a private blockchain), or combination of private and public users (e.g., a hybrid blockchain) to enter and record data into block 130 of the blockchain. Blockchain 120 may be added by multiple users and recorded by multiple nodes 110-112 in the distributed network.

[0050] Block 130 includes block entries 140-142. Block entries 140-142 may include various types of data including gaming bets, inventory records, medical records, banking and financial records, smart contracts, and any other type of combination or variation thereof. For instance, the user may create block entry 140 by entering into a contract with another user and then storing the contract as block entry 140 in blockchain 120 on nodes 110-112 in the distributed network environment. As another example, electronic devices (e.g., electronic voting machines, gambling machines, auditing software running on one or more servers, end-user devices, and the like) may connect automatically to blockchain network and request data be added in block entries.

[0051] In order to add a new block entry with data portions, blockchain may use consensus protocols like proof of stake (PoS), or proof of work (PoW), delegated proof of stake (DPoS), or the like. For example, in PoW, in order for server node 110-112 to be elected as a leader to select the next block entry 140 to be added to the blockchain, a particular server node

has to find a solution (typically by brute force) to a particular puzzle or mathematical problem. Once the solution is found, the server node publishes the solution to the other nodes for validation. When a consensus of the nodes agrees the solution is correct, the new block entry can be added to the blockchain. Examples of proof of work are SHA-256, Blake-256, CryptoNight, Quark, SHA-256, SHA-3, 4crypt, scrypt-jane, HEFTY1 or others or combinations thereof. In contrast, PoS is based on the involvement and value at risk (e.g., the stake) of the server node. DPoS is efficient variation of PoS that provides a high level of scalability by limiting the number of validators on the network to set of delegates (e.g., voters) to vote on whether to add an entry to the blockchain.

[0052] Block entries 140-142 also each include data portions 150-155. Data portions 150-155 comprise the components which make up each of block entries 140-142 and may be broken into segments based on a user request or a transaction format (both standardized and customized). For example, a portion of data from a transaction may be allocated as private if a user flags the portion of data as confidential. The portion of data may also be allocated as private if the data is of a category which was previously allocated as private. For example, a user may categorize all credit card numbers as private. Conversely, a portion of data may also be allocated as public or permissive by the user. In some implementations, the portion of data may only be designated as accessible to a receiving user if the originating or controlling user provides permission (e.g., originating party of a transaction allocates the block entry and all data portions as private and ability to view a portion of data requires consent via signature terms and condition form). This user consent feature may be included in an access platform allowing users to provide consent through an user consent section.

[0053] Some embodiments of the present technology modify the traditional protocols and workflow for adding data to the blockchain. For example, in some embodiments, the server node 110-112 is required to identify or classify portions of the data into one or more categories. This can be done, for example, using artificial intelligence or machine learning to classify the data into one or more categories (e.g., e-mail address, social security number, etc.). In some embodiments, a decentralized application (DApp) may be responsible for the initial sorting and categorization of the data. When a block entry 140-142 is added, the initial line of the entry that typically includes the hash of previous blocks and a time stamp may be amended to include information regarding the data categories within the entry, access level for each data portion, access restrictions, or the like. For example, some embodiments may create an index and/or access level information that stored within the block entry. As such, when the data is later

retrieved it can easily be identified or associated with an appropriate access level. Still yet, in some embodiments, the server node responsible for adding the data may organize the data and set different encryption levels for the different data portions 150-155. In other embodiments, a middleware may be used (e.g., on a data platform sitting between the blockchain network and the connecting devices) to decrypt encrypted data store don the blockchain, classify information, and enforce access level permissions thereby creating the customized view.

[0054] In some scenarios, the user may set a default setting allocating all of the data in the transaction as public and selectively allocate individual segments of data as private, and vice versa. Likewise, a portion of the data may also be allocated as permissive where the data is not available to the general public but may be accessible to users of various groups, such as auditing committee members, law enforcement officers, government regulation personnel, medical staff, and the like. In other examples, blockchain 120 may include default rules to allocate portions of data as private, permissive, or public.

[0055] For example, blockchain 120 may determine that any social security number should be automatically set to private access. While several examples and embodiments included herein describe the main access levels to be categorized as private, permissive, or public, it should be understood that any number of access level categories may be recognized within the scope of the present disclosure. Moreover, the status of the access levels may automatically change or be updated based on detection of certain events. For example, all data regarding a deal may remain private for a period of time at which point the system may change the access level to public for some or all of the related data.

[0056] In a next operation, blockchain network 101 receives a request to view one or more data portions 150-155 of block entry 140 from a user which includes an access code associated with at least one access level (step 202). The request to view may be initiated by a user who is a party to the transaction stored in block entry 140, such as one participant in a gaming bet. The user may also be a user merely having interest in the transaction but not directly involved with the transaction, such as a tax auditor verifying income data, a transfer agent or third party financial custodian holdings stocks and bonds, a servicer that collects debt payments on behalf of a lender or a stockholder viewing recent company dividend transactions.

[0057] In a next operation, the access code is evaluated with the blockchain of block entries to identify one or more data portions associated with the access level (step 203). The access code may be designated to the user based on a user status, such as a government

employee, package delivery employee, bank manager, etc. The access code may be determined based on an encrypted code (e.g., a private key or hash) given to user which is associated with an access level or data portion. The access code may further be validated based on a password, signature, fingerprint, barcode, processing chip, questionnaire, biometric, token, and any other method which may enable a user to verify authorization to access data portions 150-155 associated with an access level. In some example scenarios, data portions 150-155 may be separated into different blockchains or block entries based on their associated access level. In this scenario, access code 150 may be required to access the blockchain or block entry to view the portion of data associated with the access level.

[0058] In a final operation, a customized view of the block entry is generated which includes one or more data portions 150-155 associated with the access level (step 204). The customized view may be generated by a data access platform. The customized view may be modified to incorporate only those data portions associated with the validated access level or may include all data portions 150-155 with unauthorized data portions blacked out from the record view. The customized view may be surfaced in a blockchain application (e.g., a DApp) on a user device, transferred to a user in the form of a record message, or displayed in any other manner to a user or user group.

[0059] In accordance with various embodiments, the addition of data to the blockchain, security level screening, data categorization, access level assignments, auditing and/or other functionality may all be done autonomously. For example, as a user enters a casino data can be collected added to the blockchain from various systems (e.g., surveillance cameras, parking garage cameras, loyalty card systems, room access systems, entertainment databases, and the like). Given the volume of data, artificial intelligence and/or machine learning engines (e.g., using support vector machines, artificial neural networks, Bayesian networks, supervised learning, unsupervised learning, and/or other techniques) can be used to identify, associate and classify relevant data that can be added to a blockchain. The data itself may be indexed for searching and/or future ingestion. In other embodiments, the data may be segmented and added to a profile of a player. Since various portions of the data can be assigned different access levels, the person requesting the data may be automatically served only the portions of data that are appropriate for their access level. Similarly, the data may be automatically reviewed or audited to identify violations (e.g., gambling rule violations, cheating, collusion, people banned from gambling, etc.).

[0060] Similar to casino monitoring, various embodiments of the present technology can be applied to verticals that can review data automatically without humans overseeing the review. For example, some embodiments may interface with secure data sets (possible stored on a private blockchain) to gain biometrics or data about an individual. As such, government agencies (e.g., ICE or Department of Homeland Security) can provide data that can be used to identify individuals and make determinations whether they should be granted to access to particular data, activities, and/or locations. For example, various embodiments of the system may be used to screen individuals for a trusted traveler program. As the individual enters the airport, for example, surveillance cameras can collect video data which can be ingested by artificial intelligence or machine learning engines. This data can be linked with license plates, travel records, biometric data, and the like to initially identify the individual and determine if a violation is in progress, prescreen the person (e.g., for faster screening), or determine whether the user can be denied entry to the airplane or other travel method. In some embodiments, each person may have their driver's license scanned and the system can automatically classify the identification as legitimate or a fraud and search for records in the blockchain to assist in making decisions.

[0061] Figure 3 illustrates various components of a blockchain data platform utilizing a distributed ledger architecture according to various embodiments of the present technology. As illustrated in Figure 3, the blockchain data platform may use one or more servers 305A-305N. Each server can include blockchain interface 310, monitoring mechanism 315, client interface 320, rules engine 325, encryption/decryption module 330, analytics module 335, event module 340, multifactor authentication module 350, report generator 355, and/or databases 360 and/or 365 for storing logs, subscriber policies, transaction policies, location policies, and/or the like. In addition, blockchain servers 305A-205N can connect with blockchain 370, clients 375, trusted data sources 380, and/or records 385.

[0062] Each of these modules, components, or databases can be embodied as special-purpose hardware (e.g., one or more ASICS, PLDs, FPGAs, or the like), or as programmable circuitry (e.g., one or more microprocessors, microcontrollers, or the like) appropriately programmed with software and/or firmware, or as a combination of special purpose hardware and programmable circuitry. Other embodiments of the present technology may include some, all, or none of these modules and components along with other modules, applications, databases, and/or components. Still yet, some embodiments may incorporate two or more of these modules and components into a single module and/or associate a portion of the

functionality of one or more of these modules with a different module. For example, in one embodiment, rules engine 325 and event module 340 can be combined into a single module for identifying and enforcing various rules and event policies on a user terminal.

[0063] Clients 375 may connect to one of blockchain servers 305A-305N using client interface 320. Clients 375 may be able to download (or have preinstalled) firmware or software from blockchain servers 305A-305N that allows clients 375 to enter and view block entries (or selected portions thereof). The block entries may comprise a variety of transactions (e.g., financial transactions, gaming bets, medical records, inventory tracking, etc.) and a variety of access levels (private, permissive, public, etc.). In some embodiments, blockchain servers 305A-305N process an encryption code to validate access to view the one or more portions of each transaction.

[0064] In some embodiments blockchain servers 305A-305N may maintain a pointer for each of the plurality of portions in the block entries indicating at least one published location for each of the plurality of portion in the block entries. The customized view of the block entry may then be generated by retrieving the portions associated with the access level using the pointer for each of the portions in the block entries. In other embodiments, blockchain servers 305A-305N may maintain a separate block entry for the data portions associated with each of the access levels. Blockchain servers 305A-305N may evaluate the access code in the request with the block entries of blockchain 370 to identify the data portions associated with the access level. In some scenarios, blockchain servers 305A-305N may maintain a separate blockchain for the data portions associated with each of the access levels. Blockchain servers 305A-305N may then evaluate the access code in the request with blockchain 370 to identify the data portions associated with the access level.

[0065] In some examples, information stored in blockchain 370 may be encrypted using encryption/decryption module 330. In some embodiments, encryption/decryption module 330 may use various non-homomorphic encryption and/or homomorphic encryption. While the non-homomorphic encryption may provide stronger security properties, the use of homomorphic encryption would allow computation on encoded data without decryption. As a result, various components of the gaming system can interact and operate on portions of the data without exposure of sensitive data.

[0066] Monitoring mechanism 315 can monitor transactions and user activities. This can include receiving information from external sources such as, but not limited to, clients 375,

video surveillance systems, loyalty card systems, key engines, biometric sensors, and other external systems. In some embodiments, multifactor authentication may be used before allowing a user to enter or to access a monetary transaction, medical record, gaming bet, inventory activity log, and the like. For example, when a patient accesses a medical record, multifactor authentication module 350 may be used to require various types of authentications (e.g., personal pin, biometric, token, etc.). Rules engine 325 can superimpose rules on the transaction interfaces being presented on clients 375. These rules can be based various policies (e.g., subscriber policies, transaction policies, location policies, etc.) stored in database 365. Analytics module 335 can generate various analytics about layers, clients, games, medical diagnosis, payrolls, package deliveries, payouts, accounts, and/or other system components or activity. This information can be used by report generator 355 to create customized view of the transactions.

[0067] Restricted access module 340 can be used to create customized access requirements for different portions of data in each transaction and for different users/user types. The rewards may be stored within blockchain 370 in records 385. The access requirements may be generated by a user entering the transaction, determined based on previously designated user preferences, or by policies required by other parties (e.g., permissive access for medical records required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), state laws for minimum age to gamble, etc.) and present customized view of records based on those access policies. Databases 360 and/or 365 can be used for storing logs, subscriber policies, transaction policies, location policies, and/or the like. These may be local stores of data retrieved from records 385 associated with blockchain 370. In addition, servers 305A-305N and blockchain 370 can connect with trusted data sources 380 for validation of external events (e.g., outcome of sporting events, reconciliation of vender/buyer journal entries, etc.) or information (e.g., status of a security clearance) that are needed to determine data stored within records 385.

[0068] Figure 4 illustrates block diagram 400 in an implementation of an enhanced application to generate a customized view of restricted transactions recorded into a blockchain. Block diagram 400 includes inventory block entry 401, data platform 410, servers 420-422, blockchains 430-432, and record 402.

[0069] Block entry 401 is representative of any data transaction that will be permanently recorded into the blockchain. Block entry 401 is subsequently processed by miners and added to a block at the end of the blockchain by data platform 410. Block entry 401 further comprises

portions of data which have been represented herein by Product, Buyer, and Price. It should be noted that while each of the data portions is represented separately, the portions of data are part of one transaction represented by block entry 401. Block entry 401 may comprise any transaction or contract which has been executed and recorded in a distributed ledger platform environment. In this example, block entry 401 may comprise a purchase order for inventory.

[0070] Data platform 410 represents any computing system or systems capable of hosting a blockchain application, of which controller 1600 in Figure 16 is representative. Data platform 410 provides a secure distributed ledger system for recording transactions into the blockchains. Data platform 410 may be implemented across a multitude of distributed network nodes which may be accessed by a variety of users, such as tax auditors, financial institutions, gaming regulation committees, customers, company employees, and the like.

[0071] Data platform 410 can also include servers 420-422. Servers 420-422 may be representative of any computing system or systems with which the distributed network nodes may communicate. Examples include other devices having corresponding applications or services installed thereon, such that an operating user of a user device may be able to transfer a transaction to be added to a blockchain and distributed amongst the network nodes of the distributed network. Examples include media servers, web servers, and other types of end-points that may transmit transaction data to or receive transaction data from user devices and network nodes. In some embodiments, data platform can dynamically select which servers 420-422 are authorized to store the data. For example, companies or governments may have geographical restrictions, encryption standards, network security standards, or other restrictions on the server nodes on which the blockchain is stored. Data platform 410 can therefore manage the logistics of dynamically selected servers based on these restrictions. For example, if a particular server is deemed to be under attack or hacked, then data platform 410 can dynamically remove that server from the blockchain network and consider adding one or more additional servers if needed. As such, each owner of the data can set selection criteria for where the data should be stored and the minimum IT standards needed for that server group.

[0072] Block diagram 400 further includes blockchains 430-432. Blockchains 430-432 can contain a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each of the block in blockchains 430-432 contains a timestamp and a hash. The hash includes both a cryptographic hash of the current block and a cryptographic hash of the previous block in the blockchain. Each block also contains data associated with a

block entry. In this example scenario, each portion of data (Product, Buyer, and Price) have been separately recorded into a different block and in a separate blockchain 430-432.

[0073] Additionally, each of blockchains 430-432 is associated with a separate access level. For example, blockchain 430 is a public access blockchain which allows any user interacting with the distributed ledger to view the blocks and data portions stored within each block. A public user may be any user interested in viewing the transaction in blockchain 430 and no privacy exists for this portion of data. Conversely, blockchain 431 is a private blockchain which data portions may only be accessed and viewed by authorized users, such as internal company personnel. In this example scenario, Buyer has been separately stored on blockchain 431 and is private from all users interacting in the blockchain network except those with exclusive access to the data, such as managers within a company initiating the transaction. Blockchain 432 is a permissive blockchain meaning that a limited set of parties may view the data portions recorded in the block but not all users. Price has been stored within blockchain 432 and may be view by parties who are allowed access to the data, such as auditors or controllers.

[0074] Record 402 is illustrative of what a user may view when requesting to view the transaction data stored in from block entry 401. Record 402 may contain all or none of the data portions originally entered in block entry 401 and is generated based on the authorization provided by the requesting user and access level each portion of data is associated with.

[0075] Figure 5 illustrates a flow diagram in an implementation to generate a customized view of restricted transactions recorded into a blockchain. Some or all of the steps of view customization process 500 may be implemented in program instructions in the context of a component or components of the application used to carry out the customized view feature.

[0076] In operation, data platform 410 receives block entry 401 which is to be maintained in blocks of blockchains 430-432 (step 501). Block entry 401 is requested by a user from a user device in the distributed network of nodes and contains the data portions. Data platform 410 then authorizes the entry (e.g., miners validate the hash in the block) (step 502). If the block is not validated, the transaction (block entry 401) is rejected (step 503). However, if the block is accepted, each of the portions of data is evaluated for an access level and added to a block in each of blockchains 430-432 based on the identified access level (step 504).

[0077] In a next operation, data platform 410 receives a request to view one or more data portions of a block entry wherein the request comprises an access code associated with at

least one access level (step 505). The access code may be associated with a public, permissive, or private access level. Data platform 410 then evaluates the access code in the request with each of blockchains 430-432 maintaining each of the separate block records for each of the data portions (step 506). If the access code associated with the requesting user is determined to be public, a customized view (e.g., record 402) will be generated for the requesting user indicating only Product from block entry 401 (step 507). If the access code associated with the requesting user is determined to be permissive, a customized view will be generated for the requesting user indicating Product and Price from block entry 401 (step 508). If the access code associated with the requesting user is determined to be private, a customized view will be generated for the requesting user indicating all portions of the data from block entry 401 (i.e., Product, Buyer, and Price) (step 509).

[0078] Another implementation for flow diagram 600 may be in the context of a gambling validation process. For example, a user placing a bet on a large threshold win may require approval from casino managers. In this example scenario, access to the user's data in a blockchain may be required when a payout of the bet occurs to ensure that the bet was approved for the user by the casino manager.

[0079] Figure 6 illustrates a block diagram in an alternative implementation of an enhanced application to generate a customized view of restricted transactions recorded into a blockchain. Block diagram 600 includes gaming bet block entry 601, data platform 610, servers 620-622, blockchain 630, access platform 640, and record 602.

[0080] Block entry 601 is representative of any data transaction that will be permanently recorded into the blockchain. Block entry 601 is subsequently processed by miners and added to a block at the end of the blockchain by data platform 610. Block entry 601 further comprises portions of data which have been represented herein by a Bet Amount, Credit Card Number, and Age. It should be noted that while each of the data portions is represented separately, the portions of data are part of one transaction represented by block entry 601. Block entry 601 may comprise any transaction or contract which has been executed and recorded in a distributed ledger platform environment. However, in this example, block entry 601 comprises a gambling bet. It should also be noted that although requesting users, such as a third-party observer who is not a direct participant of the bet, may be able to view some data of blockchain 630, an access code may be required to view block entry 601. The access code may be in the form of a biometric validation.

[0081] Data platform 610 represents any computing system or systems capable of hosting a blockchain application, of which controller 1600 in Figure 16 is representative. Data platform 610 provides a secure distributed ledger system for recording transactions into the blockchains. Data platform 610 may be implemented across a multitude of distributed network nodes which may be accessed by a variety of users, such as auditors, financial institutions, gaming regulation committees, customers, company employees, and the like.

[0082] Data platform 610 also includes servers 620-622. Servers 620-622 may be representative of any computing system or systems with which the distributed network nodes may communicate. Examples include other devices having corresponding applications or services installed thereon, such that an operating user of a user device may be able to transfer a transaction to be added to a blockchain and distributed amongst the network nodes of the distributed network. Examples include media servers, web servers, and other types of end-points that may transmit transaction data to or receive transaction data from user devices and network nodes.

[0083] Block diagram 600 further includes blockchain 630. Blockchain 630 contains a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each of the block in blockchain 630 contains a timestamp and a hash. The hash includes both a cryptographic hash of the current block and a cryptographic hash of the previous block in the blockchain. Each block also contains data associated with a block entry. In this example scenario, each portion of data (Bet Amount, Credit Card Number, and Age) have been recorded into blockchain 630 with a separate encryption code.

[0084] Additionally, each of the encryption codes associated with each of the data portions in blockchain 630 is associated with a separate access level. For example, Bet Amount is associate with a public access encryption code which allows any user interacting with the distributed ledger to view the portion of data in the block. A public user may be any user interested in viewing the Bet Amount and no privacy exists for this portion of data. Conversely, Credit Card Number is associated with a private encryption code which may only be accessed and viewed by authorized users, such as the internal accounting department. Age is associated with a permissive encryption code which may be view by a limited set of parties but not all users. For example, Age may be required to be view by the gaming committee to ensure that all players are of a legal age to place the gambling bet. However, other players or observers of the bets may not be able to view the age of each player.

[0085] Access platform 640 represents any computing system or systems capable of validating user request to access blockchain entry data, of which controller 1600 in Figure 16 is representative. Access platform 640 provides a secure encryption mediator between the portions of data recorded in blockchain 630 and the generation of record 602 for a requesting user. Access platform 640 may be implemented across a multitude of distributed network nodes which may be accessed by a variety of users, such as tax auditors, financial institutions, gaming regulation committees, customers, company employees, and the like. Record 602 is illustrative of what a user may view when requesting to view the transaction data stored in from block entry 601. Record 602 may contain all or none of the data portions originally entered in block entry 601 and is generated based on the authorization provided by the requesting user and access level each portion of data is associated with.

[0086] Figure 7 illustrates a flow diagram in an implementation to generate a customized view of restricted transactions recorded into a blockchain. Some or all of the steps of view customization process 700 may be implemented in program instructions in the context of a component or components of the application used to carry out the customized view feature.

[0087] In operation, data platform 610 receives block entry 601 which is to be maintained in blocks of blockchain 630 (step 701). Block entry 601 is requested by a user from a user device in the distributed network of nodes and contains the data portions. Data platform 610 then authorizes the entry (e.g., miners validate the hash in the block) (step 702). If the block is not validated, the transaction (block entry 601) is rejected (step 703). However, if the block is accepted, each of the portions of data are evaluated for an access level and added to blockchain 630 (step 704) along with an encryption code based on the identified access level (step 705).

[0088] In a next operation, access platform 640 receives a request to view one or more data portions of a block entry wherein the request comprises an encryption code associated with at least one access level (step 706). The encryption code may be associated with a public, permissive, or private access level. Access platform 640 then evaluates the encryption code in the request with each of the portion of data in blockchain 630 (step 707). If the encryption code associated with the requesting user is determined to be public, a customized view (e.g., record 602) will be generated for the requesting user indicating only Bet Amount from block entry 601 (step 708). If the encryption code associated with the requesting user is determined to be permissive, a customized view will be generated for the requesting user indicating Bet Amount and Age from block entry 601 (step 709). If the encryption code associated with the

requesting user is determined to be private, a customized view will be generated for the requesting user indicating all portions of the data from block entry 601 (i.e., Bet Amount, Credit Card Number, and Age) (step 710).

[0089] Figure 8 illustrates a block diagram in an alternative implementation of an enhanced application to generate a customized view of restricted transactions recorded into a blockchain. Block diagram 800 includes monetary transfer block entry 801, data platform 810, servers 820-822, blockchain 830, access platform 840, and record 802.

[0090] Block entry 801 is representative of any data transaction that will be permanently recorded into the blockchain. Block entry 801 is subsequently processed by miners and added to a block at the end of the blockchain by data platform 810. Block entry 801 further comprises portions of data which have been represented herein by Parties to the Transaction, Bank Account Number, and Available Funds. It should be noted that while each of the data portions is represented separately, the portions of data are part of one transaction represented by block entry 801. Block entry 801 may comprise any transaction or contract which has been executed and recorded in a distributed ledger platform environment. However, in this example, block entry 801 comprises a banking transaction transferring money from one user's bank account to another user's bank account.

[0091] Data platform 810 represents any computing system or systems capable of hosting a blockchain application, of which controller 1600 in Figure 16 is representative. Data platform 810 provides a secure distributed ledger system for recording transactions into the blockchains. Data platform 810 may be implemented across a multitude of distributed network nodes which may be accessed by a variety of users, such as tax auditors, financial institutions, gaming regulation committees, customers, company employees, and the like.

[0092] Data platform 810 also includes servers 820-822. Servers 820-822 may be representative of any computing system or systems with which the distributed network nodes may communicate. Examples include other devices having corresponding applications or services installed thereon, such that an operating user of a user device may be able to transfer a transaction to be added to a blockchain and distributed amongst the network nodes of the distributed network. Examples include media servers, web servers, and other types of end-points that may transmit transaction data to or receive transaction data from user devices and network nodes.

[0093] Block diagram 800 further includes blockchain 830. Blockchain 830 contains a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each of the block in blockchain 830 contains a timestamp and a hash. The hash includes both a cryptographic hash of the current block and a cryptographic hash of the previous block in the blockchain. Each block also contains data associated with a block entry. In this example scenario, each portion of data (Parties, Account Number, and Available Funds) have been recorded into blockchain 830 with a separate access level flag.

[0094] Additionally, each of the access level flags associated with each of the data portions in blockchain 830 is associated with a separate access level. For example, Parties is associated with a public access flag which allows any user interacting with the distributed ledger to view the portion of data in the block. A public user may be any user interested in viewing the Parties to the Transaction and no privacy exists for this portion of data. Conversely, Account Number is associated with a private access flag which may only be accessed and viewed by authorized users, such as the transferring bank for each party. Available Funds is associated with a permissive access flag which may be view by a limited set of parties but not all users. For example, Available Funds may be required to be view by receiving bank to ensure that funds are available in the transferring account to complete the monetary transaction.

[0095] Access platform 840 represents any computing system or systems capable of validating user request to access blockchain entry data, of which controller 1600 in Figure 16 is representative. Access platform 840 provides a secure access flag mediator between the portions of data recorded in blockchain 830 and the generation of record 802 for a requesting user. Access platform 840 may be implemented across a multitude of distributed network nodes which may be accessed by a variety of users, such as tax auditors, financial institutions, gaming regulation committees, customers, company employees, and the like. Record 802 is illustrative of what a user may view when requesting to view the transaction data stored in from block entry 801. Record 802 may contain all or none of the data portions originally entered in block entry 801 and is generated based on the authorization provided by the requesting user and access level each portion of data is associated with.

[0096] Figure 9 illustrates a flow diagram in an implementation to generate a customized view of restricted transactions recorded into a blockchain. Some or all of the steps of view customization process 900 may be implemented in program instructions in the context of a component or components of the application used to carry out the customized view feature.

[0097] In operation, data platform 810 receives block entry 801 which is to be maintained in blocks of blockchain 830 (step 901). Block entry 801 is requested by a user from a user device in the distributed network of nodes and contains the data portions. Data platform 810 then authorizes the entry (e.g., miners validate the hash in the block) (step 902). If the block is not validated, the transaction (block entry 801) is rejected (step 903). However, if the block is accepted, each of the portions of data are evaluated for an access level and added to blockchain 830 (step 904) along with an access flag based on the identified access level (step 905).

[0098] In a next operation, access platform 840 receives a request to view one or more data portions of a block entry wherein the request comprises an access code associated with at least one access level (step 906). The access code may be associated with a public, permissive, or private access level. Access platform 840 then evaluates the access code in the request with each of the portion of data in blockchain 830 (step 907). If the access code associated with the requesting user is determined to be public, a customized view (e.g., record 802) will be generated for the requesting user indicating only Parties from block entry 801 (step 908). If the access code associated with the requesting user is determined to be permissive, a customized view will be generated for the requesting user indicating Parties and Available Funds from block entry 801 (step 909). If the access code associated with the requesting user is determined to be private, a customized view will be generated for the requesting user indicating all portions of the data from block entry 801 (i.e., Parties, Account Number, and Available Funds) (step 910).

[0099] Figure 10 illustrates an exemplary operational architecture in an implementation of a financial auditing scenario to generate a customized view of restricted transactions recorded into a blockchain. In operation, user 1010 transfers paycheck 1030 to user 1020 in exchange for services. A record of the transaction is transferred from user 1010 to database 1040 indicating the name of the service and the expense cost. The record is then maintained in blockchain 1060 via server 1050. It should be noted that in this scenario, the transaction is also recorded on the receiving end by user 1020 where a record of the transaction indicating a profit and the service is transferred to database 1042 and maintained in blockchain 1060 via server 1050.

[00100] In a next operation, government tax auditor 1070 requests to view the profit recorded for user 1020. User 1070 may not be authorized to view the service recorded in the record or the expense from user 1010. Server 1050 may receive the request and process an

access code indicating that at this point in time, user 1070 is only authorized to view the profit for user 1020. A customized view of the record is then generated for user 1070 by server 1050 indicating only the profit for user 1020. Although user 1070 is unable to see the full record of the transaction, user 1070 is able to trust that the portion of the record indicating the profit of user 1020 is valid since it has been maintained in blockchain 1060.

[00101] Figure 11 illustrates an alternative operational architecture in an implementation of a gaming regulation scenario to generate a customized view of restricted transactions recorded into a blockchain. In operation, user 1110 signs sports bet 1130 with user 1111. A record of sports bet 1130 is transferred from the users to database 1140 indicating the predicted teams and the driver's license number of users 1110-1111. The record is then maintained in blockchain 1160 via server 1150. It should be noted that in this scenario, the transaction also initiates a transfer from sports scoring committee 1132 to database 1142 indicating the official score of the game. The official score of the game is transferred to database 1142 and maintained in blockchain 1160 via server 1150.

[00102] In a next operation, sporting bet management user 1170 may request to see the predicted results along with the official score of the game from blockchain 1160. User 1170 may not be authorized to view the driver's licenses of each of users 1110-111. Server 1150 may receive the request and process an access code indicating that at this point in time, user 1170 is only authorized to view the predicted results of each of users 1110-1111 and the official score. A customized view of the record is then generated by server 1150 indicating only the predicted results and the official score for user 1170. Although user 1170 is unable to see the full record of the transaction, user 1170 is able to trust that the portion of the record indicating that users 1110-1111 have a valid driver's license on file since this data has been maintained in blockchain 1160.

[00103] Figure 12 illustrates an alternative operational architecture in an implementation of an inventory tracking scenario to generate a customized view of restricted transactions recorded into a blockchain. In operation, user 1210 transfers cargo of packages 1230 to user 1220 to be delivered to various users, including user 1270 tracking Package A. A record of the departure time transaction for cargo of packages 1230 is transferred from user 1210 to database 1240 indicating the departure time of Package A and Package B. The record is then maintained in blockchain 1260 via server 1250. It should be noted that in this scenario, the arrival time transaction for cargo of packages 1230 is also recorded on the receiving end by user 1220 where

a record of the transaction indicating the arrival time of Package A and Package B is transferred to database 1242 and maintained in blockchain 1260 via server 1250.

[00104] In a next operation, user tracking Package A 1270 requests to view the departure time and arrival time recorded for Package A. User 1270 may not be authorized to view the departure time and arrival time recorded for Package B. Server 1250 may receive the request and process an access code indicating that at this point in time, user 1270 is only authorized to view the departure time and arrival time recorded for Package A. A customized view of the record is then generated for user 1270 by server 1250 indicating only departure time and arrival time recorded for Package A.

[00105] Figure 13 illustrates an exemplary customized view of restricted transaction recorded into a blockchain. Figure 13 includes computing system 1301 comprises one or more devices capable of running a blockchain application natively or in the context of a web browser, streaming an application, or executing an application in any other manner. Computing system 1301 may include various hardware and software elements in a supporting architecture suitable for generating a customized view of a payroll transaction record. One such representative architecture is illustrated in Figure 16 with respect to controller 1600.

[00106] Computing system 1301 also includes blockchain application component 1302 capable of maintaining a complete record of the blockchain transactions in accordance with the processes described herein. User interface 1303 includes customized view 1310 which may be produced by blockchain application component. User interface 110 may display portions of data from a block entry which a user is authorized to view. The user may initiate initially only have access to view public portions of the block entry, such as the name of each employee who is on the payroll.

[00107] An encryption code may then be transferred in a request to view permissive portions of data. Once computing system 1301 verifies the encryption code, permissive portions of data may be added to customized view 1310. The permissive portions of data include the wages and birthdates of each employees on the payroll transaction. However, the social security numbers of each of the employees may remain private and therefore, the user will be unable to view the social security data in customized view 1310.

[00108] Figure 14 illustrates an alternative exemplary customized view of restricted transaction recorded into a blockchain. Figure 14 includes server node 1401 storing a copy of blockchain 1402. Blockchain 1402 stores blocks which have been chain using hash codes,

such as blocks 1410 and 1412. Each block contains transactions which may be further broken down into portions of data. For example, block 1412 stores online poker game bet entry 1420. Bet entry 1420 includes names of each of the players, a bet amount for each of the players, an amount of funds each player has available to make the bet, and a player rank index. It should be noted that additional data may also be included in block 1412, such as game statistics, win/loss percentages, etc.

[00109] For each user access the bet entry, a check mark is included to indicate which portions of data may be viewed by each of the users. For example, Sue is accessing the poker game bet entry using mobile device 1430. In this example scenario, Sue is authorized to view each of the names of the players and the bet amounts since the names and bet amounts are accessible to the public. Sue is also allowed private access to her own funds amount and rank. However, Sue does not have access to the available funds and rank of the other players. As can be seen in the customized view displayed on mobile device 1430, Sue views authorized data portions 1440 and is blocked from viewing unauthorized data portions 1441.

[00110] Figure 15 illustrates an alternative operational architecture in an implementation of a data access system capable of providing a customized view of restricted or sensitive data recorded into a blockchain. As illustrated in Figure 15, users 1510A-1510N can use various electronic devices to request access to a document, electronic record, physical location (e.g., safe, room, building, area, etc.), or information. For example, in accordance with various embodiments users 1510A-1510N may have difference access levels such as security clearance that grants the user access to classified information (e.g., state or organizational secrets) or to restricted areas. Typically, a security clearance (e.g., classified, secret, top secret, etc.) is not sufficient to gain access to all documents and/or data. Instead, the individual must also have a need to know the specific information.

[00111] The request can be submitted to access control framework 1520 which can translate and validate the requests from different systems (e.g., application, key card system, fingerprint readers, biometric devices, passwords, multi-factor authentication, and the like). Upon validation, the access control framework can submit the request to security applicator 1530 which can process the request using various security protocols. For example, the security level of the requests document or location may require additional multiple validations (e.g., password and hardware device, biometrics, location verification, PINs, passwords, etc.). Security application, in some embodiments, may pull this information from a field or metadata within a block on a blockchain associated with the data.

[00112] The document or data 1550A-1550B stored in blockchain 1540 may have different fields or portions that can be accessed by different individuals with differing "needs to know" or access levels (e.g., a compliance officer vs. a lower level employee of a company, individual with higher security clearance level vs. one with a lower security clearance level, etc.). For example, in some embodiments, various redaction mappings may be stored in the blockchain and applied by document generator 1560 before being presented to users 1510A-1510N. As such, two users requesting the same document or data may be presented with different results.

[00113] As an example, a freedom of information access request may yield redacted documents which have been deemed as available to the public while an individual with security clearance and a need to know will be presented with a different level of access. In accordance with various embodiments an initial request may be received from a user. The system can identify the information that is compliant with the request and set a timer period for responding to the request (e.g., 30 days) to the FOIA request. The system can then determine whether each piece of information compliant with the request has any classification restrictions. If any of the information is determined to be unrestricted (e.g., no classification levels), then the system can respond to the user who made the request with a response that includes information without inspection. This type of feature reduces the workload of governmental employees and ensures that the time period for response is met (e.g., by prioritizing and reassigning review among employees). In some embodiments, if enough time remains, the system may request a human review and approve the included information before sending.

[00114] When the system identifies confidential information, the system would next evaluate the access and clearance. If for example, the person requesting the data had a higher access/clearance than an administrator, then the information would be automatically sent. If redactions need to be made to comply with the security clearance, then document generator 1560 may apply any redactions needed and/or remove documents that should not be included in the response. While not illustrated in Figure 15, some embodiments may include a machine learning/artificial intelligence component to review the data and/or metadata and identify portions that should not be included.

[00115] Other embodiments may have other types of individuals seeking varying information (e.g., people seeking information on a gambler, a banking client, regulators performing audits, etc.). Many such use cases exist. Also, some embodiments may use decentralized applications (Dapps) that have backend code running on a decentralized peer-to-

peer network to submit the request, retrieve information from the blockchains, and communicate with other applications (e.g., other Dapps).

[00116] Security applicator 1530 may also review the status of the credentials or security level of the user. The record of the user may be stored on blockchain 1545. For example, information regarding background checks, bank account information, travel information, projects the user is associated with (past and present), family history, medical history, credentials, biometrics, passwords, signatures, and the like can be stored on in the user's record. Security applicator 1530 may retrieve that information and utilize the information in generating the customized view of the data or document.

[00117] Figure 16 illustrates a block diagram illustrating an example machine representing the computer systemization of the host computer system. Controller 1600 may be in communication with entities including one or more users 1625 client/terminal devices 1620, user input devices 1605, peripheral devices 1610, optional co-processor device(s) (e.g., cryptographic processor devices) 1615, and networks 1630. Users may engage with controller 1600 via terminal devices 1620 over networks 1630. In some embodiments, all or a portion of the communications between terminal devices 1620 and controller 1600 can be encrypted. Various laws, standards, or best practices may require cryptography for storing, transmitting, and/or utilization of various types data, information, code, signaling, etc.

[00118] Computers may employ central processing units (CPUs) or processors to process information. Processors may include programmable general-purpose or special-purpose microprocessors, programmable controllers, application-specific integrated circuits (ASICs), programmable logic devices (PLDs), embedded components, a combination of such devices and the like. Processors execute program components in response to user and/or system-generated requests. One or more of these components may be implemented in software, hardware or both hardware and software. Processors pass instructions (e.g., operational and data instructions) to enable various operations.

[00119] Controller 1600 may include clock 1665, CPU 1670, memory such as read only memory (ROM) 1685 and random access memory (RAM) 1680 and co-processor 1675 among others. These controller components may be connected to a system bus 1660, and through the system bus 1660 to an interface bus 1635. Further, user input devices 1605, peripheral devices 1610, co-processor devices 1615, and the like, may be connected through the interface bus 1635 to the system bus 1660. The interface bus 1635 may be connected to a number of interface

adapters such as processor interface 1640, input output interfaces (I/O) 1645, network interfaces 1650, storage interfaces 1655, and the like.

[00120] Processor interface 1640 may facilitate communication between co-processor devices 1615 and co-processor 1675. In one implementation, processor interface 1640 may expedite encryption and decryption of requests or data. Input output interfaces (I/O) 1645 facilitate communication between user input devices 1605, peripheral devices 1610, co-processor devices 1615, and/or the like and components of controller 1600 using protocols such as those for handling audio, data, video interface, wireless transceivers, or the like (e.g., Bluetooth®, IEEE 894a-b, serial, universal serial bus (USB), Digital Visual Interface (DVI),802.11a/b/g/n/x, cellular, etc.). Network interfaces 1650 may be in communication with the network 1630. Through the network 1630, controller 1600 may be accessible to remote terminal devices 1620. Network interfaces 1650 may use various wired and wireless connection protocols such as, direct connect, Ethernet, wireless connection such as IEEE 802.11a-x, miracast and the like. Some components of the interactive gaming system may include various protocols or comply with various standards or certifications set forth by different associations or regulatory agencies. For example, some embodiments may use the slot accounting system (SAS) protocol or comply with the game to system (G2S) standard.

[00121] Examples of network 1630 include the Internet, Local Area Network (LAN), Metropolitan Area Network (MAN), a Wide Area Network (WAN), wireless network (e.g., using Wireless Application Protocol WAP), a secured custom connection, and the like. The network interfaces 1650 can include a firewall which can, in some aspects, govern and/or manage permission to access/proxy data in a computer network, and track varying levels of trust between different machines and/or applications. The firewall can be any number of modules having any combination of hardware and/or software components able to enforce a predetermined set of access rights between a particular set of machines and applications, machines and machines, and/or applications and applications, for example, to regulate the flow of traffic and resource sharing between these varying entities.

[00122] The firewall may additionally manage and/or have access to an access control list which details permissions including, for example, the access and operation rights of an object by an individual, a machine, and/or an application, and the circumstances under which the permission rights stand. Other network security functions performed or included in the functions of the firewall, can be, for example, but are not limited to, intrusion-prevention, intrusion detection, next-generation firewall, personal firewall, etc., without deviating from the

novel art of this disclosure. It should be appreciated that controller 1600 may be capable of using network interfaces 1650 to transfer and receive payment amounts. The payment may be driven by an application executed by controller 1600, such as a National Fighting Club (NFC) application tap using Bluetooth®.

[00123] Storage interfaces 1655 may be in communication with a number of storage devices such as, storage devices 1690, removable disc devices, and the like. The storage interfaces 1655 may use various connection protocols such as Serial Advanced Technology Attachment (SATA), IEEE 894, Ethernet, Fiber, Universal Serial Bus (USB), and the like.

[00124] User input devices 1605 and peripheral devices 1610 may be connected to I/O interface 1645 and potentially other interfaces, buses and/or components. User input devices 1605 may include card readers, finger print readers, joysticks, keyboards, microphones, mouse, remote controls, retina readers, touch screens, sensors, and/or the like. Peripheral devices 1610 may include antenna, audio devices (e.g., microphone, speakers, *etc.*), cameras, external processors, communication devices, radio frequency identifiers (RFIDs), scanners, printers, storage devices, transceivers, and/or the like. Co-processor devices 1615 may be connected to controller 1600 through interface bus 1635, and may include microcontrollers, processors, interfaces or other devices.

[00125] Computer executable instructions and data may be stored in memory (e.g., registers, cache memory, random access memory, flash, *etc.*) which is accessible by processors. These stored instruction codes (e.g., programs) may engage the processor components, motherboard and/or other system components to perform desired operations. Controller 1600 may employ various forms of memory including on-chip CPU memory (e.g., registers), RAM 1680, ROM 1685, and storage devices 1690. Storage devices 1690 may employ any number of tangible, non-transitory storage devices or systems such as fixed or removable magnetic disk drive, an optical drive, solid state memory devices and other processor-readable storage media. Computer-executable instructions stored in the memory may include an interactive gaming platform having one or more program modules such as routines, programs, objects, components, data structures, and so on that perform particular tasks or implement particular abstract data types. For example, the memory may contain operating system (OS) component 1695, modules and other components, database tables, and the like. These modules/components may be stored and accessed from the storage devices, including from external storage devices accessible through an interface bus 1635.

[00126] The database components can store programs executed by the processor to process the stored data. The database components may be implemented in the form of a database that is relational, scalable and secure. Examples of such database include DB2, MySQL, Oracle, Sybase, and the like. Alternatively, the database may be implemented using various standard data-structures, such as an array, hash, list, stack, structured text file (e.g., XML), table, and/or the like. Such data-structures may be stored in memory and/or in structured files.

[00127] Controller 1600 may be implemented in distributed computing environments, where tasks or modules are performed by remote processing devices, which are linked through a communications network, such as a Local Area Network ("LAN"), Wide Area Network ("WAN"), the Internet, and the like. In a distributed computing environment, program modules or subroutines may be located in both local and remote memory storage devices. Distributed computing may be employed to load balance and/or aggregate resources for processing. Alternatively, aspects of controller 1600 may be distributed electronically over the Internet or over other networks (including wireless networks). Those skilled in the relevant art(s) will recognize that portions of the interactive gaming system may reside on a server computer, while corresponding portions reside on a client computer. Data structures and transmission of data particular to aspects of controller 1600 are also encompassed within the scope of the disclosure.

[00128] Certain inventive aspects may be appreciated from the foregoing disclosure, of which the following are various examples.

[00129] The functional block diagrams, operational scenarios and sequences, and flow diagrams provided in the Figures are representative of exemplary systems, environments, and methodologies for performing novel aspects of the disclosure. While, for purposes of simplicity of explanation, methods included herein may be in the form of a functional diagram, operational scenario or sequence, or flow diagram, and may be described as a series of acts, it is to be understood and appreciated that the methods are not limited by the order of acts, as some acts may, in accordance therewith, occur in a different order and/or concurrently with other acts from that shown and described herein. Those skilled in the art will understand and appreciate that a method could alternatively be represented as a series of interrelated states or events, such as in a state diagram. Moreover, not all acts illustrated in a methodology may be required for a novel implementation.

CLAIMS

What is claimed is:

1. A computer apparatus comprising:

one or more computer readable storage media;

one or more processors operatively coupled to the one or more computer readable storage media; and

program instructions stored on the one or more computer readable storage media that, when executed by the one or more processors, direct the one or more processors to at least:

maintain a blockchain of block entries requested by a plurality of users from user devices in a distributed network of nodes,

wherein the block entries each comprise a plurality of data portions that are each associated with an access level;

receive a request to view one or more data portions of a block entry wherein the request comprises an access code associated with at least one access level;

evaluate the access code in the request with the blockchain of block entries to identify one or more data portions associated with the access level; and

generate a customized view of the block entry including the one or more data portions associated with the access level.

2. The computer apparatus of claim 1, wherein to evaluate the access code in the request with the blockchain of block entries comprises the one or more processors configured to process an encrypted code to validate access to view the one or more data portions associated with the access level.

3. The computer apparatus of claim 1, further comprising the one or more processors configured to maintain a pointer for each of the plurality of data portions in the block entries indicating at least one published location in the distributed network of nodes for each of the plurality of data portion in the block entries; and

wherein to generate the customized view of the block entry including the one or more data portions associated with the access level comprises the one or more processors configured to retrieve the one or more data portions associated with

the access level using the pointer for each of the plurality of data portions in the block entries.

4. The computer apparatus of claim 1, wherein:

to maintain the blockchain of block entries requested by the plurality of users from the user devices comprises the one or more processors configured to maintain a separate block entry for the one or more data portions associated with each of the access levels; and

to evaluate the access code in the request with the blockchain of block entries to identify the one or more data portions associated with the access level comprises the one or more processors configured to process the access code to validate access to view one of the blockchains for the one or more data portions associated with each of the access levels.

5. The computer apparatus of claim 1, wherein:

to maintain the blockchain of block entries requested by the plurality of users from the user devices comprises the one or more processors are configured to maintain a separate blockchain for the one or more data portions associated with each of the access levels; and

to evaluate the access code in the request with the blockchain of block entries to identify the one or more data portions associated with the access level comprises the one or more processors are configured to process the access code to validate access to view one of the blockchains for the one or more data portions associated with each of the access levels.

6. The computer apparatus of claim 1, wherein the received request to view the at least the data portion of the block entry comprises an inventory tracking request to view the at least the data portion of the block entry.

7. The computer apparatus of claim 1, wherein the received request to view the at least the data portion of the block entry comprises a financial auditing request to view the at least the data portion of the block entry.

8. The computer apparatus of claim 1, wherein the received request to view the at least the data portion of the block entry comprises a gaming regulation request to view the at least the data portion of the block entry.

9. The computer apparatus of claim 1, wherein the access level associated with the at least the data portion of the block entry comprises at least one of a private access level, a permissive access level, and a public access level.

10. A method for generating a customized view of blockchain transactions comprising:

maintaining a blockchain of block entries requested by a plurality of users from user devices in a distributed network of nodes,

wherein the block entries each comprise a plurality of data portions that are each associated with an access level;

receiving a request to view one or more data portions of a block entry,

wherein the request comprises an access code associated with at least one access level;

evaluating the access code in the request with the blockchain of block entries to identify one or more data portions associated with the access level; and

generating a customized view of the block entry including the one or more data portions associated with the access level.

11. The method of claim 10, wherein evaluating the access code in the request with the blockchain of block entries comprises processing an encrypted code to validate access to view the one or more data portions associated with the access level.

12. The method of claim 10, further comprising maintaining a pointer for each of the plurality of data portions in the block entries indicating at least one published location for each of the plurality of data portion in the block entries; and

wherein generating the customized view of the block entry including the one or more data portions associated with the access level comprises retrieving the one or more data portions associated with the access level using the pointer for each of the plurality of data portions in the block entries.

13. The method of claim 10, wherein:

maintaining the blockchain of block entries requested by the plurality of users from the user devices comprises maintaining a separate block entry for the one or more data portions associated with each of the access levels; and

evaluating the access code in the request with the blockchain of block entries to identify the one or more data portions associated with the access level comprises processing the access code to validate access to view one of the blockchains for the one or more data portions associated with each of the access levels.

14. The method of claim 10, wherein:

maintaining the blockchain of block entries requested by the plurality of users from the user devices comprises maintaining a separate blockchain for the one or more data portions associated with each of the access levels; and

evaluating the access code in the request with the blockchain of block entries to identify the one or more data portions associated with the access level comprises processing the access code to validate access to view one of the blockchains for the one or more data portions associated with each of the access levels.

15. The method of claim 10, wherein the received request to view the at least the data portion of the block entry comprises an inventory tracking request to view the at least the data portion of the block entry.

16. The method of claim 10, wherein the received request to view the at least the data portion of the block entry comprises a financial auditing request to view the at least the data portion of the block entry.

17. The method of claim 10, wherein the received request to view the at least the data portion of the block entry comprises a gaming regulation request to view the at least the data portion of the block entry.

18. The method of claim 10, wherein the access level associated with the at least the data portion of the block entry comprises at least one of a private access level, a permissive access level, and a public access level.

19. The method of claim 10, wherein the access level associated with the data portion includes a security clearance level.

20. The method of claim 19, wherein the block entry includes redaction mappings based on the security clearance level and the method further includes applying the redaction mapping to obfuscate some of the one or more data portions of the block entry.

21. The method of claim 10, wherein the block entry includes multiple redaction mapping based on the at least one access level.

22. A method comprising:

receiving a request from a user to view one or more data portions of a block entry, wherein the request from the user is associated with at least one access level;

creating a customized view, based on the at least one access level associated with the user, of the one or more data portions of the block entry.

23. The method of claim 22, wherein the at least one access level includes a security clearance level.

24. The method of claim 23, wherein the block entry includes redaction mappings based on the at least one access level and the method further includes applying the redaction mapping to obfuscate some of the one or more data portions of the block entry.

25. The method of claim 24, wherein the block entry includes multiple redaction mapping based on the at least one access level.

26. A system comprising:

a blockchain having multiple block entries; and

a data platform configured to -

receive a request from to view one or more data portions from one of the multiple block entries,

wherein the request is associated with at least one access level;

access the blockchain to retrieve the one or more data portions corresponding to the at least one access level; and

create a customized view, based on the at least one access level, of the one or more data portions of the block entry.

27. The system of claim 26, wherein the blockchain includes a private blockchain, a public blockchain, or a hybrid blockchain.

28. The system of claim 26, further comprising an artificial intelligence or machine learning engine to ingest the one or more data portions when the one or more data portions are added to the blockchain and automatically audit the multiple block entries.

29. The system of claim 26, wherein the data platform creates the customized view by decrypting the one or more data portions.

30. A method comprising:

maintaining a distributed ledger of transactions by a plurality of users from devices, wherein the transactions each comprise a plurality of transaction segments each associated with an authorization level;

receiving a request to view one or more transaction segments wherein the request comprises an access identifier associated with the view of the one or more transaction segments of the transaction;

evaluating the access identifier in the request with the view of the one or more transaction segments of transactions to identify one or more transaction segments associated with the access identifier; and

generating a customized view of the transaction including the one or more transaction segments associated with the access identifier.

31. One or more non-transitory computer readable storage media having program instructions stored thereon, wherein the program instructions, when executed by a processing system, direct the processing system to at least:

maintain a blockchain of block entries requested by a plurality of users from user devices, wherein the block entries each comprise a plurality of data portions that are each associated with an access level;

receive a request to view one or more data portions of a block entry wherein the request comprises an access code associated with at least one access level;

evaluate the access code in the request with the blockchain of block entries to identify one or more data portions associated with the access level; and

generate a customized view of the block entry including the one or more data portions associated with the access level.

32. A method for generating a customized view of financial records comprising:

maintaining a blockchain of banking entries requested by a plurality of users from user devices in a distributed network of nodes,

wherein the banking entries each comprise a plurality of account numbers and account amounts that are each associated with an access level;

receiving a request to view one or more account numbers and account amounts of a banking entry,

wherein the request comprises an access code associated with at least one access level;

evaluating the access code in the request with the blockchain of banking entries to identify one or more account numbers or account amounts associated with the access level; and

generating a customized view of the banking entry including the one or more account numbers or account amounts associated with the access level.

33. A method for generating a customized view of medical records comprising:

maintaining a blockchain of patient records requested by a plurality of users from user devices in a distributed network of nodes, wherein the patient records each comprise a plurality of medical diagnosis and treatments that are each associated with an access level;

receiving a request to view one or more medical diagnosis and treatments of a patient record wherein the request comprises an authorization code associated with at least one access level;

evaluating the authorization code in the request with the blockchain of patient records to identify one or more medical diagnosis and treatments associated with the access level; and

generating a customized view of the patient record including the one or more medical diagnosis and treatments associated with the access level.

34. A method for generating a customized view of gaming bets comprising:

maintaining a blockchain of gaming bets requested by a plurality of users from user devices in a distributed network of nodes, wherein the gaming bets each comprise a plurality of player records, predicted outcomes, and bet amounts that are each associated with an access level;

receiving a request to view one or more player records, predicted outcomes, and bet amounts of a gaming bet wherein the request comprises a pin code associated with at least one access level;

evaluating the pin code in the request with the blockchain of gaming bets to identify one or more player records, predicted outcomes, and bet amounts associated with the access level; and

generating a customized view of the gaming bet including the one or more player records, predicted outcomes, and bet amounts associated with the access level.

35. A method for generating a customized view of firearm sales comprising:

maintaining a blockchain of firearm sales requested by a plurality of users from user devices in a distributed network of nodes, wherein the firearm sales each comprise a plurality of purchaser names, ages, and driver's license numbers that are each associated with an access level;

receiving a request to view one or more purchaser names, ages, and driver's license numbers of a firearm sale wherein the request comprises a fingerprint associated with at least one access level;

evaluating the fingerprint in the request with the blockchain of firearm sale to identify one or more purchaser names, ages, and driver's license numbers associated with the access level; and

generating a customized view of the firearm sale including the one or more purchaser names, ages, and driver's license numbers associated with the access level.

36. A method for generating a customized view of pharmaceutical inventory logs comprising:

maintaining a blockchain of pharmaceutical inventory logs entered by a plurality of users from user devices in a distributed network of nodes, wherein the pharmaceutical inventory logs each comprise a plurality of drug manufacturers, distributers, and retailers that are each associated with an access level;

receiving a request to view one or more drug manufacturers, distributers, and retailers of a pharmaceutical inventory log wherein the request comprises a barcode associated with at least one access level;

evaluating the barcode in the request with the blockchain of pharmaceutical inventory logs to identify one or more drug manufacturers, distributers, and retailers associated with the access level; and

generating a customized view of the pharmaceutical inventory log including the one or more drug manufacturers, distributers, and retailers associated with the access level.