



US 20250265643A1

(19) United States

(12) Patent Application Publication

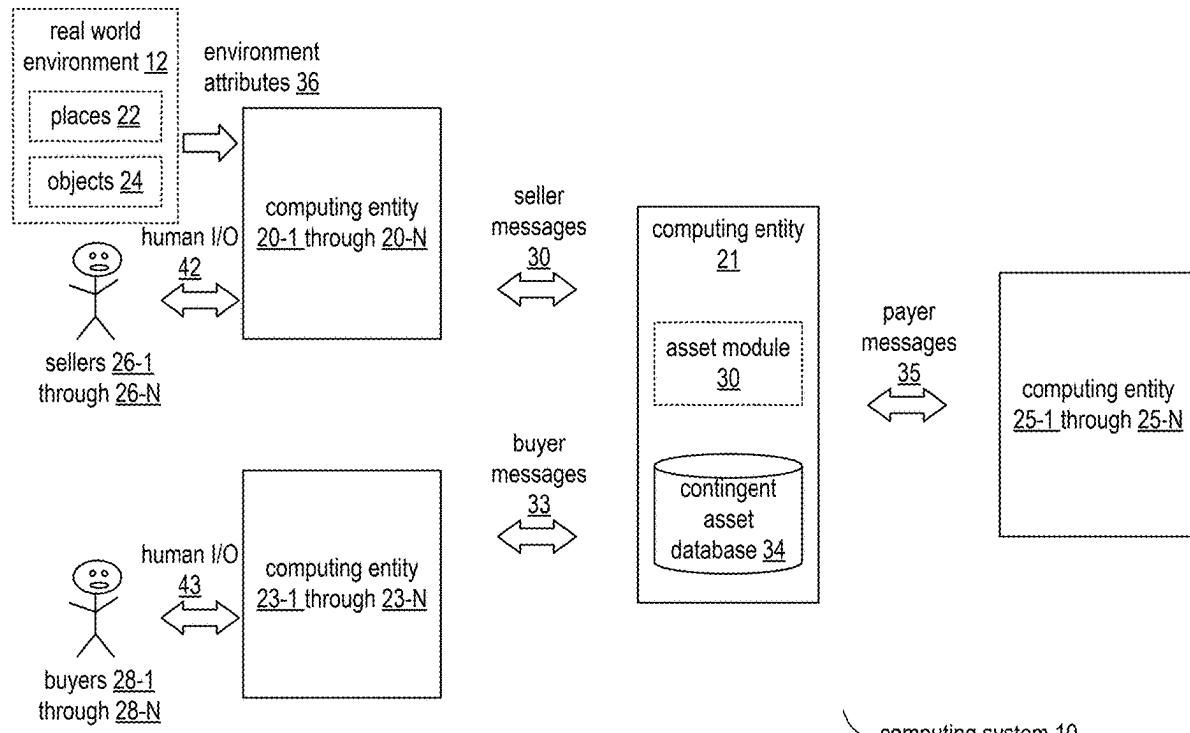
Shannon, III et al.

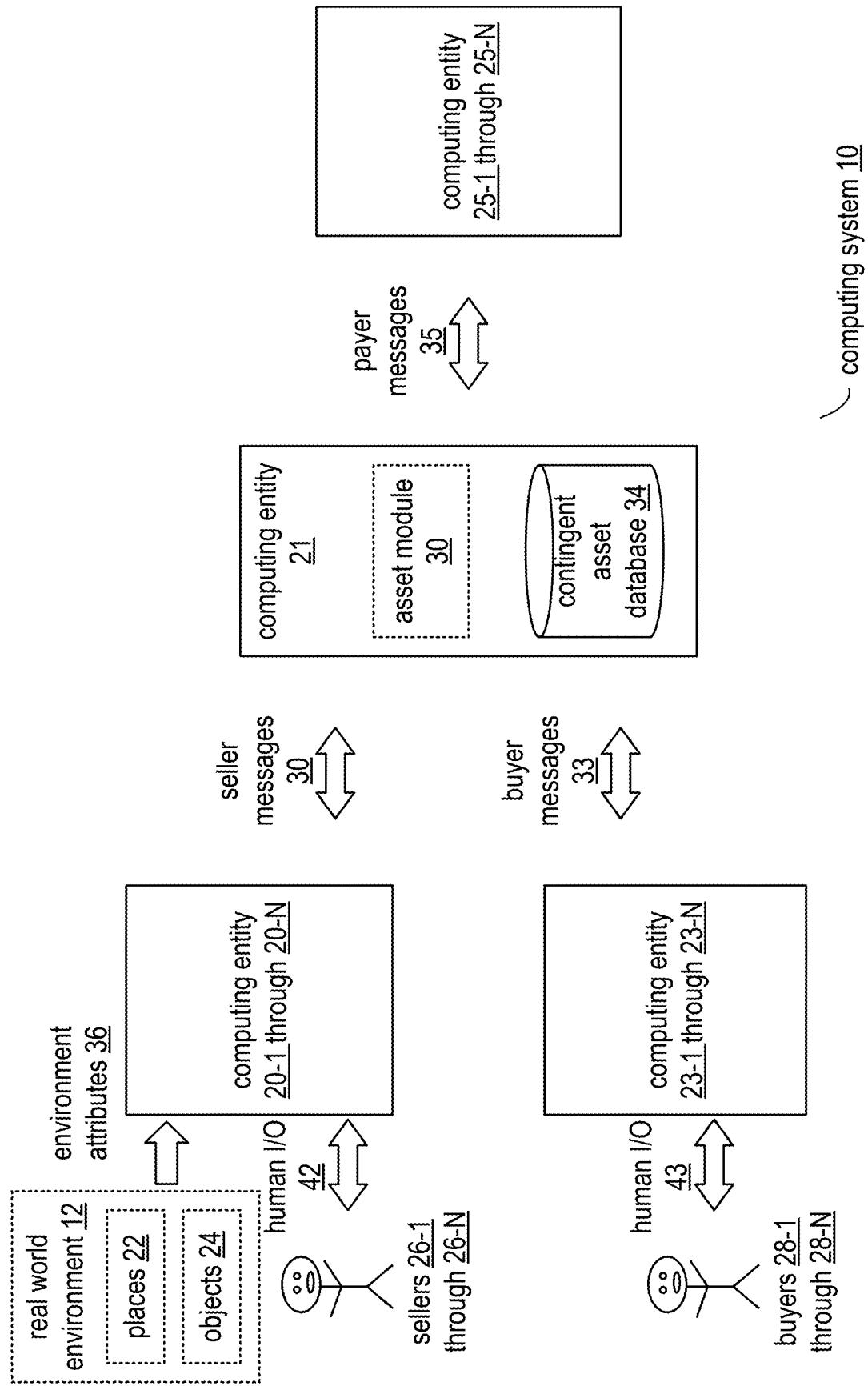
(10) Pub. No.: US 2025/0265643 A1

(43) Pub. Date: Aug. 21, 2025

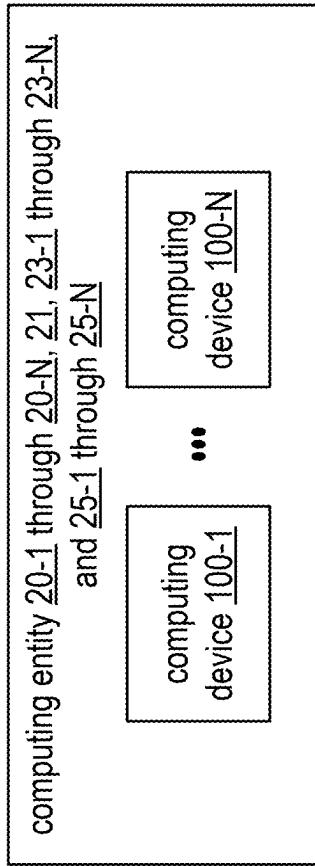
(54) IDENTIFYING A PUBLIC BENEFIT ASSETS  
SECURE TOKEN(60) Provisional application No. 63/215,850, filed on Jun.  
28, 2021.(71) Applicant: **Rebate Assets, LLC**, Rockford, IL  
(US)(72) Inventors: **Peter M. Shannon, III**, Western  
Springs, IL (US); **Gary W. Grube**,  
Barrington Hills, IL (US)(73) Assignee: **Rebate Assets, LLC**, Rockford, IL  
(US)(21) Appl. No.: **19/184,014**(22) Filed: **Apr. 21, 2025****Related U.S. Application Data**(63) Continuation of application No. 18/104,866, filed on  
Feb. 2, 2023, now Pat. No. 12,282,952, which is a  
continuation-in-part of application No. 18/082,758,  
filed on Dec. 16, 2022, now Pat. No. 12,260,402,  
which is a continuation-in-part of application No.  
17/959,919, filed on Oct. 4, 2022, now Pat. No.  
12,124,552, which is a continuation-in-part of appli-  
cation No. 17/842,146, filed on Jun. 16, 2022, now  
Pat. No. 12,062,050.**Publication Classification**(51) **Int. Cl.**  
*G06Q 40/03* (2023.01)  
*G06Q 20/38* (2012.01)  
*G06Q 20/40* (2012.01)(52) **U.S. Cl.**  
CPC ..... *G06Q 40/03* (2023.01); *G06Q 20/3825*  
(2013.01); *G06Q 20/3829* (2013.01); *G06Q*  
*20/389* (2013.01); *G06Q 20/4014* (2013.01)(57) **ABSTRACT**

A method executed by a computing entity includes identifying, based on at least one of a public benefit project type and a public benefit project geographic location of selection criteria for a set of public benefit credit assets, a secure first token on an object distributed ledger representing the set of public benefit credit assets. The method further includes establishing control over the secure first token representing the set of public benefit credit assets, where only a device possessing control over the secure first token may modify the secure first token.

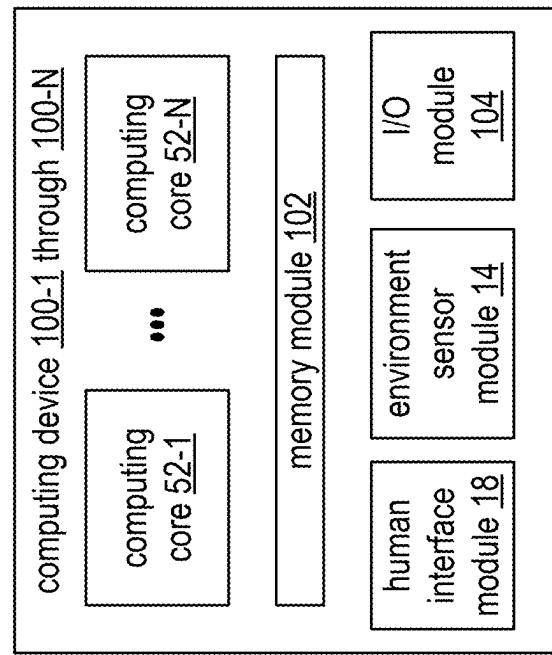




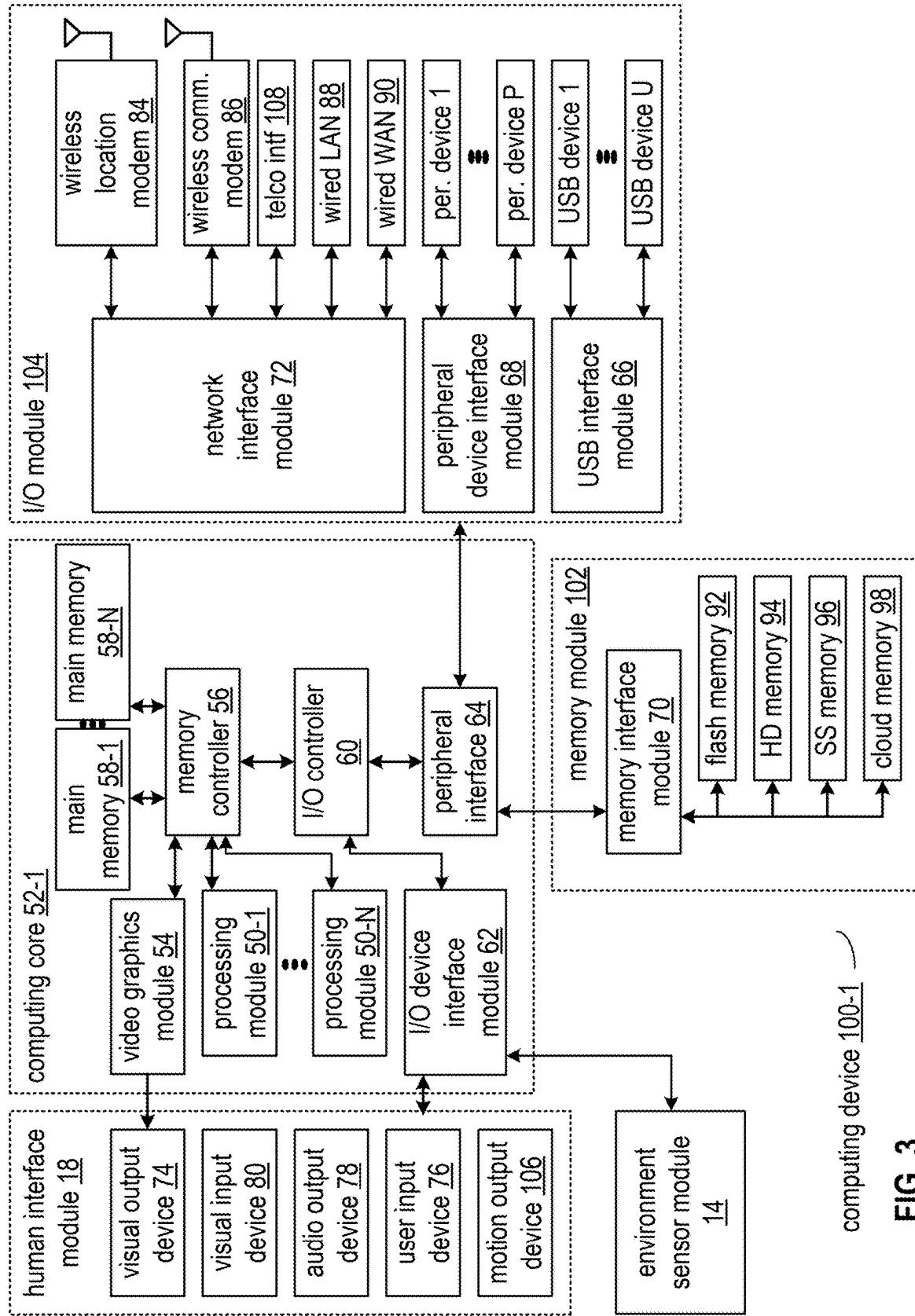
**FIG. 1**



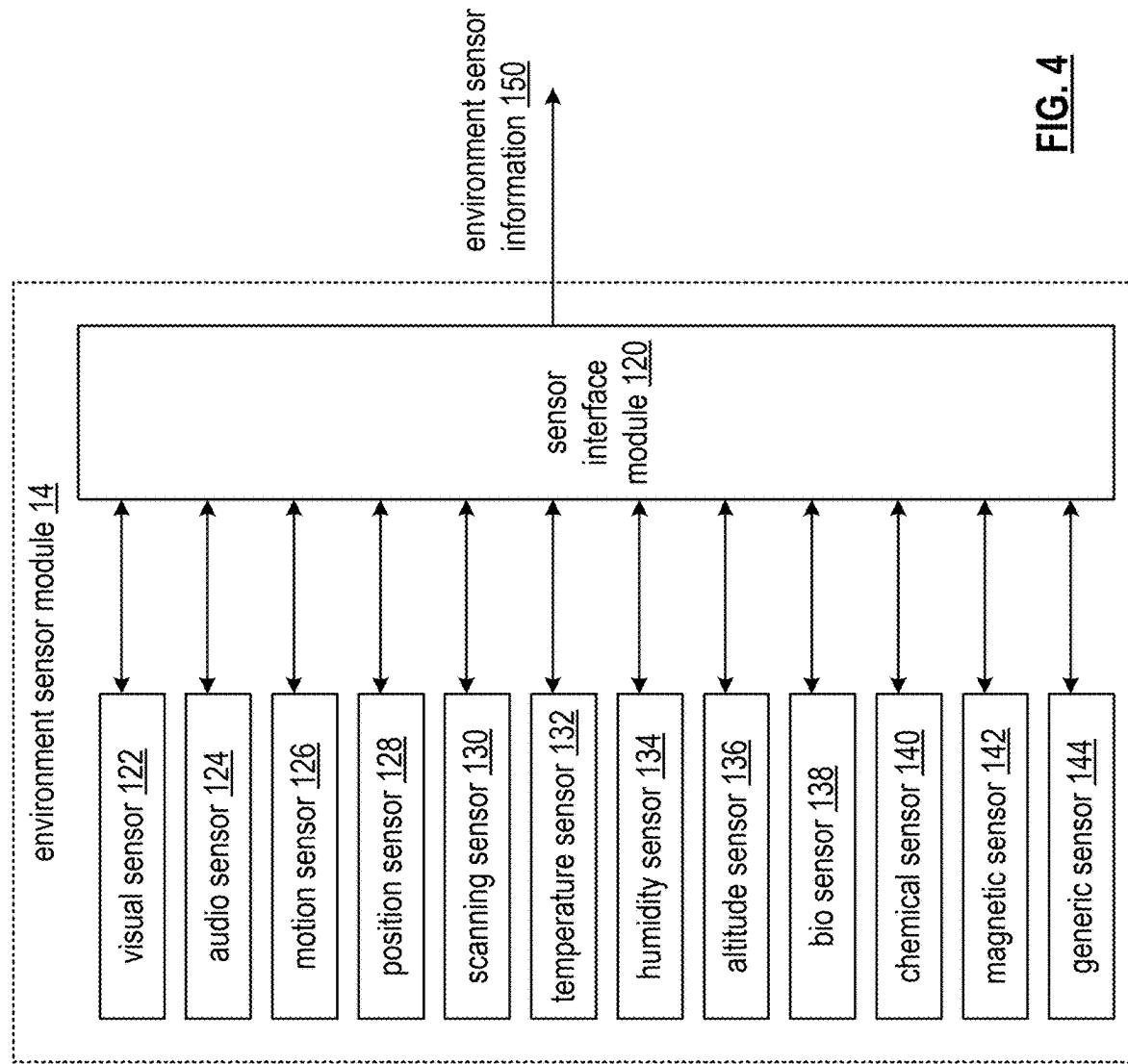
**FIG. 2A**



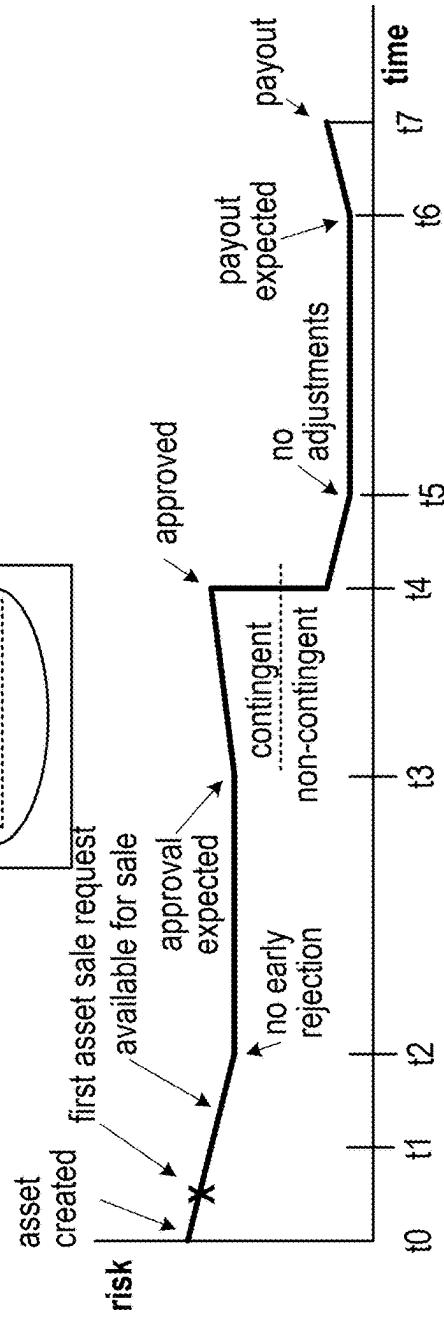
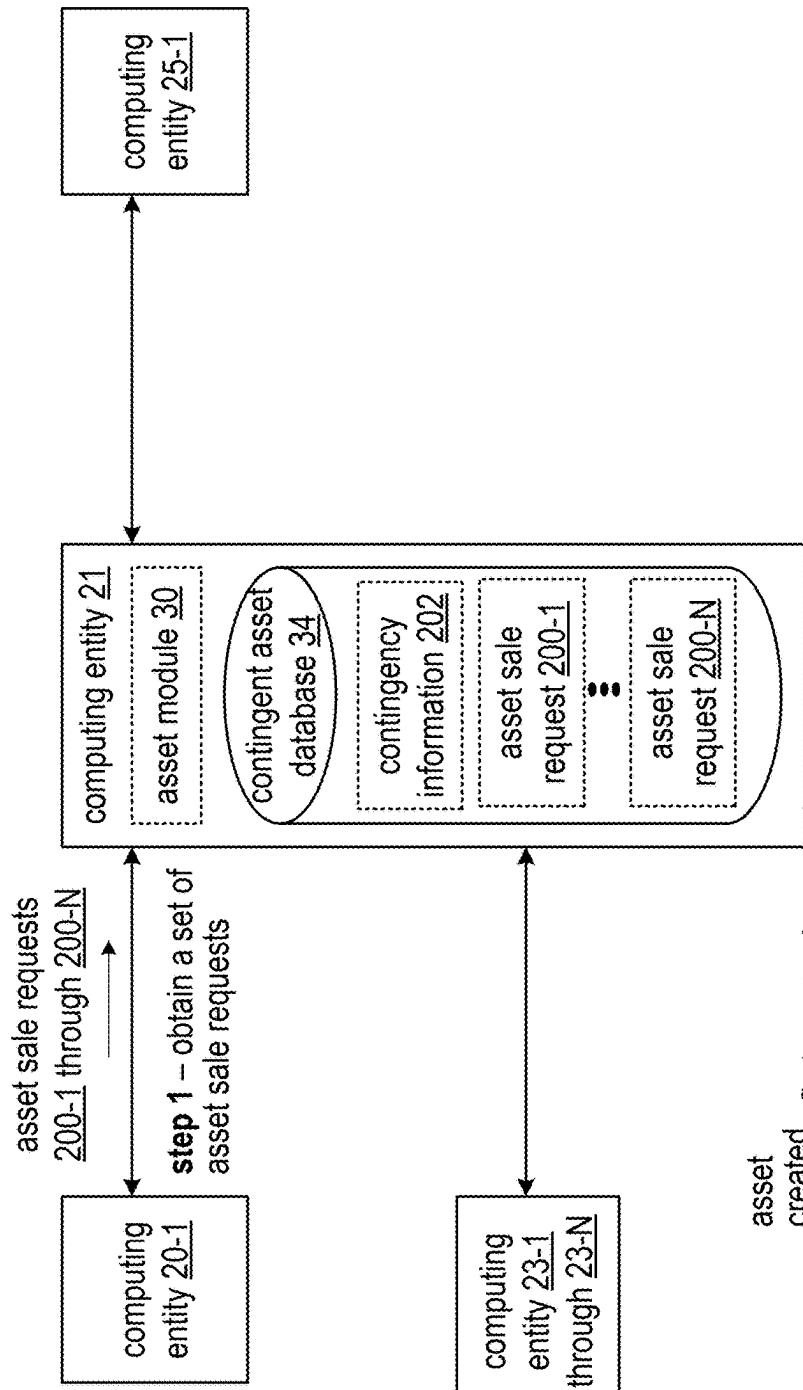
**FIG. 2B**

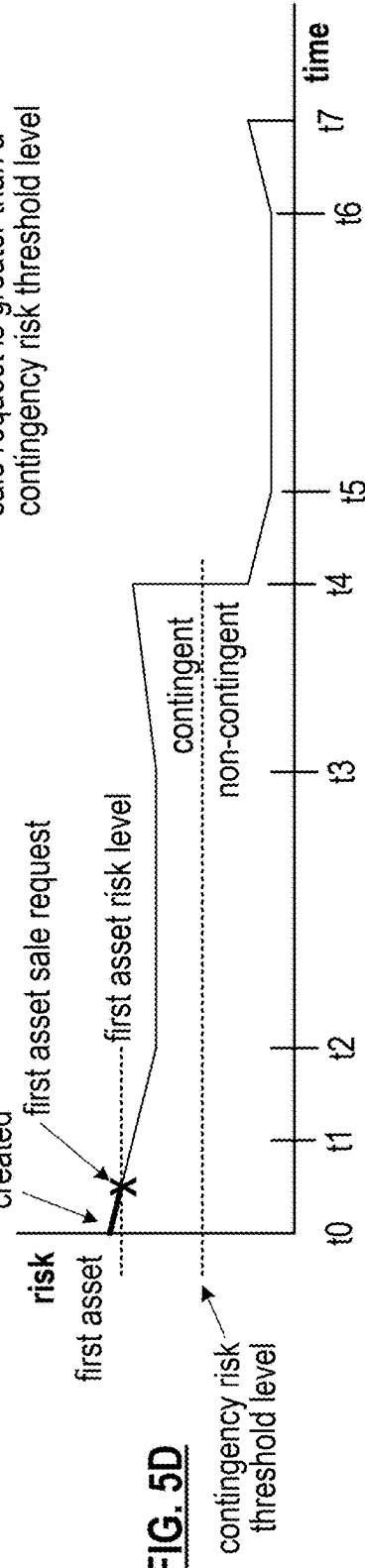
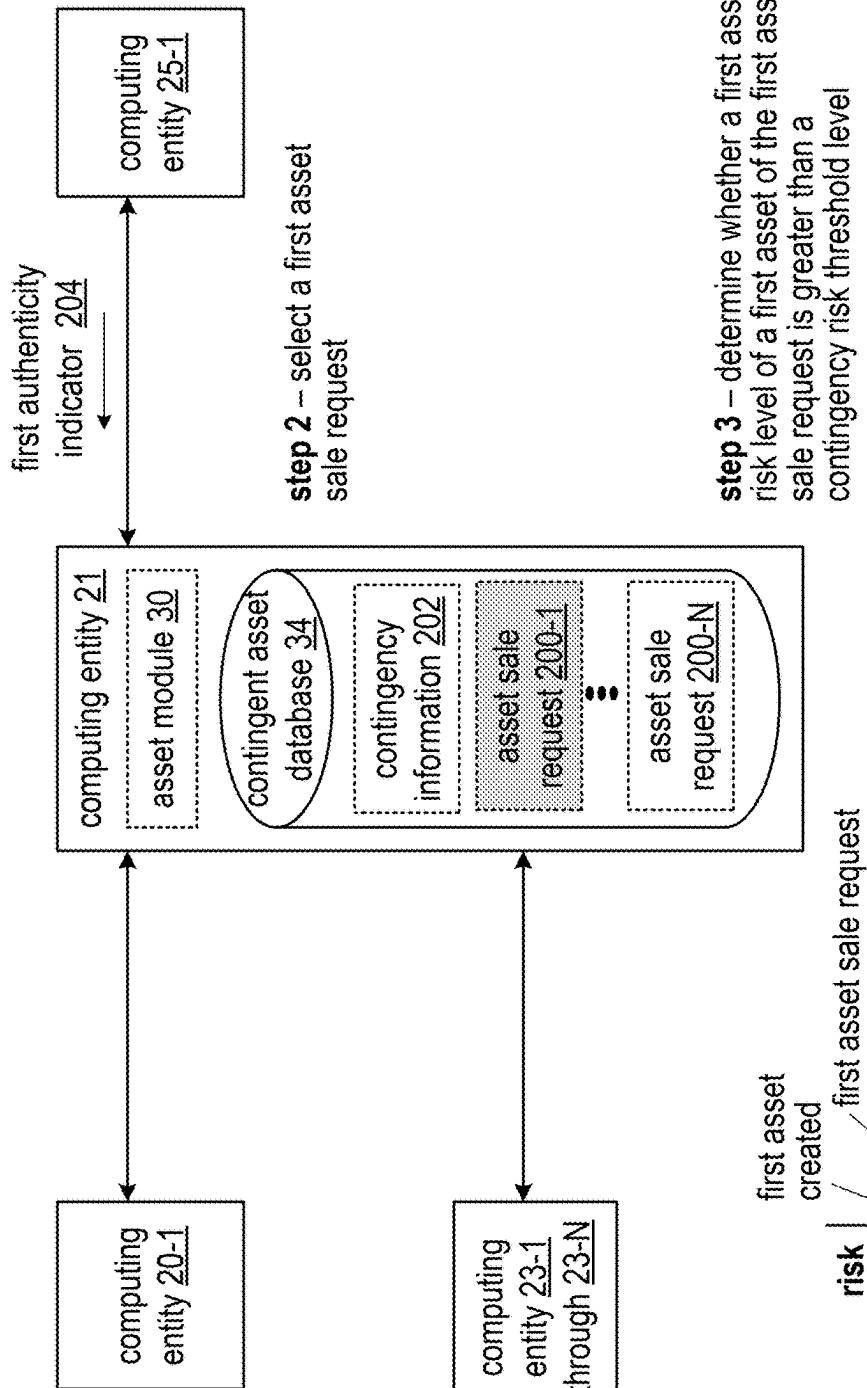


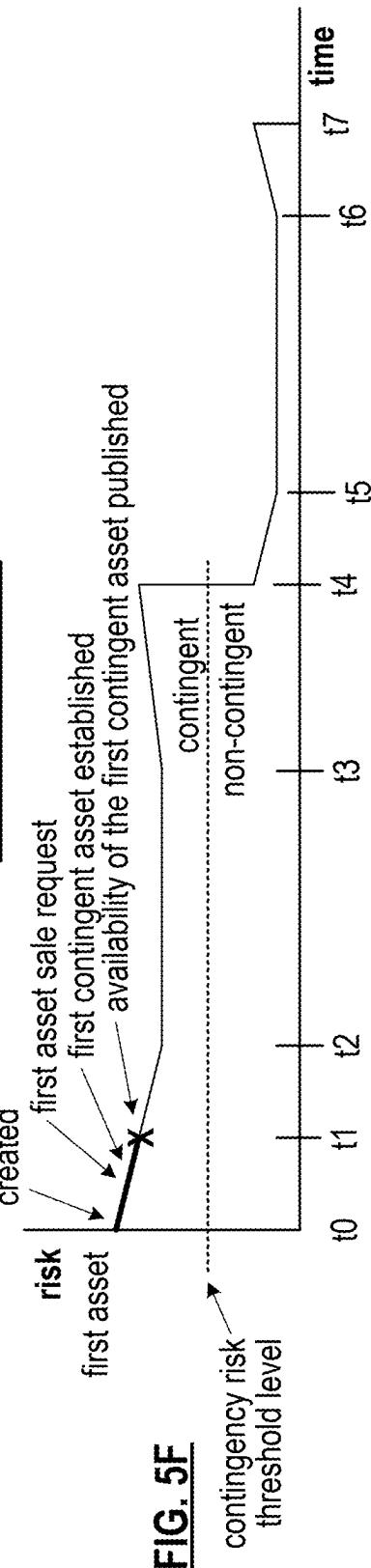
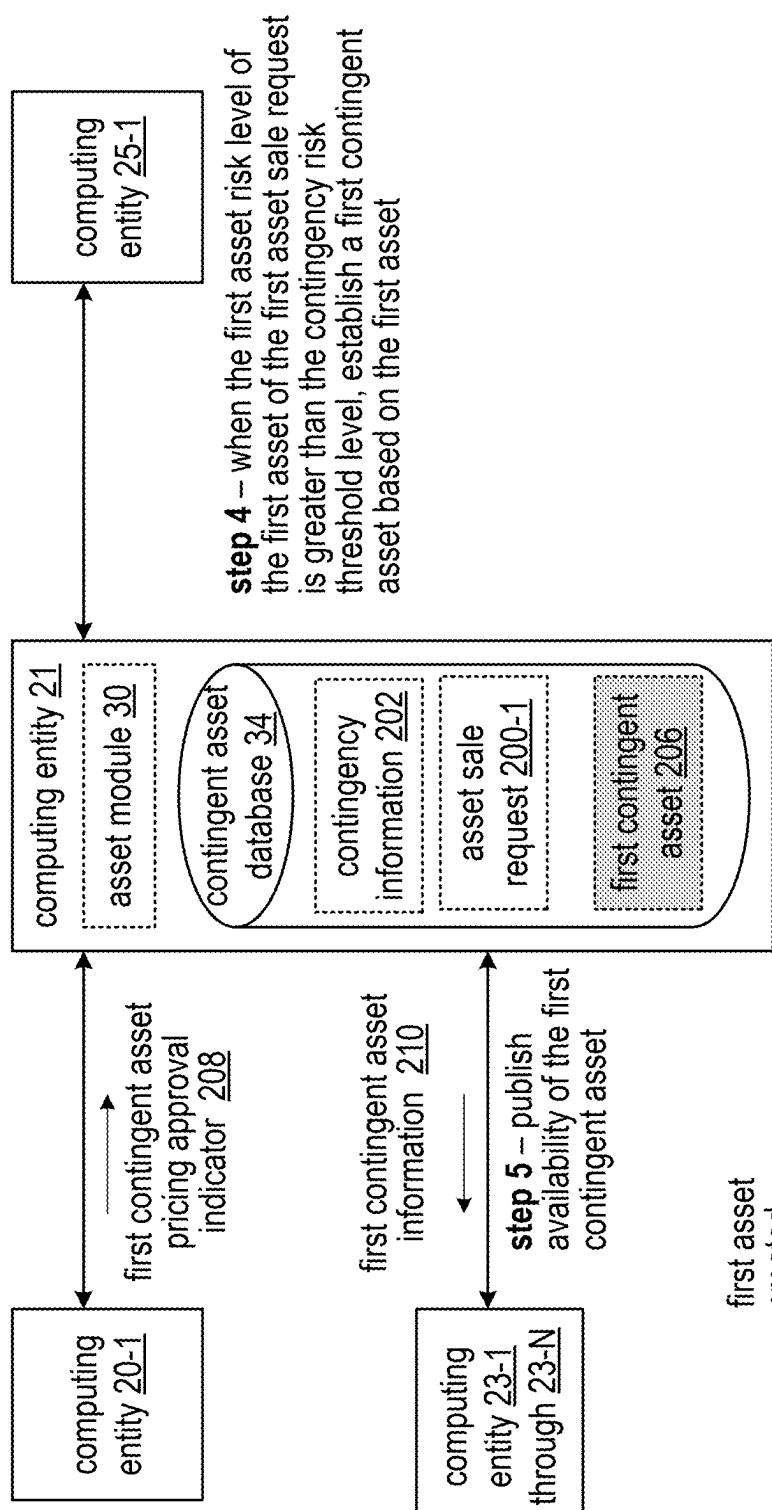
**FIG. 3**

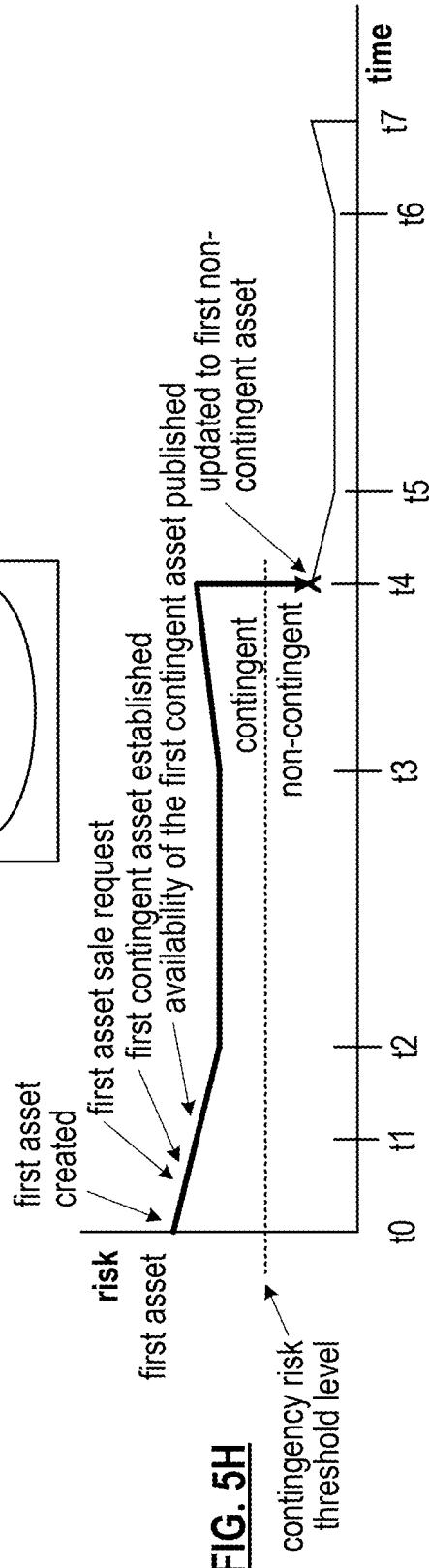
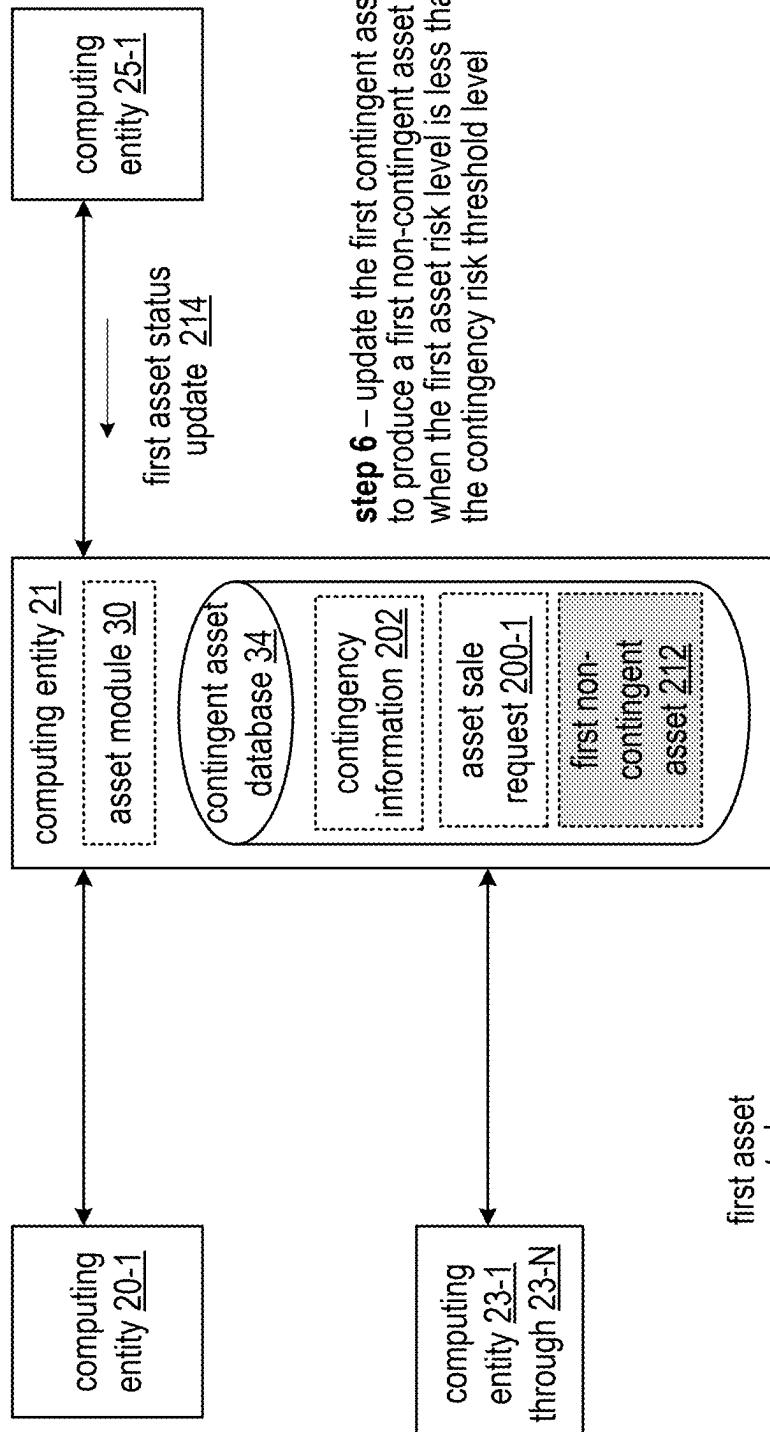


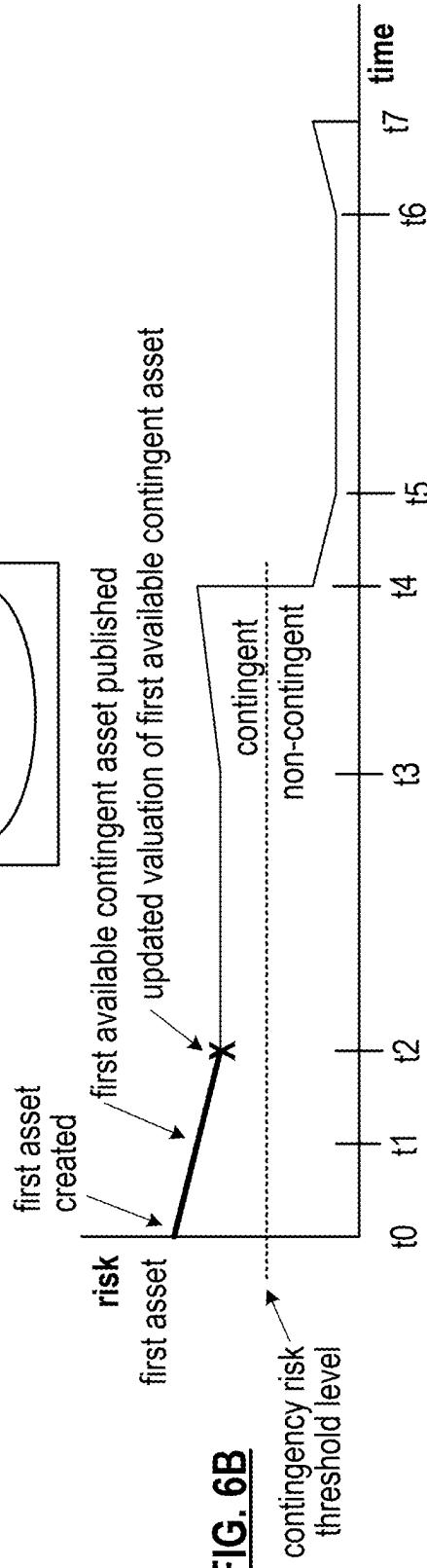
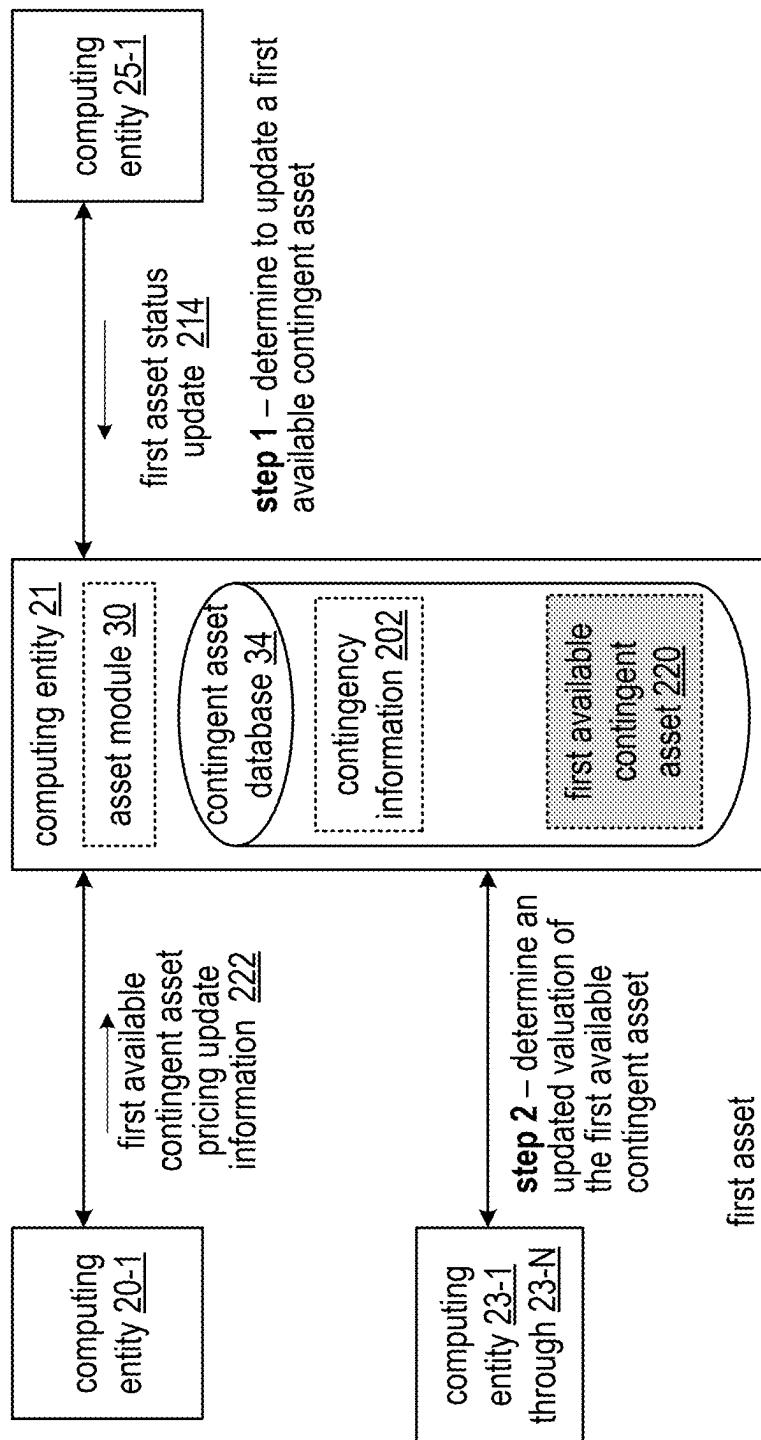
**FIG. 4**

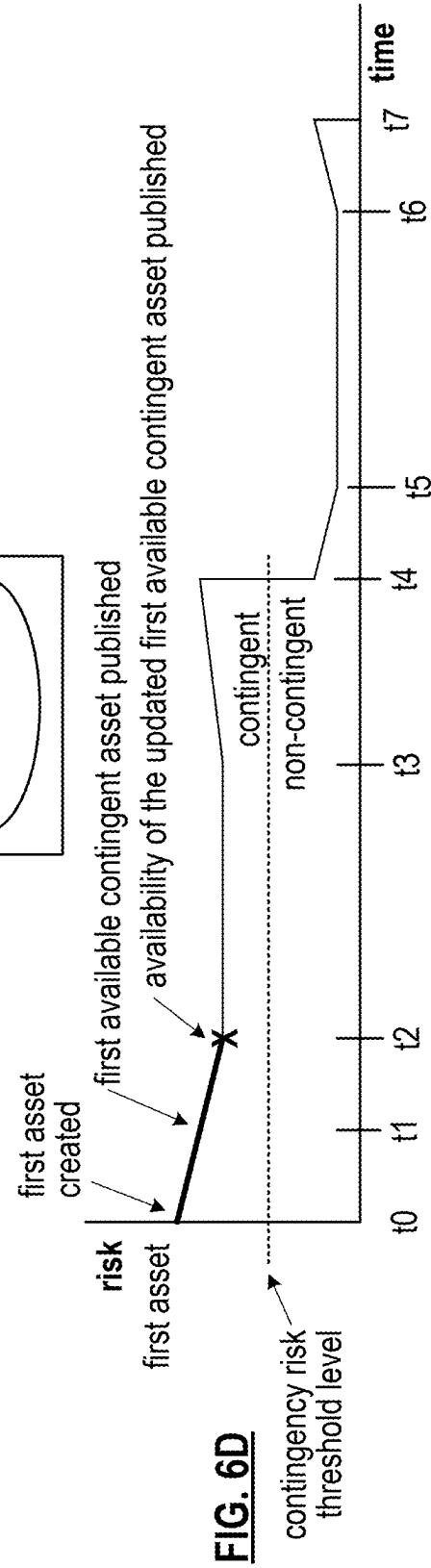
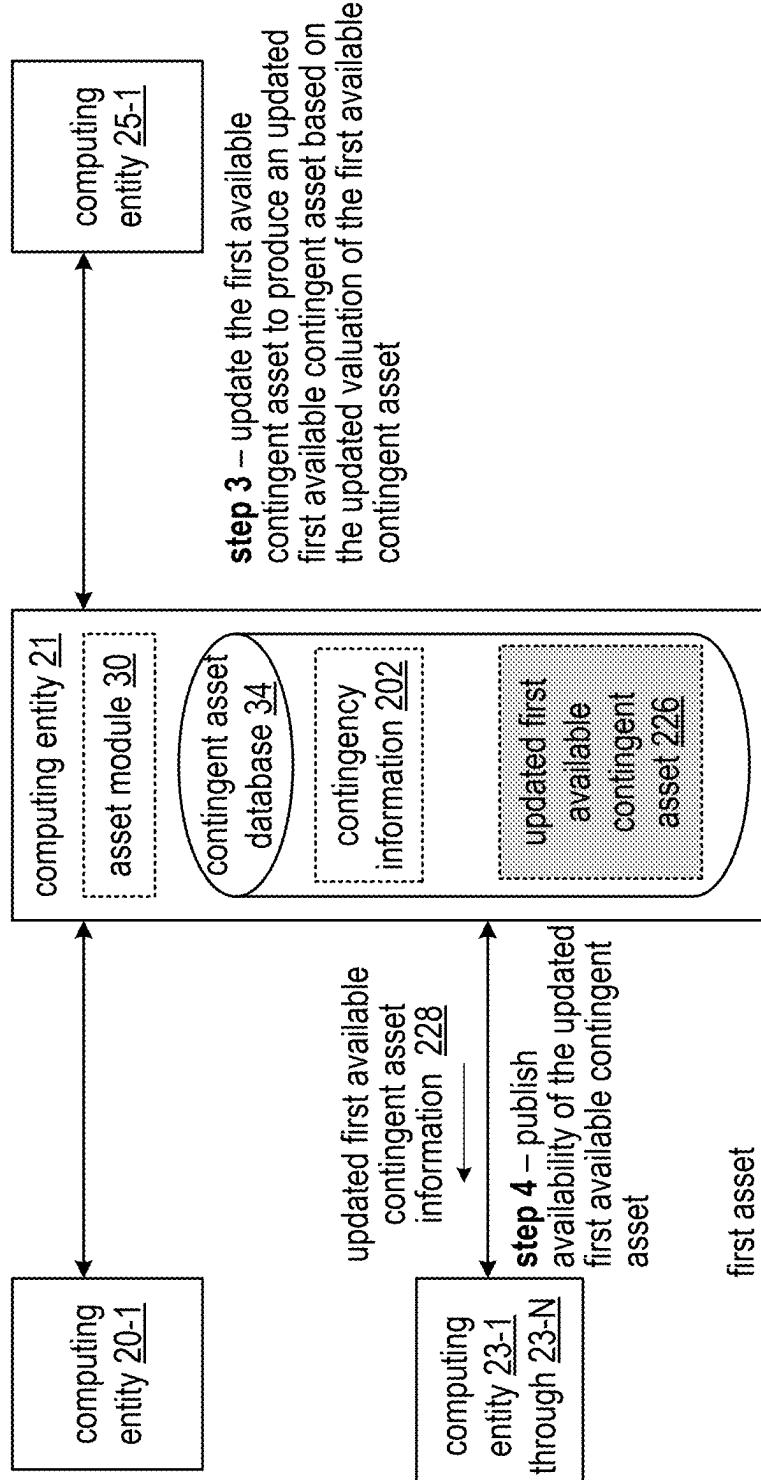


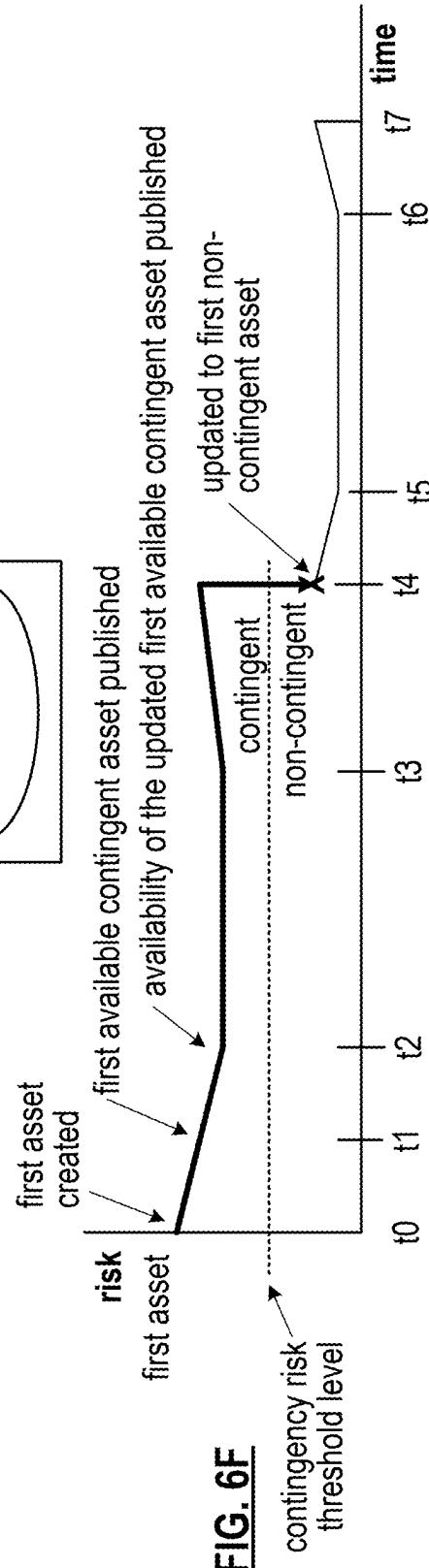
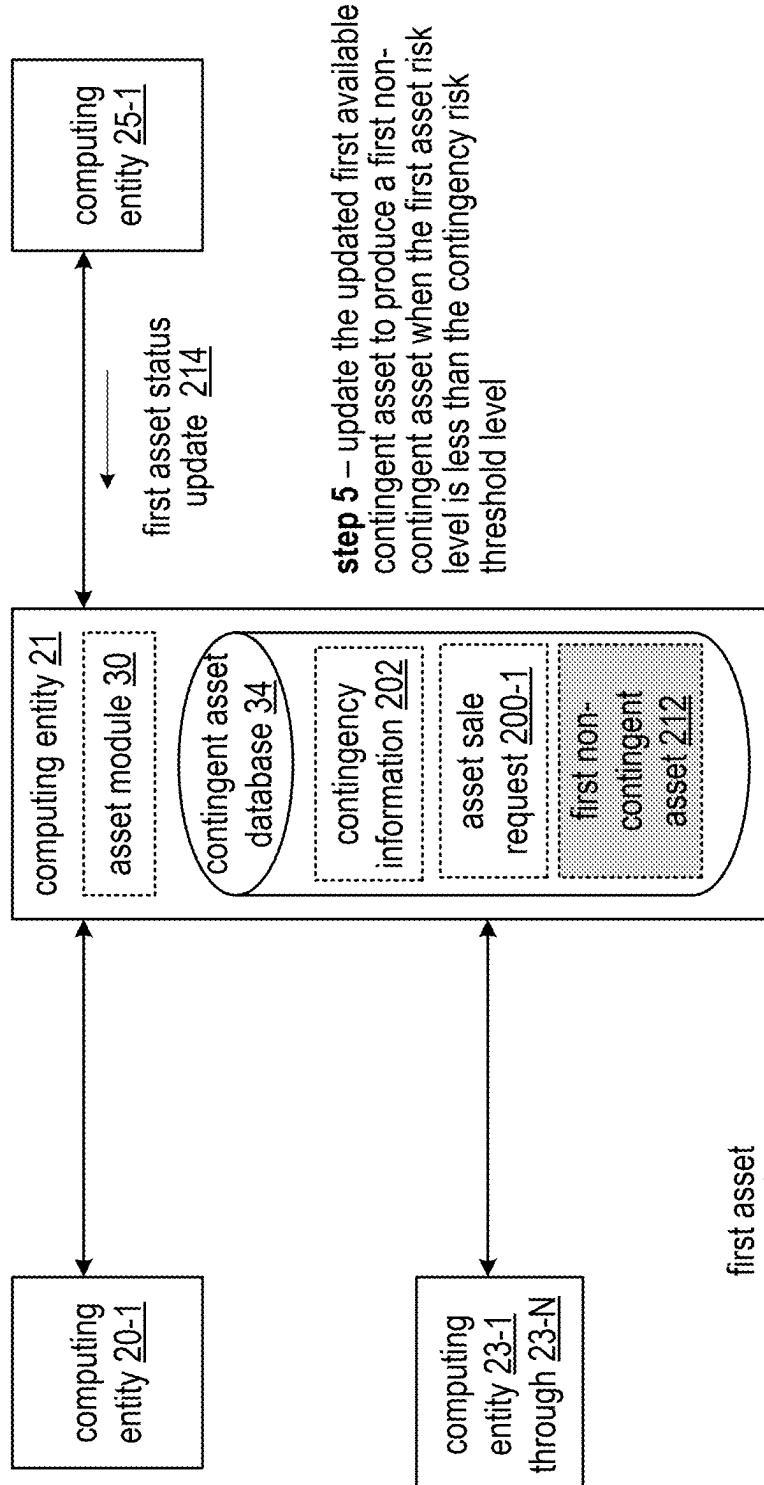


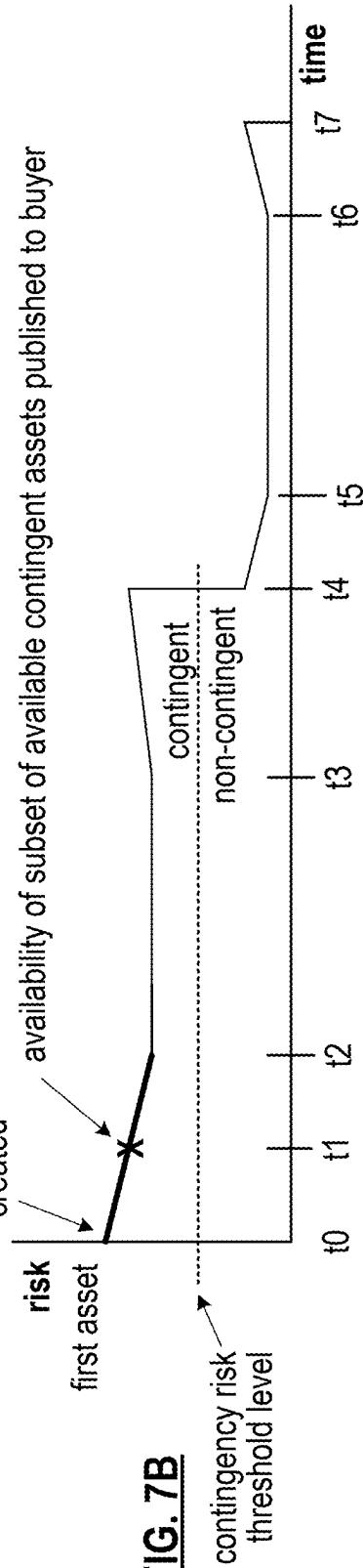
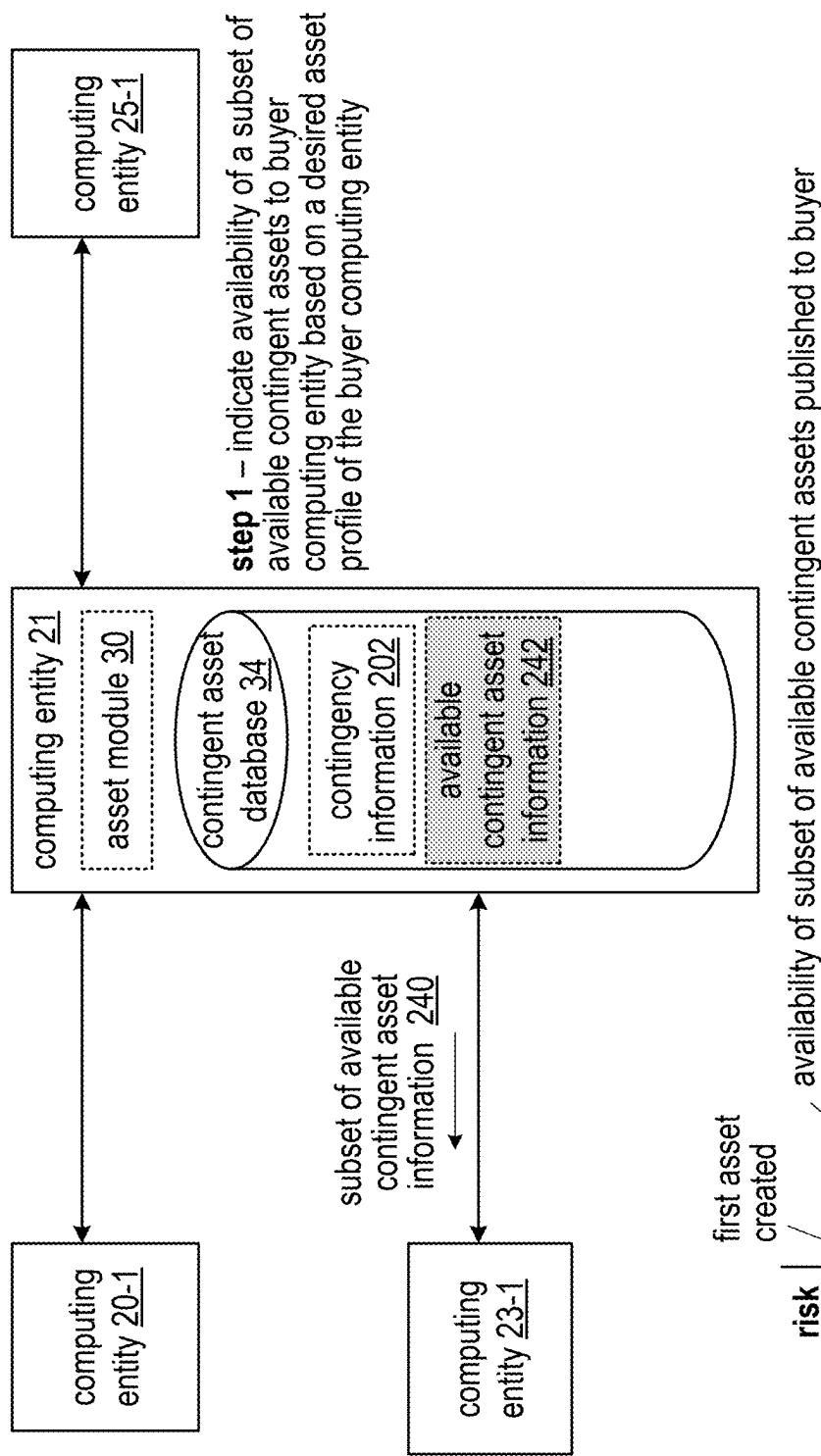


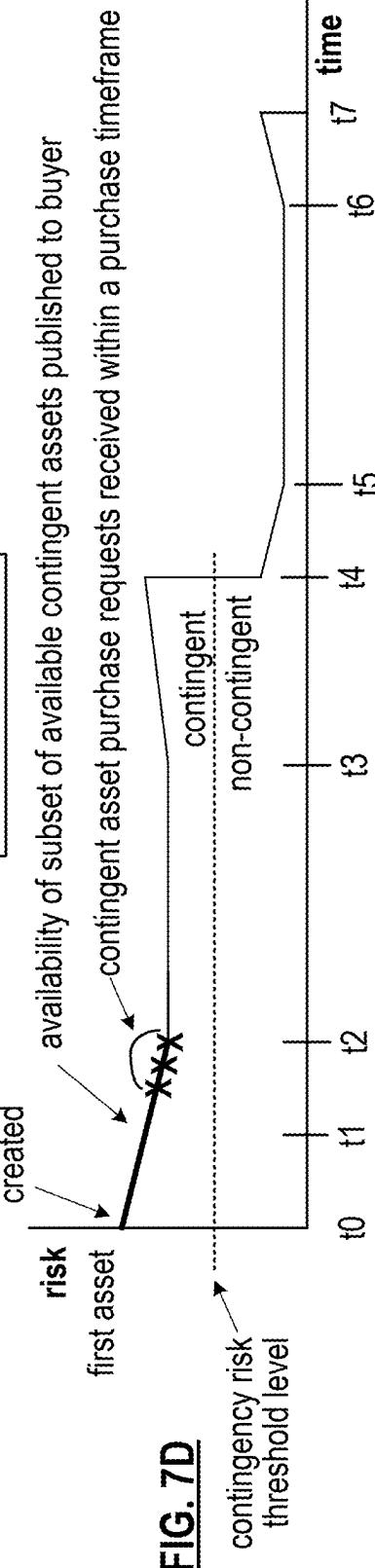
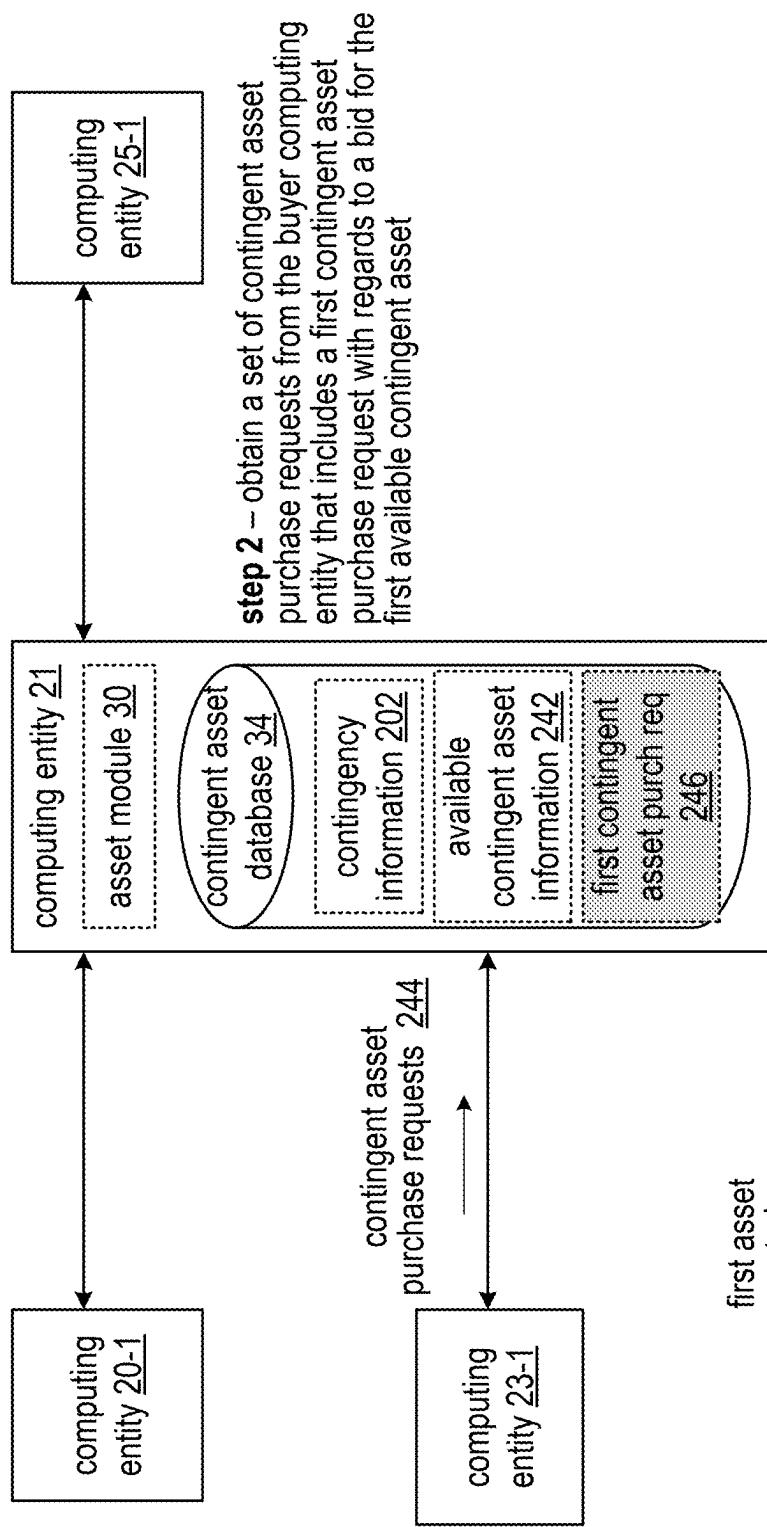


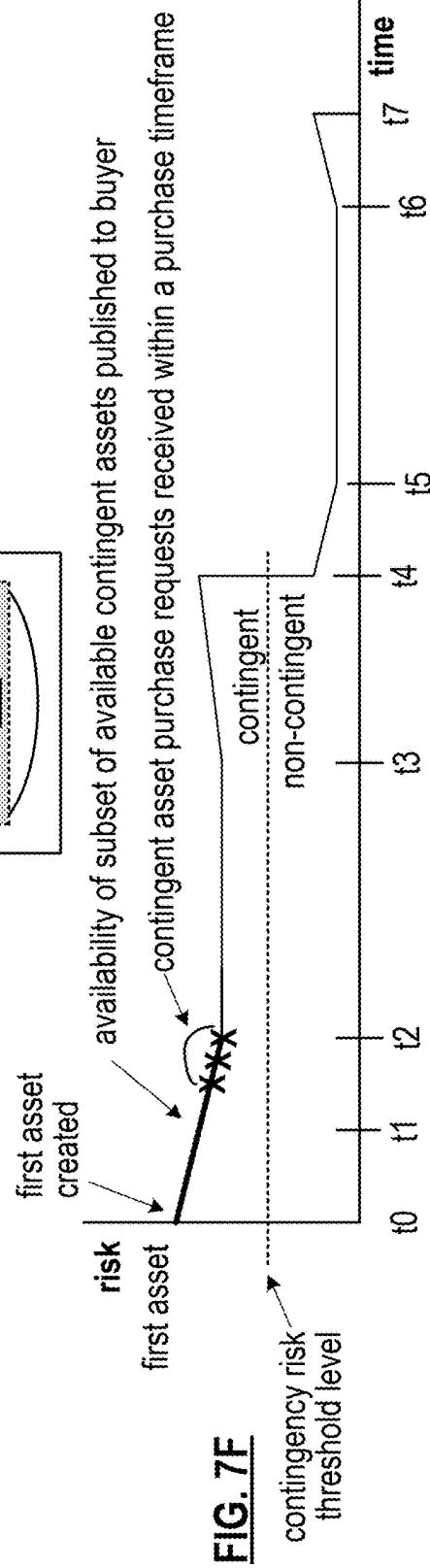
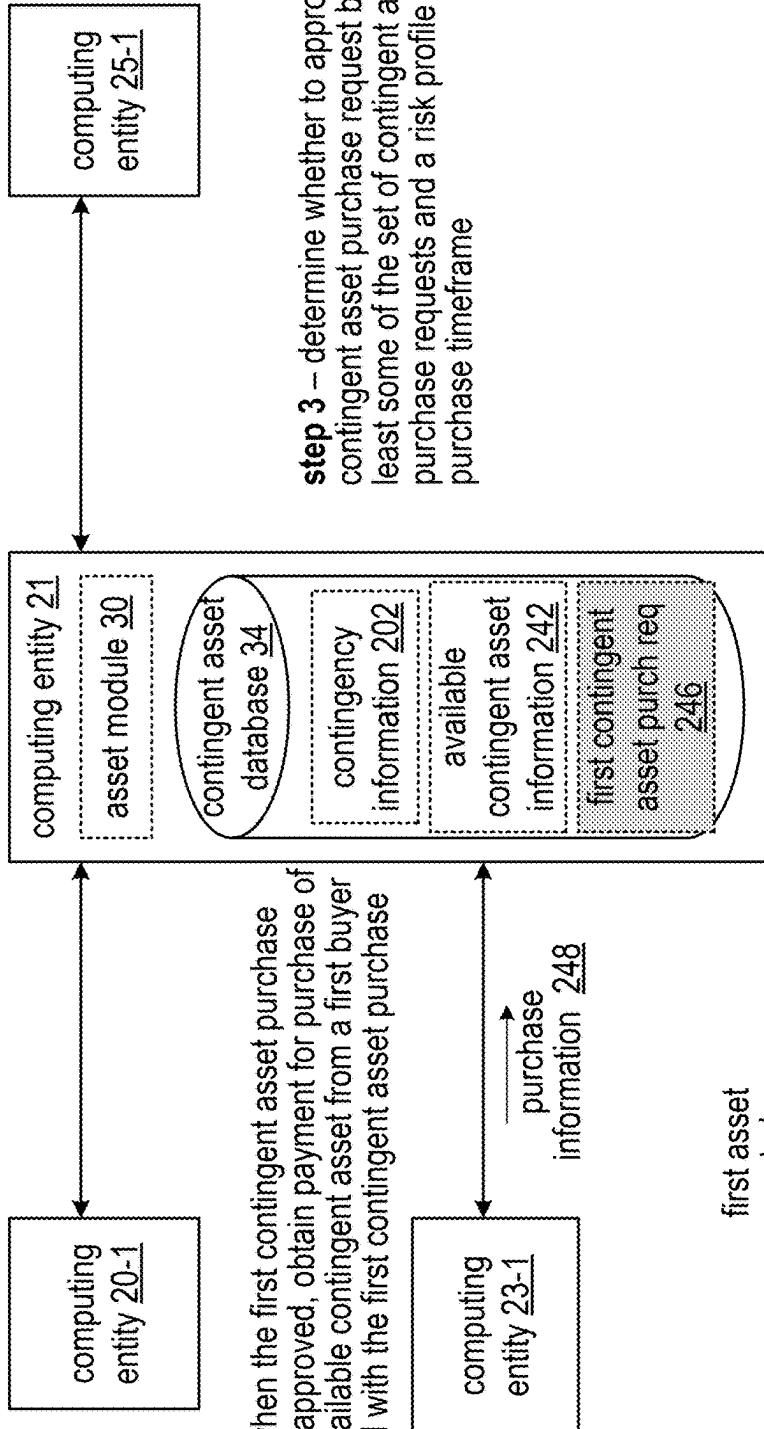


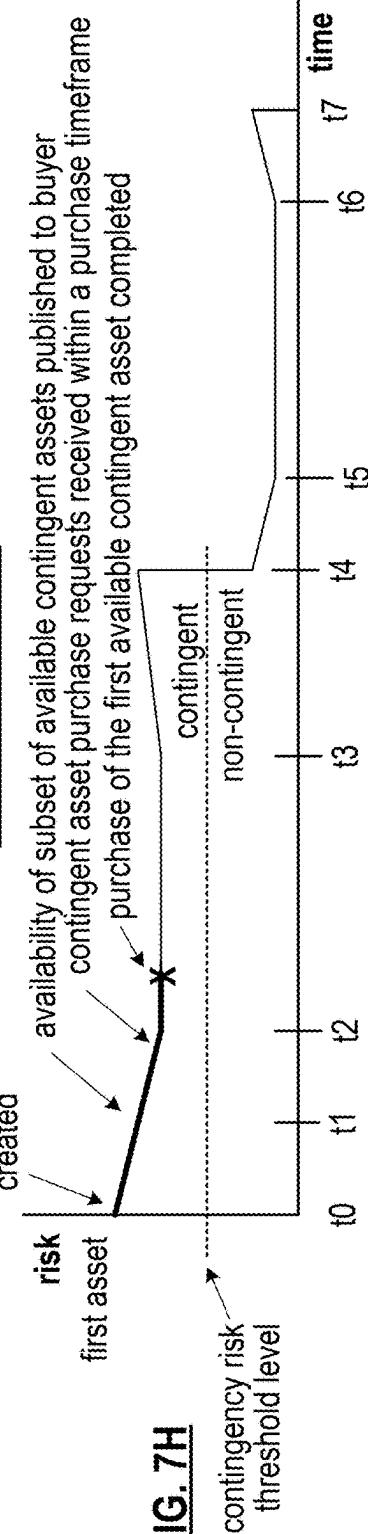
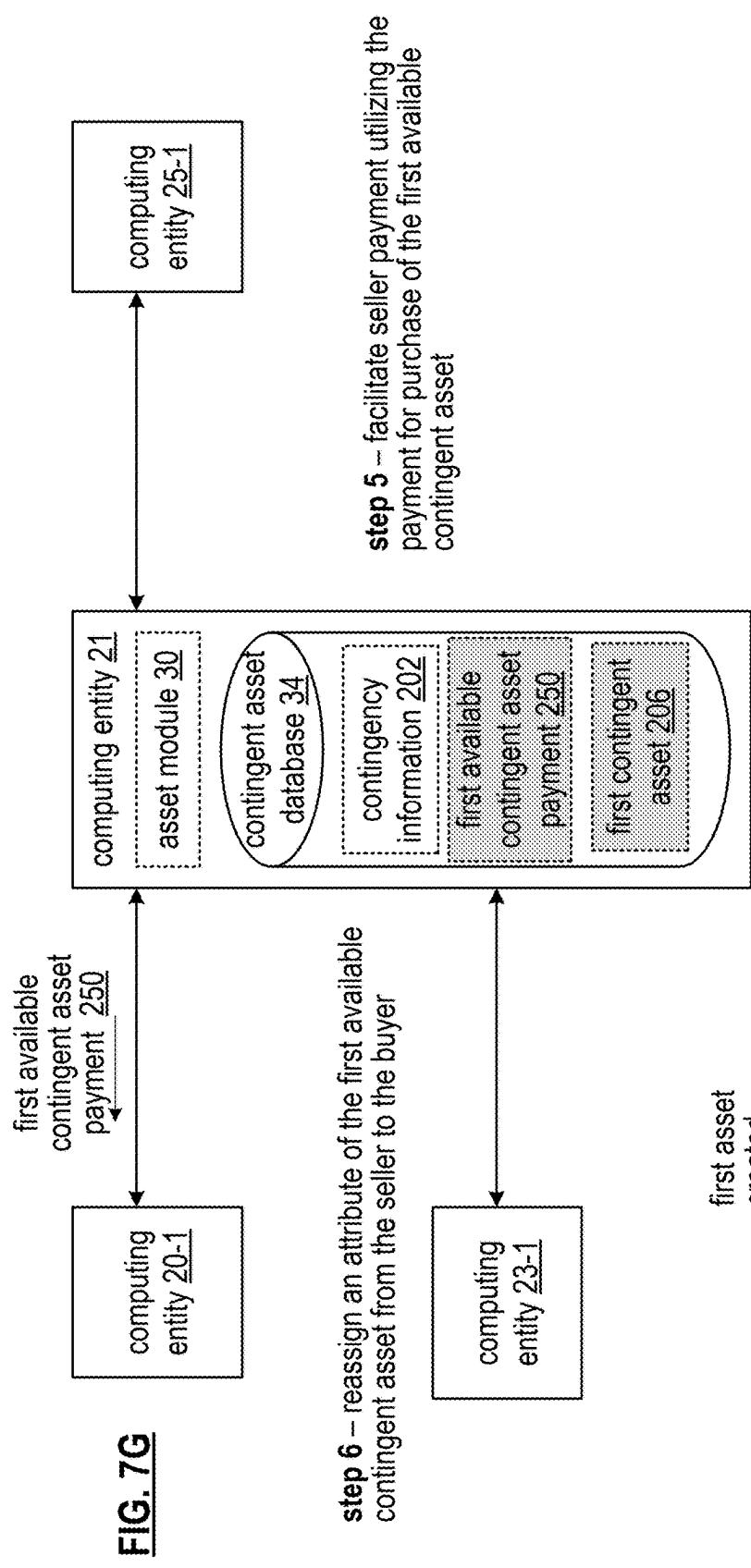


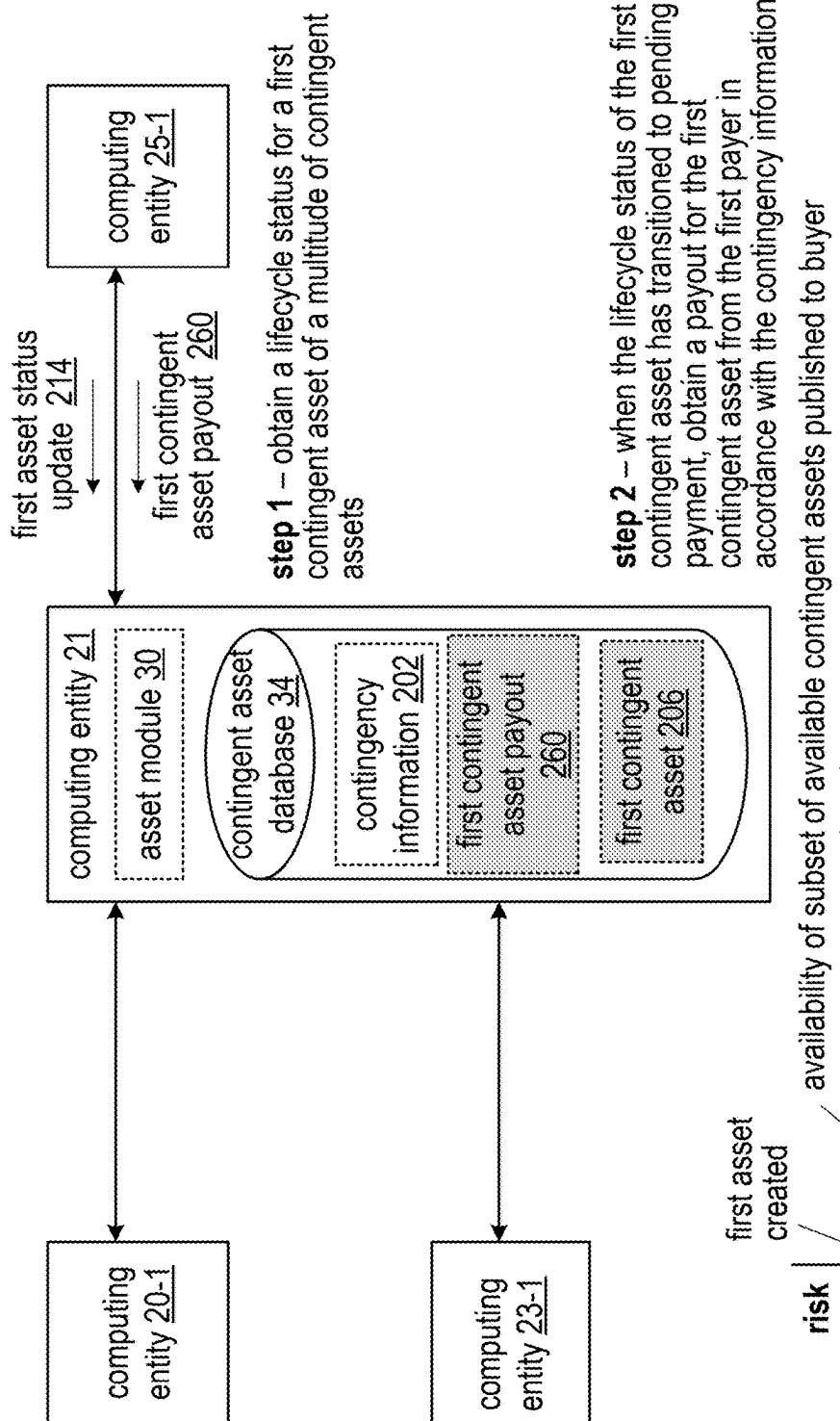












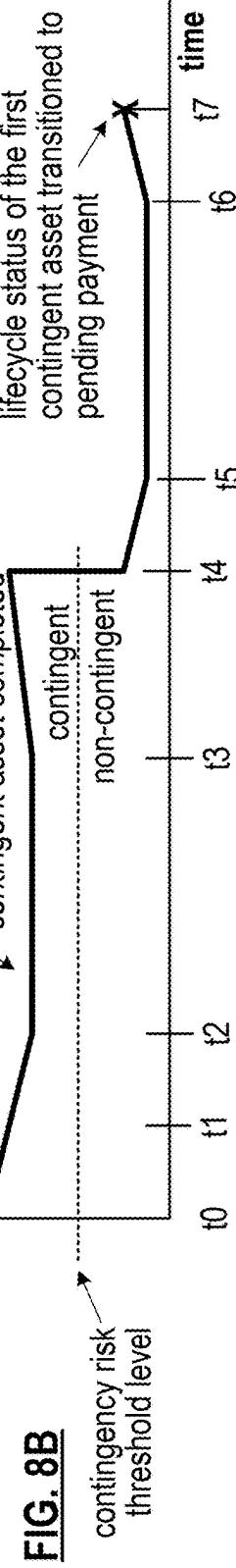
**step 1 – obtain a lifecycle status for a first contingent asset of a multitude of contingent assets**

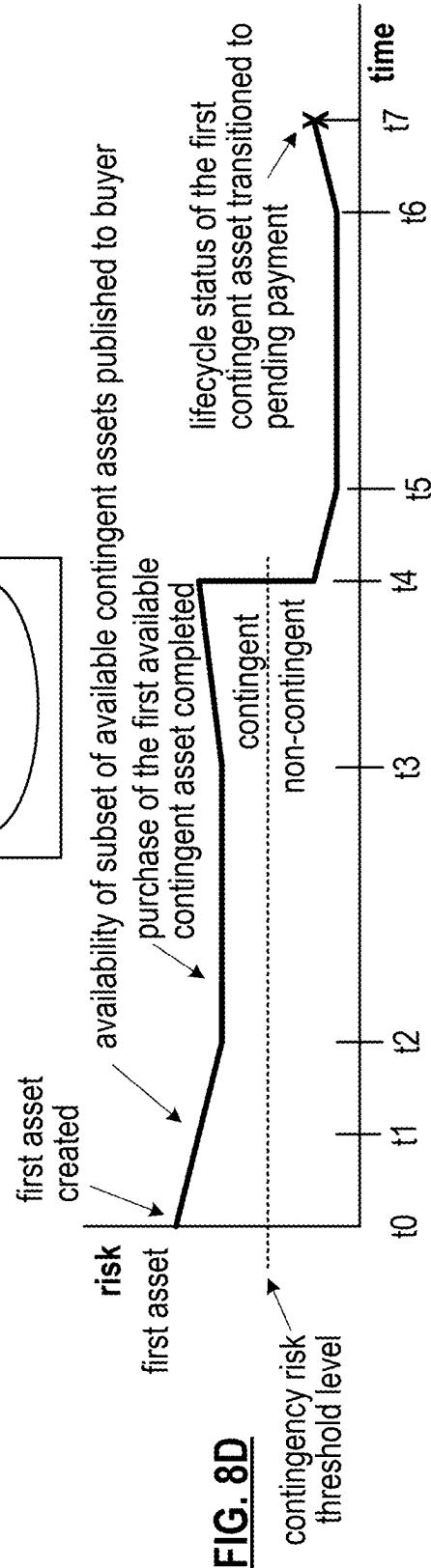
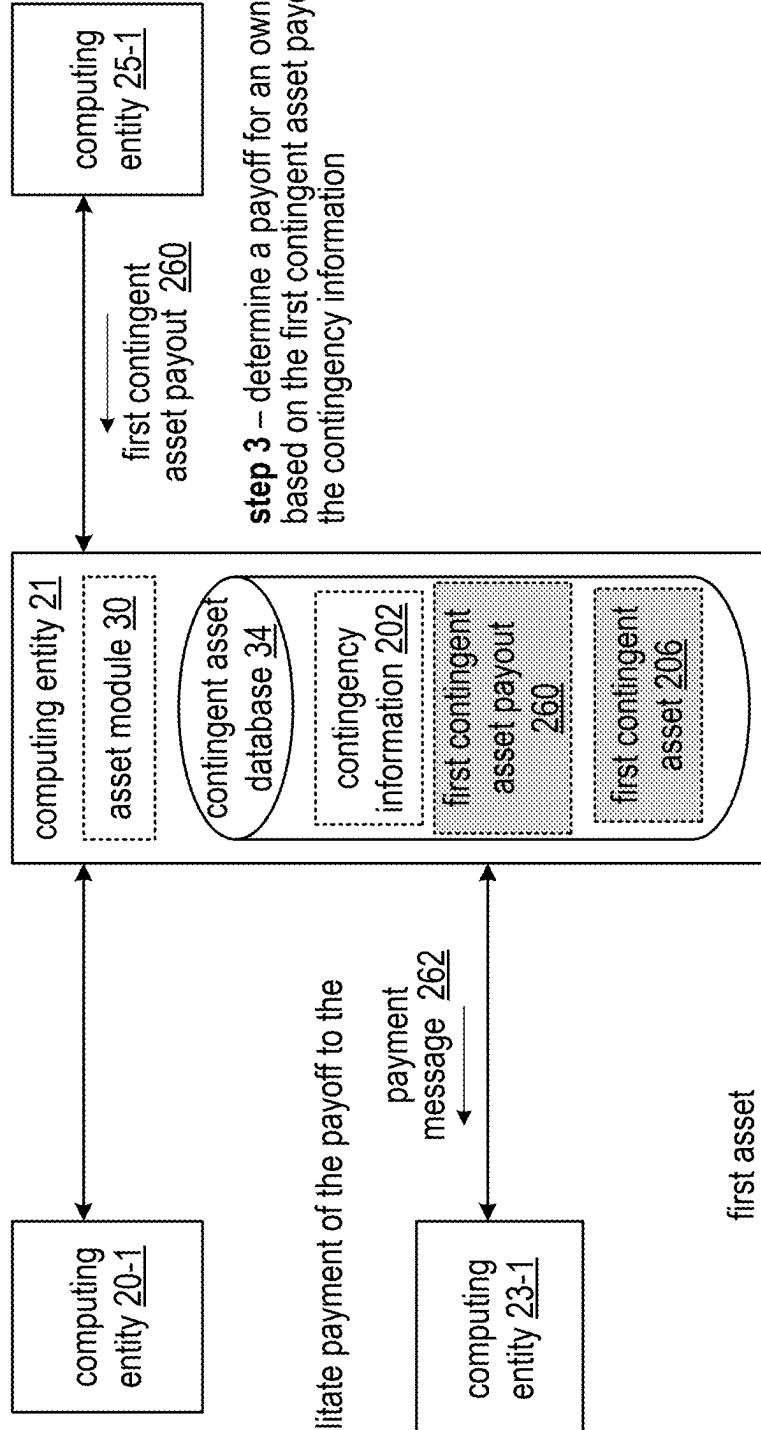
**step 2 – when the lifecycle status of the first contingent asset has transitioned to pending payment, obtain a payout for the first contingent asset from the first payer in accordance with the contingency information**

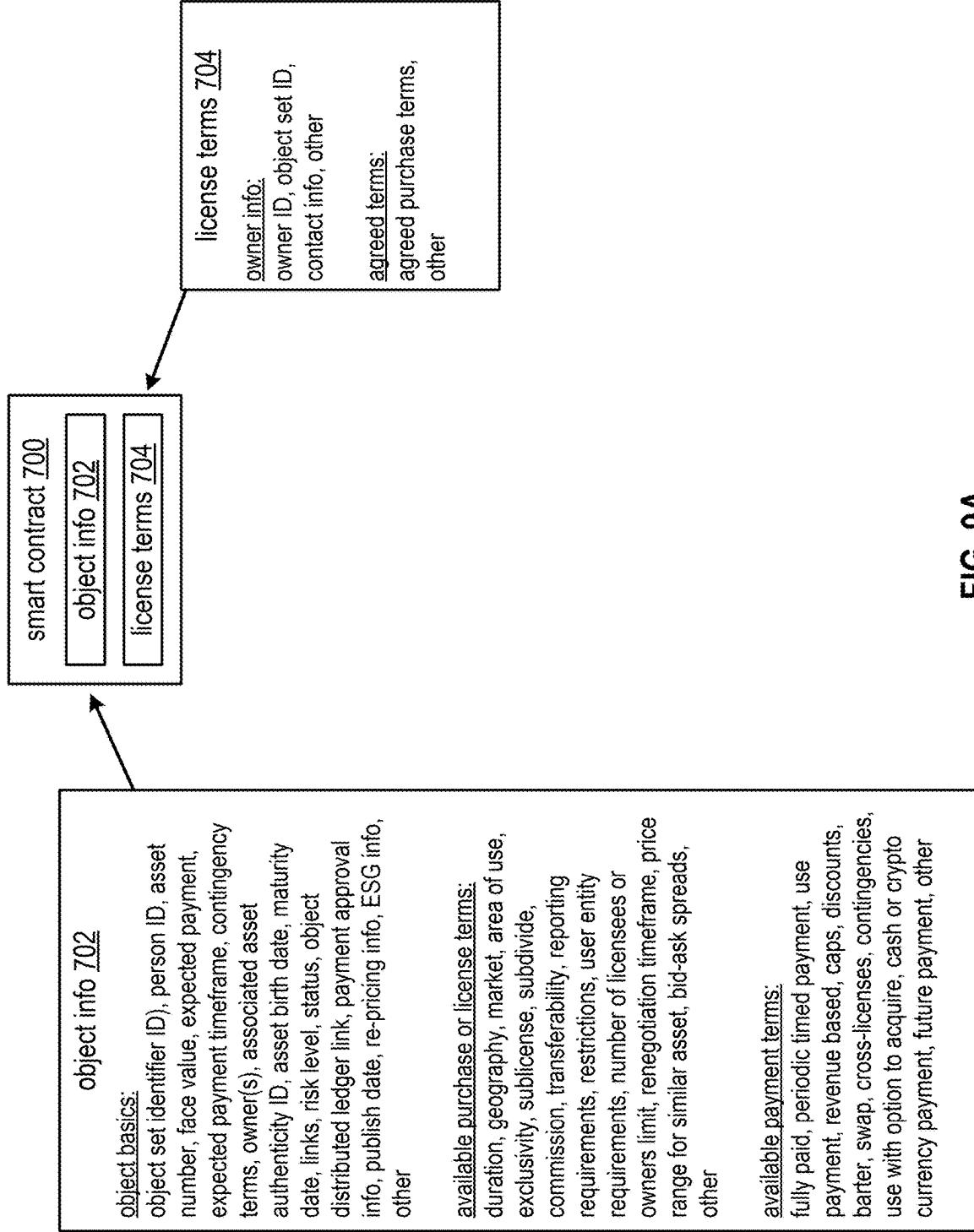
availability of subset of available contingent assets published to buyer  
purchase of the first available contingent asset completed

first asset created  
contingent non-contingent

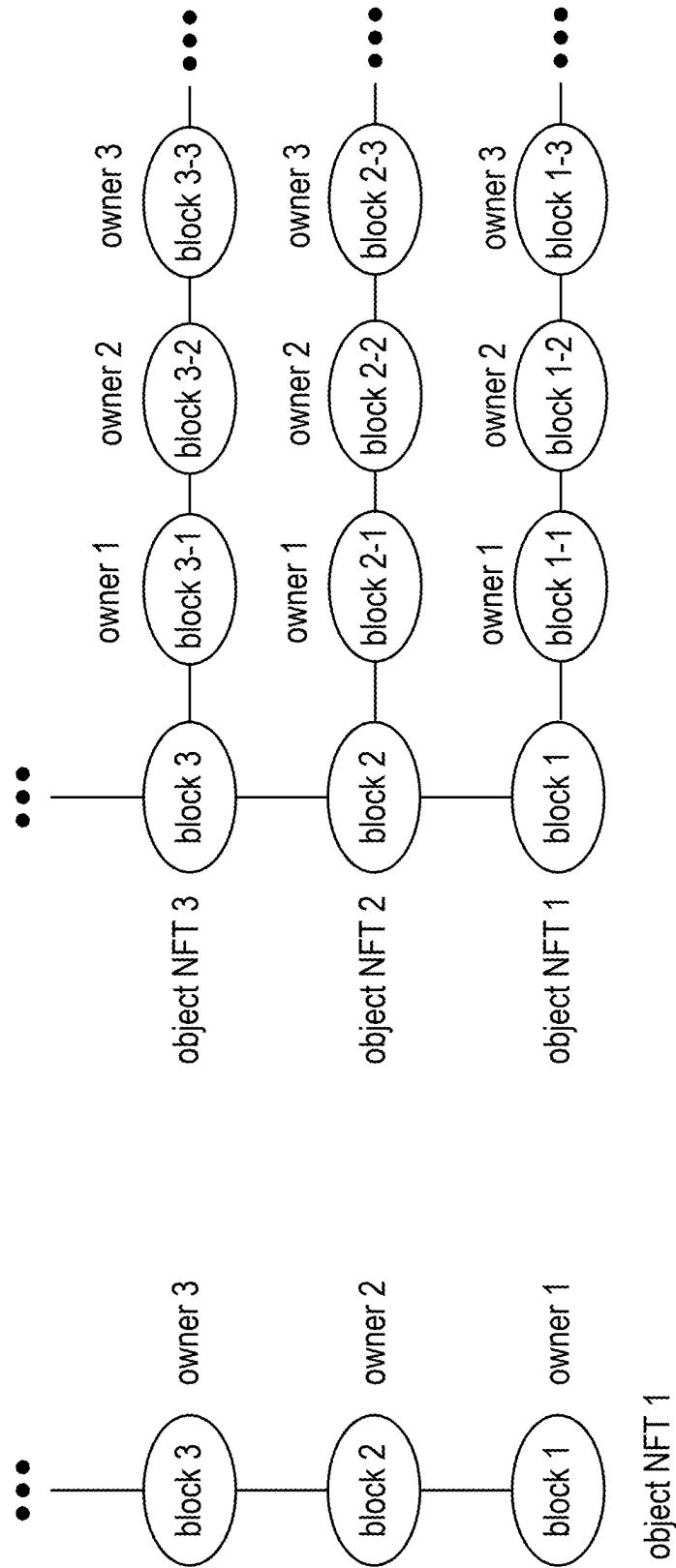
risk  
first asset





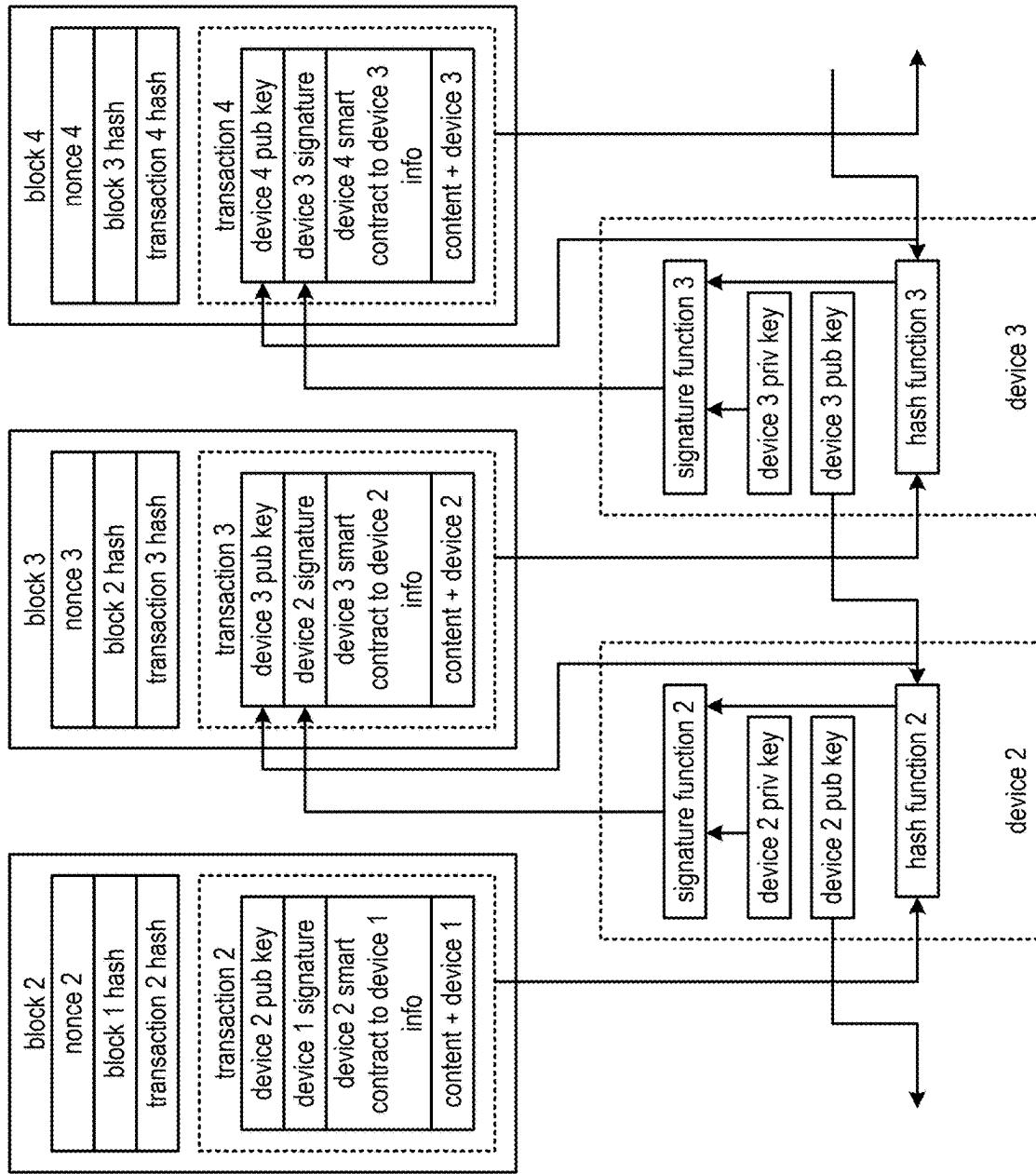


**FIG. 9A**

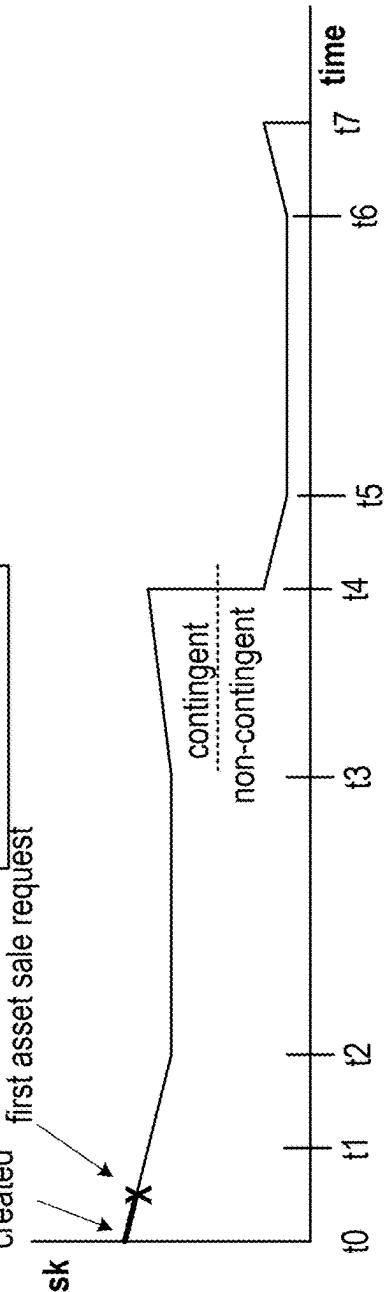
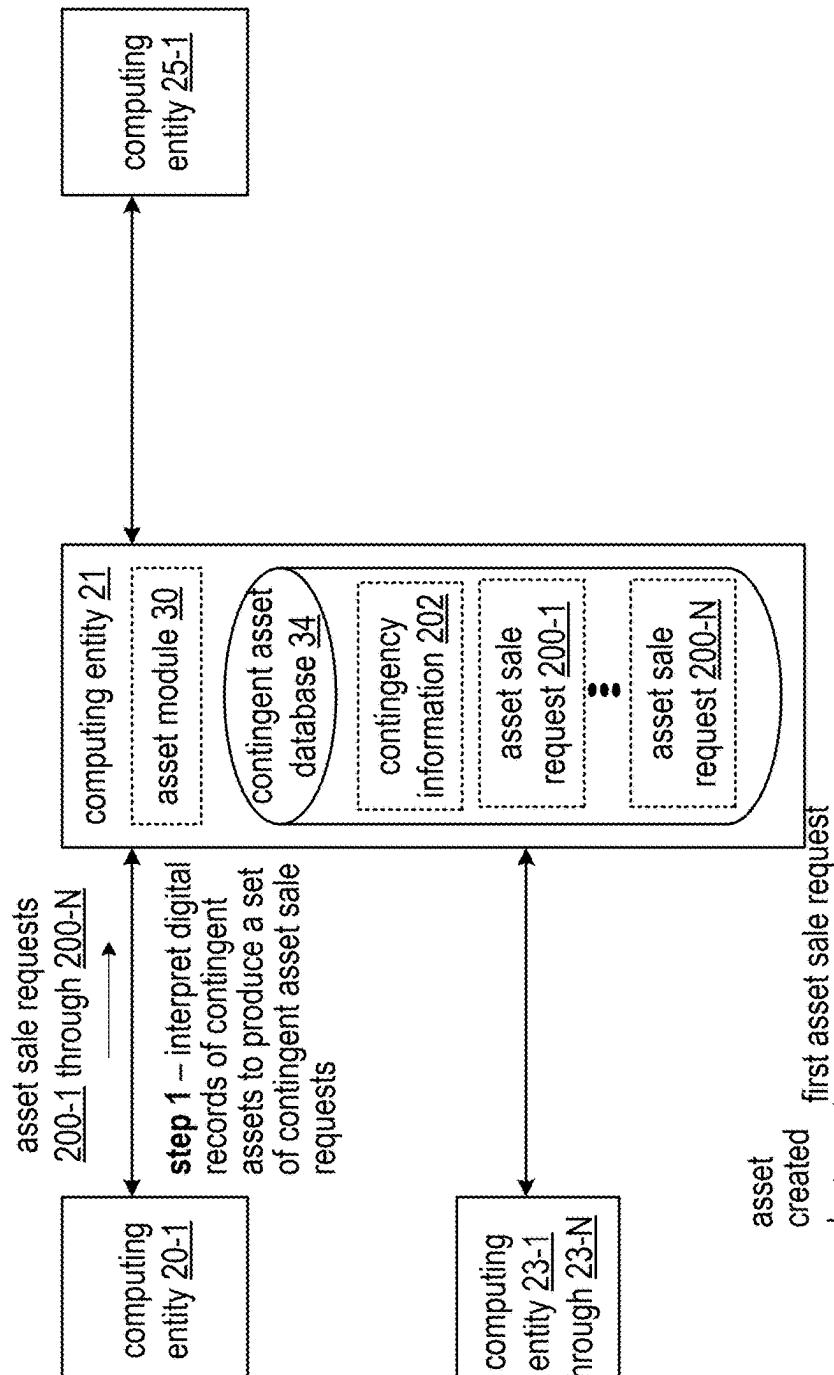


**FIG. 9B**

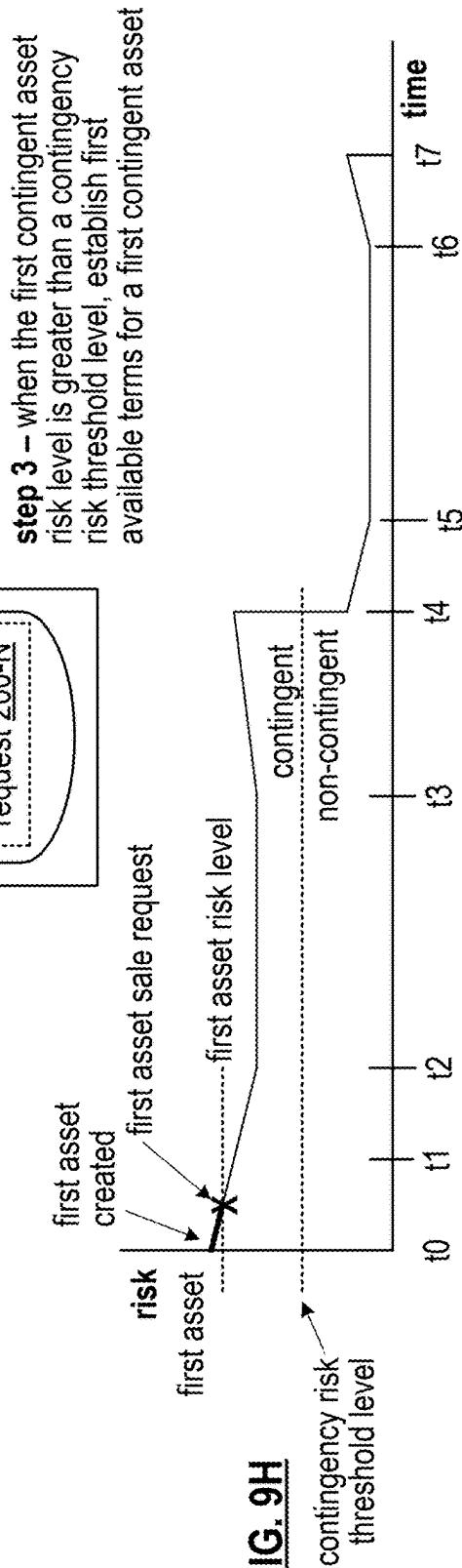
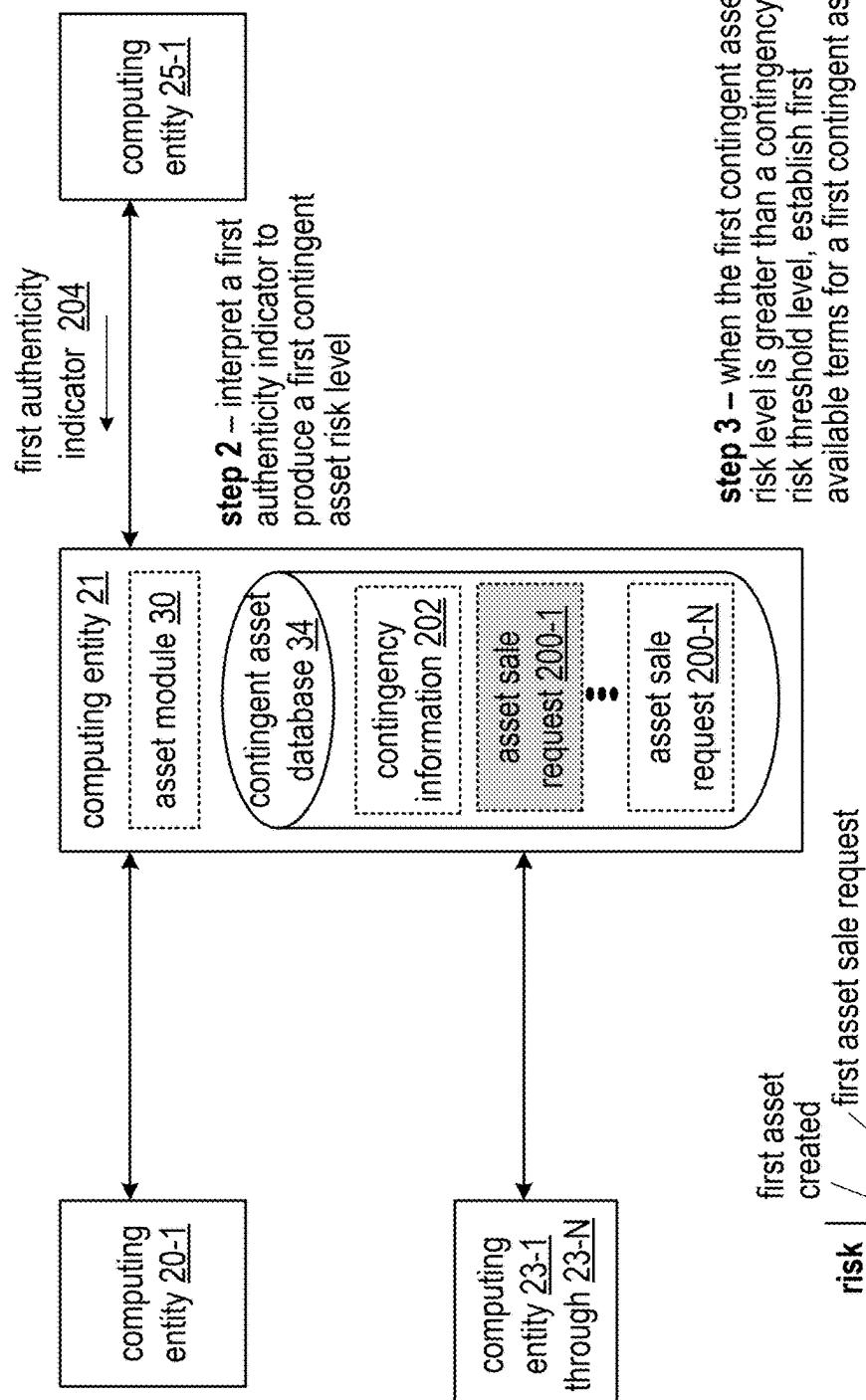
**FIG. 9C**

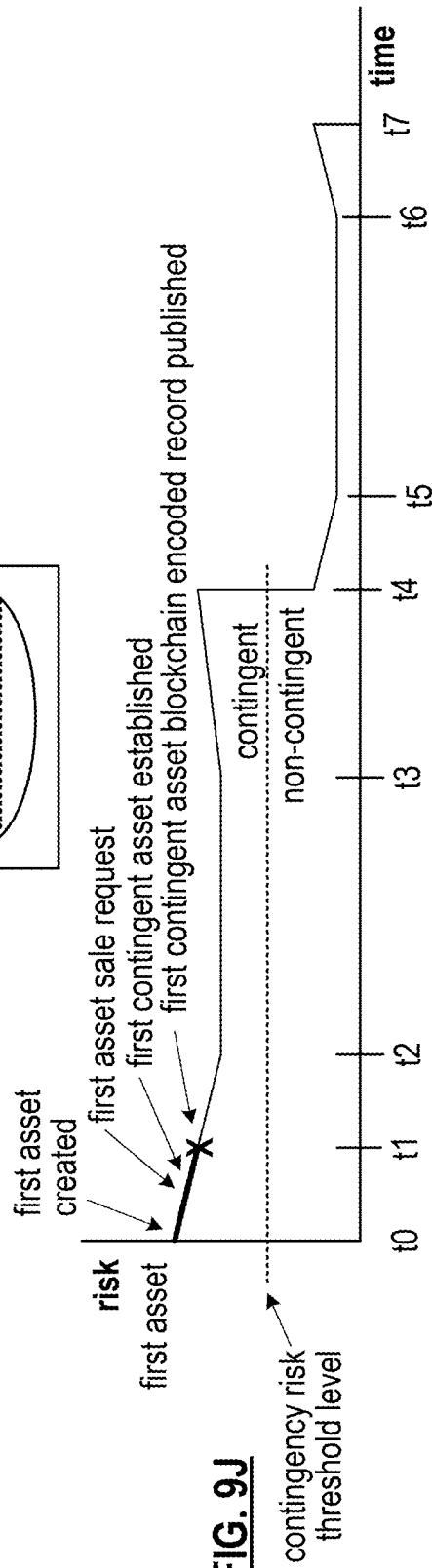
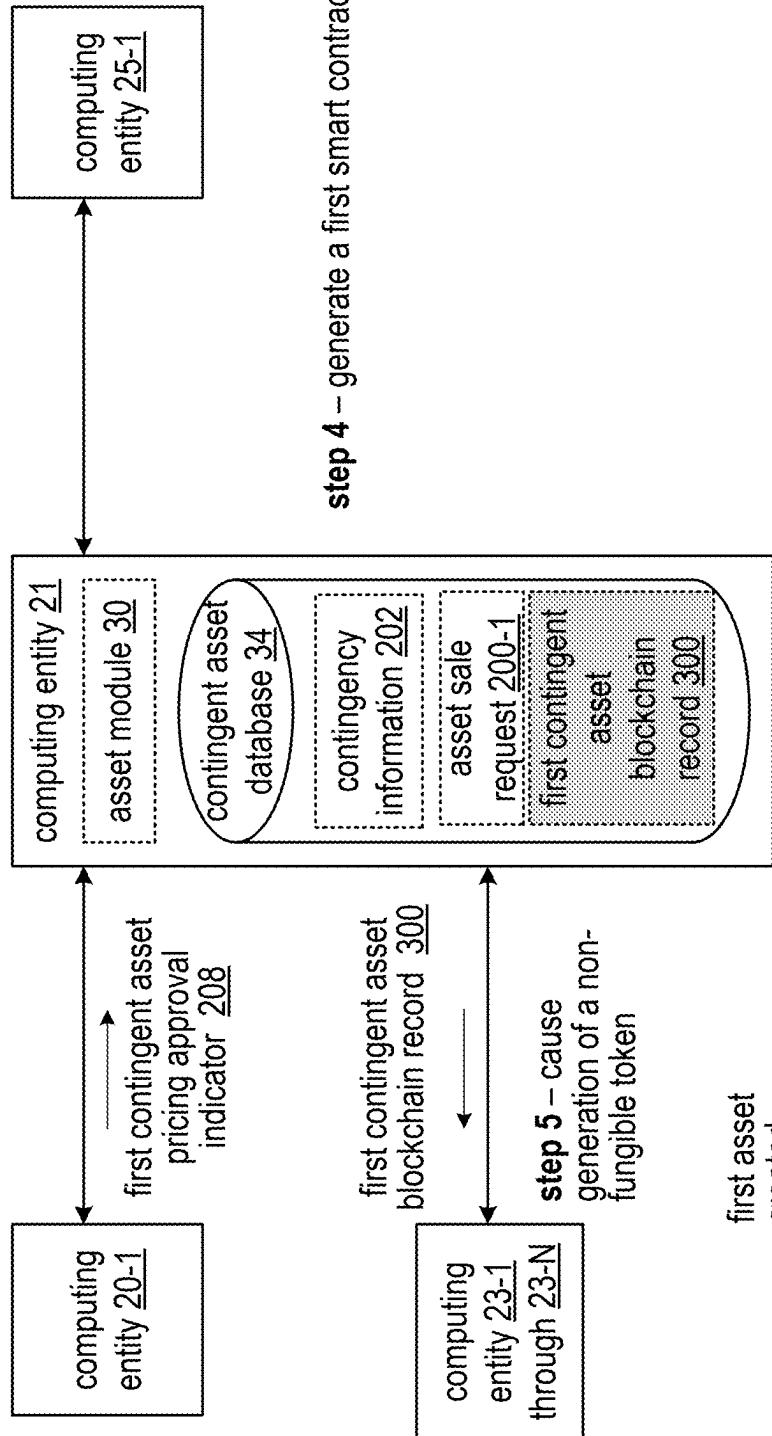


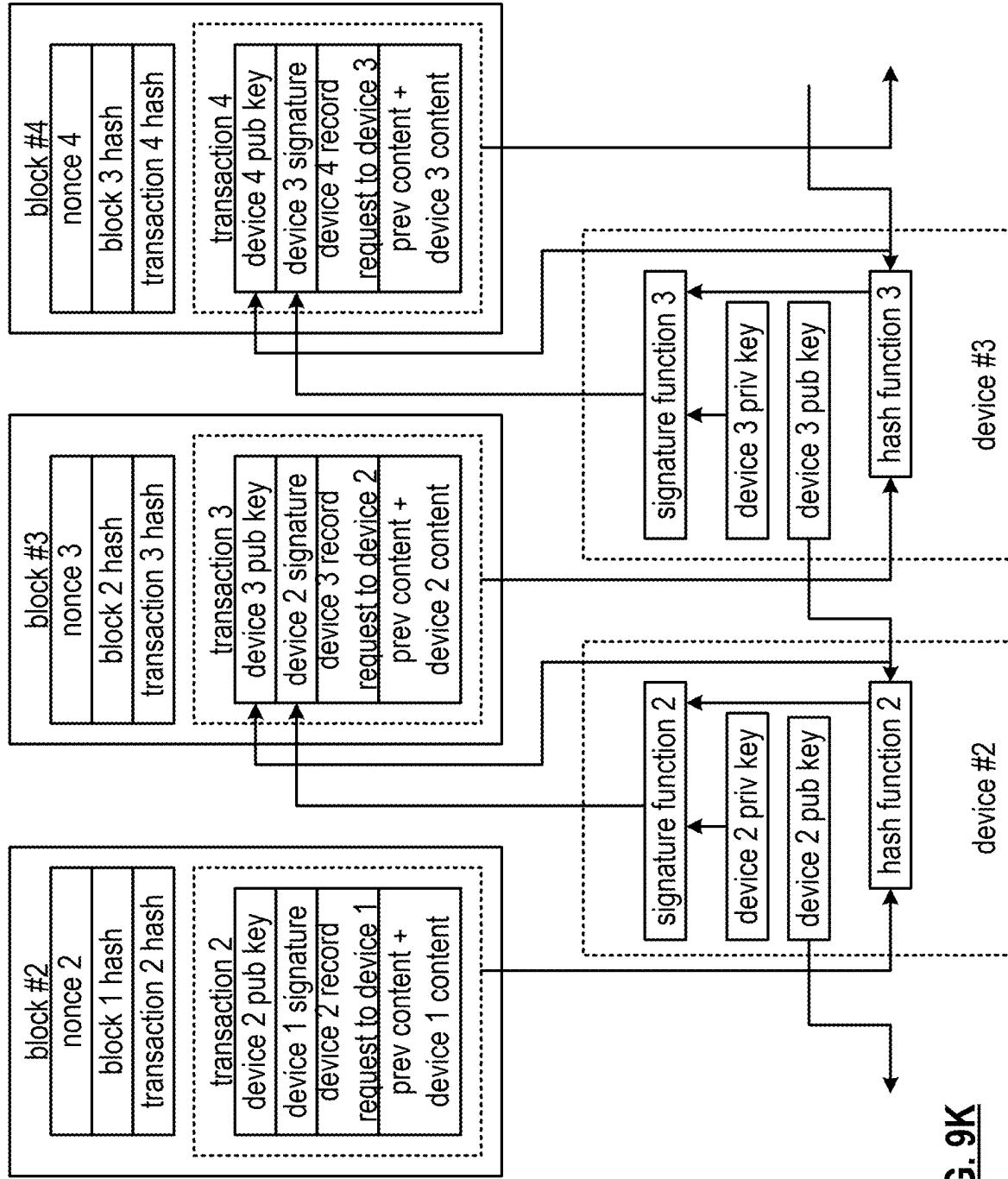
**FIG. 9D**



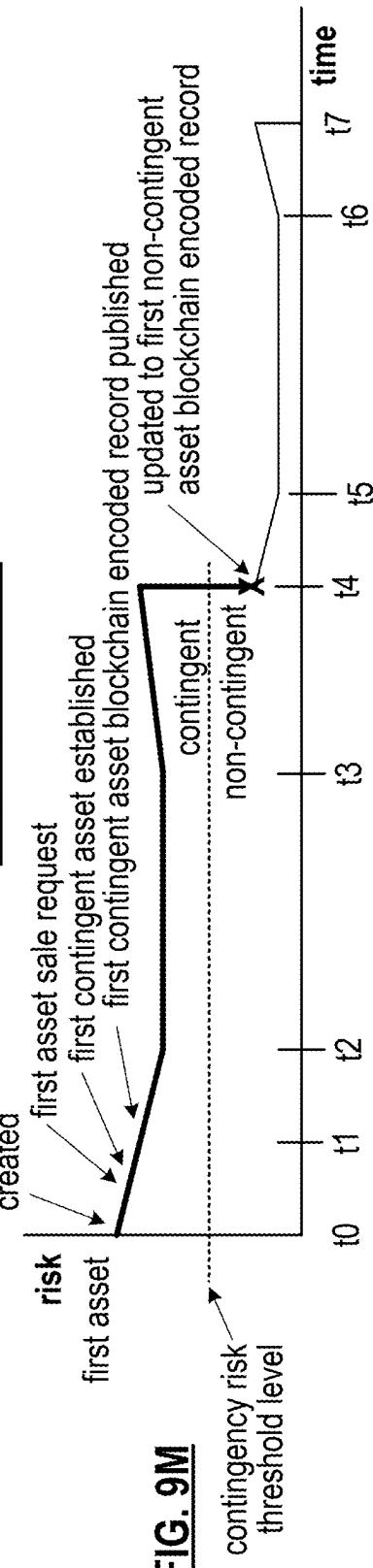
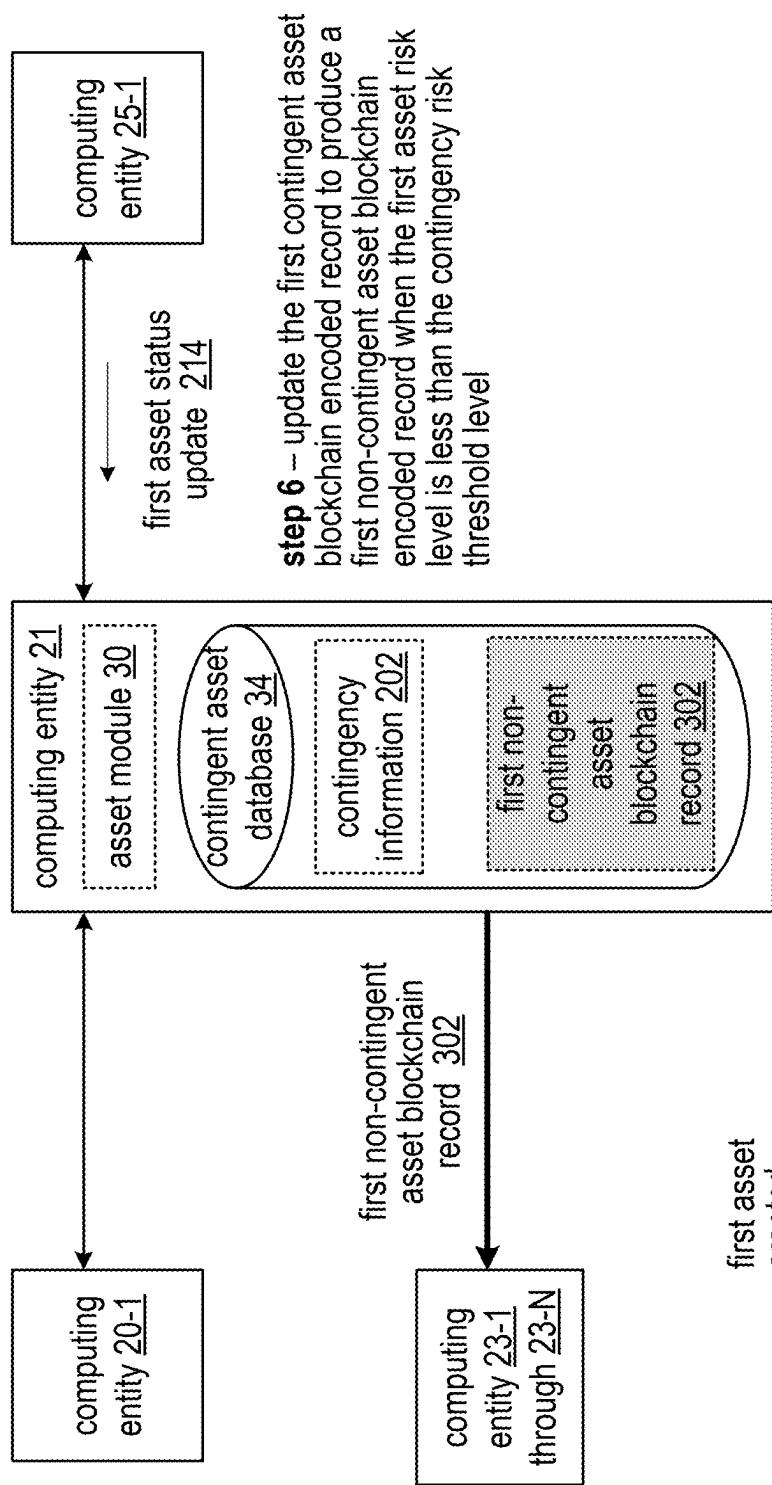
**FIG. 9F**

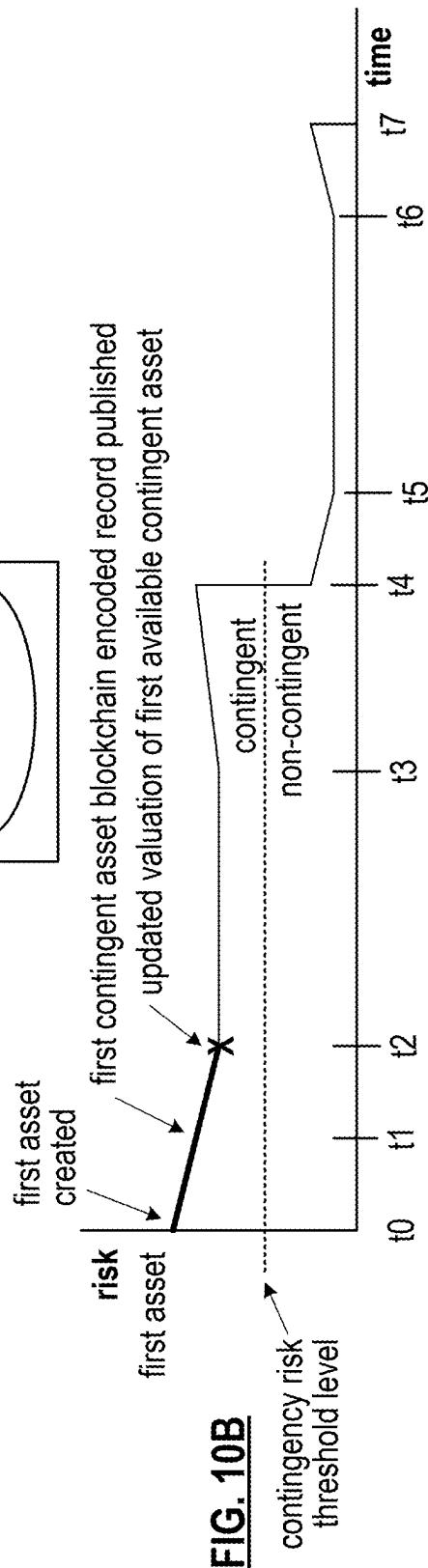
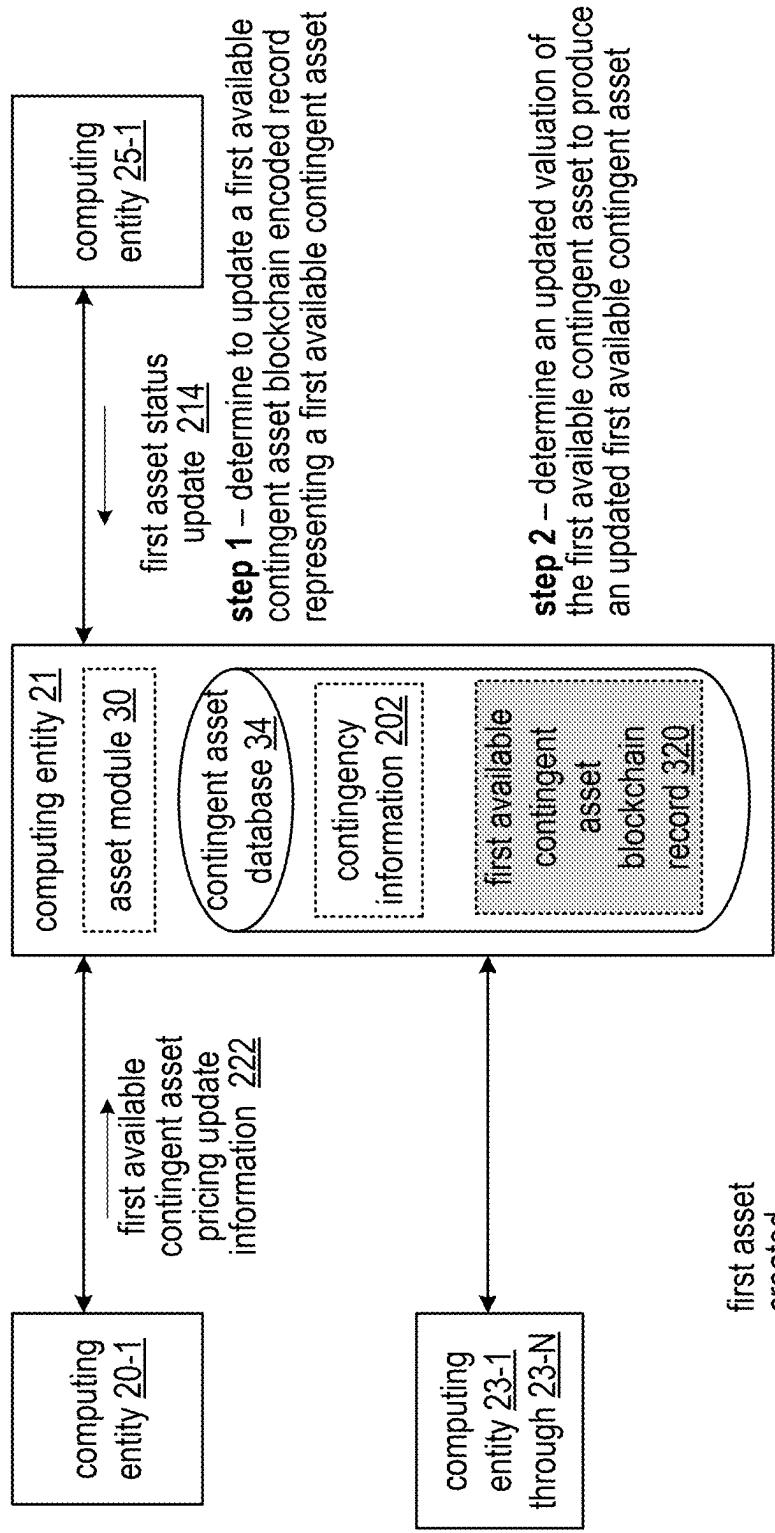


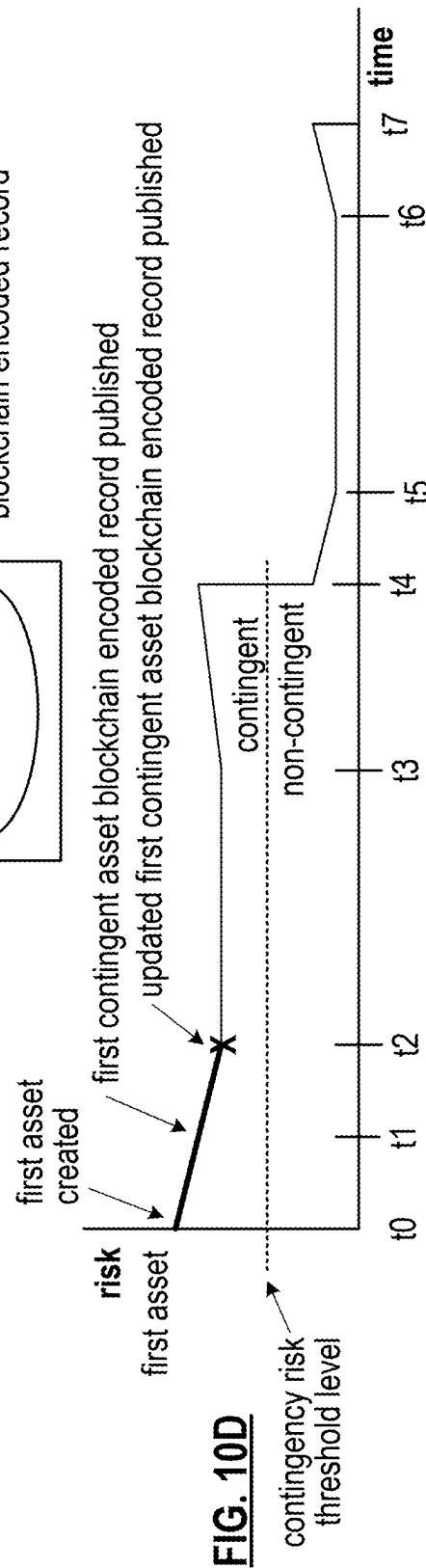
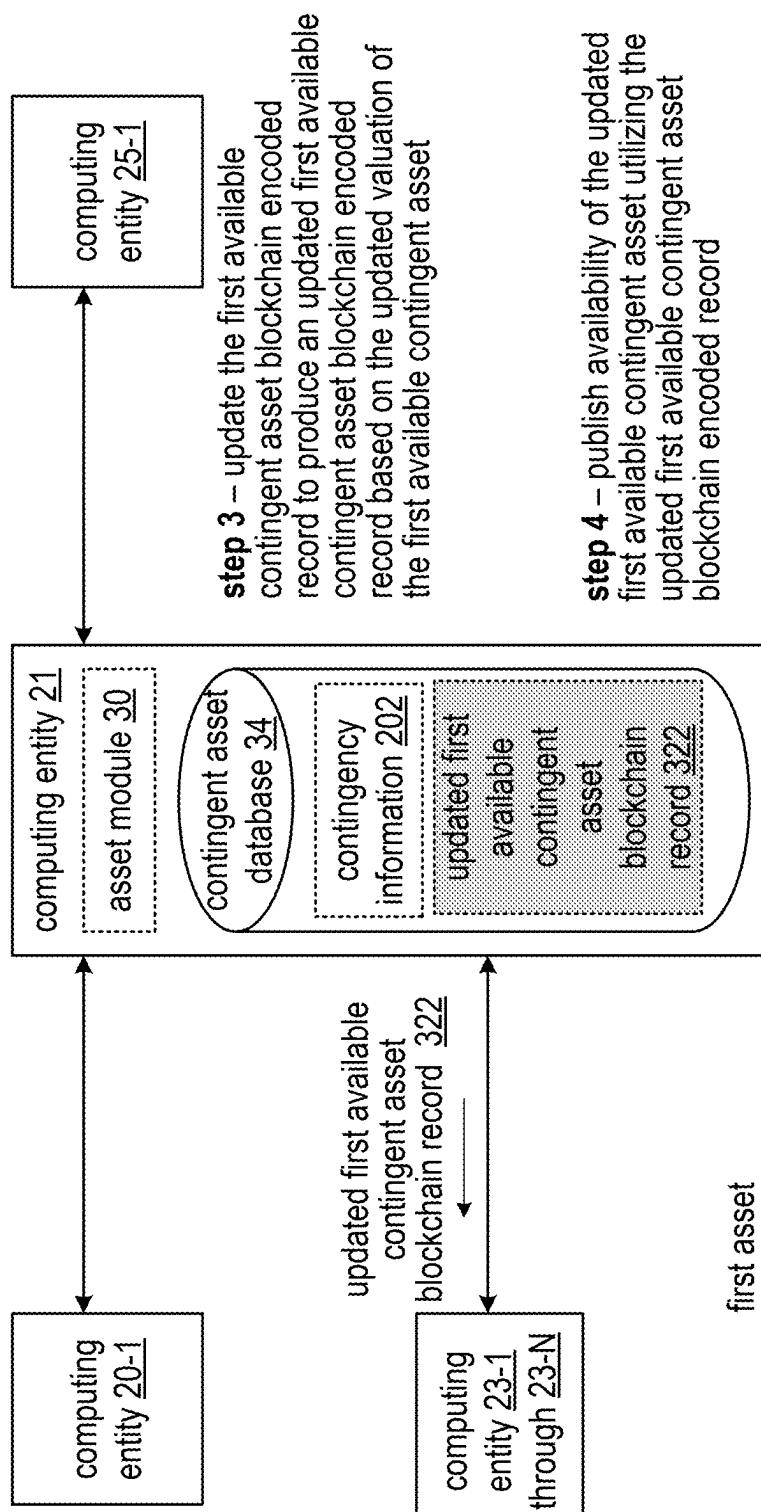


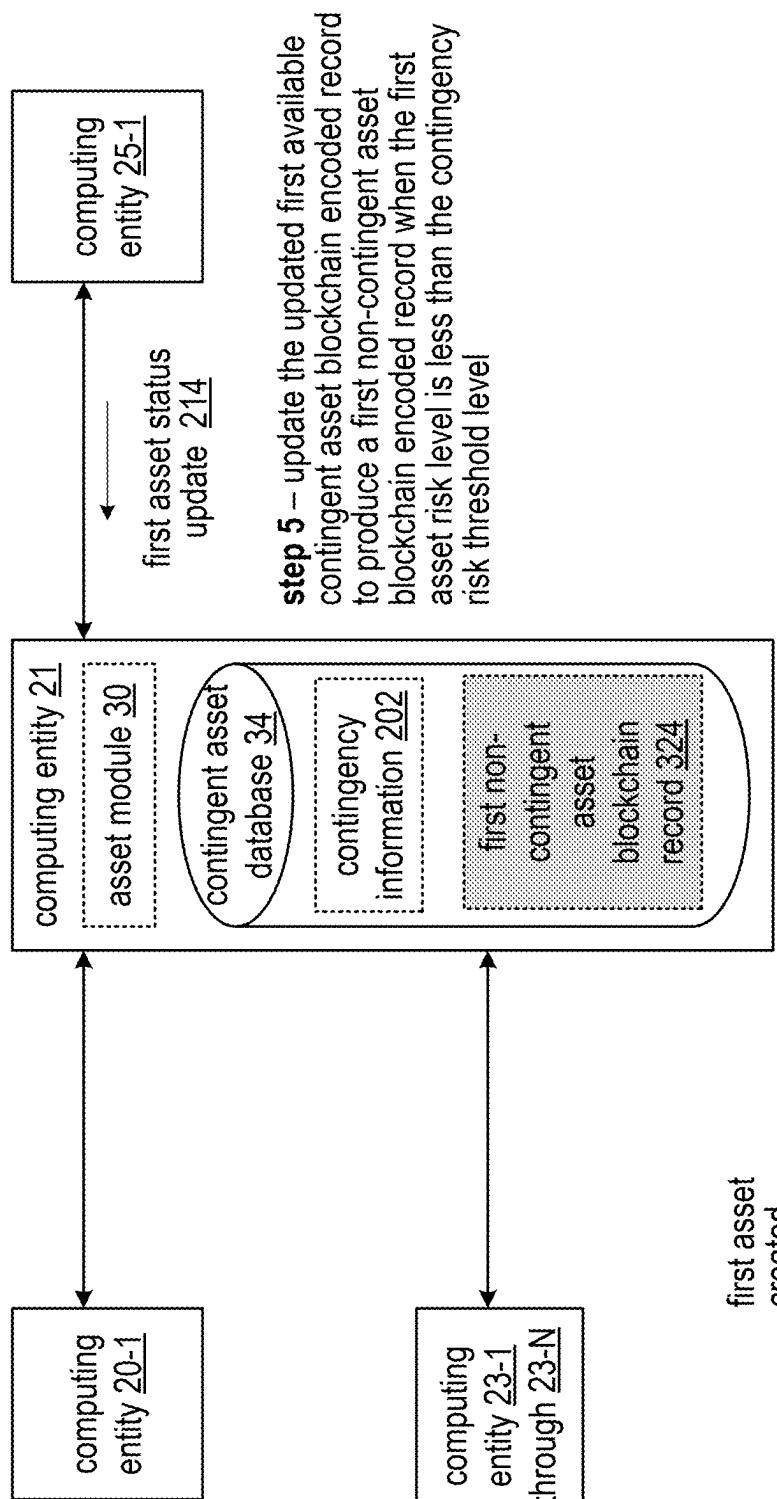


**FIG. 9K**

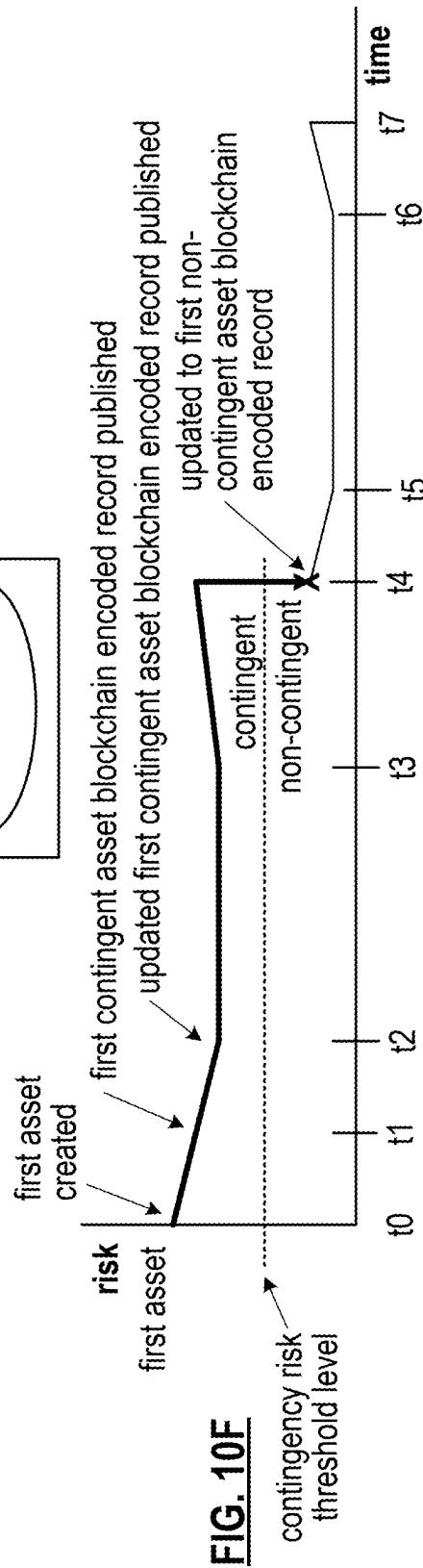


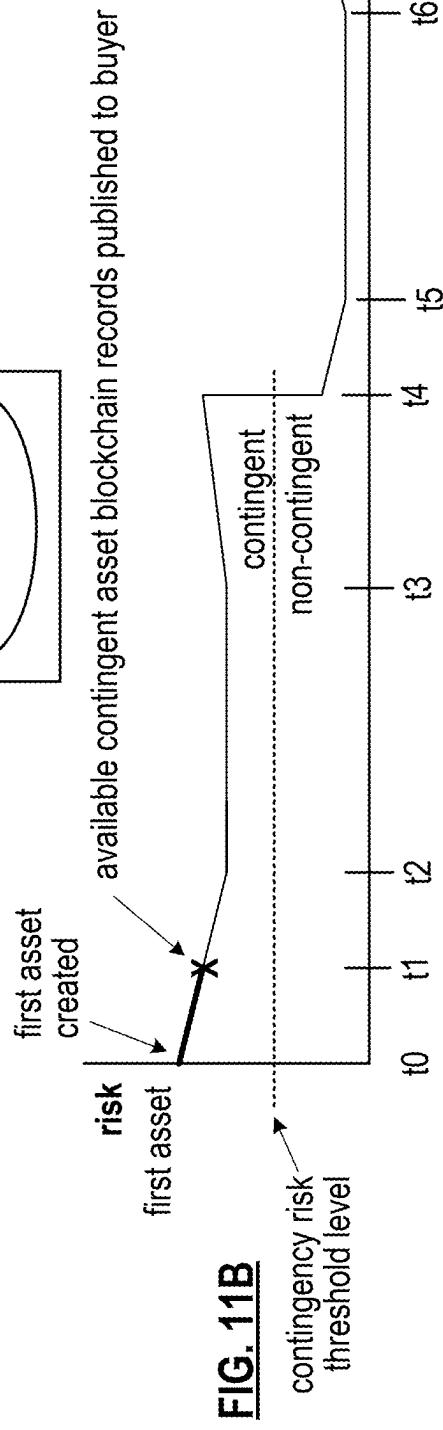
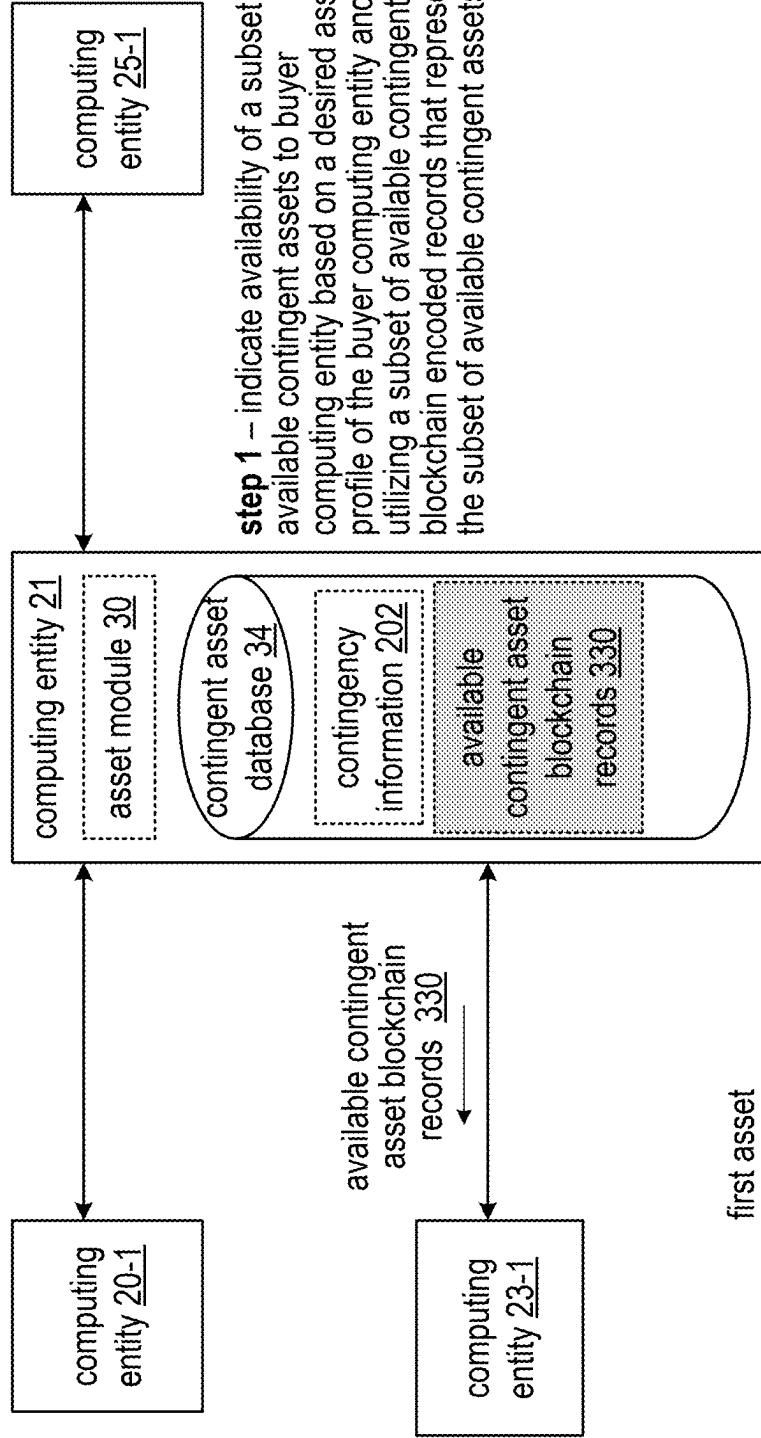


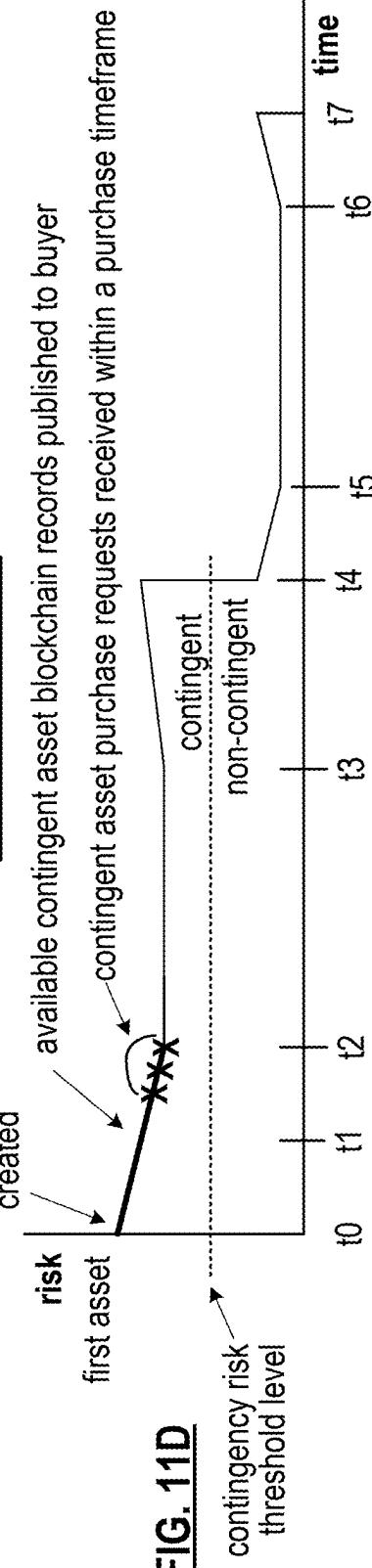
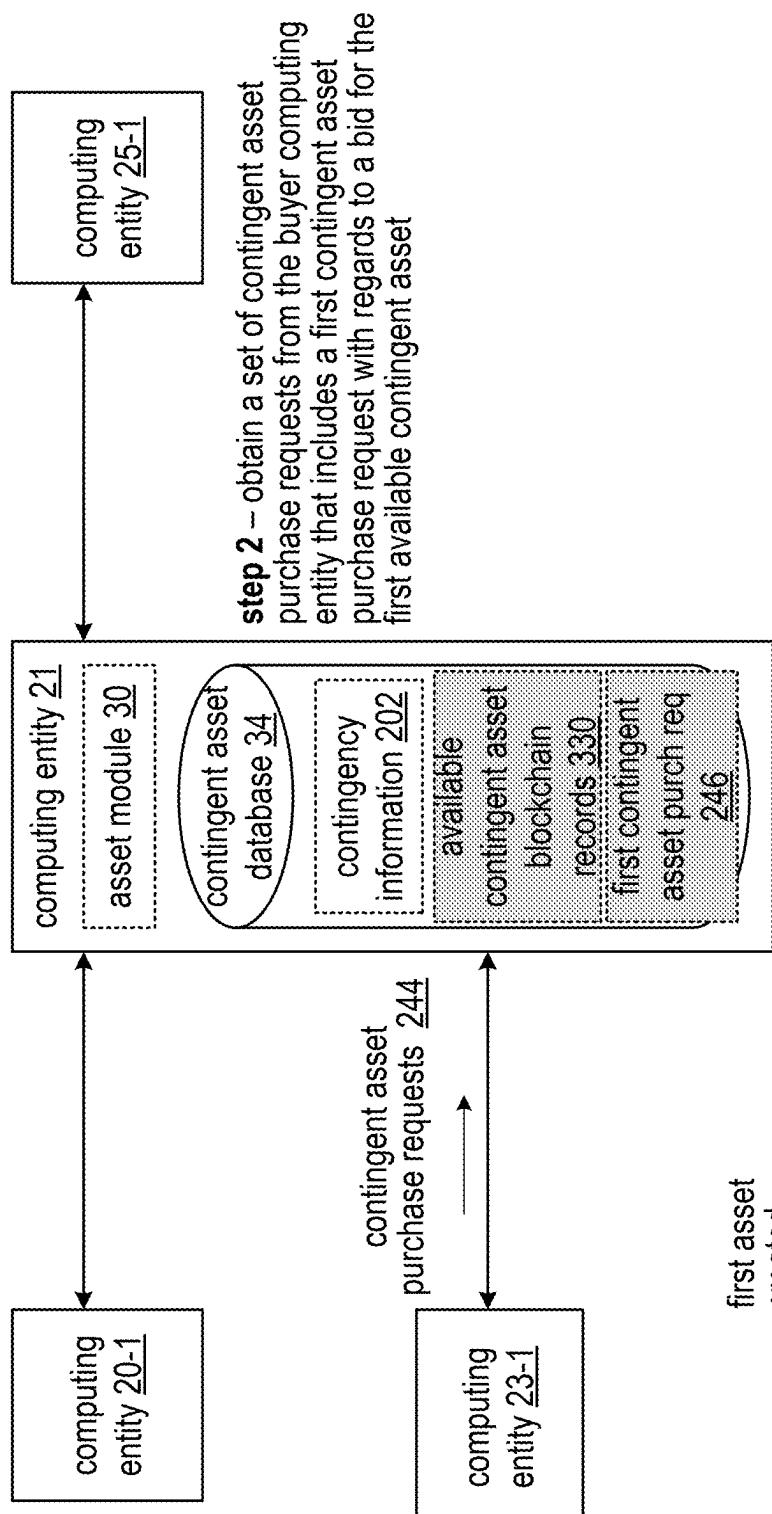


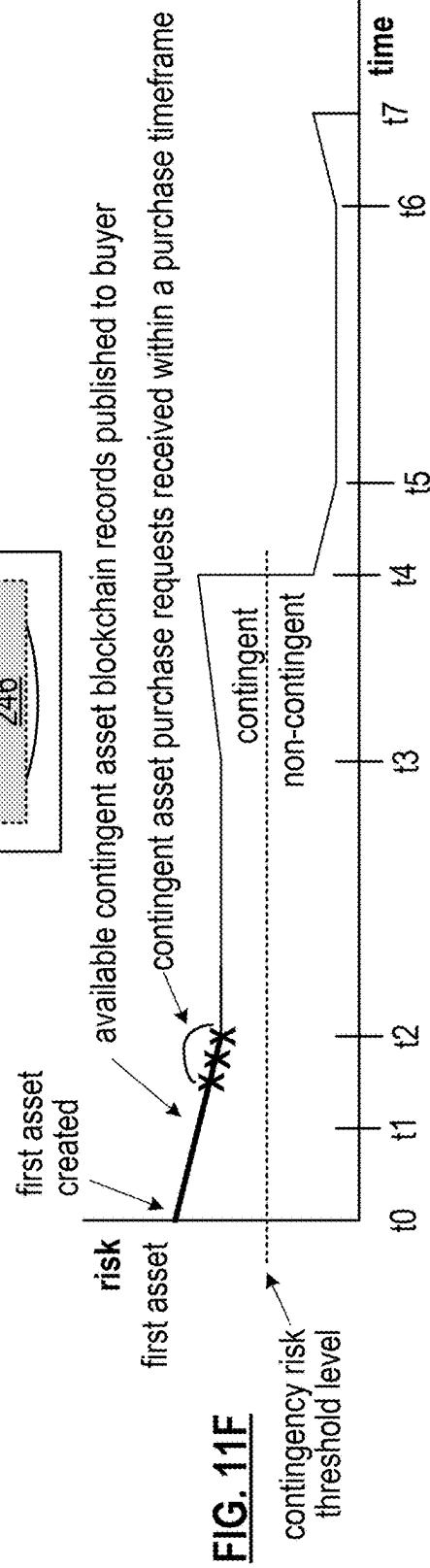
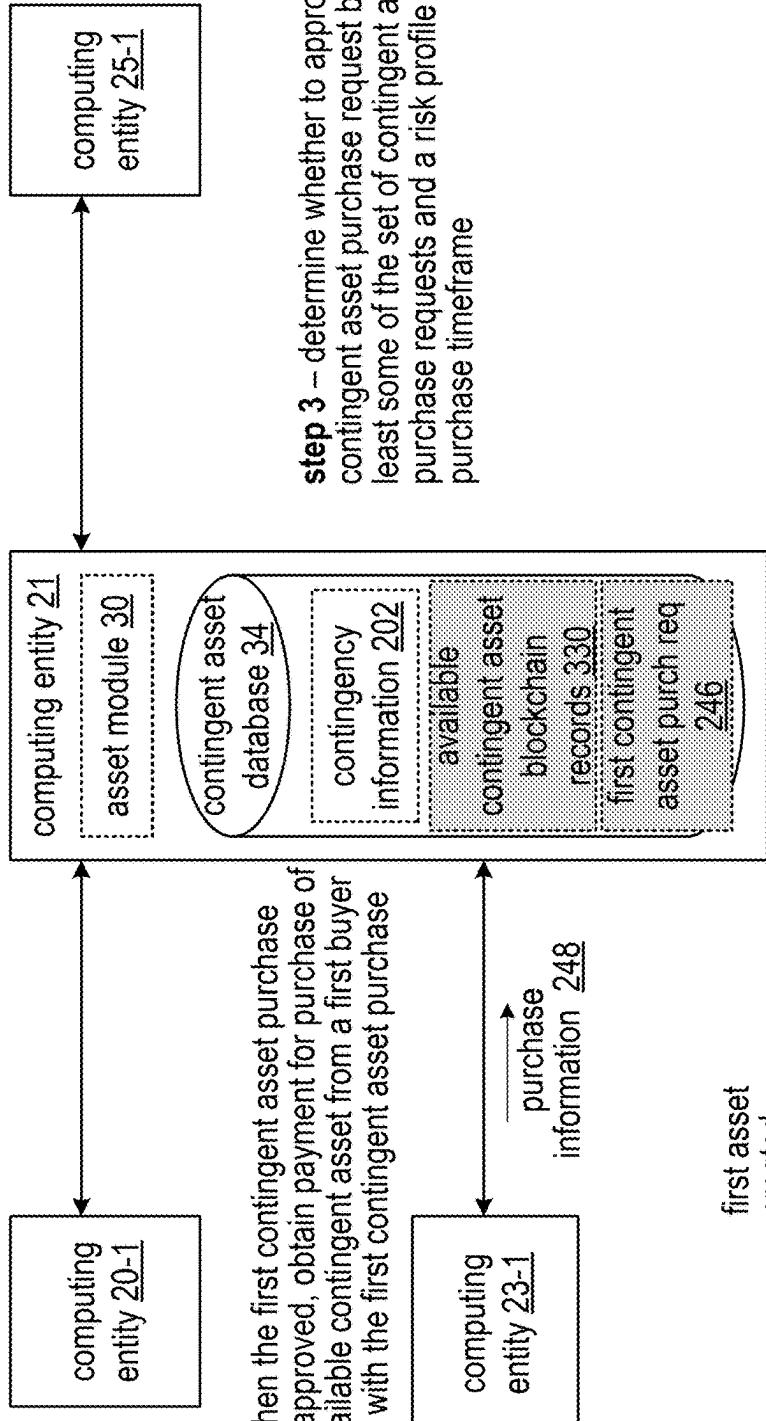


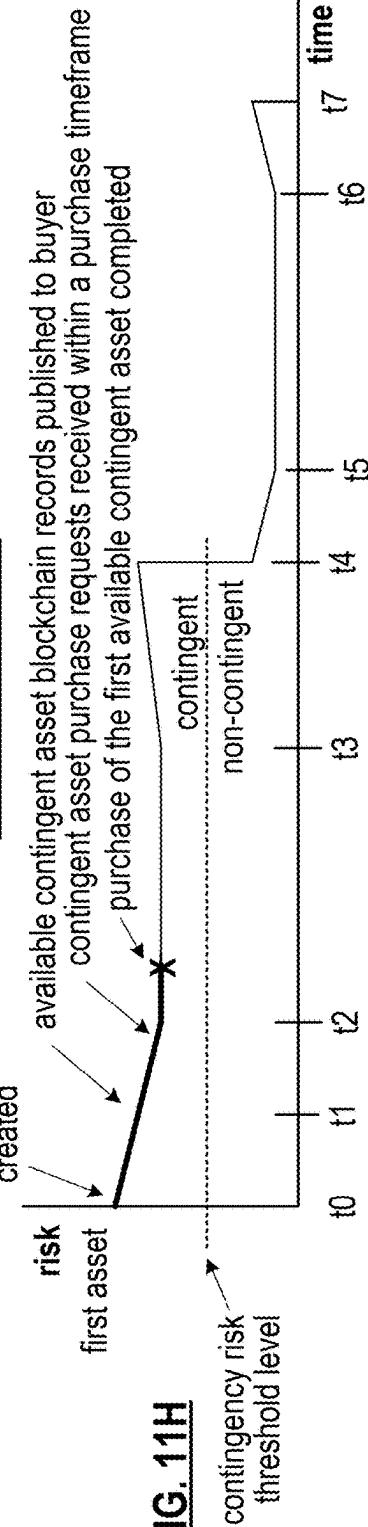
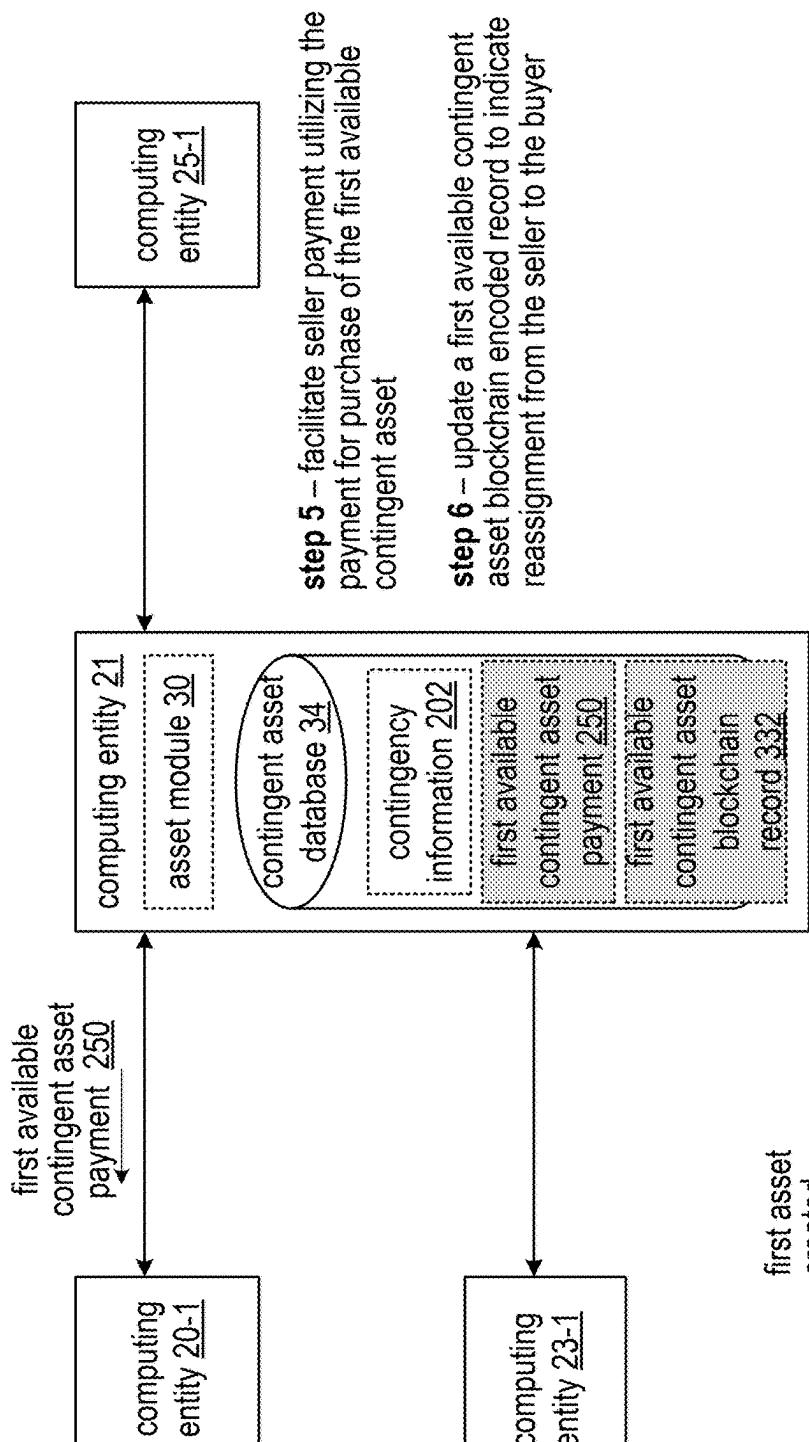
**step 5 – update the updated first available contingent asset blockchain encoded record to produce a first non-contingent asset blockchain encoded record when the first asset risk level is less than the contingency risk threshold level**

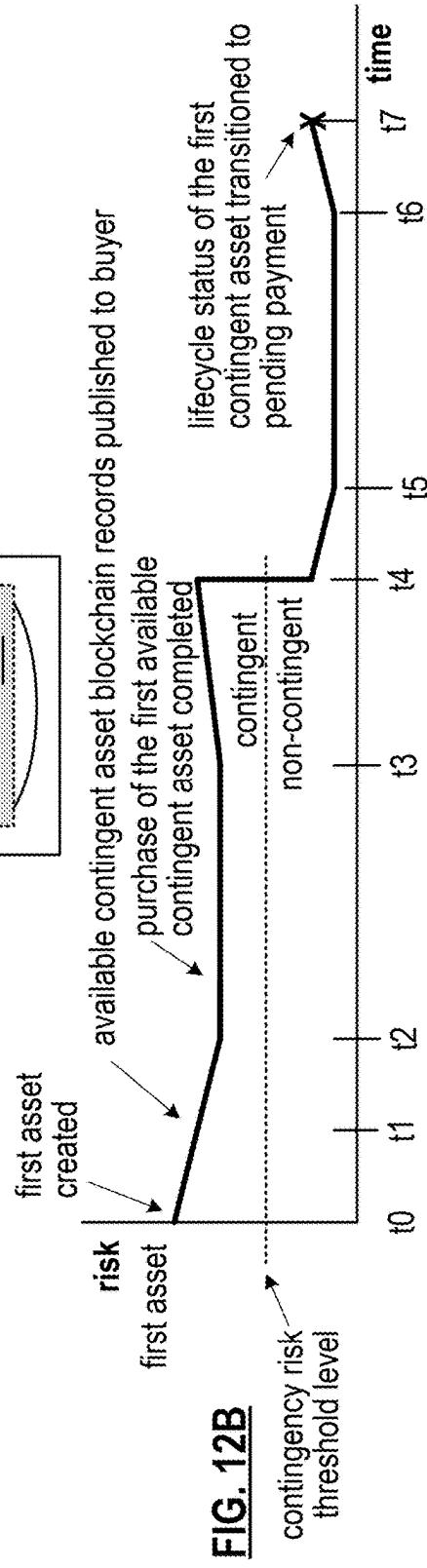
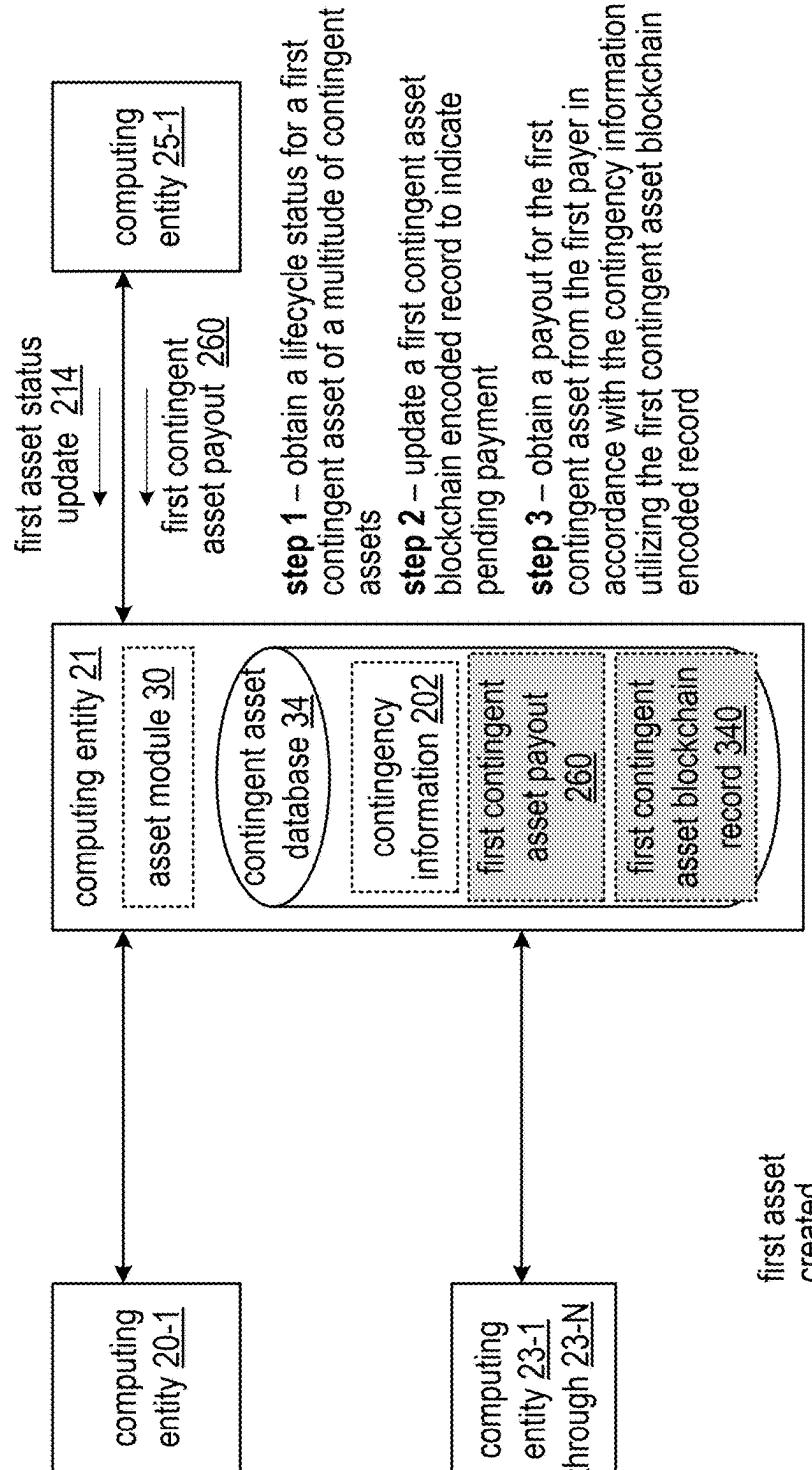


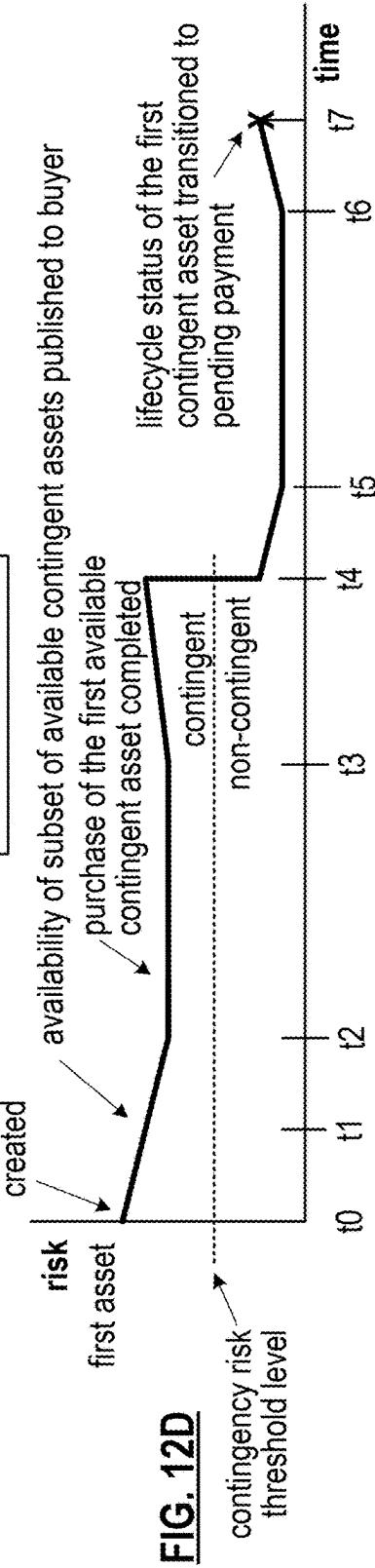
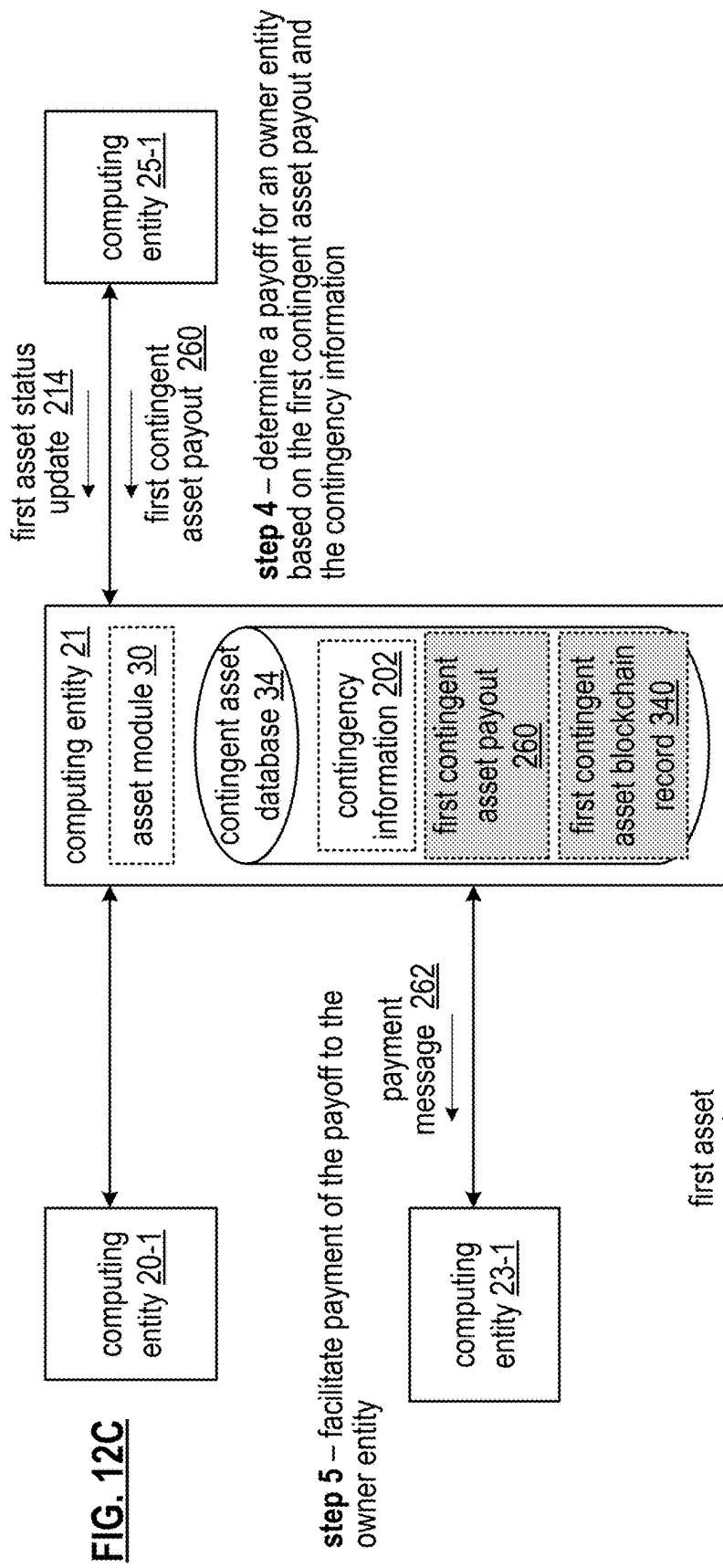


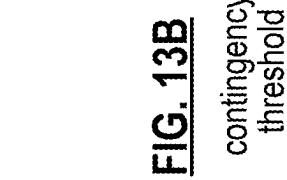
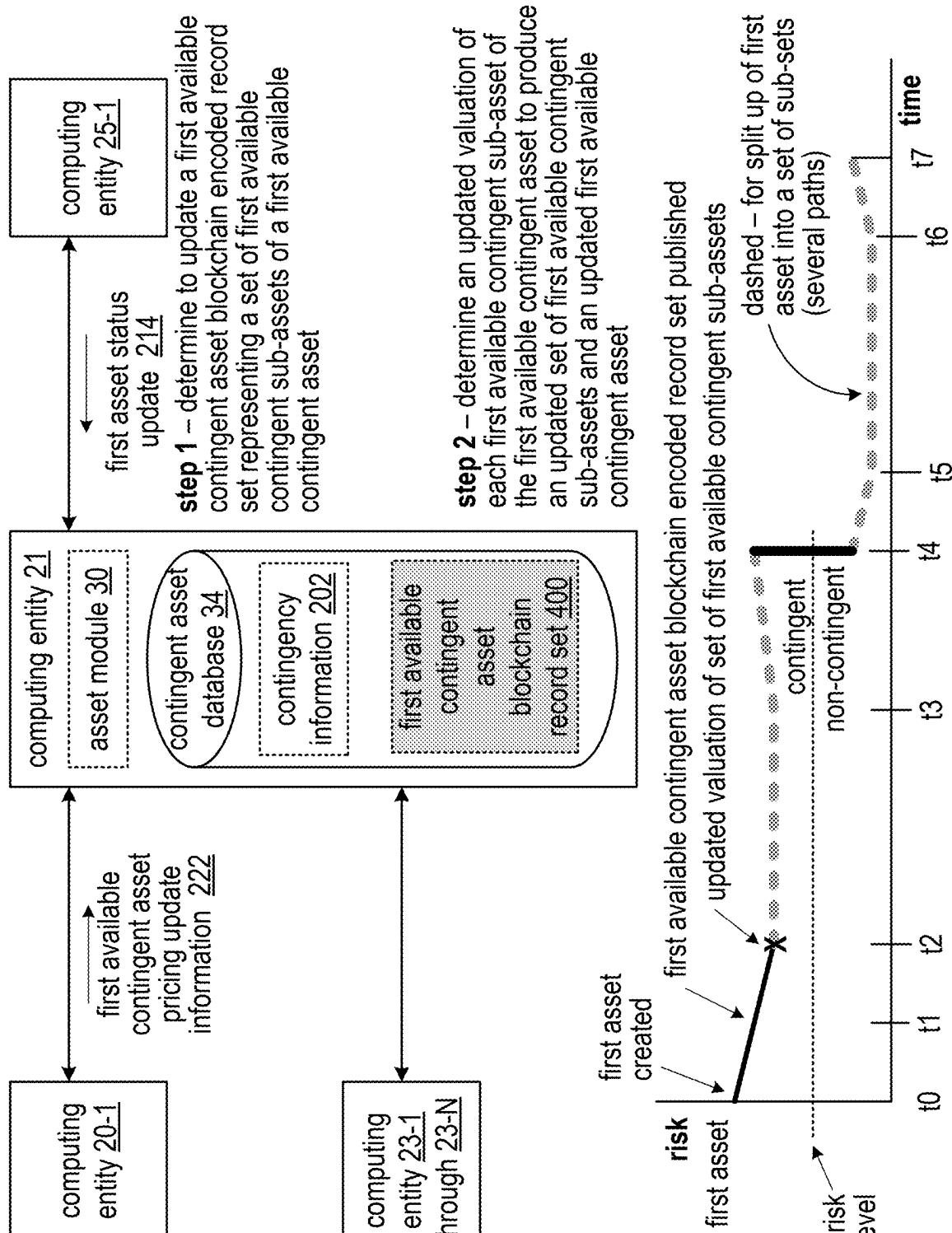


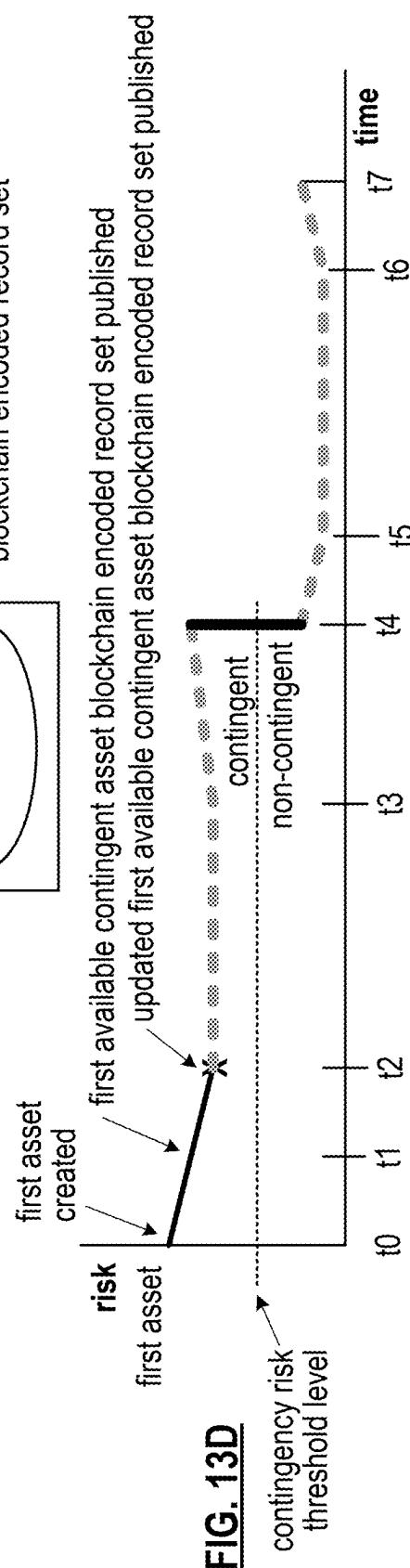
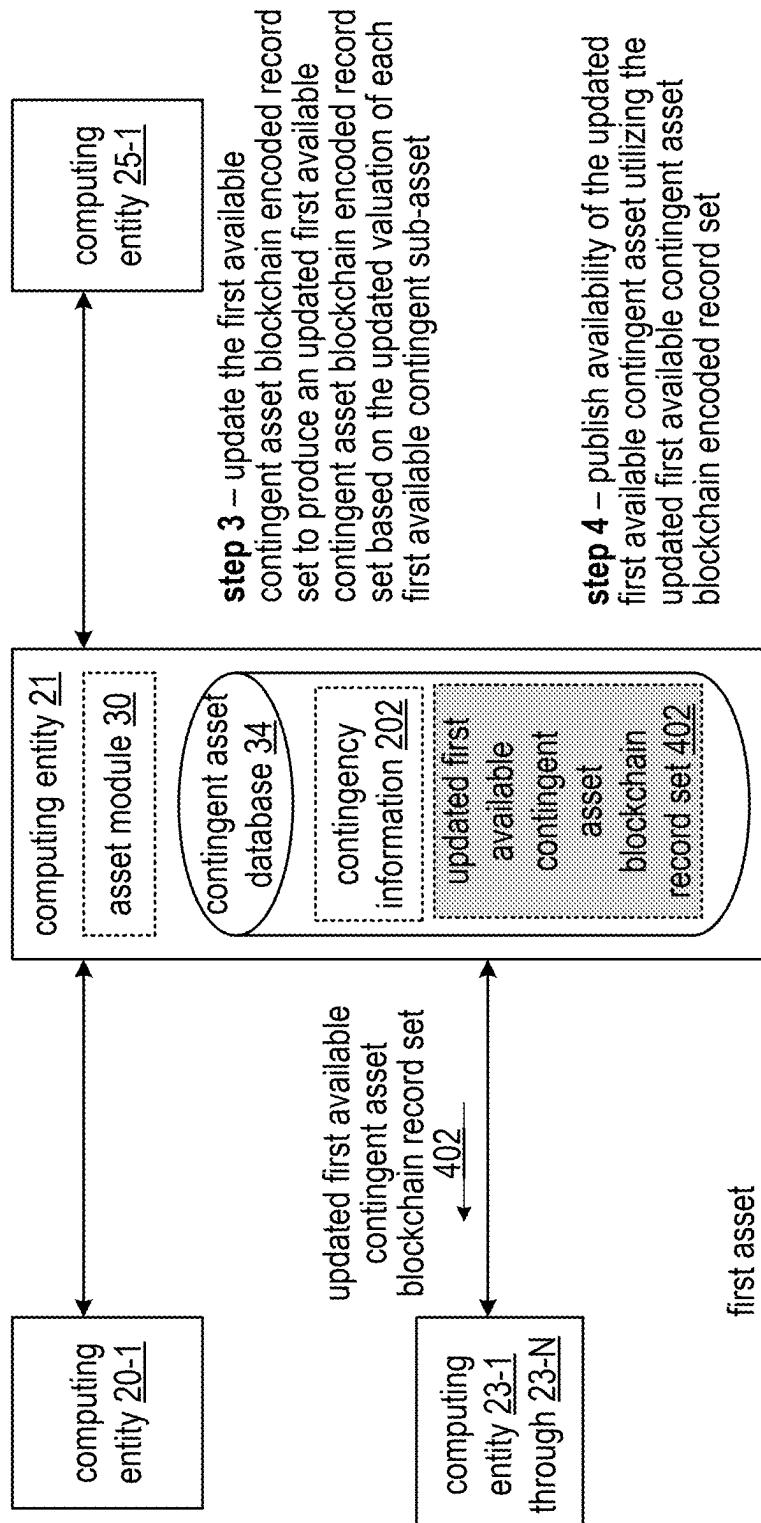


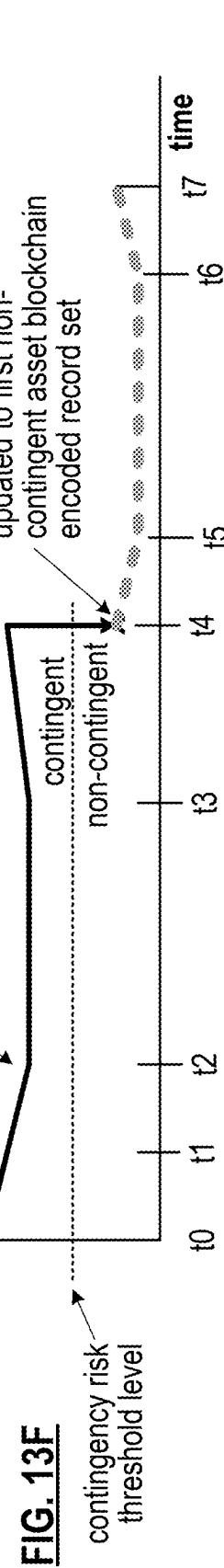
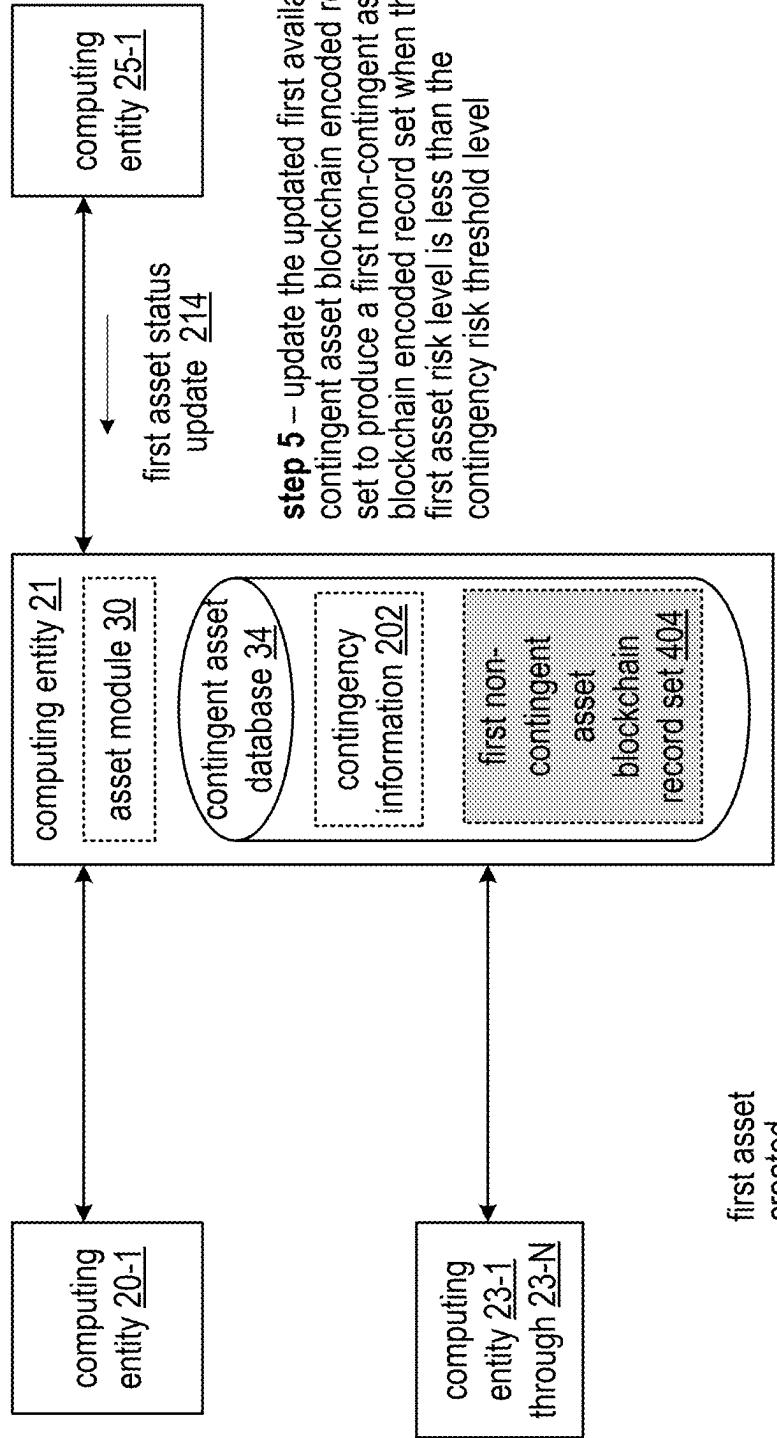


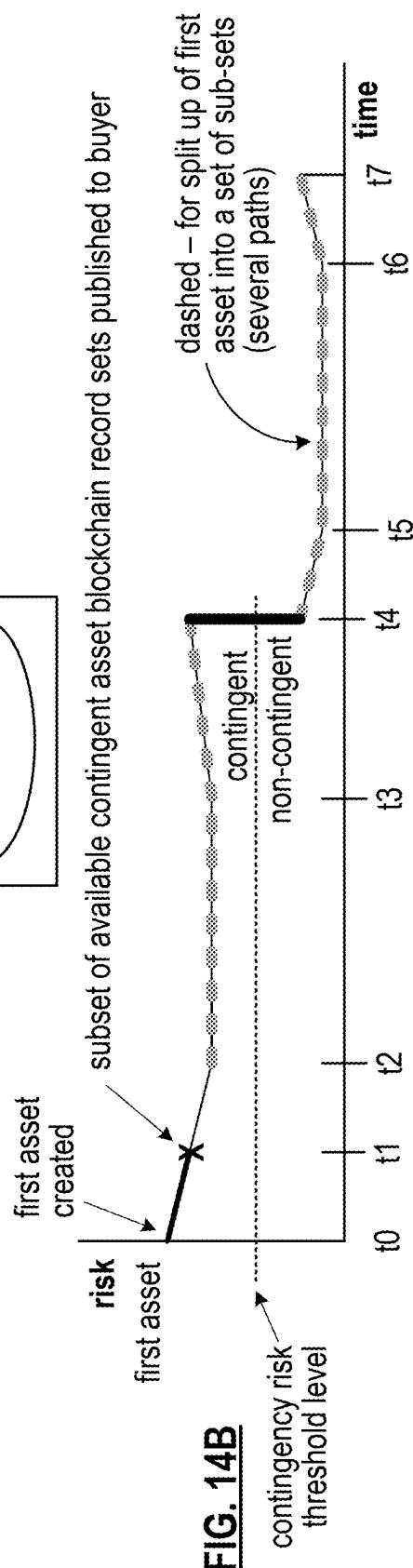
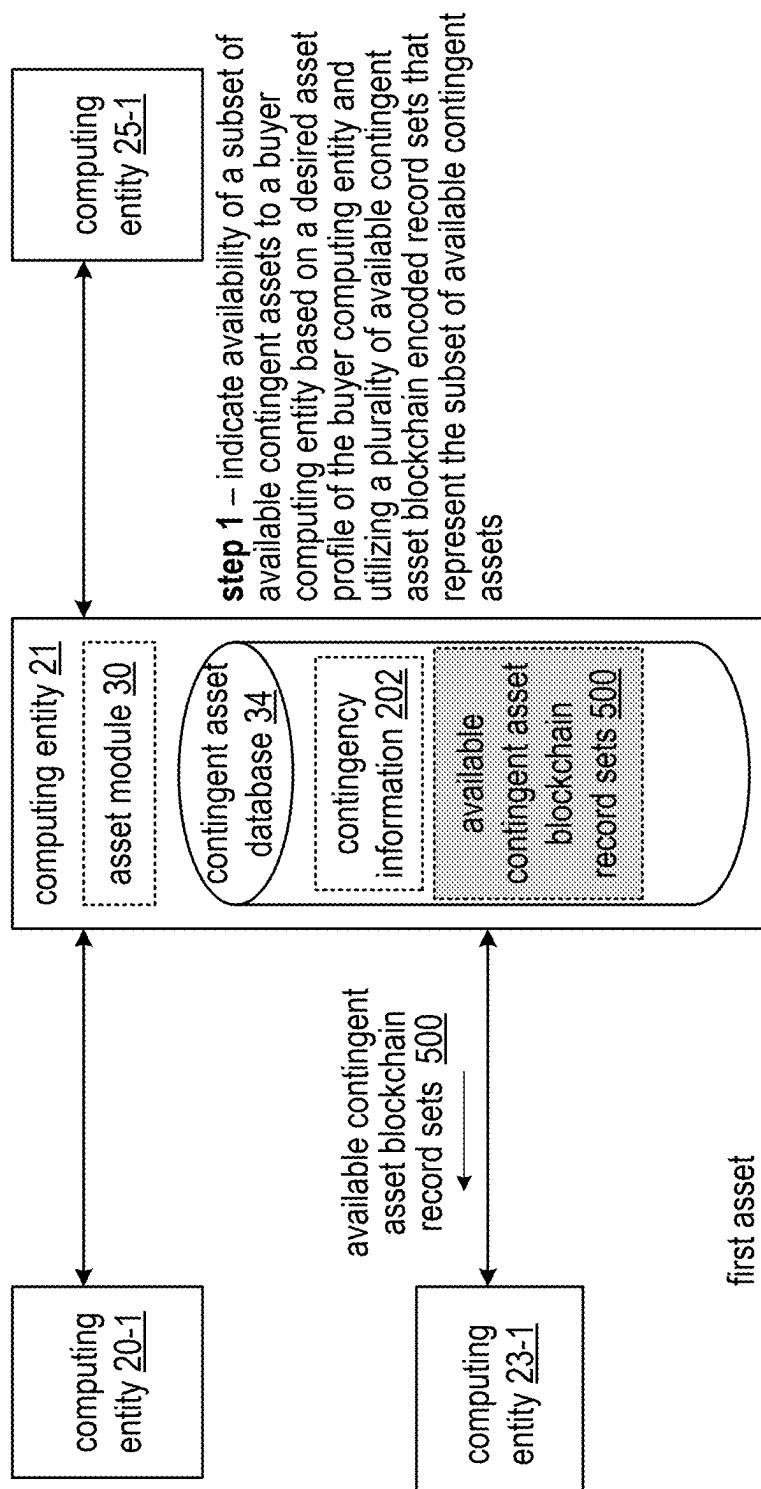


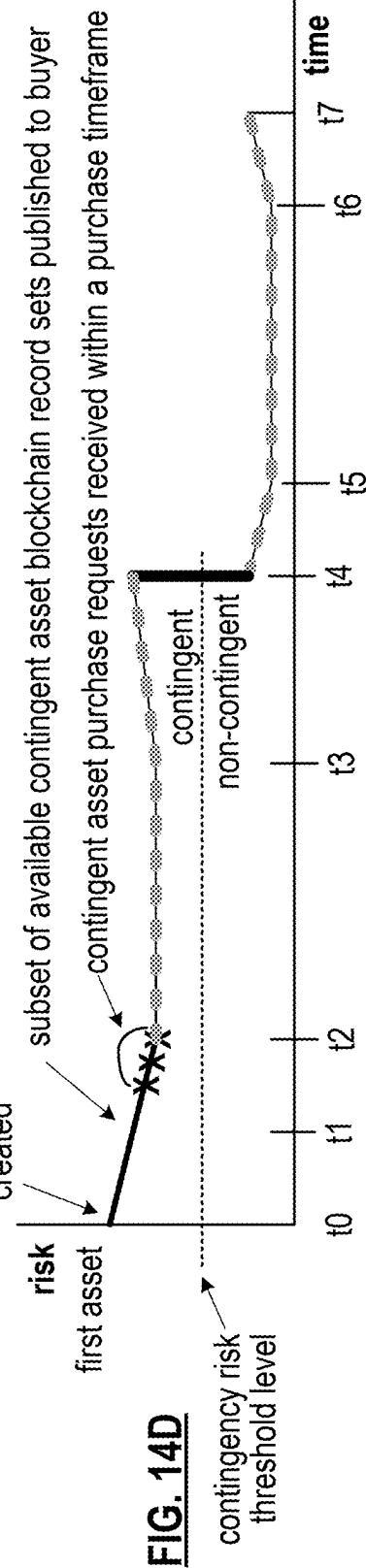
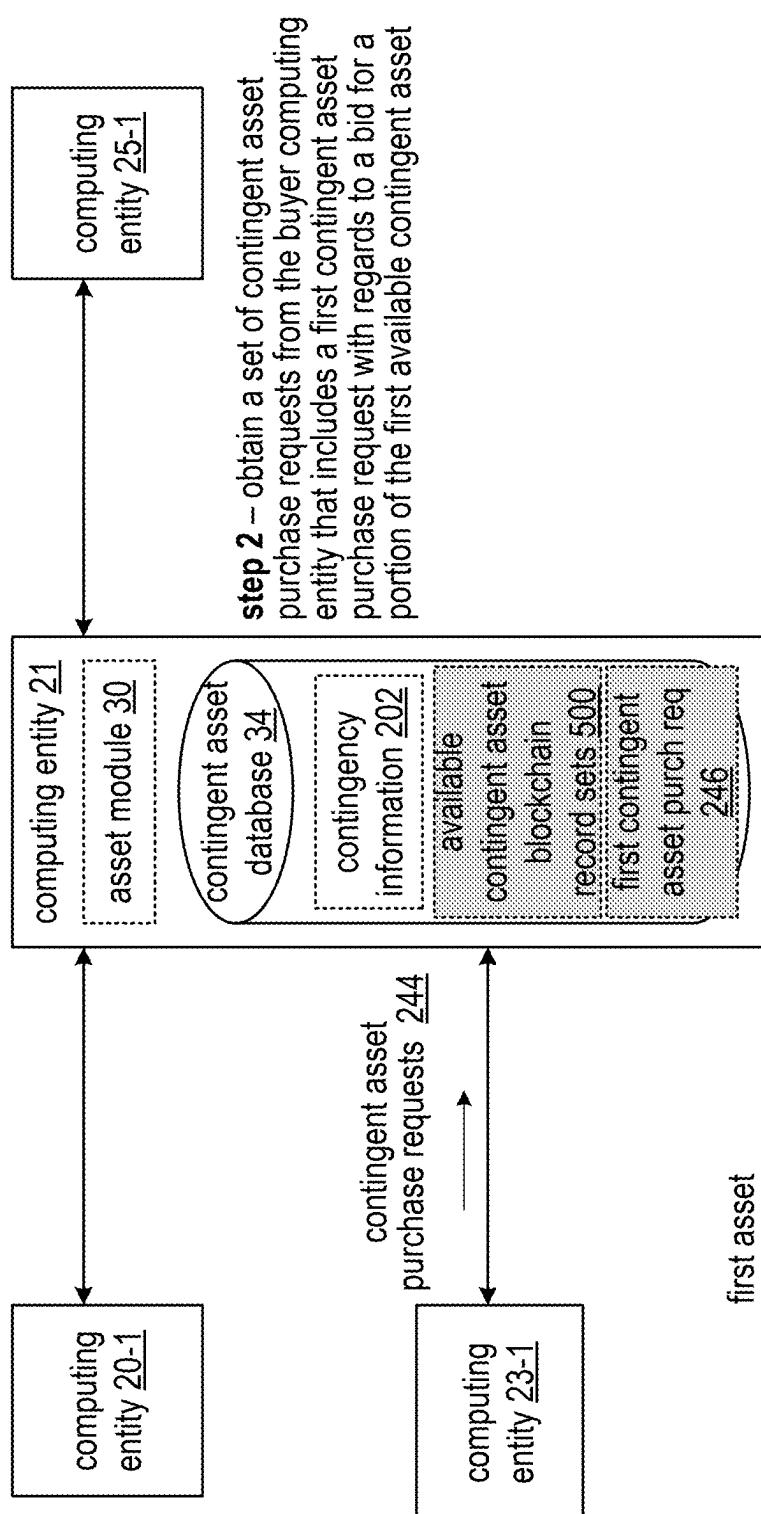


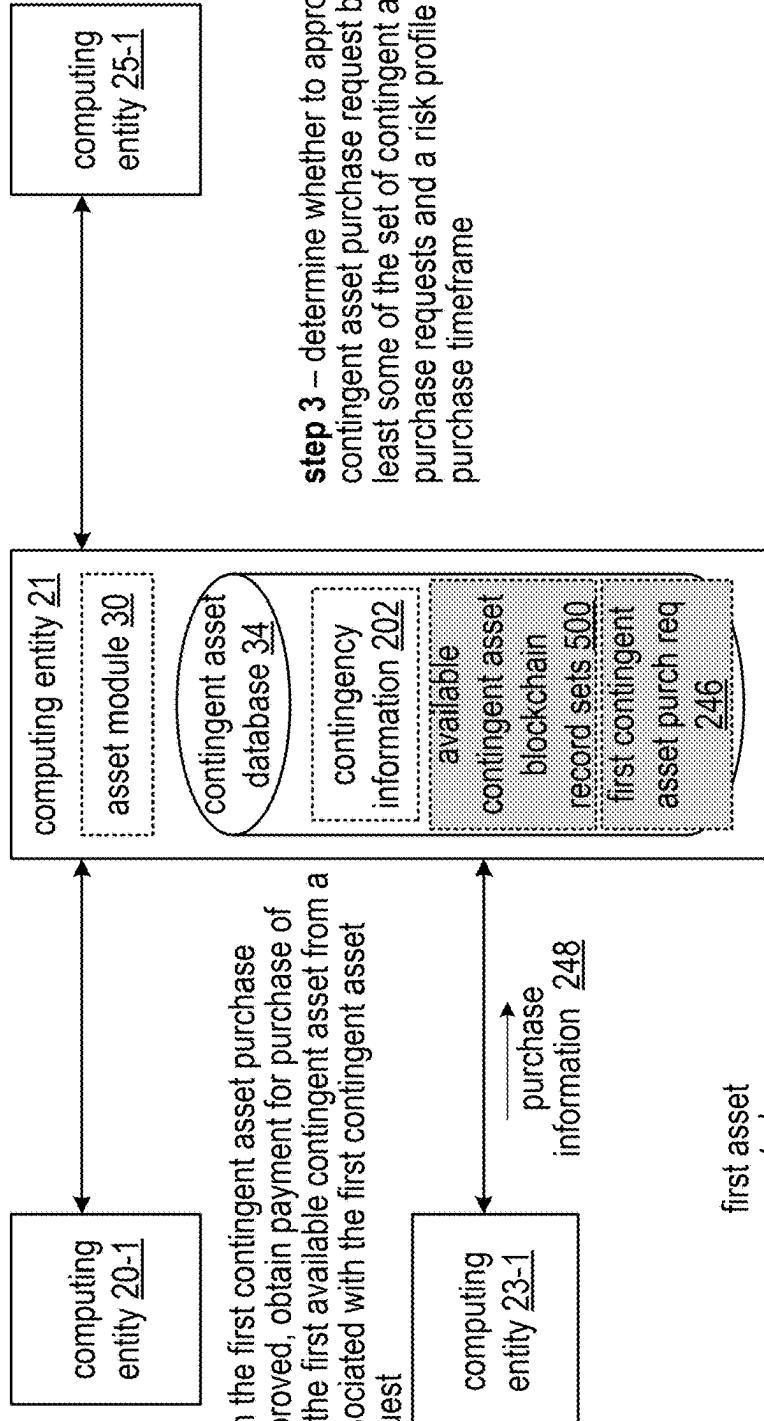




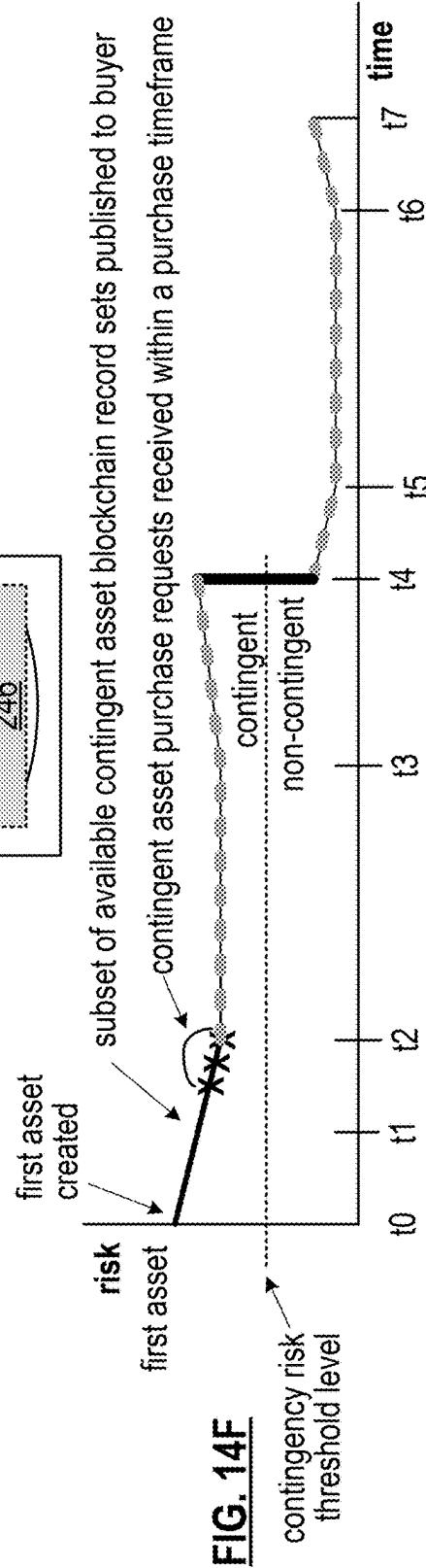


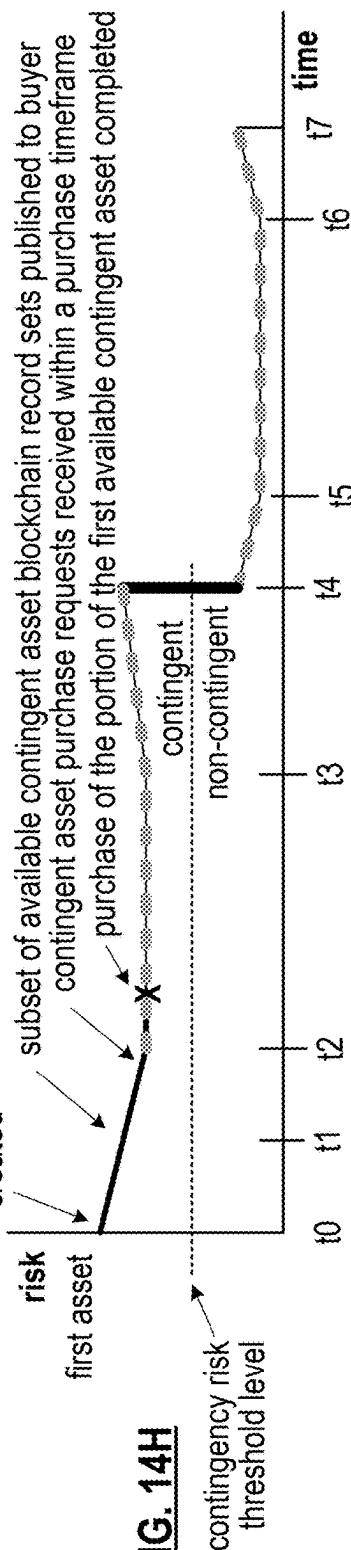
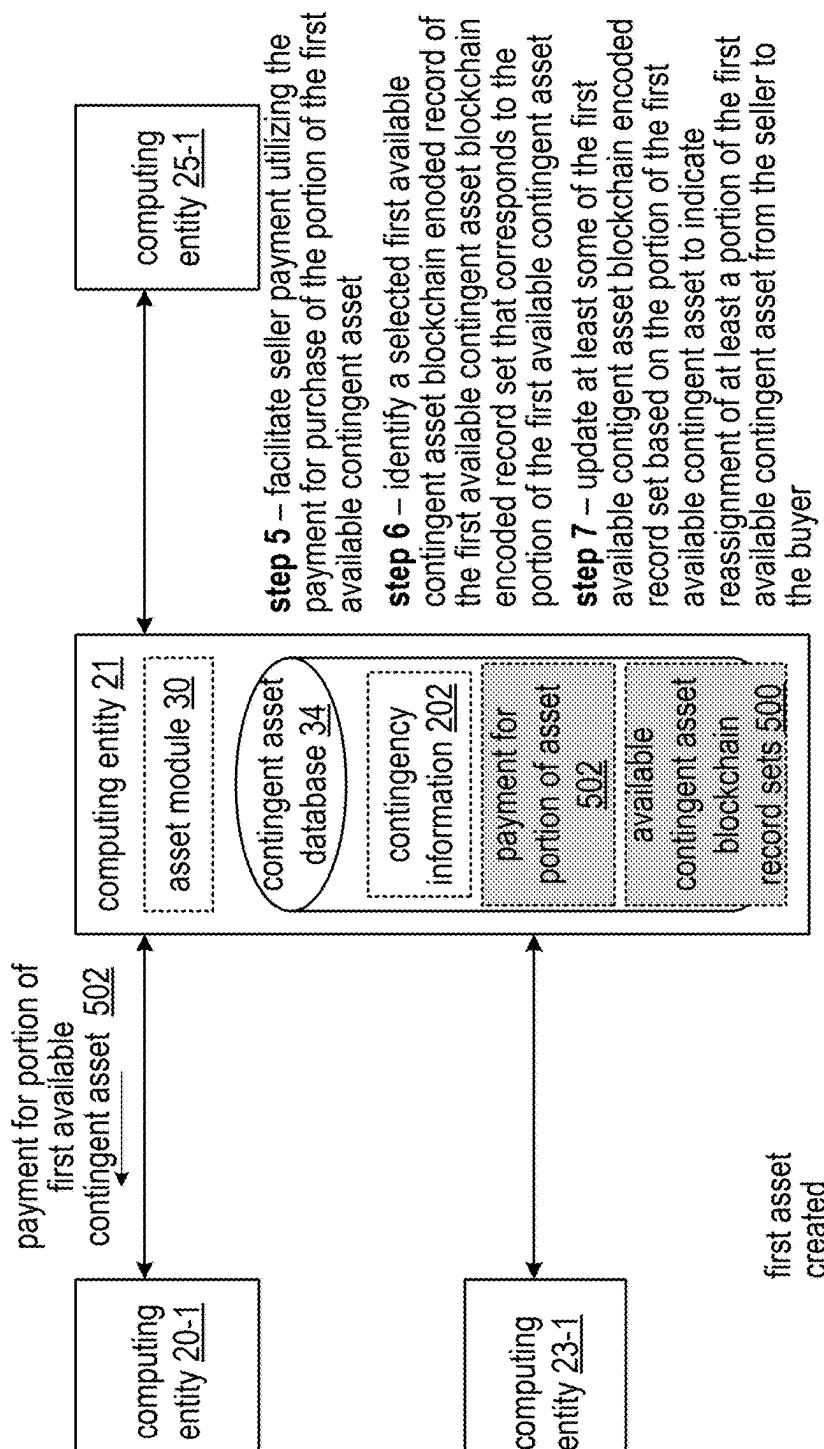


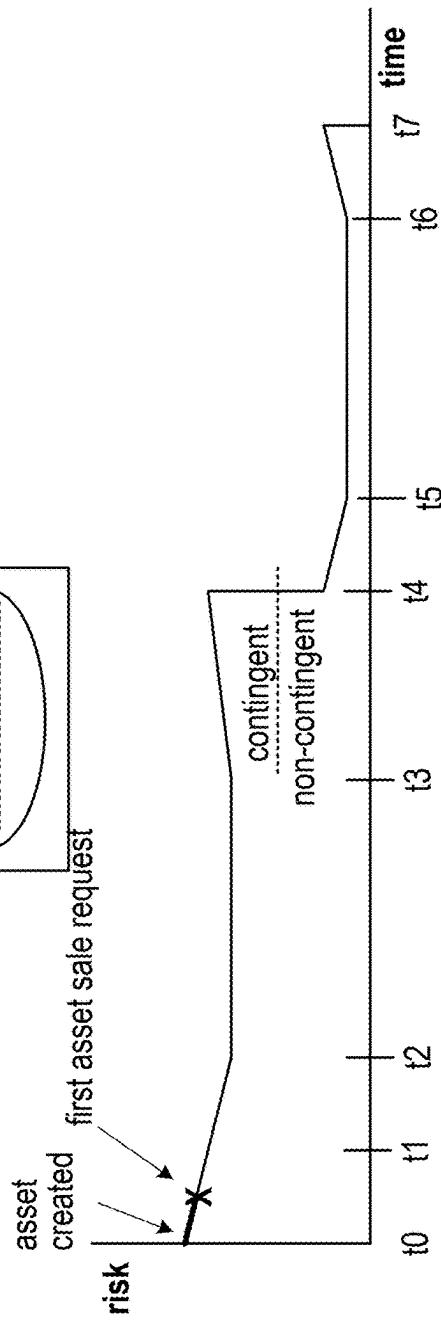
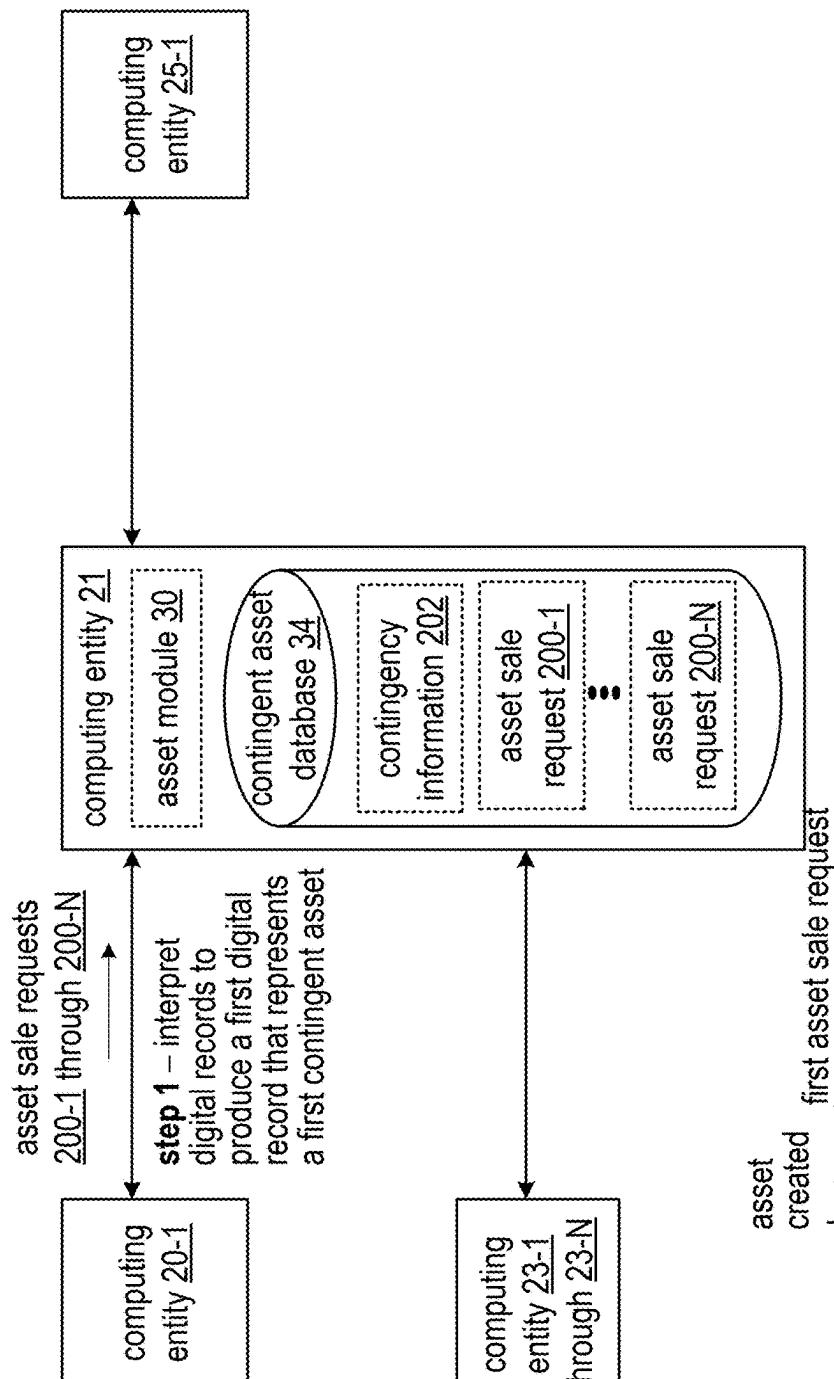




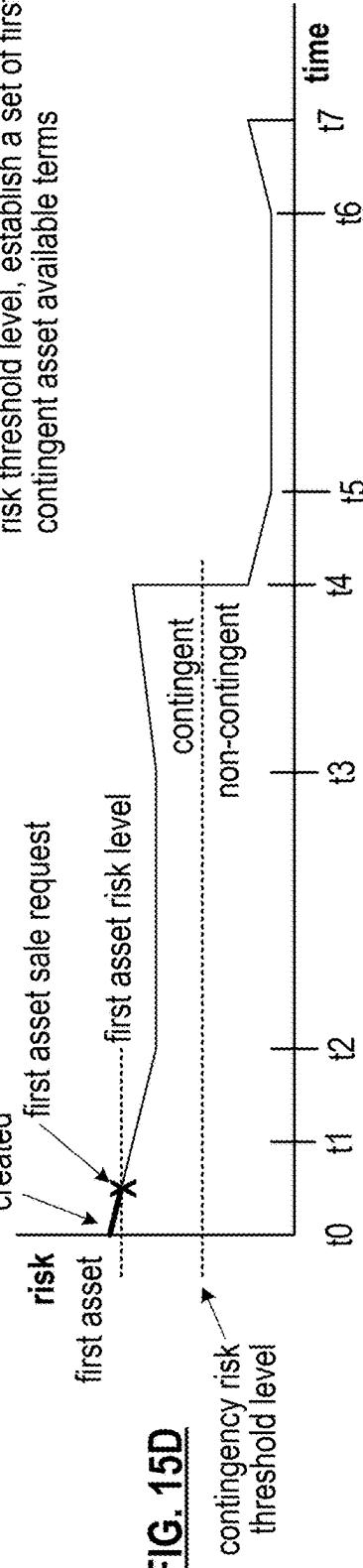
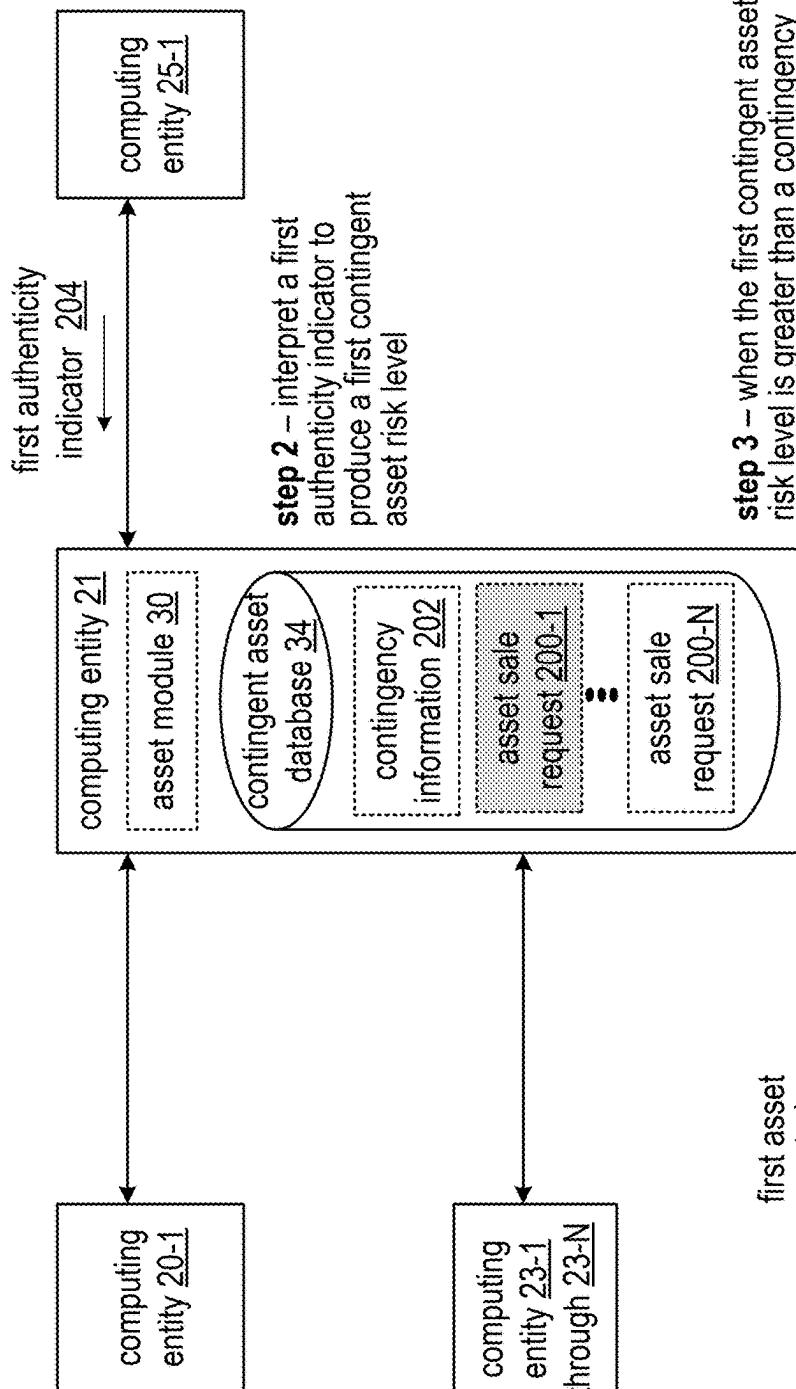
**step 3 –** determine whether to approve the first contingent asset purchase request based on at least some of the set of contingent asset purchase requests and a risk profile during the purchase timeframe

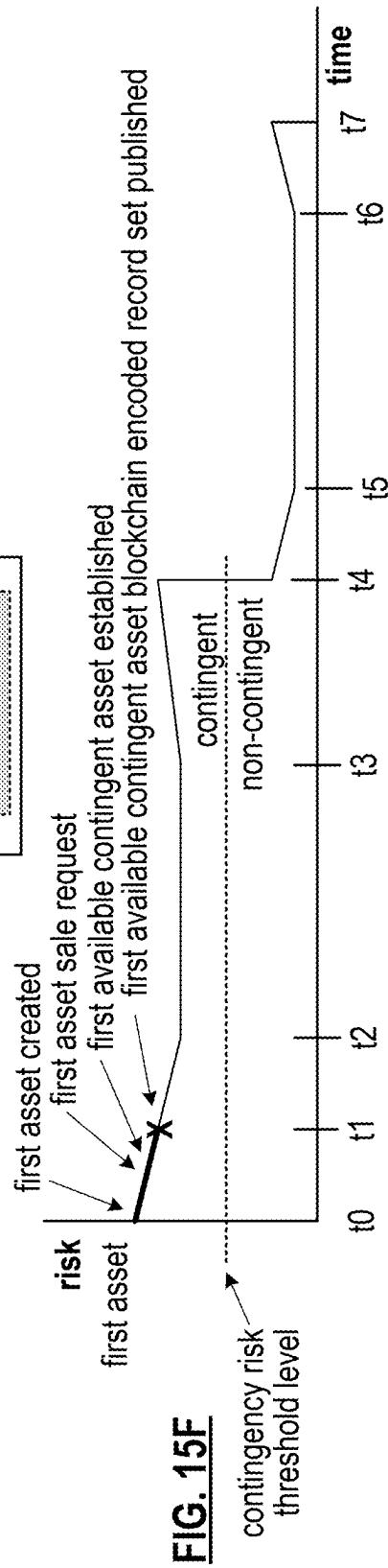
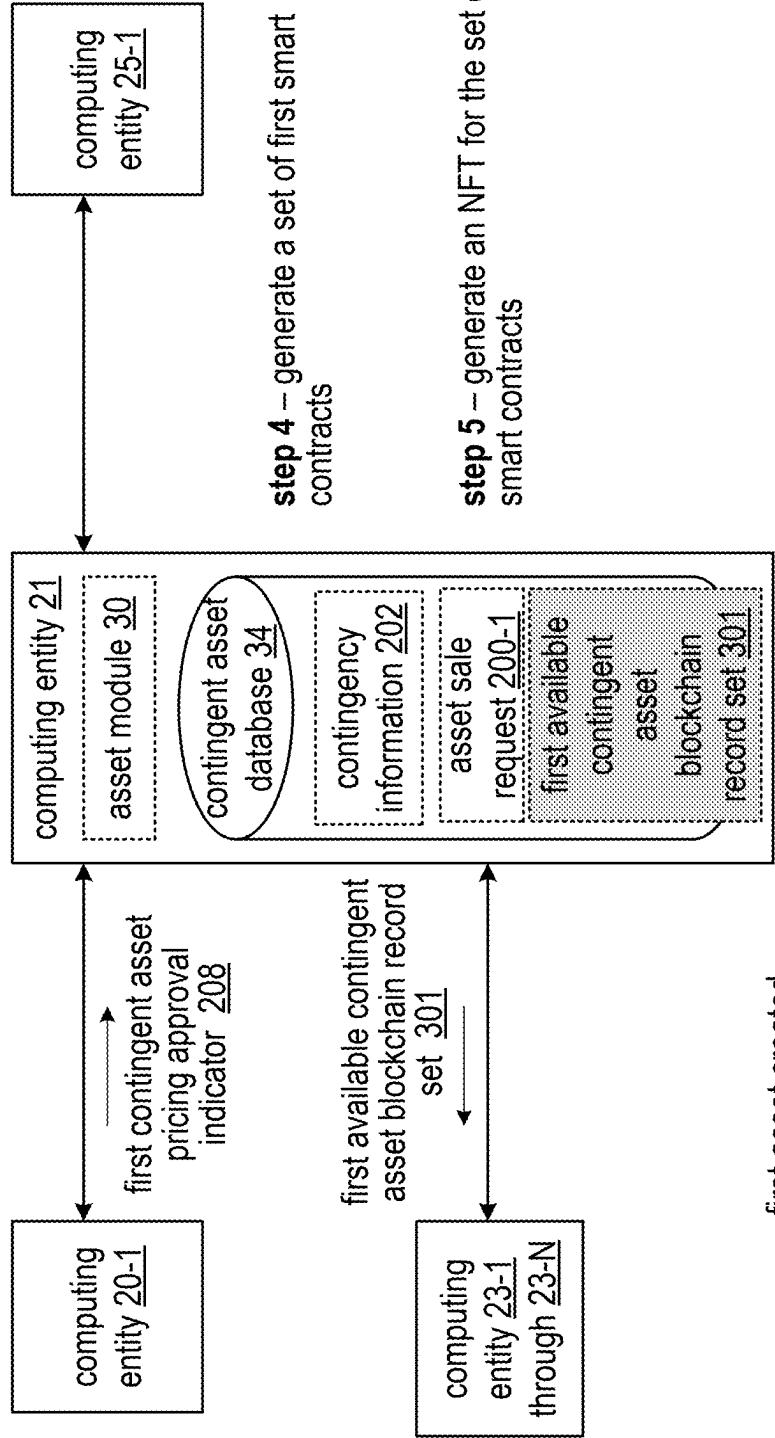


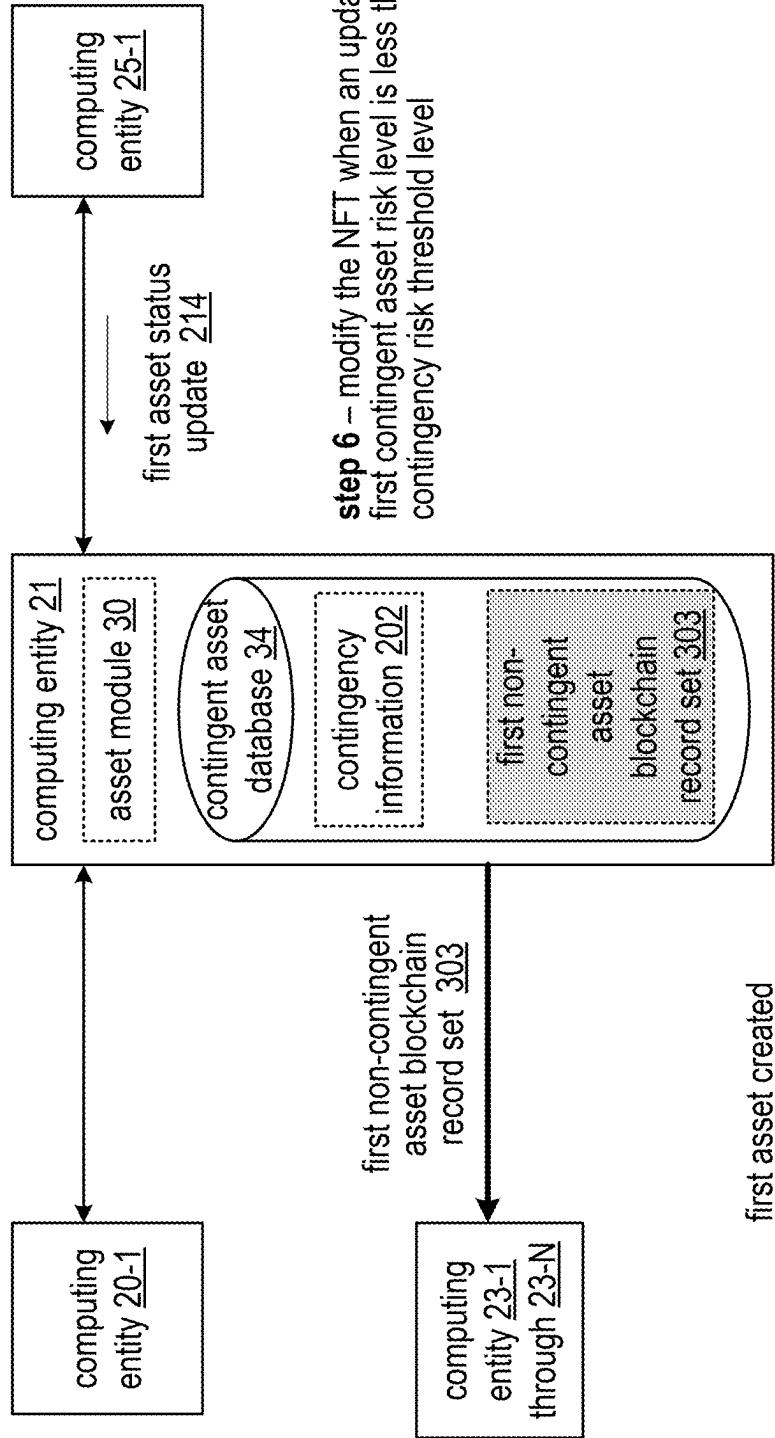




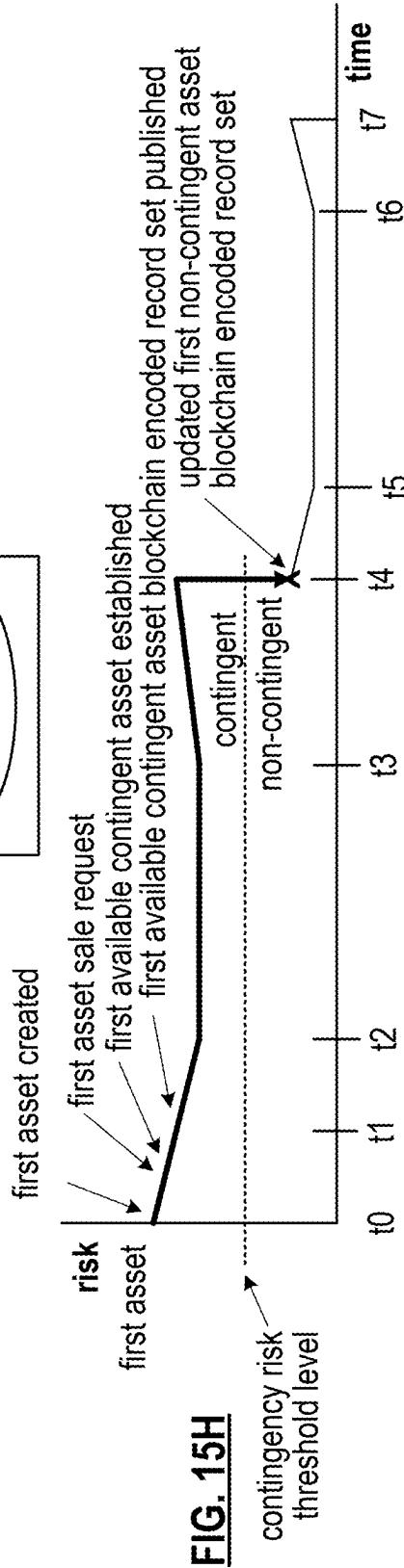
**FIG. 15B**

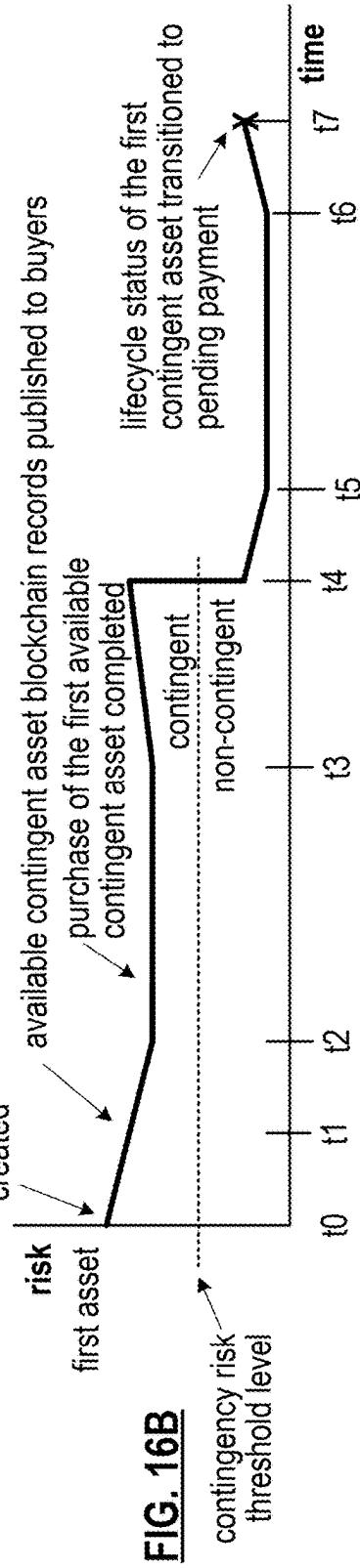
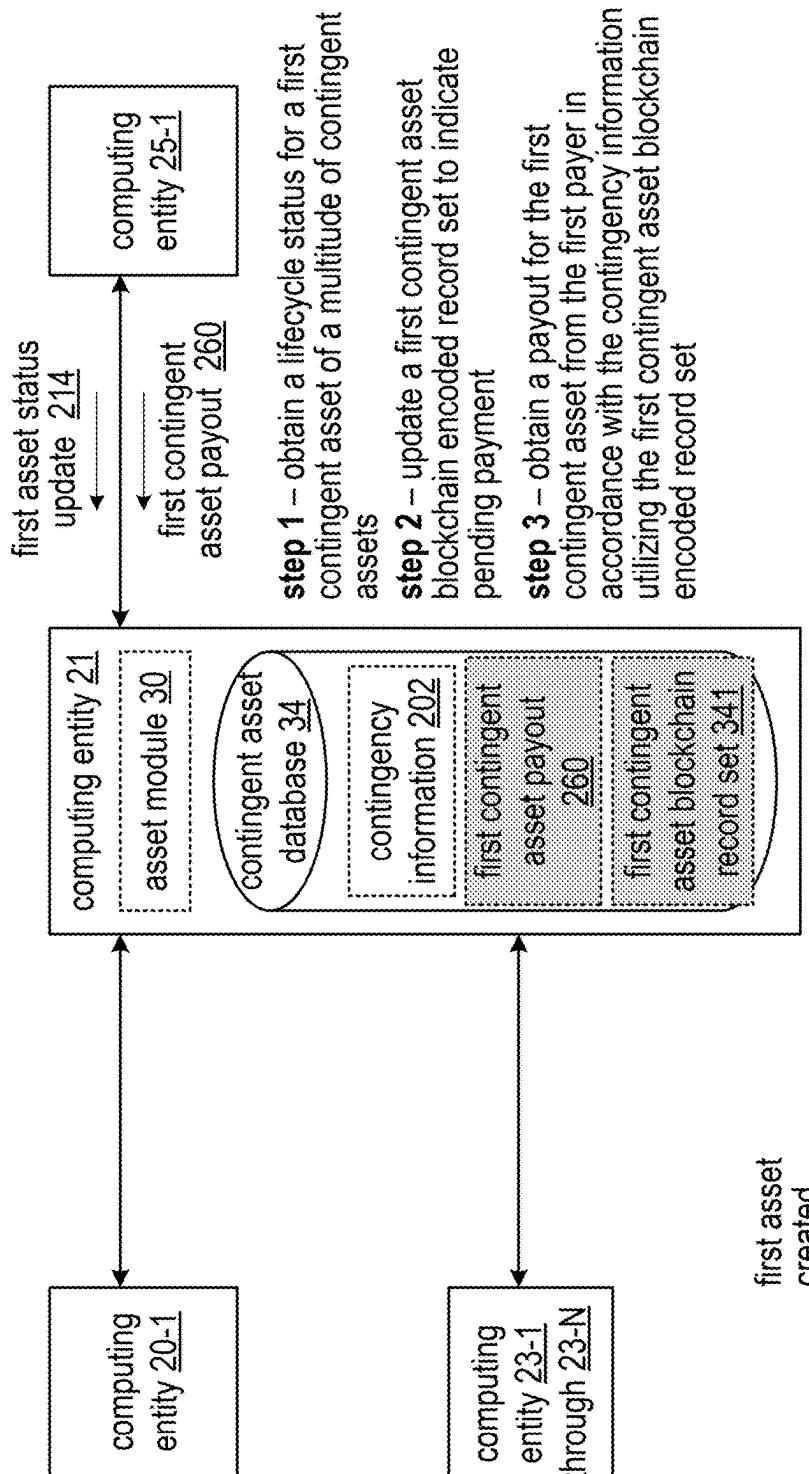


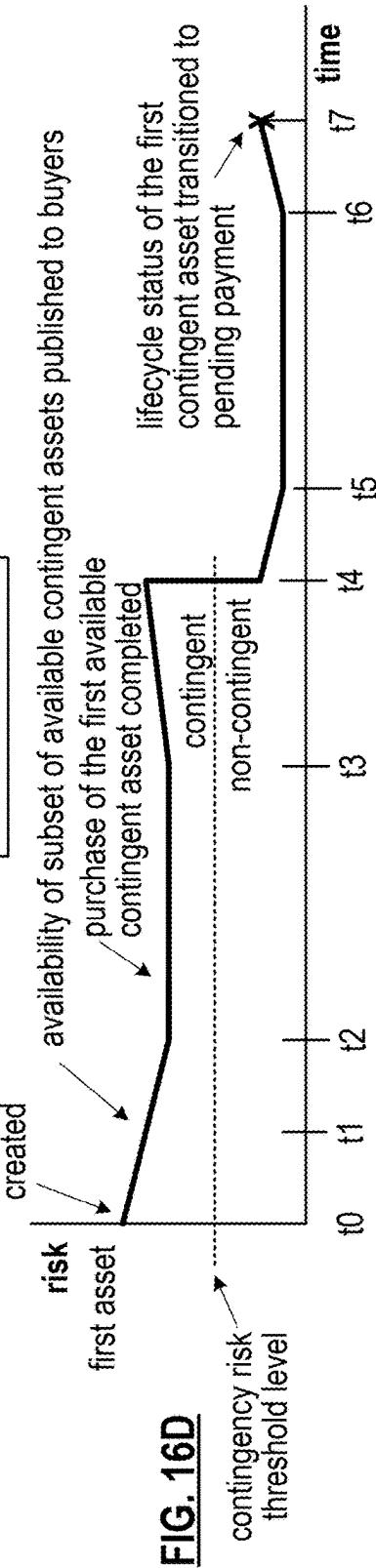
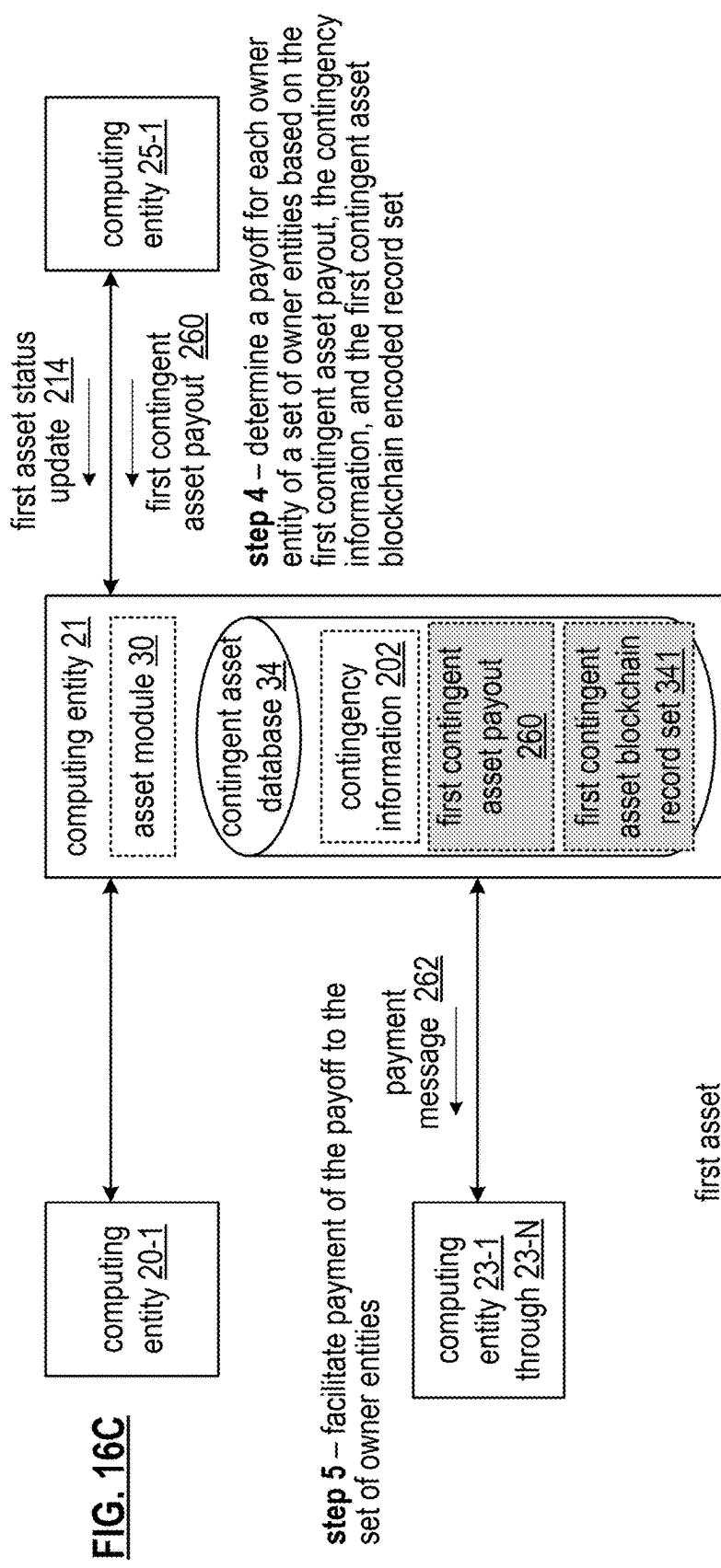


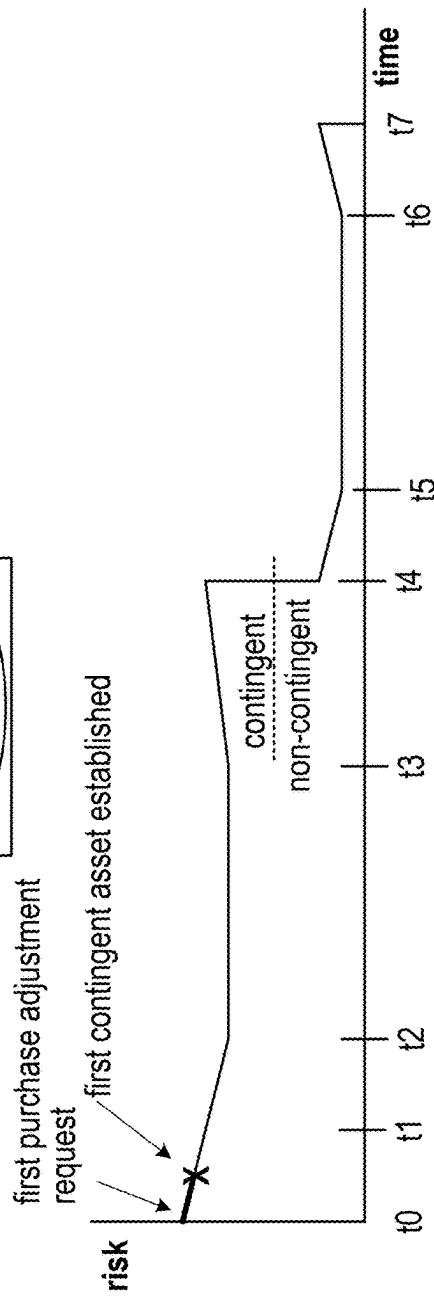
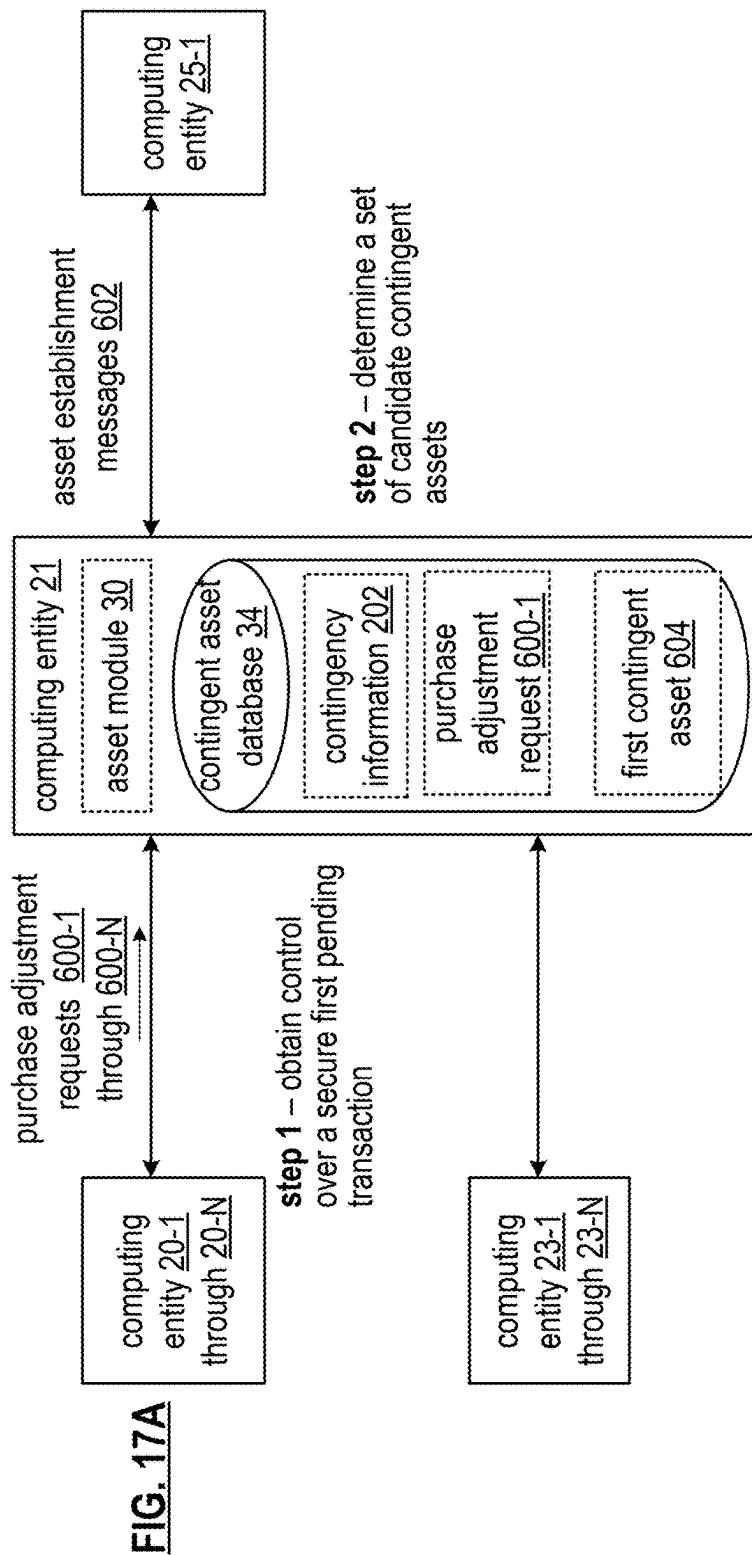


**step 6 – modify the NFT when an updated first contingent asset risk level is less than the contingency risk threshold level**

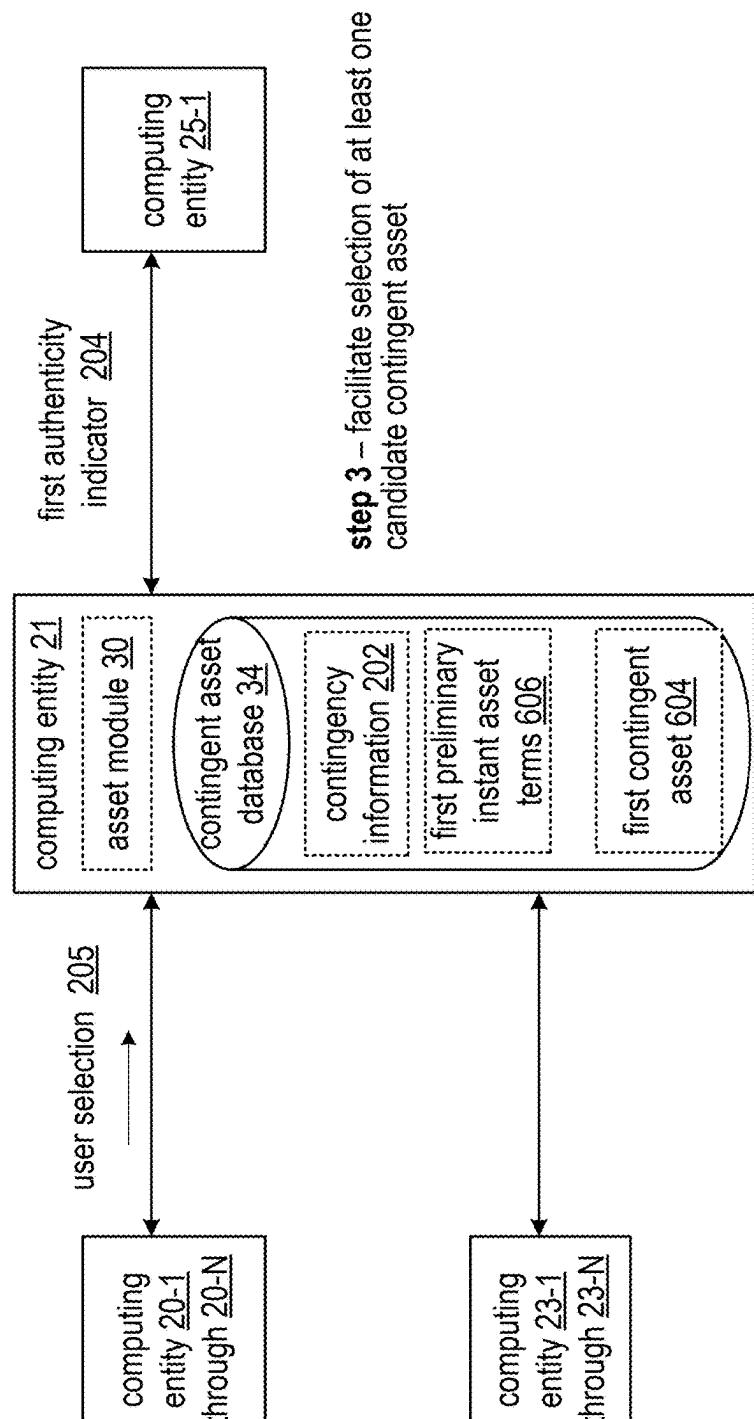








**FIG. 17B**

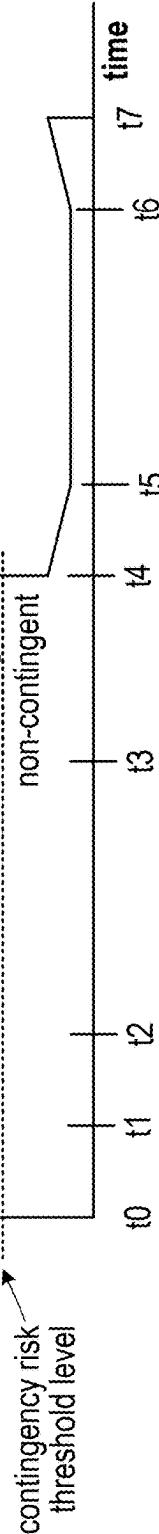


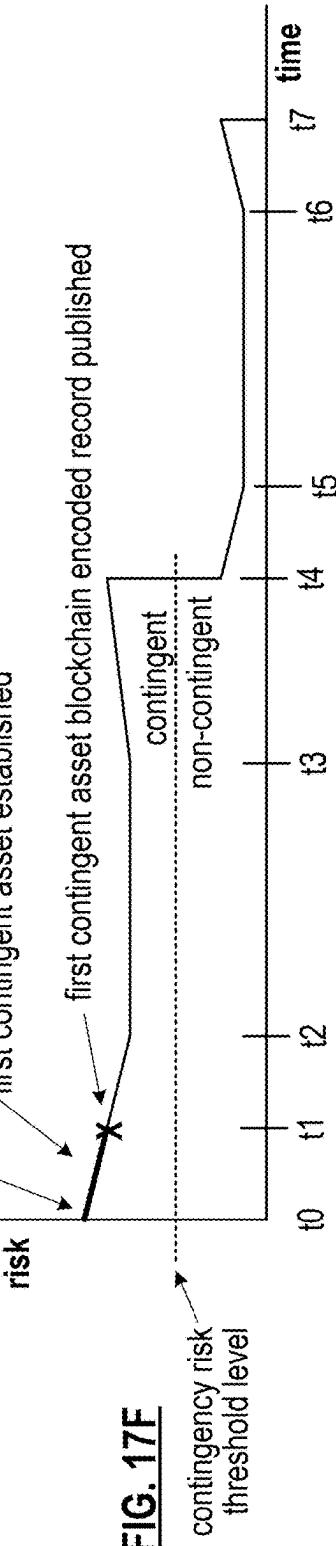
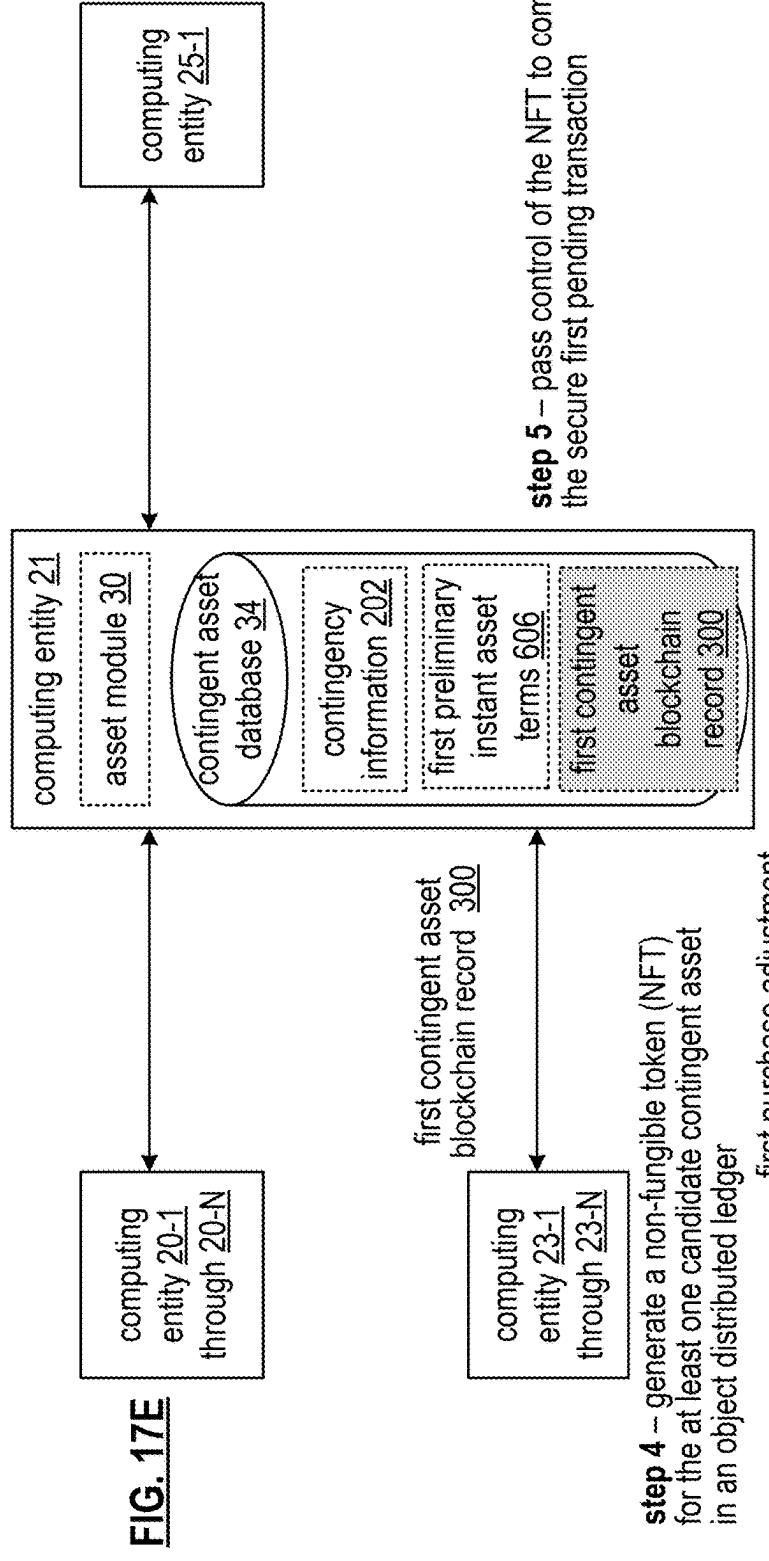
**step 3 – facilitate selection of at least one candidate contingent asset**

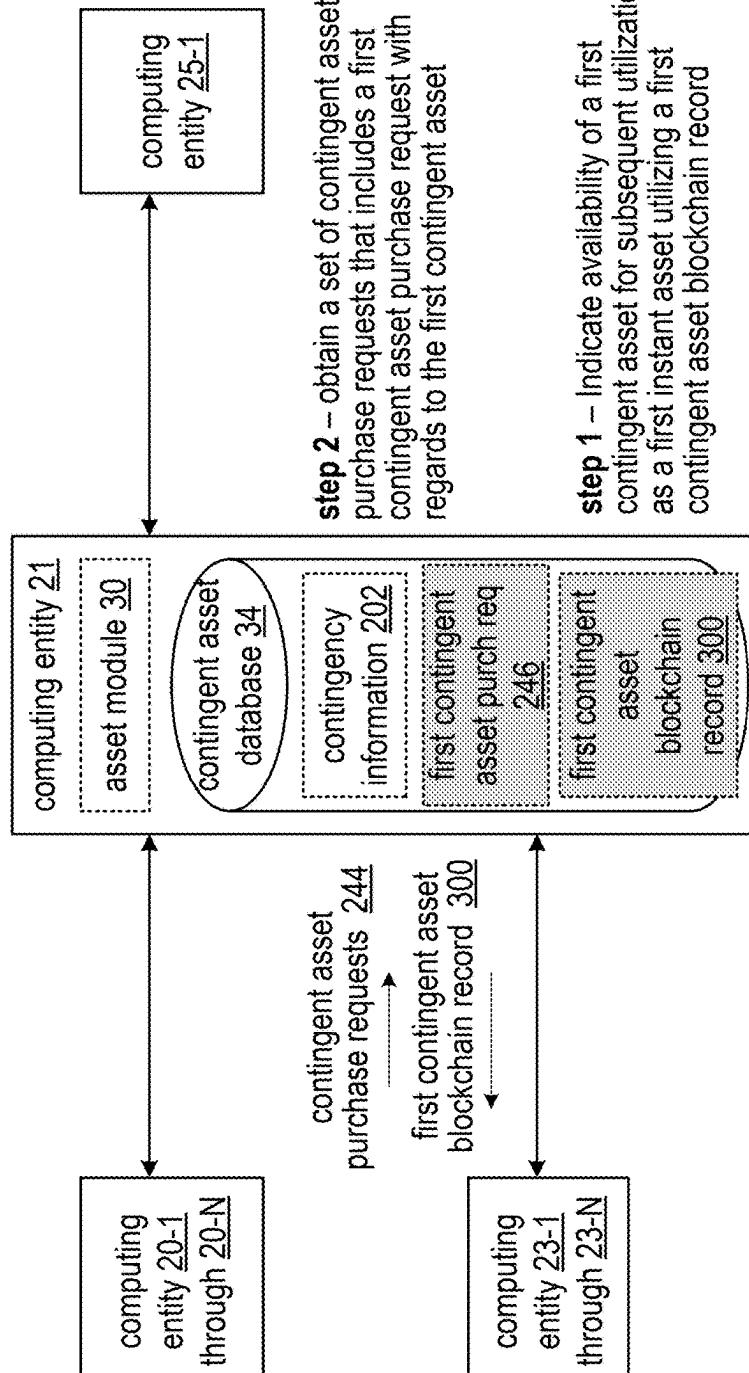
first purchase adjustment request  
first contingent asset established



**FIG. 17D**







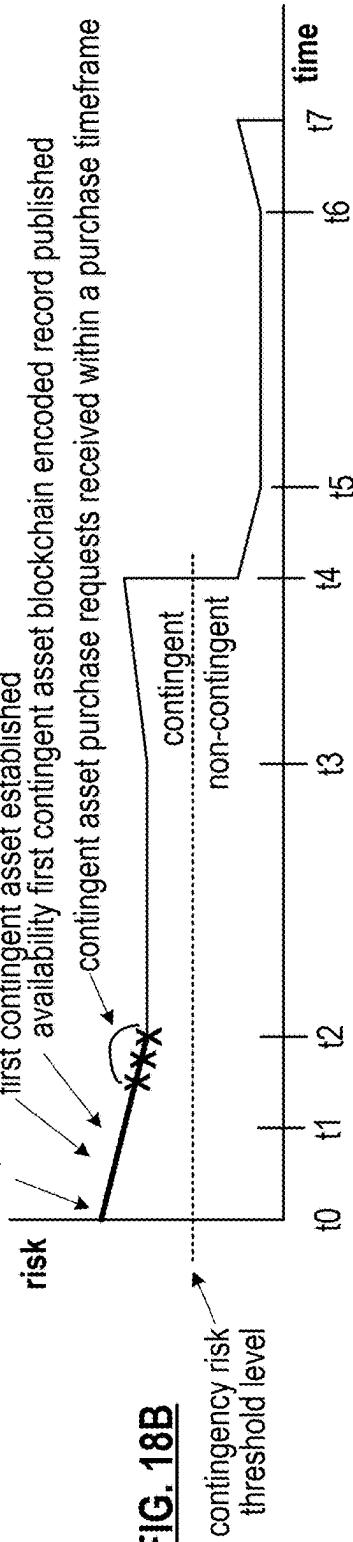
**step 2 – obtain a set of contingent asset purchase requests that includes a first contingent asset purchase request with regards to the first contingent asset**

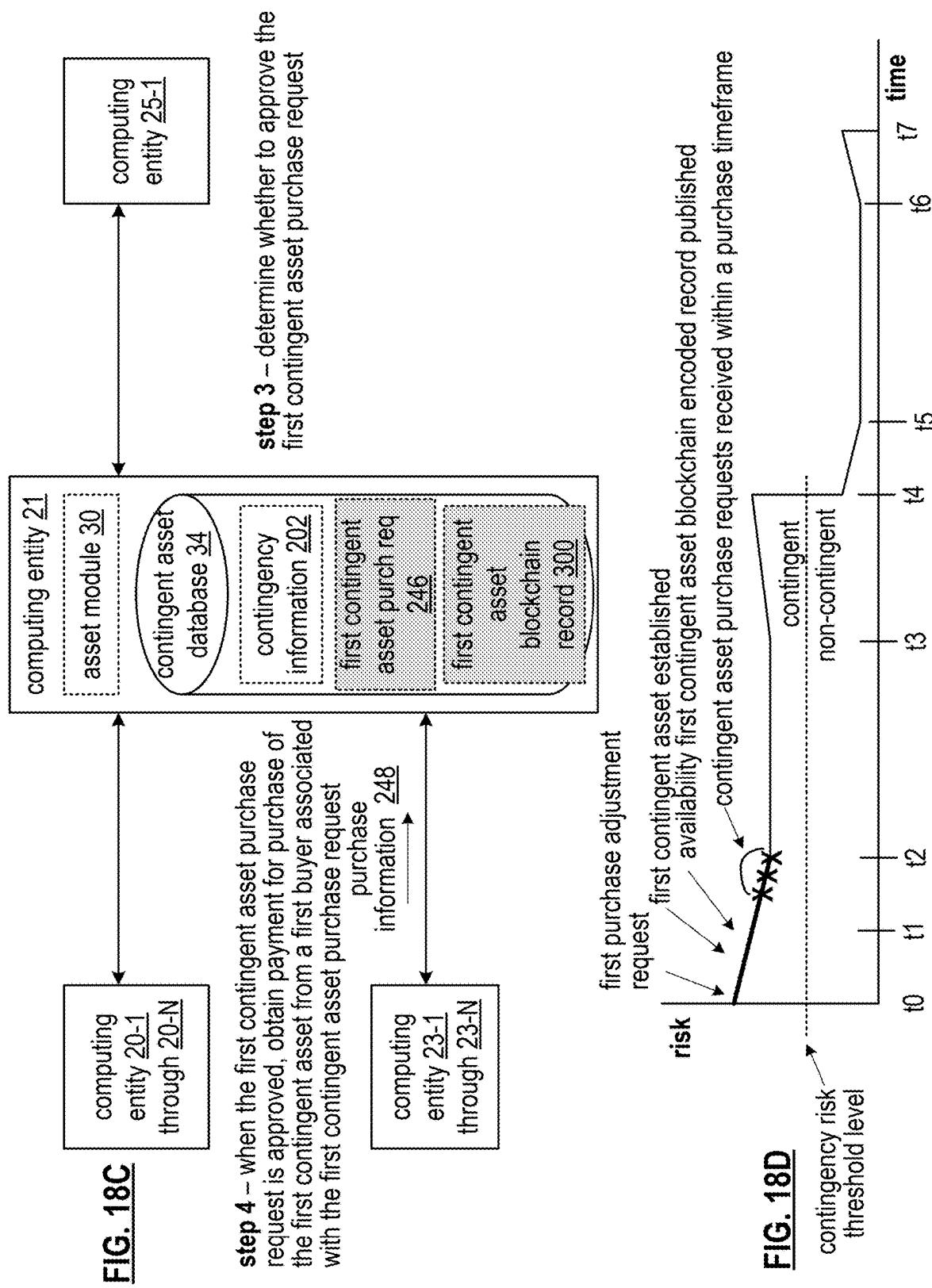
**step 1 – Indicate availability of a first contingent asset for subsequent utilization as a first instant asset utilizing a first contingent asset blockchain record**

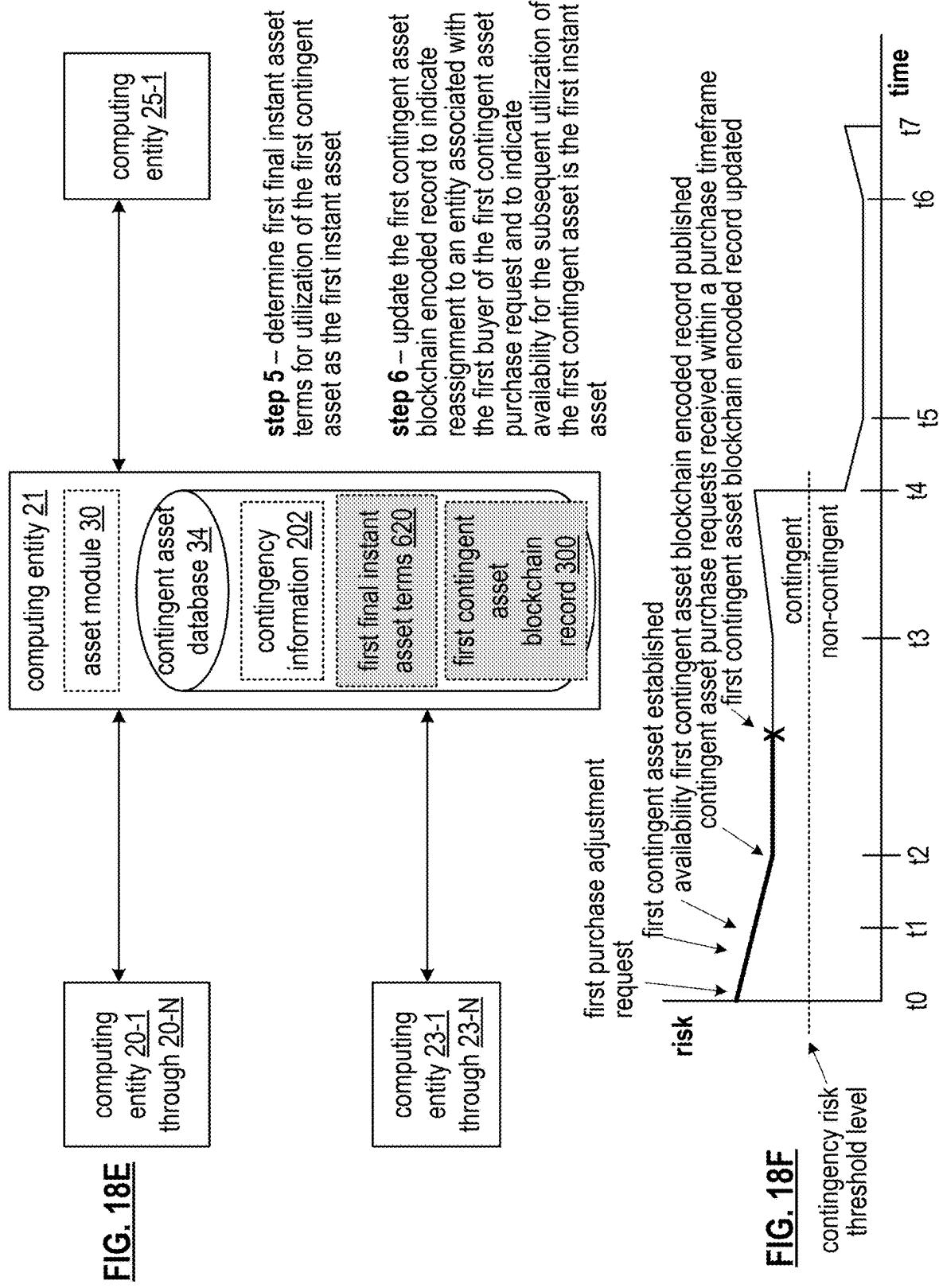
first purchase adjustment request

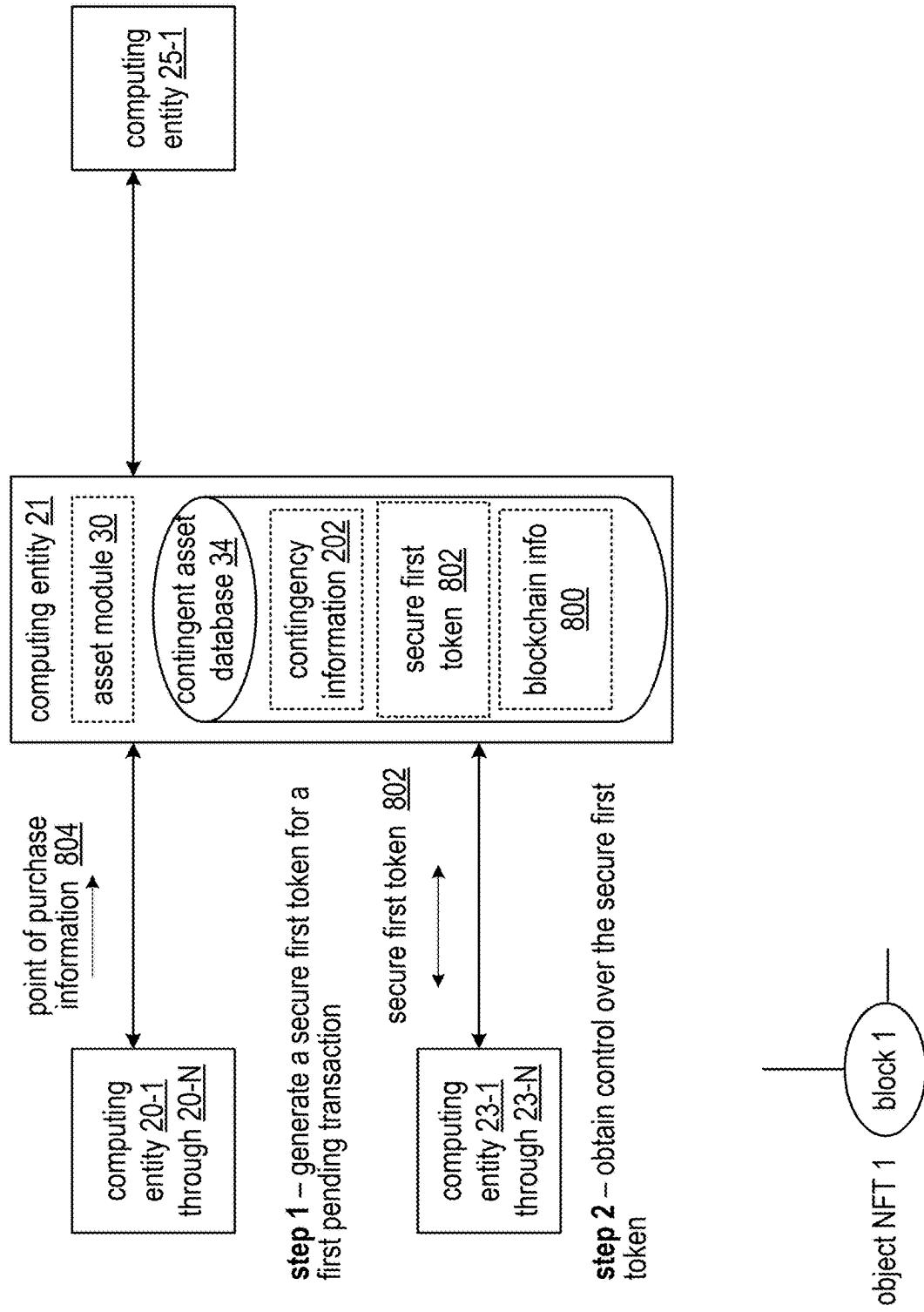
first contingent asset established availability first contingent asset blockchain encoded record published

contingent asset purchase requests received within a purchase timeframe

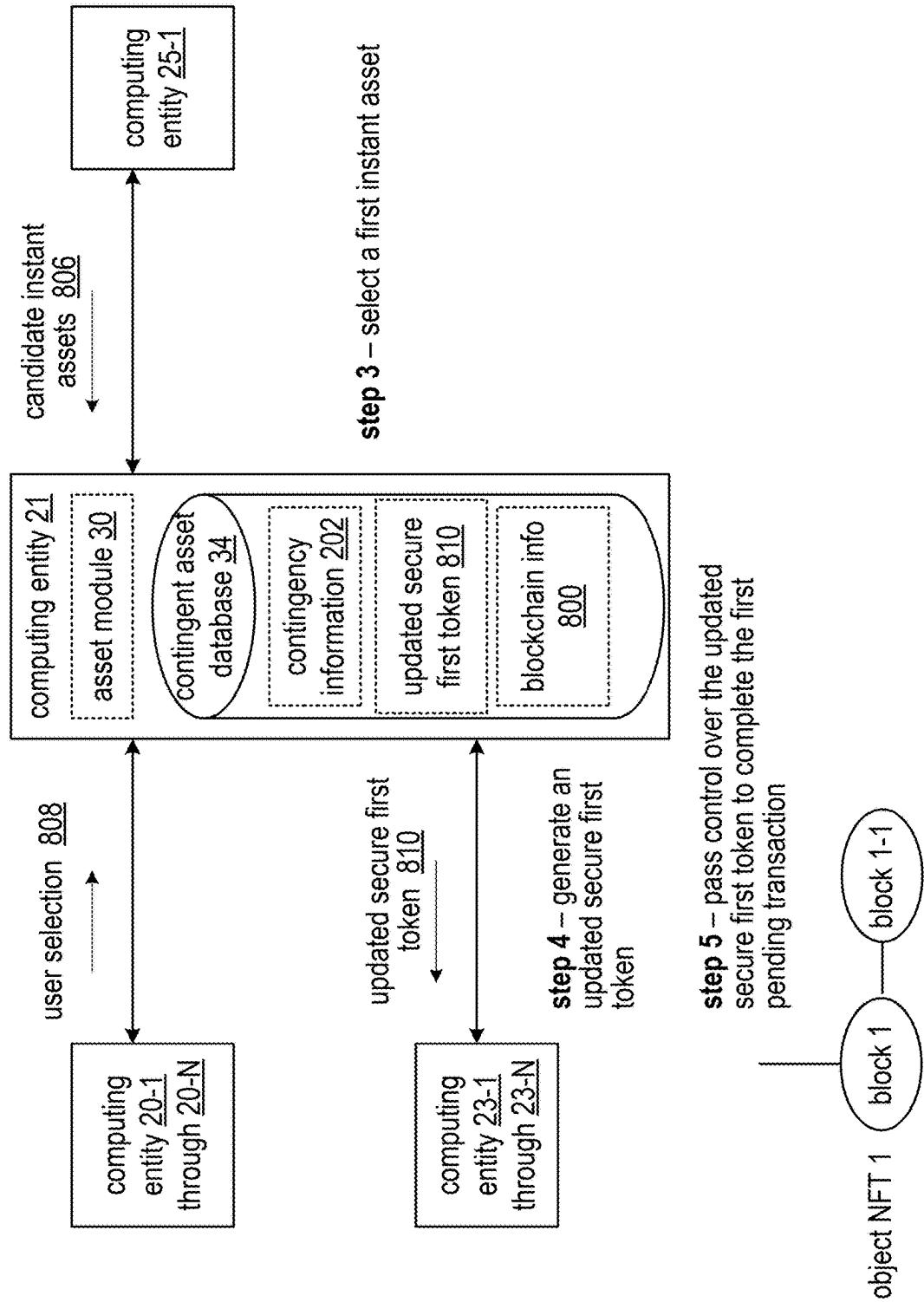




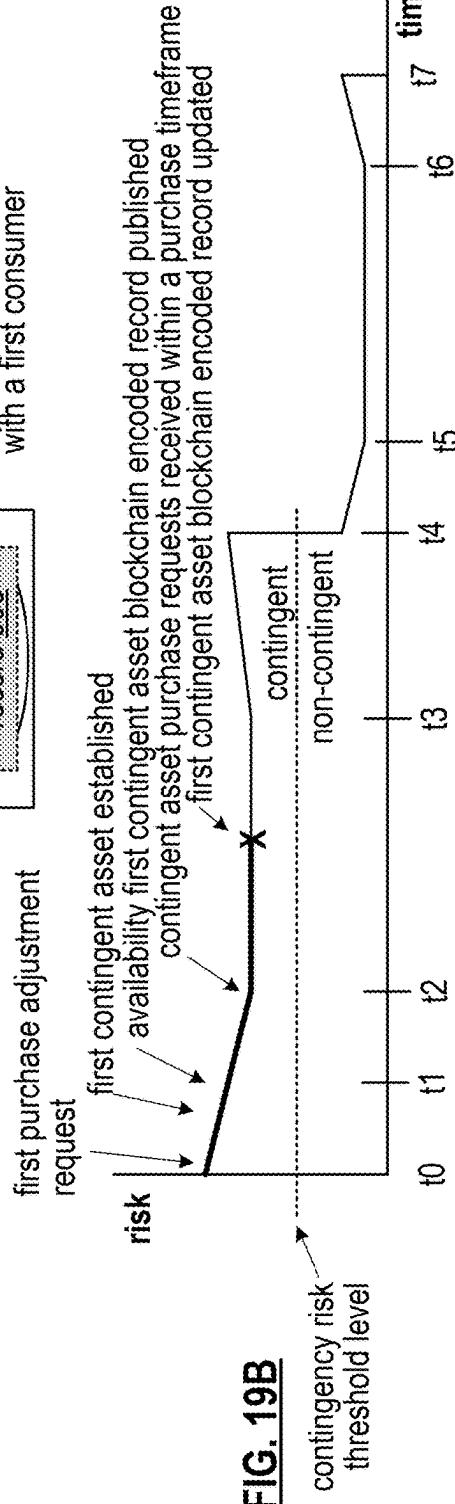
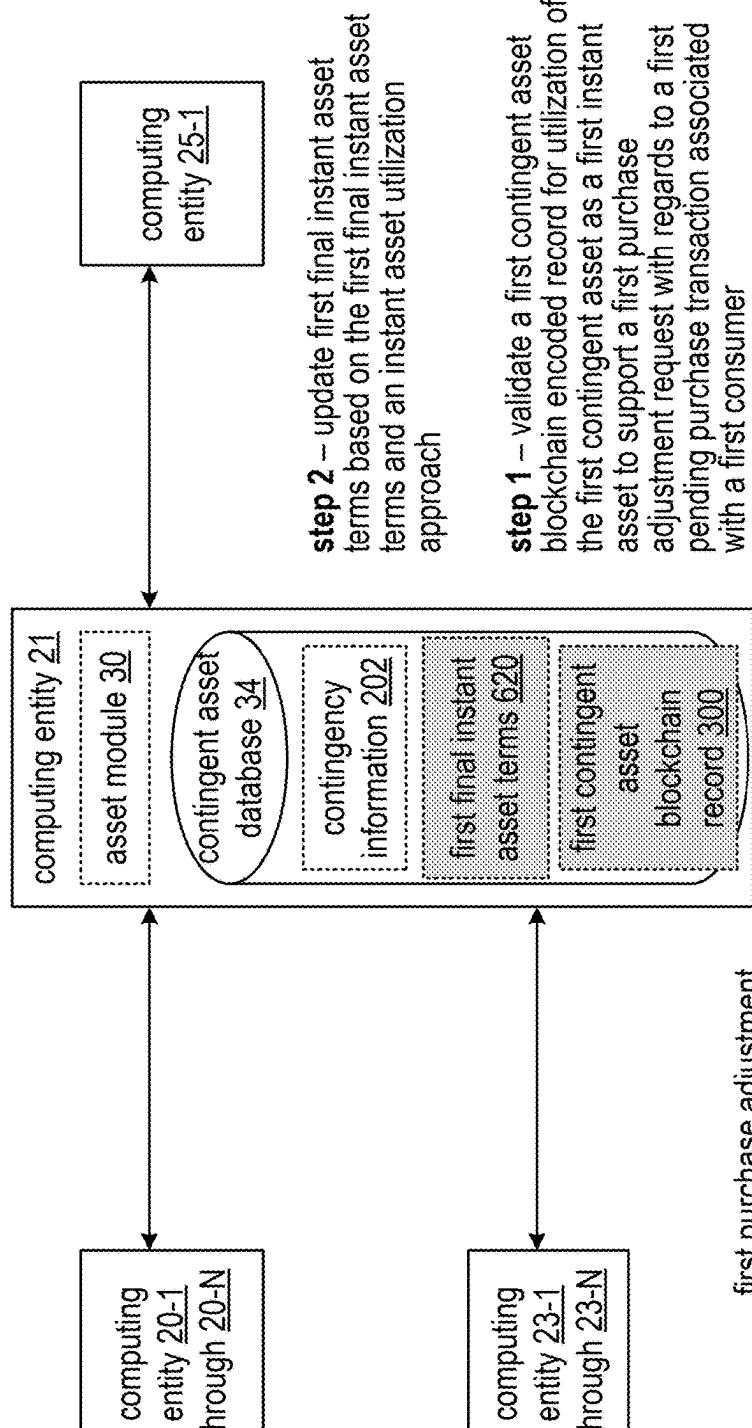


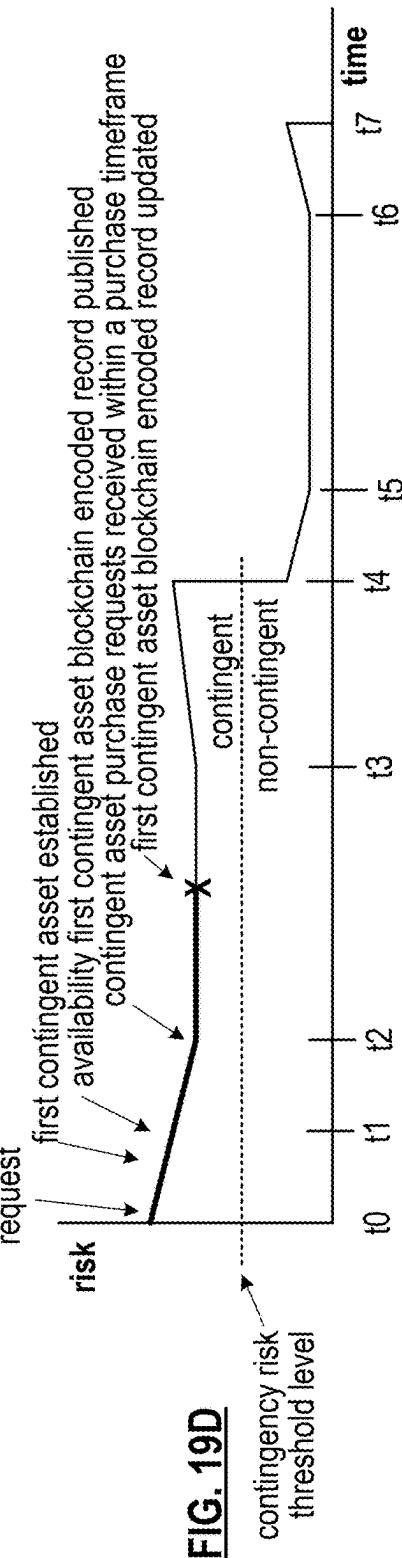
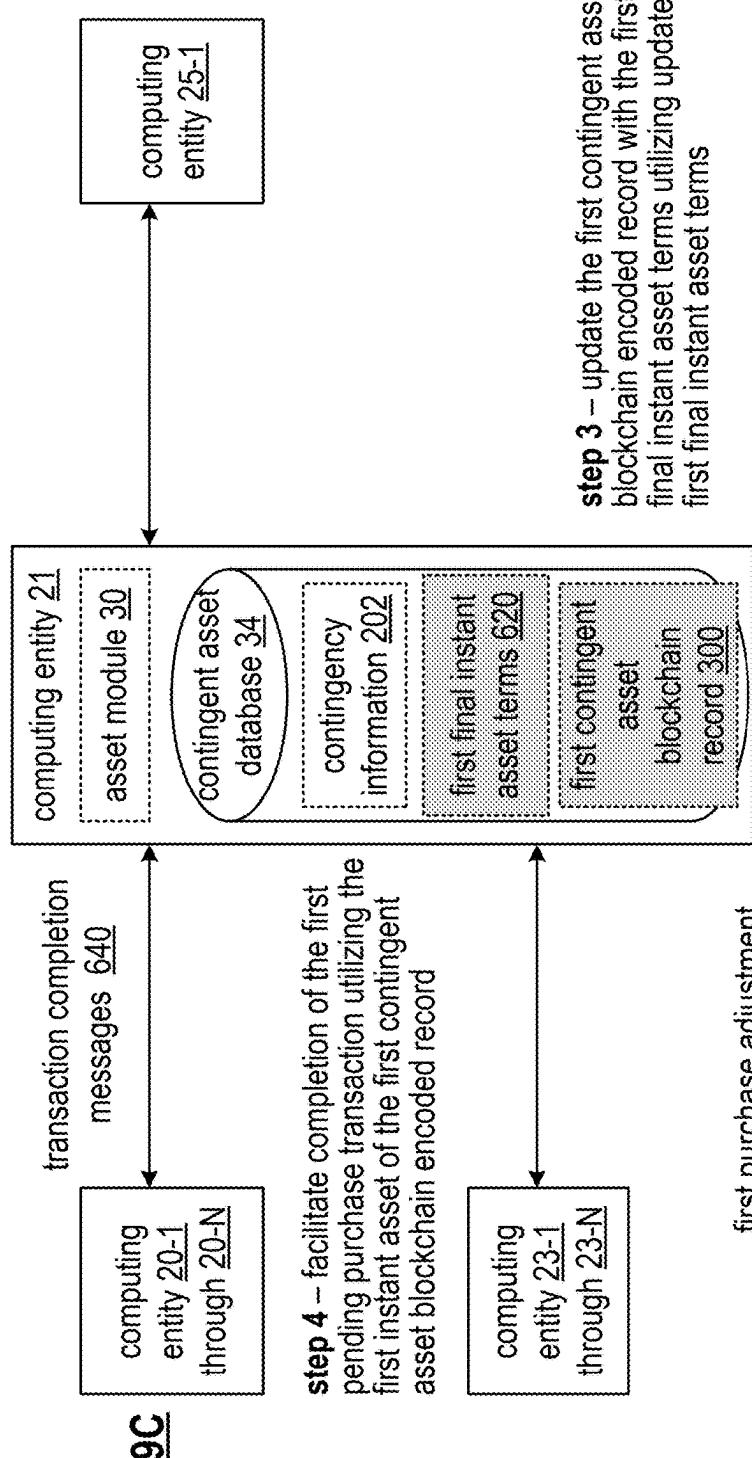


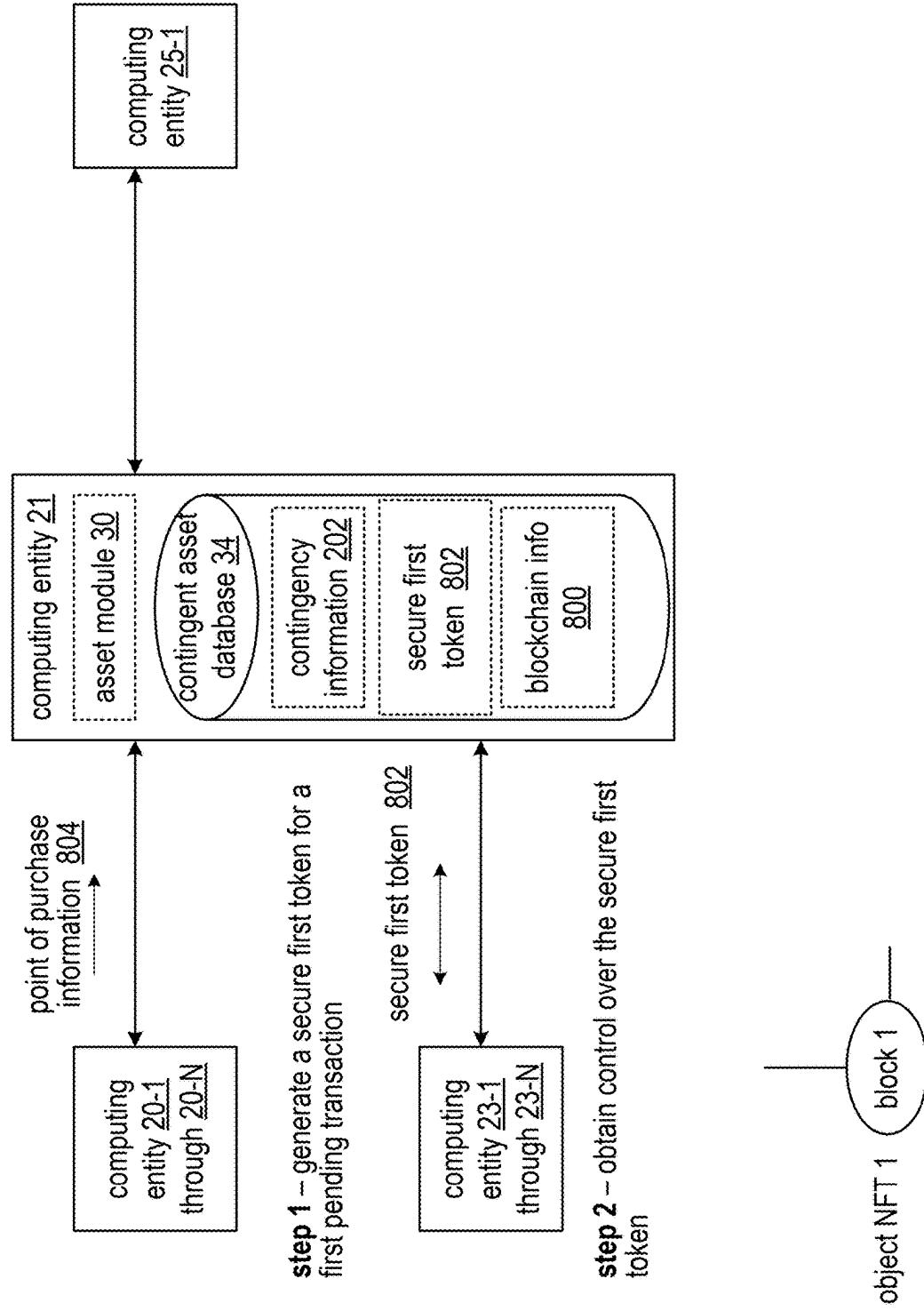
**FIG. 18G**



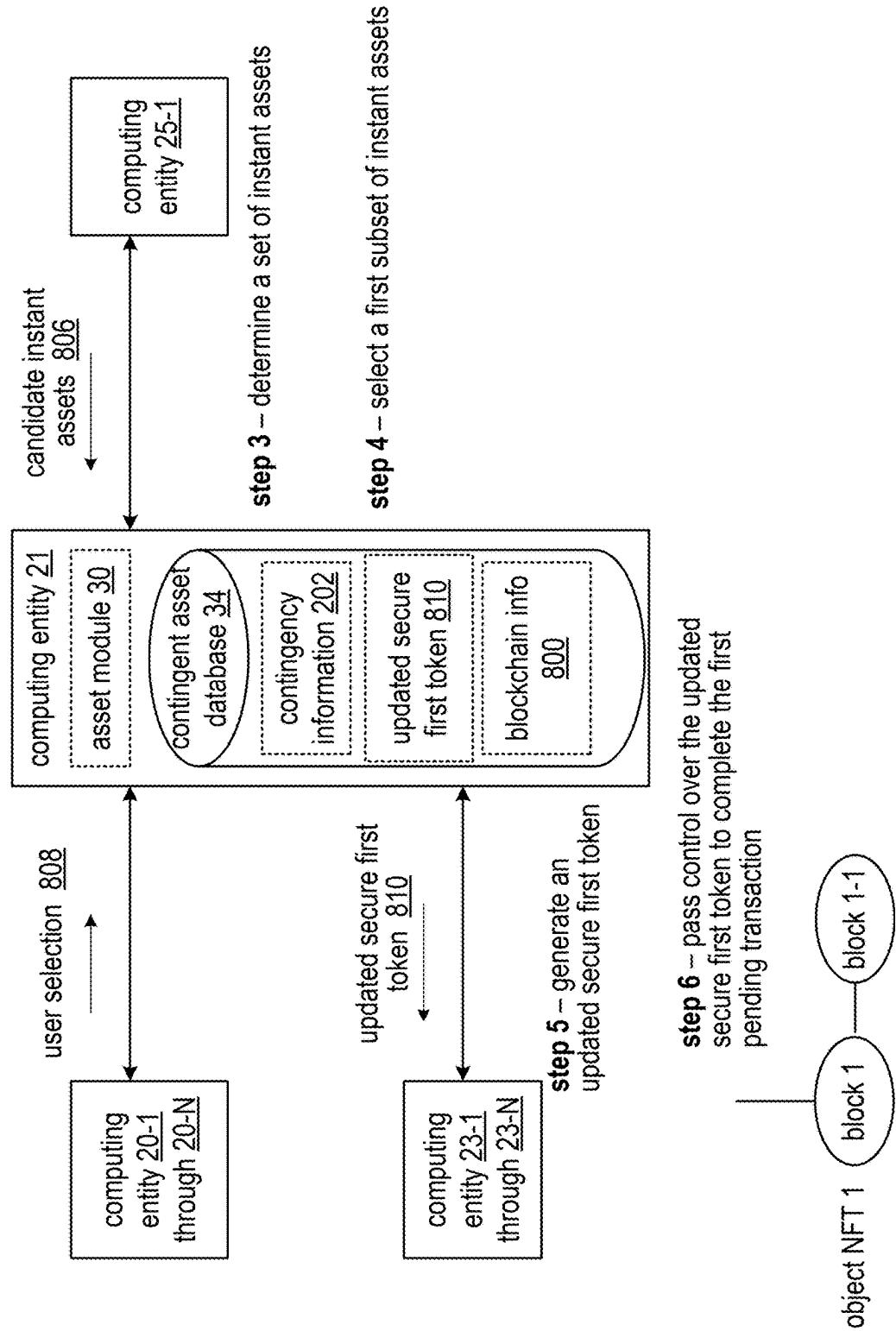
**FIG. 18H**



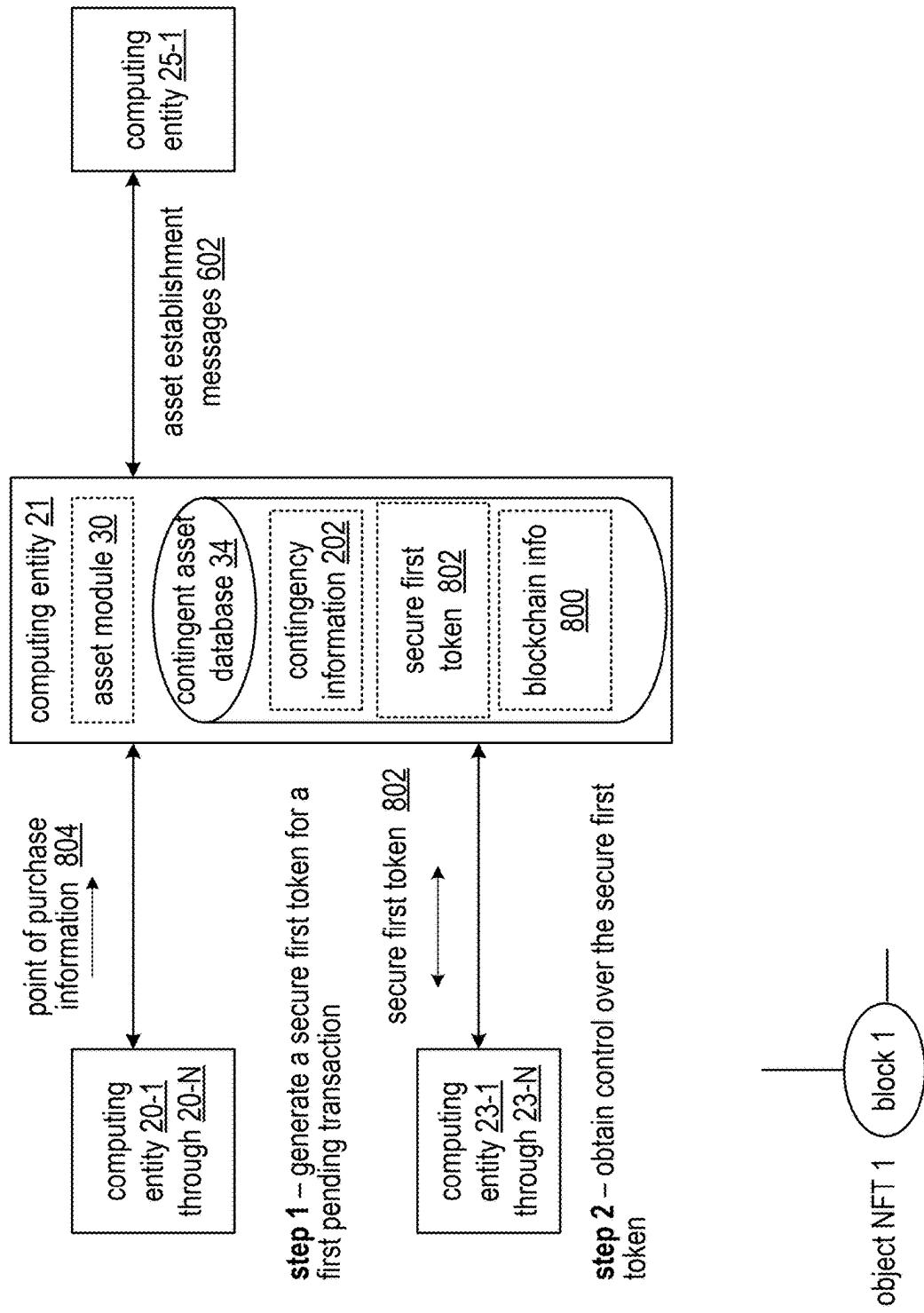




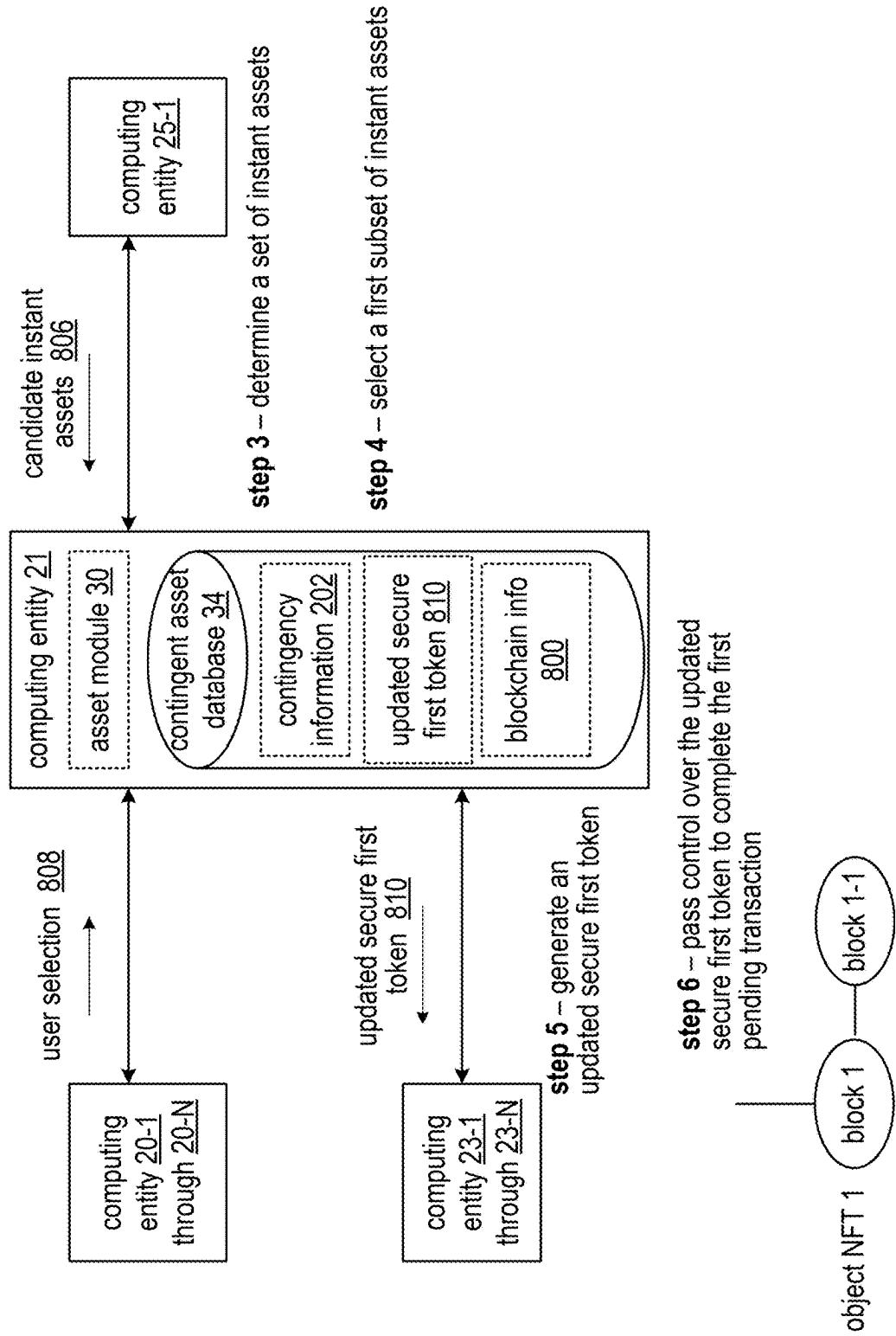
**FIG. 19E**



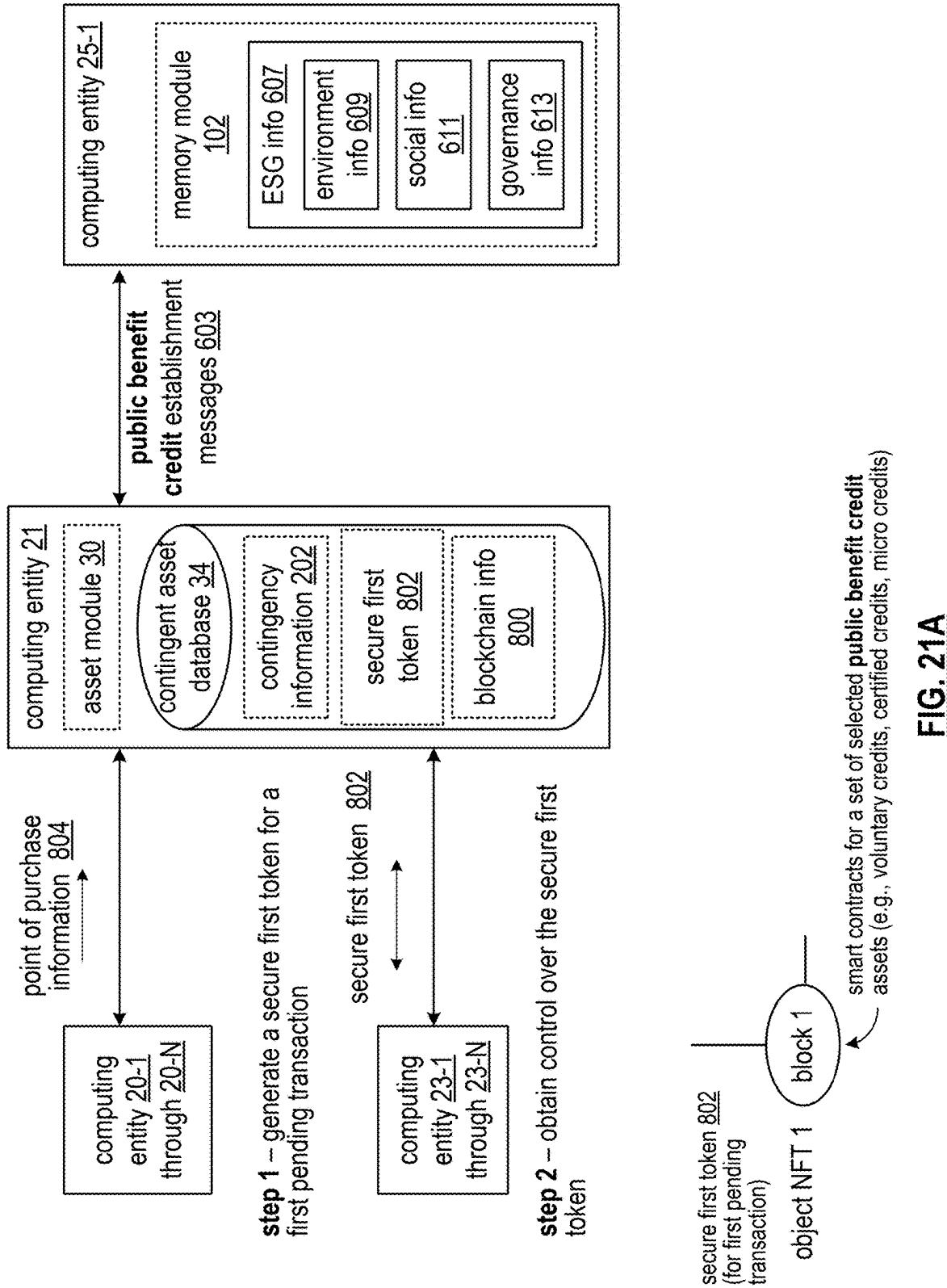
**FIG. 19F**



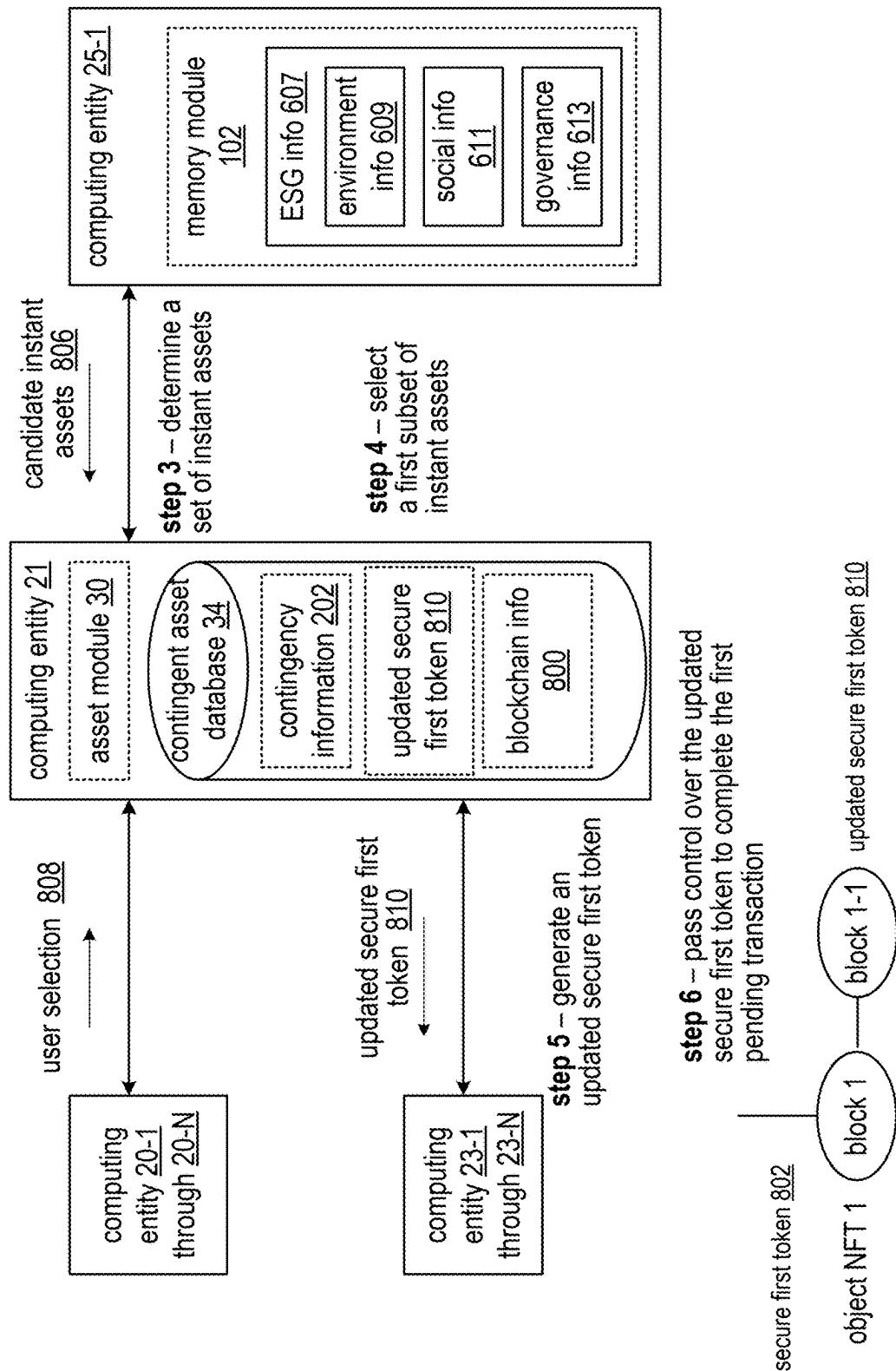
**FIG. 20A**



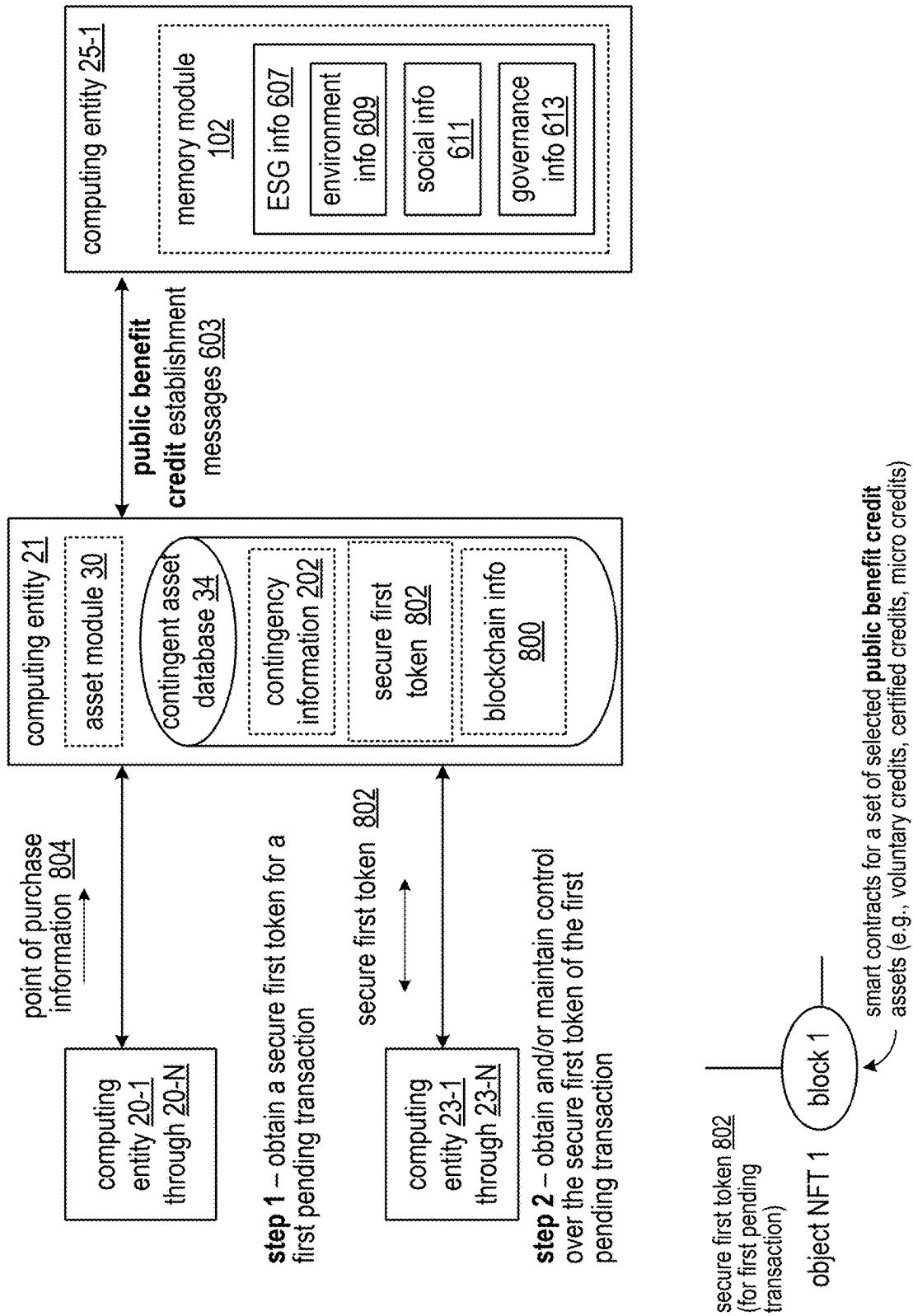
**FIG. 20B**



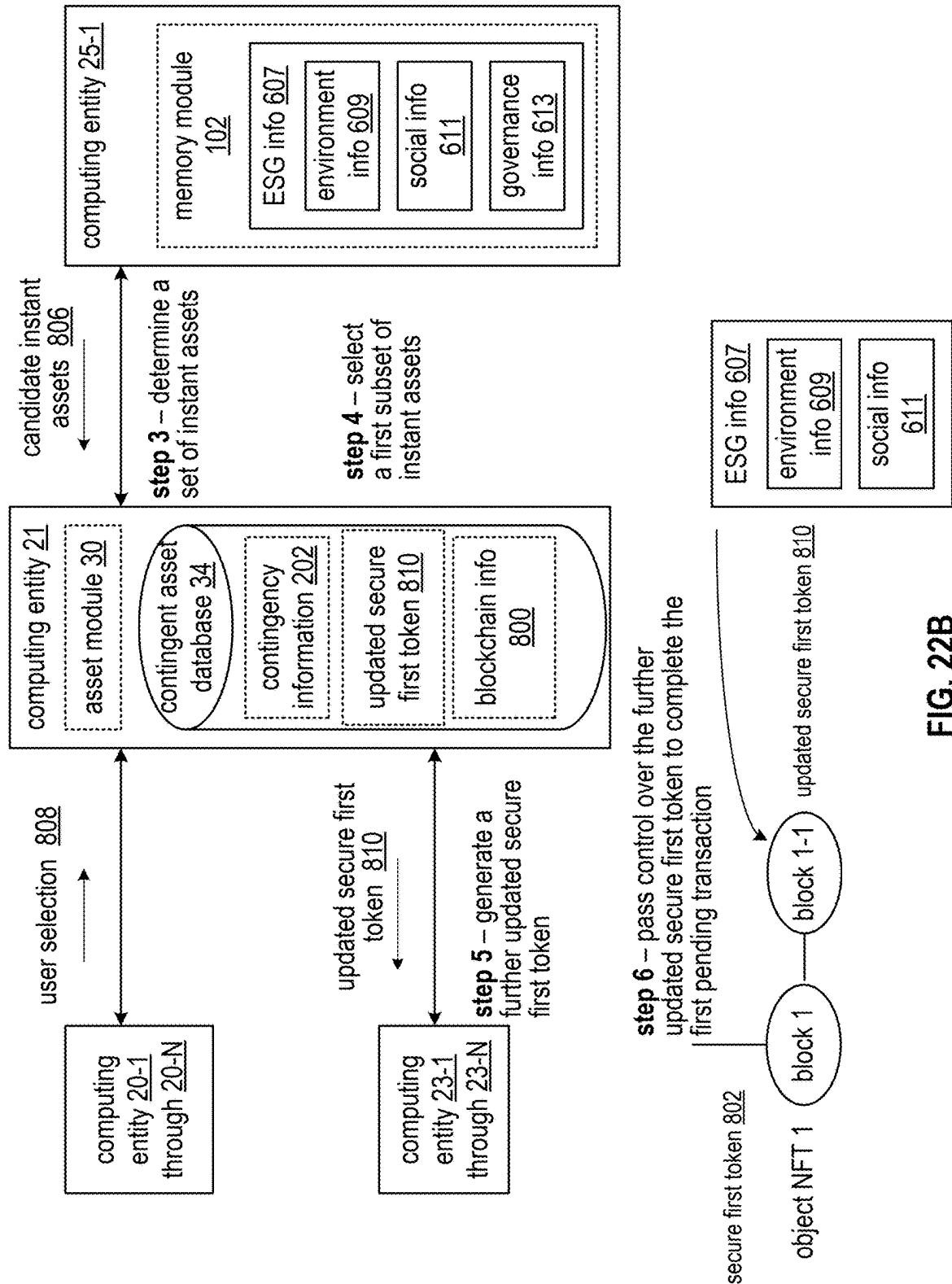
**FIG. 21A**



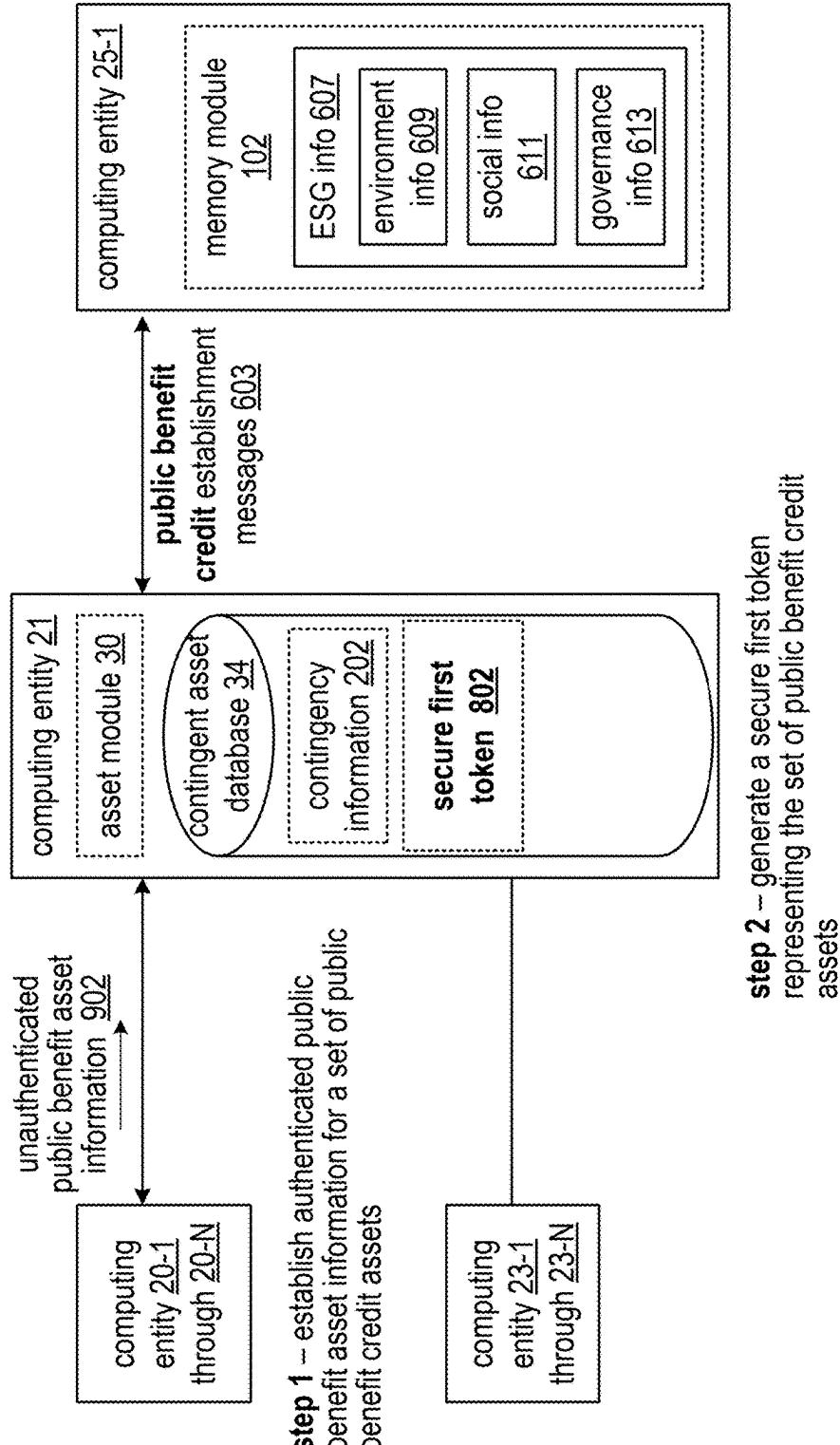
**FIG. 21B**



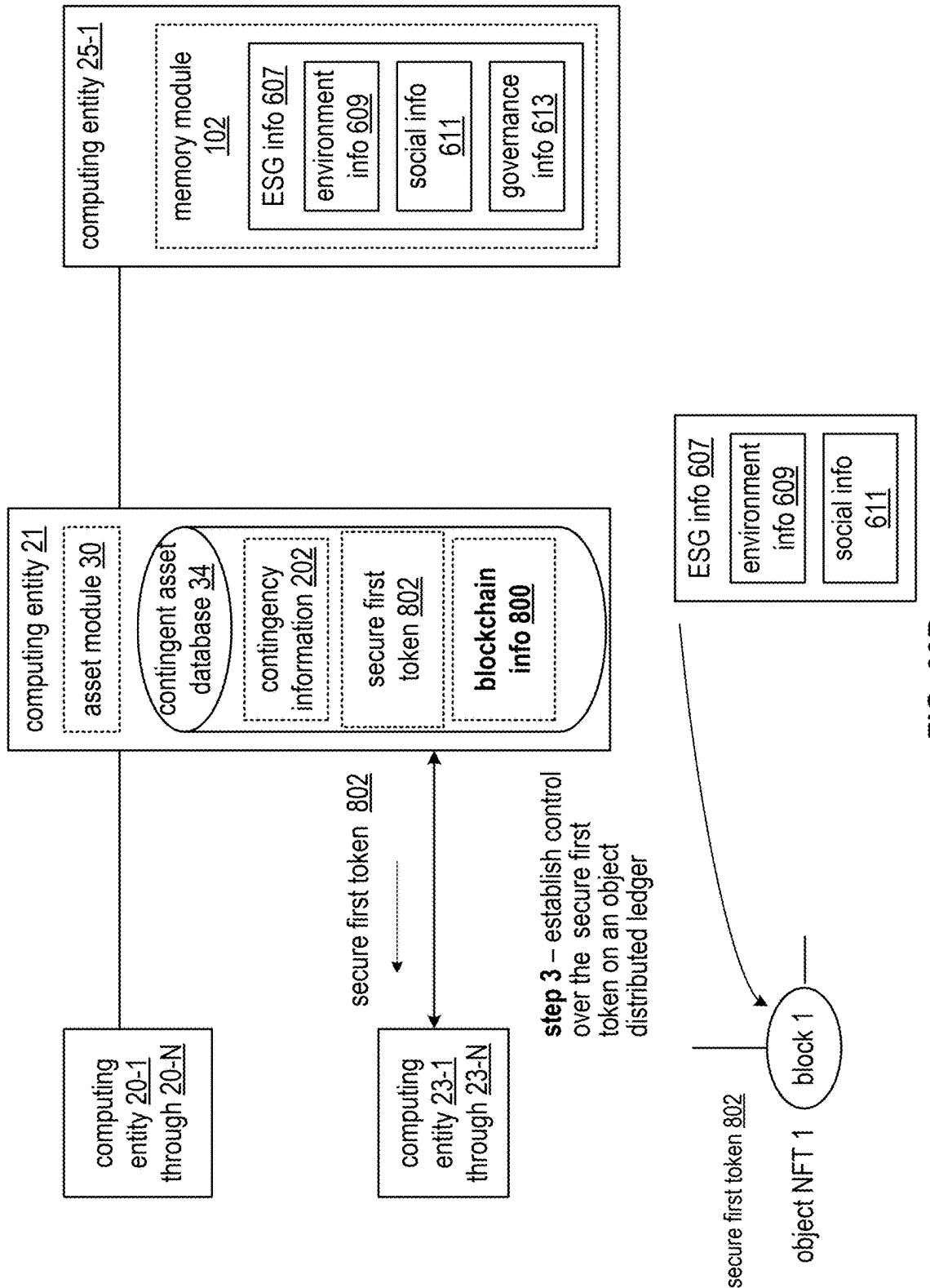
**FIG. 22A**

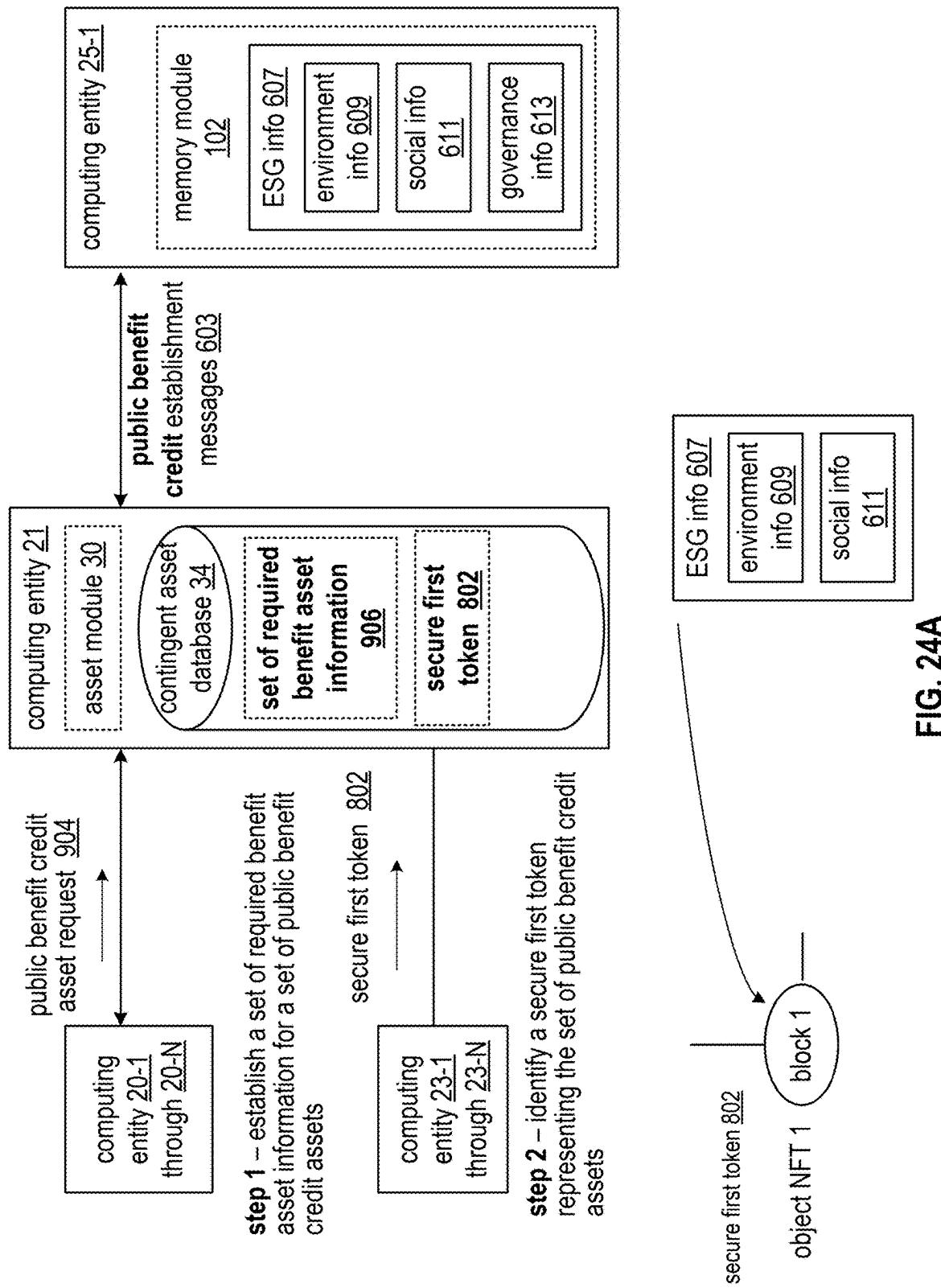


**FIG. 22B**

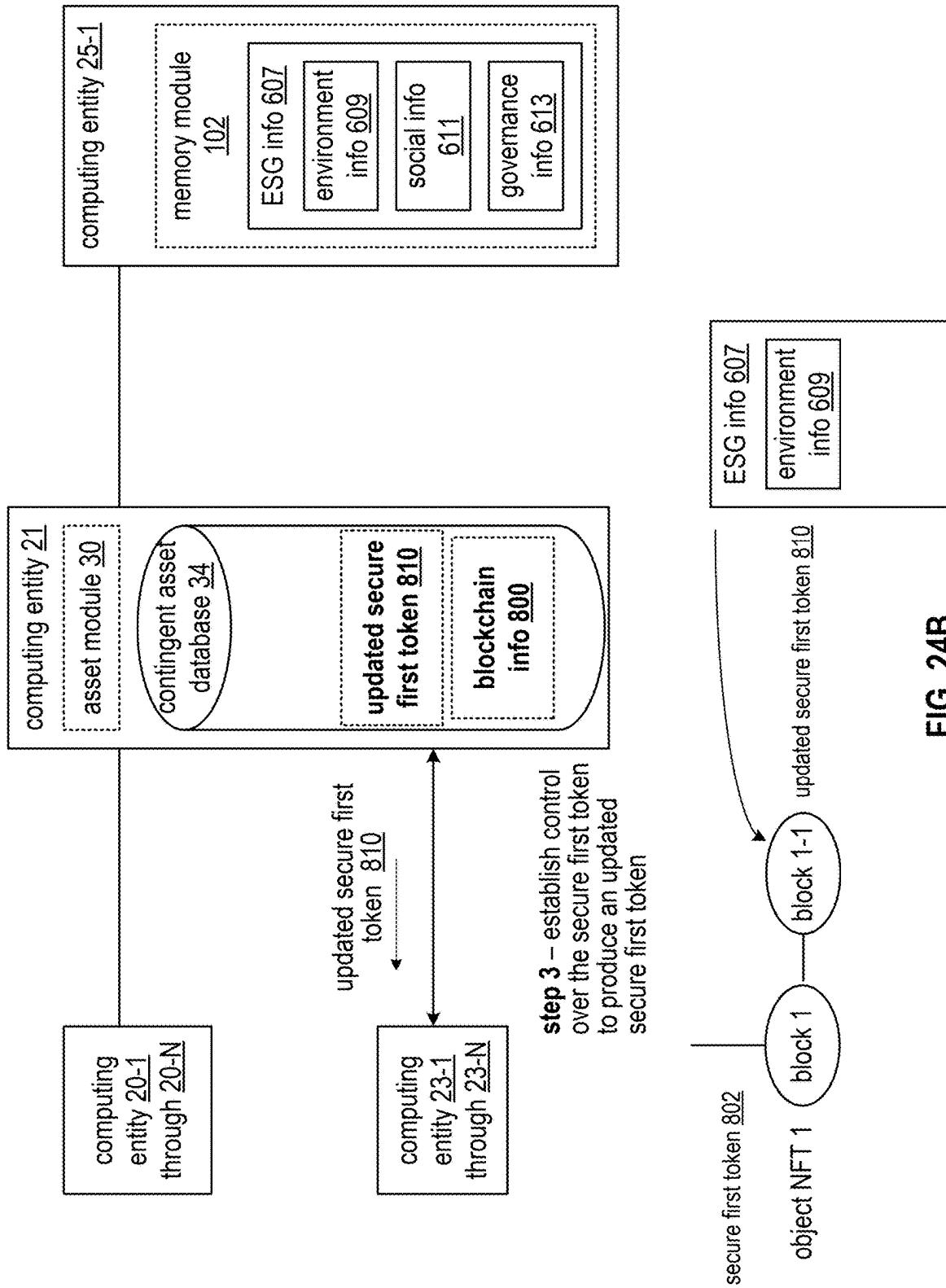


**FIG. 23A**

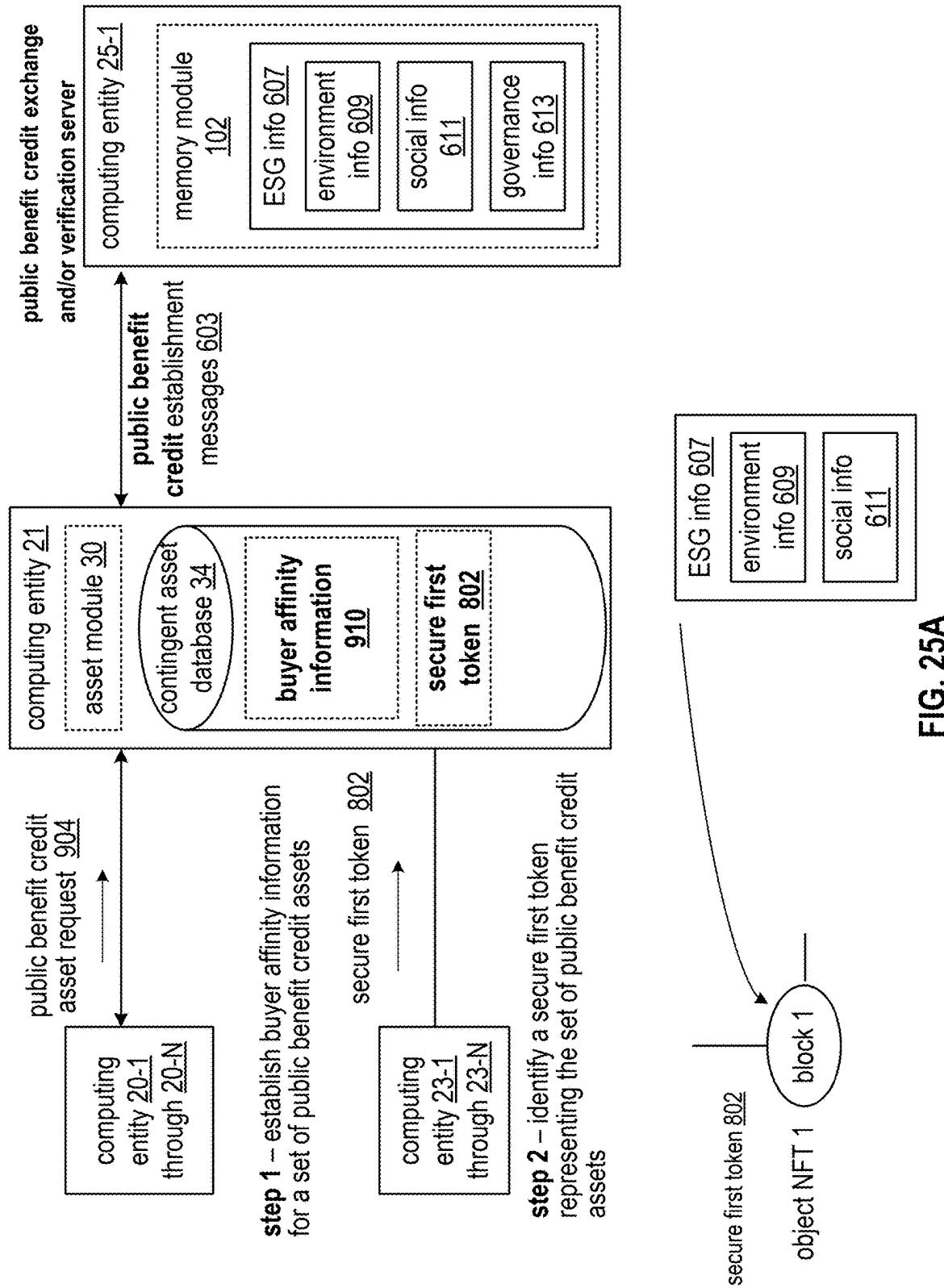




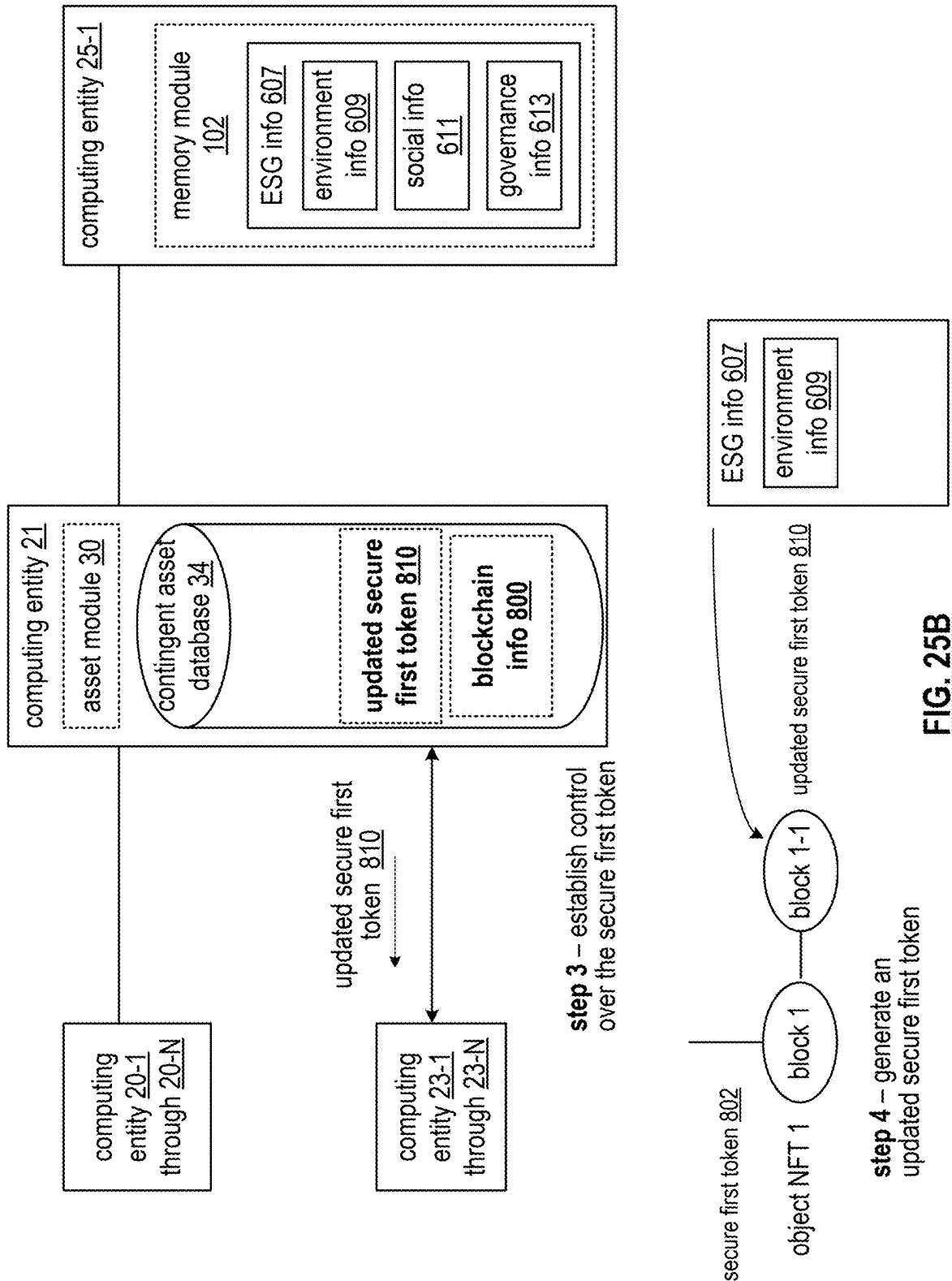
**FIG. 24A**



**FIG. 24B**



**FIG. 25A**



**FIG. 25B**

**IDENTIFYING A PUBLIC BENEFIT ASSETS  
SECURE TOKEN****CROSS-REFERENCE TO RELATED  
APPLICATIONS**

[0001] The present U.S. Utility patent application claims priority pursuant to 35 U.S.C. § 120 as a continuation of U.S. Utility application Ser. No. 18/104,866, entitled “IDENTIFYING A PUBLIC BENEFIT ASSETS SECURE TOKEN,” filed Feb. 2, 2023, issuing Apr. 22, 2025 as U.S. Pat. No. 12,282,952, which claims priority pursuant to 35 U.S.C. § 120 as a continuation-in-part of U.S. Utility application Ser. No. 18/082,758, entitled “UPDATING A SET OF PUBLIC BENEFIT ASSETS SECURE TOKEN,” filed Dec. 16, 2022, issued Mar. 25, 2025 as U.S. Pat. No. 12,260,402, which claims priority pursuant to 35 U.S.C. § 120 as a continuation-in-part of U.S. Utility application Ser. No. 17/959,919, entitled “UPDATING A SECURE TOKEN OF A CONTINGENT ASSET,” filed Oct. 4, 2022, issued Oct. 22, 2024 as U.S. Pat. No. 12,124,552, which claims priority pursuant to 35 U.S.C. § 120 as a continuation-in-part of U.S. Utility application Ser. No. 17/842,146, entitled “UTILIZING RISK TO PROCESS RECORDS REPRESENTING CONTINGENT ASSETS,” filed Jun. 16, 2022, issued Aug. 13, 2024 as U.S. Pat. No. 12,062,050, which claims priority pursuant to 35 U.S.C. § 119 (e) to U.S. Provisional Application No. 63/215,850, entitled “UTILIZING RISK TO TRANSACT CONTINGENT ASSETS,” filed Jun. 28, 2021, expired, all of which are hereby incorporated herein by reference in their entirety and made part of the present U.S. Utility patent application for all purposes.

**STATEMENT REGARDING FEDERALLY  
SPONSORED RESEARCH OR DEVELOPMENT**

[0002] Not Applicable.

**INCORPORATION-BY-REFERENCE OF  
MATERIAL SUBMITTED ON A COMPACT  
DISC**

[0003] Not Applicable.

**BACKGROUND OF THE INVENTION****Technical Field of the Invention**

[0004] This invention relates generally to computer systems and more particularly to computer systems providing risk analysis.

**Description of Related Art**

[0005] Computer systems communicate data, process data, and/or store data. Such computer systems include computing devices that range from wireless smart phones, laptops, tablets, personal computers (PC), work stations, personal three-dimensional (3-D) content viewers, and video game devices, to data centers where data servers store and provide access to digital content. Some digital content is utilized to represent various aspects of assets. Examples of representations includes an asset type, an asset value, a value guarantee, an asset owner identifier, etc.

[0006] A variety of asset computing systems utilize asset listing and asset transaction techniques when asset valuation is not subject to a contingency. For example, a stock asset is

offered on an exchange at a market price and is sold to a buyer. As another example, a receivable asset is offered on another exchange at another market price and is sold to another buyer.

**BRIEF DESCRIPTION OF THE SEVERAL  
VIEWS OF THE DRAWING(S)**

[0007] FIG. 1 is a schematic block diagram of an embodiment of a computing system in accordance with the present invention;

[0008] FIG. 2A is a schematic block diagram of an embodiment of a computing entity of a computing system in accordance with the present invention;

[0009] FIG. 2B is a schematic block diagram of an embodiment of a computing device of a computing system in accordance with the present invention;

[0010] FIG. 3 is a schematic block diagram of another embodiment of a computing device of a computing system in accordance with the present invention;

[0011] FIG. 4 is a schematic block diagram of an embodiment of an environment sensor module of a computing system in accordance with the present invention;

[0012] FIGS. 5A-5H are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of listing a contingent asset for sale in accordance with the present invention;

[0013] FIGS. 6A-6F are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of updating a listing of a contingent asset for sale in accordance with the present invention;

[0014] FIGS. 7A-7H are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of executing a sale of a contingent asset to a buyer from a seller in accordance with the present invention;

[0015] FIGS. 8A-8D are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of facilitating payment from a payer to a buyer for a contingent asset in accordance with the present invention;

[0016] FIG. 9A is a schematic block diagram of a data structure for a smart contract in accordance with the present invention;

[0017] FIGS. 9B and 9C are schematic block diagrams of organization of object distributed ledgers in accordance with the present invention;

[0018] FIG. 9D is a schematic block diagram of an embodiment of a blockchain associated with an object distributed ledger in accordance with the present invention;

[0019] FIGS. 9E-9M are schematic block diagrams of another embodiment of a computing system, contingent asset risk charts, and a blockchain record illustrating an example of listing a contingent asset for sale utilizing an object distributed ledger in accordance with the present invention;

[0020] FIGS. 10A-10F are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of updating a listing for a contingent asset for sale utilizing a blockchain record in accordance with the present invention;

[0021] FIGS. 11A-11H are schematic block diagrams of another embodiment of a computing system and a contin-

gent asset risk chart illustrating an example of executing a sale of a contingent asset to a buyer from a seller utilizing a blockchain record in accordance with the present invention;

[0022] FIGS. 12A-12D are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of facilitating payment from a payer to a buyer for a contingent asset utilizing a blockchain record in accordance with the present invention;

[0023] FIGS. 13A-13F are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of updating a listing for a contingent asset for sale utilizing a split blockchain record in accordance with the present invention;

[0024] FIGS. 14A-14H are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of executing a sale of a portion of a contingent asset to a buyer from a seller utilizing a split blockchain record in accordance with the present invention;

[0025] FIGS. 15A-15H are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of listing a contingent asset for sale utilizing a split blockchain record in accordance with the present invention.

[0026] FIGS. 16A-16D are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of facilitating payment from a payer to a buyer for a contingent asset utilizing a split blockchain record in accordance with the present invention;

[0027] FIGS. 17A-17F are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of creating a contingent asset for conversion into an instant asset at a point of purchase in accordance with the present invention;

[0028] FIGS. 18A-18F are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of executing a sale of a contingent asset for conversion into an instant asset at a point of purchase in accordance with the present invention;

[0029] FIGS. 18G-18H are schematic block diagrams of an embodiment of a computing system illustrating an example of securely converting a contingent asset into an instant asset at a point of purchase in accordance with the present invention; and

[0030] FIGS. 19A-19D are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of utilizing a contingent asset for conversion into an instant asset at a point of purchase in accordance with the present invention;

[0031] FIGS. 19E-19F are schematic block diagrams of an embodiment of a computing system illustrating an example of updating a secure token of a contingent asset in accordance with the present invention;

[0032] FIGS. 20A-20B are schematic block diagrams of an embodiment of a computing system illustrating an example of updating a secure token of a carbon credit asset in accordance with the present invention;

[0033] FIGS. 21A-21B are schematic block diagrams of an embodiment of a computing system illustrating an

example of updating a secure token of a set of public benefit assets in accordance with the present invention;

[0034] FIGS. 22A-22B are schematic block diagrams of an embodiment of a computing system illustrating an example of utilizing a secure token of a set of public benefit assets in accordance with the present invention;

[0035] FIGS. 23A-23B are schematic block diagrams of an embodiment of a computing system illustrating an example of generating a secure token of a set of public benefit assets in accordance with the present invention;

[0036] FIGS. 24A-24B are schematic block diagrams of an embodiment of a computing system illustrating an example of identifying a secure token of a set of public benefit assets in accordance with the present invention; and

[0037] FIGS. 25A-25B are schematic block diagrams of an embodiment of a computing system illustrating an example of identifying a secure token of a set of public benefit assets in accordance with the present invention.

#### DETAILED DESCRIPTION OF THE INVENTION

[0038] FIG. 1 is a schematic block diagram of an embodiment of a computing system 10 that includes a real world environment 12, computing entities 20-1 through 20-N, a computing entity 21, computing entities 23-1 through 23-N, and computing entities 25-1 through 25-N. The real-world environment 12 includes places 22 and objects 24. The computing entity 21 includes an asset module 30, and a contingent asset database 34. In an embodiment, the computing entity 21 serves as an exchange computing entity. In another embodiment, the computing entity 21 serves as a marketplace computing entity and/or device. In an embodiment, the computing entities 25-1 through 25-N serve as an asset authenticity computing entity (e.g., where tasks include authenticating validity and information with regards to a contingent asset). In an embodiment, the computing entities 23-1 through 23-N serve as blockchain nodes and/or as object ledger computing entities and/or object ledger computing devices of an object distributed ledger and/or computing entities associating with buyers of contingent assets.

[0039] The places 22 includes any physical area. Examples of places 22 includes a room, a series of rooms, an entire building, a portion of a building, an outdoor space, a neighborhood, a city, etc. The objects 24 includes things within the places. Examples of objects 24 includes people, equipment, lights, heating and air conditioning systems, building materials, furniture, personal items, tools, and representations of information (i.e., video recordings, audio recordings, captured text, etc.).

[0040] In an example of operation of the computing system 10, the computing entity 20-1 communicates with seller 26-1 of a plurality of sellers 26-1 through 26-N utilizing human input/output (I/O) 42. The computing entity 20-1 (e.g., an object owner computing entity) interprets the human I/O 42 and environment attributes 36 from the real world environment 12 to produce a seller message 30, where the seller message 30 is associated with a request to sell a contingent asset. The contingent asset includes a potential liability for a payer to pay an owner of the contingent asset subsequent to a contingency aspect of the contingent asset being satisfied. The contingency aspect includes an approval requirement for the contingent asset. For example, when unapproved the payer is not yet fully liable to pay the owner.

As another example, when approved, the payer is liable to pay the owner with regards to the liability in accordance with terms of the liability.

[0041] The environment attributes 36 includes detectable measures of the real-world environment 12 to facilitate generation of a multi-dimensional (e.g., including time) representation of the real-world environment 12 in a virtual reality and/or augmented reality environment. For example, the environment attributes 36 includes XYZ position information, place information of the places 22, and object information of the objects 24 (i.e., background, foreground, homeowner, contractor, etc.). The XYZ position information includes portrayal in a world space industry standard format (e.g., with reference to an absolute position). For instance, the environment attributes 36 portrays a representation of recent energy efficiency improvements made to a house.

[0042] Having generated the seller message 30, the computing entity 20-1 sends the seller message 30 to the computing entity 21. The asset module 30 of the computing entity 21 generates a contingent asset record associated with the contingent asset. The asset module 30 issues a payer message 35 to the computing entity 25-1, where the payer message 35 includes a request to authenticate the contingent asset.

[0043] Having received the payer message 35, the computing entity 25-1 authenticates the contingent asset (e.g., verifies that the contingent asset has been created). The computing entity 25-1 issues another payer message 35 to the computing entity 21, where the other payer message 35 indicates that the contingent asset is favorably authenticated.

[0044] When the contingent asset has been favorably authenticated, the computing entity 21 determines a risk level associated with a contingent asset lifecycle of the contingent asset for at least a portion of the lifecycle. The contingent asset lifecycle starts when the contingent asset is created and ends when the liability associated with the contingent asset has been paid out in accordance with the terms of the liability. The contingent asset lifecycle is discussed in greater detail with reference to FIG. 5A.

[0045] The determining of the risk level associated with the contingent asset is based on numerous parameters and will ultimately be utilized to determine fair valuation of the contingent asset at any time during the contingent asset lifecycle. As it is the intention of the computing entity 21 to facilitate sale of the contingent asset from the seller 26-1 to at least one buyer of buyers 28-1 through 28-N via the computing entities 23-1 through 23-N, the determining of the risk level associated with the contingent asset includes an aggregate of a plurality of estimated risk levels. The plurality of estimated risk levels includes various risks associated with the seller 26-1, with the buyer, with a payer associated with the computing entity 25-1, and with the contingent asset itself. The determining of the risk level associated with a contingent asset will be discussed in greater detail with reference to FIGS. 5A-5H.

[0046] Having determined the risk level associated with the condition asset, the computing entity 21 negotiates aspects of a listing for the contingent asset with the computing entity 20-1 via further seller messages 30 on behalf of the seller 26-1 (e.g., agreed-upon listing price, timeframe, restrictions, etc.). The computing entity 21 communicates a listing for the contingent asset via a buyer messages 33 with the computing entities 23-1 through 23-N associated with the buyers 28-1 through 28-N.

[0047] Having received a buyer message 33 with regards to the listing of the contingent asset, the computing entity 23-1 determines whether to offer a bid for the contingent asset on behalf of the buyer 28-1. Alternatively, the computing entity 21 determines whether to offer the bid on behalf of one of the buyers. For example, the buyer 28-1 provides human I/O 43 to the computing entity 23-1 with a bid price and a maximum price to initiate making an offer for the condition asset.

[0048] When making a bid, the computing entity 23-1 issues a further buyer message 33 to the computing entity 21 that includes information associated with the bid for the contingent asset. When successful, the computing entity 21 updates the record for the contingent asset to indicate that the buyer 28-1 is now the owner for the contingent asset (e.g., and not the seller 26-1). The updating the record includes disassociating the computing entity 20-1 with the contingent asset and associating the computing entity 23-1 with the contingent asset.

[0049] When the computing entity 21 detects that the contingency aspect of the contingent asset has been satisfied, the computing entity 21 updates the record associated with the contingent asset to indicate that a status has changed from contingent to noncontingent for the asset associated with the original contingent asset. For example, the asset module 30 receives another payer message 35 from the computing entity 25-1 that includes the indication that the status has changed to noncontingent, updates the record for the contingent asset, and stores the updated record in the contingent asset database 34. Alternatively, or in addition to, the computing entity 21 publishes the updated status to the computing entities associated with the buyers utilizing the updated record when the asset is available and has not been purchased by one of the buyers.

[0050] When the computing entity 21 detects the end of the contingent asset lifecycle (e.g., receiving a payer message 35 from the computing entity 25-1 that indicates that the payer liability is now to be settled), the computing entity 21 facilitates payment to one or more current owners (e.g., the buyer 28-1). For example, the computing entity 21 receives another payer message 35 from the computing entity 25-1 that includes payment information. The computing entity determines payoff information based on the payment information and issues another buyer message 33 to the computing entity 23-1 that includes the payoff information.

[0051] FIG. 2A is a schematic block diagram of an embodiment of the computing entity (e.g., 20-1 through 20-N; 21; 23-1 through 23-N; and 25-1 through 25-N) of the computing system 10 of FIG. 1. The computing entity includes one or more computing devices 100-1 through 100-N. A computing device is any electronic device that communicates data, processes data, represents data (e.g., user interface) and/or stores data.

[0052] Computing devices include portable computing devices and fixed computing devices. Examples of portable computing devices include an embedded controller, a smart sensor, a social networking device, a gaming device, a smart phone, a laptop computer, a tablet computer, a video game controller, and/or any other portable device that includes a computing core. Examples of fixed computing devices includes a personal computer, a computer server, a cable set-top box, a fixed display device, an appliance, and industrial controller, a video game counsel, a home entertainment

controller, a critical infrastructure controller, and/or any type of home, office or cloud computing equipment that includes a computing core.

[0053] FIG. 2B is a schematic block diagram of an embodiment of a computing device (e.g., 100-1 through 100-N) of the computing entity of FIG. 2A that includes one or more computing cores 52-1 through 52-N, a memory module 102, a human interface module 18, an environment sensor module 14, and an input/output (I/O) module 104. In alternative embodiments, the human interface module 18, the environment sensor module 14, the I/O module 104, and the memory module 102 may be standalone (e.g., external to the computing device). An embodiment of the computing device is discussed in greater detail with reference to FIG. 3.

[0054] FIG. 3 is a schematic block diagram of another embodiment of the computing device 100-1 of the computing system 10 that includes the human interface module 18, the environment sensor module 14, the computing core 52-1, the memory module 102, and the I/O module 104. The human interface module 18 includes one or more visual output devices 74 (e.g., video graphics display, 3-D viewer, touchscreen, LED, etc.), one or more visual input devices 80 (e.g., a still image camera, a video camera, a 3-D video camera, photocell, etc.), and one or more audio output devices 78 (e.g., speaker(s), headphone jack, a motor, etc.). The human interface module 18 further includes one or more user input devices 76 (e.g., keypad, keyboard, touchscreen, voice to text, a push button, a microphone, a card reader, a door position switch, a biometric input device, etc.) and one or more motion output devices 106 (e.g., servos, motors, lifts, pumps, actuators, anything to get real-world objects to move).

[0055] The computing core 52-1 includes a video graphics module 54, one or more processing modules 50-1 through 50-N, a memory controller 56, one or more main memories 58-1 through 58-N (e.g., RAM), one or more input/output (I/O) device interface modules 62, an input/output (I/O) controller 60, and a peripheral interface 64. A processing module is as defined at the end of the detailed description.

[0056] The memory module 102 includes a memory interface module 70 and one or more memory devices, including flash memory devices 92, hard drive (HD) memory 94, solid state (SS) memory 96, and cloud memory 98. The cloud memory 98 includes an on-line storage system and an on-line backup system.

[0057] The I/O module 104 includes a network interface module 72, a peripheral device interface module 68, and a universal serial bus (USB) interface module 66. Each of the I/O device interface module 62, the peripheral interface 64, the memory interface module 70, the network interface module 72, the peripheral device interface module 68, and the USB interface modules 66 includes a combination of hardware (e.g., connectors, wiring, etc.) and operational instructions stored on memory (e.g., driver software) that are executed by one or more of the processing modules 50-1 through 50-N and/or a processing circuit within the particular module.

[0058] The I/O module 104 further includes one or more wireless location modems 84 (e.g., global positioning satellite (GPS), Wi-Fi, angle of arrival, time difference of arrival, signal strength, dedicated wireless location, etc.) and one or more wireless communication modems 86 (e.g., a cellular network transceiver, a wireless data network trans-

ceiver, a Wi-Fi transceiver, a Bluetooth transceiver, a 315 MHz transceiver, a zig bee transceiver, a 60 GHz transceiver, etc.). The I/O module 104 further includes a telco interface 108 (e.g., to interface to a public switched telephone network), a wired local area network (LAN) 88 (e.g., optical, electrical), and a wired wide area network (WAN) 90 (e.g., optical, electrical). The I/O module 104 further includes one or more peripheral devices (e.g., peripheral devices 1-P) and one or more universal serial bus (USB) devices (USB devices 1-U). In other embodiments, the computing device 100-1 may include more or less devices and modules than shown in this example embodiment.

[0059] FIG. 4 is a schematic block diagram of an embodiment of the environment sensor module 14 of the computing device of FIG. 2B that includes a sensor interface module 120 to output environment sensor information 150 based on information communicated with a set of sensors. The set of sensors includes a visual sensor 122 (e.g., to the camera, 3-D camera, 360° view camera, a camera array, an optical spectrometer, etc.) and an audio sensor 124 (e.g., a microphone, a microphone array). The set of sensors further includes a motion sensor 126 (e.g., a solid-state Gyro, a vibration detector, a laser motion detector) and a position sensor 128 (e.g., a Hall effect sensor, an image detector, a GPS receiver, a radar system).

[0060] The set of sensors further includes a scanning sensor 130 (e.g., CAT scan, MRI, x-ray, ultrasound, radio scatter, particle detector, laser measure, further radar) and a temperature sensor 132 (e.g., thermometer, thermal coupler). The set of sensors further includes a humidity sensor 134 (resistance based, capacitance based) and an altitude sensor 136 (e.g., pressure based, GPS-based, laser-based).

[0061] The set of sensors further includes a biosensor 138 (e.g., enzyme, microbial) and a chemical sensor 140 (e.g., mass spectrometer, gas, polymer). The set of sensors further includes a magnetic sensor 142 (e.g., Hall effect, piezo electric, coil, magnetic tunnel junction) and any generic sensor 144 (e.g., including a hybrid combination of two or more of the other sensors).

[0062] FIGS. 5A-5H are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of listing a contingent asset for sale. The computing system includes the computing entity 20-1 of FIG. 1, the computing entity 21 of FIG. 1, computing entities 23-1 through 23-N of FIG. 1, and the computing entity 25-1 of FIG. 1.

[0063] FIG. 5A illustrates an example method of operation of the listing of the contingent asset for sale where in a first step the asset module 30 obtains a set of asset sale requests 200-1 through 200-N from the computing entity 20-1. A first asset of a first asset sale request of the set of asset sale requests assigns a face value level of a potential first liability of a first payer to a first seller associated with the first asset. At least a portion of the face value of the potential first liability is to be paid by the first payer to the first seller in accordance with contingency information and subsequent to completion of a first asset lifecycle of the first asset. The set of asset sale requests are generated within a sales timeframe.

[0064] Turning to FIG. 5B where a risk chart represents a portrayal of overall risk of the contingent asset over the lifecycle of the contingent asset, the lifecycle begins at time to when the asset is created. For example, the seller requests that the payer acknowledge the potential liability of the payer to the seller in the form of the contingent asset.

**[0065]** The overall risk level is based on an aggregate of risks of all of the entities involved in transactions of the asset or even other associated assets (e.g., assets associated with other asset sale requests within the sales timeframe) and the asset itself. The risks of the asset itself include one or more of a contingent asset program type associated with the payer, a history of payouts for similar assets of similar program types, a face value amount of the asset (e.g., an original requested amount of the potential liability by the seller), and an age of the asset (e.g., time since asset creation along the asset lifecycle).

**[0066]** Subsequent to creation of the asset, the seller generates an asset sale request with the hopes to receive at least some payment in exchange for the asset far before the end of the lifecycle. Subsequent to the asset sale request, the asset becomes available for sale. In the example of the risk level, the risk is gradually decreasing as time goes on since no early rejection by the payer has been generated. Subsequent to the asset sale request, the payer approves the potential liability such that the contingency of approval has been removed and the asset is now associated with the noncontingent status at t4. Prior to approval, the example indicates that the risk is gradually increasing since approval is expected but not yet received.

**[0067]** The example indicates that the risk level drops significantly upon approval of the of the contingency since the liability has greater certainty of a subsequent payout. The example indicates that the risk is gradually falling after approval since no adjustments to an amount of the payout have been received yet from the payer. The example indicates a gradual increase in the risk just prior to the payout when the payout is expected at t7. Lifecycle ends when the payer facilitates the payout of the liability (e.g., from the payer to one or more owners of the asset).

**[0068]** Alternatively, at any time during the lifecycle, the risk jumps significantly when the payer rejects the potential liability of the payer. Further alternatively, the asset is sold such that the seller is disassociated from ownership and that one or more buyers are associated with ownership of the asset. The transitioning of ownership is possible at any time during the lifecycle of the asset but more likely after the asset is made available for sale and before the approval of the liability.

**[0069]** Returning to FIG. 5A, the contingency information for each asset includes a variety of elements that are maintained in the contingent asset database 34 by the asset module 30. The contingency information includes an asset identifier (ID), an ask price (e.g., what the seller would like to receive), a reserve price (e.g., a minimum price that is acceptable), a lifecycle status indicator (e.g., indicating a current association of the asset to the lifecycle such as contingent, noncontingent, pending payment, payment approved, rejected and closed, payment completed and closed, etc.), and ownership information (e.g., one or more identifiers associated with current owners which may include the seller, percentage ownership levels by owner).

**[0070]** The contingency information further includes at least one payer identifier, a percentage of the potential liability assigned to each payer, a payer program identifier (e.g., an energy efficiency rebate program ID, a four new tire purchase rebate program ID, etc.), and time stamp information (e.g., dates and times for each step of any information transfer or transaction associated with the asset). The contingency information further includes a face value of the

potential liability (e.g., a rebate amount when 100% of the liability is to be paid), an estimated payout level (e.g., a value less than or equal to the face value which is a function of available funds and/or compliance to the program etc.), an estimated payout timeframe (e.g., t7 of the lifecycle), and bid information (e.g., bid amount, bid timestamp, entity ID associated with the bid). The contingency information further includes risk information (e.g., the overall risk level associated with the asset and component risk levels that make up the overall risk level such as asset risk, seller risk, payer risk, and buyer risk).

**[0071]** The contingency information further includes related asset information, an authenticity indicator, and asset split information. The related asset information includes other asset identifiers associated with the asset, relationships between the asset and the other assets (e.g., same seller, same program, same payer, same buyer, similar risk information, etc.). The authenticity indicator includes an indication of when the asset is deemed authentic (e.g., a verified payer agrees to the potential liability), and unknown authenticity, and a not authentic (e.g., no payer agrees to the potential liability implied by the asset).

**[0072]** The asset split information includes a number of portions of the asset, a percentage of each portion, portion options (e.g., any additional terms to do with transactions associated with the asset such as recourse where the seller agrees to pay to cover downside associated with a rejection of the request for the potential liability from the payer), and pricing information proportion. The pricing information proportion of the asset includes an ask price, a bid price, a bid-ask spread, and a reserve price.

**[0073]** Returning to the first step of the example method of operation, where the computing entity 21 obtains the asset sale request 200-1 associated with the first asset, the asset module 30 obtains the asset sale request 200-1 by at least one of identifying desired assets associated with the computing entity 20-1 (e.g., identify what a seller associated with the computing entity 20-1 should offer for sale), requesting that the computing entity 20-1 issue the sale request, and receiving the sale request from the computing entity 20-1. In an embodiment the computing entity 20-1 is associated with a third party representing one or more sellers.

**[0074]** The asset sale request 200-1 includes one or more of an ask price, a reserve price, recourse information (e.g., terms of the recourse, a credit card number, etc.), an asset ID (e.g., of the first asset), a face value of the potential liability, a payer identifier, and a percentage liability of each of one or more payers when more than one payer is associated with the potential liability. The asset sale request further includes one or more of the lifecycle status, the ownership information, the payer program ID, the timestamp information, the related asset information, and the asset split information.

**[0075]** Each asset sale request of the asset sale request 200-1 through 200-N include similar attributes as described above. In an instance, the set of asset sale requests are related by an intention to sell a block of assets that are all associated with the same payer and same payer program. The risk level associated with the block of similar assets is lower than the individual risk levels if sold separately since the block is generally viewed as more legitimate, especially when the payer actively supports larger blocks of assets.

**[0076]** FIG. 5C further illustrates the example method of operation of the listing of the contingent asset for sale where,

having obtained the set of asset sale requests, in a second step the computing entity 21 selects a first asset sale request of the set of asset sale requests based on a first authenticity indicator associated with the first asset sale request. The selecting includes obtaining the first authenticity indicator (e.g., requesting from the payer, determining the authenticity indicator, extracting the authenticity indicator from the first asset sale request when the payer provided the authenticity indicator to the seller, and receiving the authenticity indicator from the payer). For example, the asset module 30 receives a first authenticity indicator 204 from the computing entity 25-1. The selecting further includes interpreting the first authenticity indicator. For instance, the asset module 30 interprets the first authenticity indicator 204 to indicate that the first asset is authentic.

[0077] The selecting the first asset sale request further includes determining that the first asset has not yet been listed for sale and identifying an asset of the set of asset sale requests as the first asset when the asset is a most desired asset of assets of the set of asset sale requests. The identifying includes identifying a best fit for the seller to sell, detecting an asset risk level below a maximum risk threshold level, determining that other sales by the seller are associated with risk levels below a maximum seller risk threshold level, verifying that the payer is associated with a risk level below a maximum payer risk threshold level, and verifying that the seller has sold an aggregate of assets that is below a maximum seller cap.

[0078] Having selected the first asset sale request, in a third step of the example method of operation of the listing of the contingent asset for sale, the computing entity 21 determines whether a first asset risk level of the first asset of the first asset sale request is greater than a contingency risk threshold level as illustrated in FIG. 5D. The first asset is created by a computing entity associated with the first payer (e.g., the computing entity 25-1, the computing entity 20-1 on behalf of the computing entity 25-1, the computing entity 21 on behalf of the computing entity 25-1).

[0079] The determining includes one or more of obtaining risk levels of relevant attributes, calculating the first asset risk level based on the risk levels of the relevant attributes, and comparing the first asset risk level to the contingency risk threshold level. For example, the asset module 30 obtains the risk levels of the relevant attributes to include risks associated with the payer, the seller, the type of asset, parameters of the sale request, and status of the contingent asset (e.g., contingent versus noncontingent and lifecycle status). As a further example, the asset module 30 maps the risk levels of the relevant attributes to the first asset risk level for comparison to the contingency risk threshold level to determine that the first asset risk level is greater than the contingency risk threshold level.

[0080] FIG. 5E further illustrates the example method of operation of the listing of the contingent asset for sale where, having determined whether the first asset risk level is greater than the contingency risk threshold level, in a fourth step, when the first asset risk level of the first asset of the first asset sale request is greater than the contingency risk threshold level, the computing entity 21 establishes a first contingent asset based on the first asset of the first asset sale request. The establishing the first contingent asset includes a series of sub-steps.

[0081] A first sub-step includes generating a record for the first contingent asset to include the first asset ID, the seller

ID, the payer ID, and seller desired pricing and or timing. A second sub-step includes determining pricing information based on risks and the seller desired pricing. For example, the asset module 30 generates the pricing information based on one or more of a desired sale price from the seller, an estimated probability of payer approval, expected payment timeframe, and expected payment level, an expected rate of return either on the asset or on an annualized basis, recent bid prices for similar assets, and recent bid-ask spreads for pools of similar assets.

[0082] Having determined the pricing information, a third sub-step includes verifying the pricing information with the seller. For example, the asset module 30 receives a first contingent asset pricing approval indicator 208 from the computing entity 20-1 to verify the pricing information with the seller.

[0083] A fourth sub-step includes updating the record for the first contingent asset to further include the pricing information. For example, the asset module 30 modifies the first contingent asset 206 within the contingent asset database 34 to include the updated record.

[0084] Having established the first contingent asset, a fifth step of the example method of operation of listing of a contingent asset for sale includes the computing entity 21 publishing availability of the first contingent asset to a plurality of other computing entities (e.g., to a plurality of potential buyers). The publishing includes one or more of generating first contingent asset information 210 (e.g., an exchange listing) utilizing the updated record, posting the listing on an exchange (e.g., storing the updated record in the contingent asset database 34 and making that portion of the database available to potential buyers), and sending the first contingent asset information 210 to at least some of the computing entities 23-1 through 23-N to reach buyers with the listing.

[0085] FIG. 5F illustrates the risk chart where the first contingent asset has been established in step 4 of the example. The chart further illustrates availability of the first contingent asset upon publishing in step 5 of the example.

[0086] FIG. 5G further illustrates the example method of operation of the listing of the contingent asset for sale where, having published availability of the first contingent asset, in a sixth step the computing entity 21 updates the first contingent asset to produce a first non-contingent asset as illustrated on the risk chart of FIG. 5H, when the first asset risk level of the first contingent asset is less than the contingency risk threshold level providing desired certainty for parties associated with ownership of the first asset during the first asset lifecycle. The updating includes determining the first asset risk level, comparing the first asset risk level to the contingency risk threshold level, and updating the record associated with the first contingent asset to indicate the first non-contingent asset has been created.

[0087] The determining of the first asset risk level includes obtaining the status of the first asset. The obtaining includes one or more of interpreting a first asset status update 214 from the computing entity 25-1 (e.g., indicating one of a payment approval status, approval pending, or approval rejected), receipt has seen the risk information associated with the first asset including updating a probability that the payer will pay at the end of the asset lifecycle.

[0088] The updating of the record associated with the first contingent asset includes one or more of changing a status from contingent to non-contingent, determining an updated

price (e.g., raising the price when the asset is unsold and the payer has approved a subsequent payout), and generating a first non-contingent asset **212** to include the updated record. Alternatively, or in addition to, the asset module **30** further publishes the updated record by sending the first non-contingent asset **212** to the computing entities **23-1** through **23-N** when the first asset has not been sold.

**[0089]** The method described above in conjunction with a processing module of any computing entity of the computing system **10** can alternatively be performed by other modules of the computing system **10** of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system **10**, cause one or more computing devices of the computing system **10** to perform any or all of the method steps described above.

**[0090]** FIGS. 6A-6F are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of updating a listing of a contingent asset for sale. The computing system includes the computing entity **20-1** of FIG. 1, the computing entity **21** of FIG. 1, computing entities **23-1** through **23-N** of FIG. 1, and the computing entity **25-1** of FIG. 1.

**[0091]** FIG. 6A illustrates an example method of operation of the updating of the listing of the contingent asset for sale where a first step includes the computing entity **21** determining to update a first available contingent asset **220** of a multitude of available contingent assets. The first available contingent asset **220** assigns a potential first liability of a first payer to a first seller associated with the first available contingent asset. At least a portion of the potential first liability is to be paid by the first payer to the first seller in accordance with contingency information **202** and subsequent to completion of a first asset lifecycle, as illustrated in FIG. 6B, of the first available contingent asset.

**[0092]** The determining to update the first available contingent asset **220** includes a variety of approaches. A first approach includes the asset module **30** detecting that an update time frame has elapsed. A second approach includes the asset module **30** interpreting a first asset status update **214** from the computing entity **25-1** (e.g., from the payer). A third approach includes the asset module **30** interpreting first available contingent asset pricing update information **222** from the computing entity **20-1** (e.g., from the seller). For instance, the seller requests a lower asking price. As another instance, the seller requests more time to sell the first asset.

**[0093]** A fourth approach includes the asset module **30** detecting that value has changed on a pool of related assets. A fifth approach includes the asset module **30** determining that a price change for the first asset is required to hit a desired rate of return. A sixth approach includes the asset module **30** detecting that bids for the first asset are under the asking price by more than a maximum difference threshold level (e.g., suggesting the first asset has been overpriced).

**[0094]** Having determined to update the first available contingent asset, a second step of the example method of operation of the updating of the listing of a contingent asset

for sale includes the computing entity **21** determining an updated valuation of the first available contingent asset as depicted at **t2** on the risk chart of FIG. 6B. The determining includes the asset module **30** reassessing the risk associated with the first asset and recalculating the value of the first available contingent asset based on one or more of a new estimate of the probability of payer approval, an updated expected payment, updated expected payment timing, an updated expected rate of return, recent bid prices for the first asset, and recent bid-ask spreads for other pools of similar assets.

**[0095]** FIG. 6C further illustrates the example method of operation of the updating of the listing of the contingent asset for sale where, having determined the updated valuation of the first available contingent asset, the computing entity **21** updates the first available contingent asset to produce an updated first available contingent asset **226** based on the updated valuation of the first available contingent asset. For example, the asset module **30** updates the record of the first available contingent asset to produce the updated first available contingent asset **226** utilizing the updated valuation. Alternatively, or in addition to, the asset module **30** updates aspects of the contingency information **202** as a function of the new valuation.

**[0096]** Having updated the first available contingent asset, a fourth step of the example method of operation of the updating of the listing of the contingent asset for sale includes the computing entity **21** publishing availability of the updated first available contingent asset **226** to a plurality of other computing entities **23-1** through **23-N** (e.g., to buyers) as illustrated in FIG. 6D. The publishing includes the asset module **30** performing one or more of generating an exchange listing, posting the exchange listing on an exchange, generating a record that includes updated first contingent asset information as updated first available contingent asset information **228**, sending the updated first available contingent asset information **228** (e.g., the record of the updated first contingent asset) to a plurality of other computing entities (e.g., to the computing entities **23-1** through **23-N**).

**[0097]** FIG. 6E further illustrates the example method of operation of the updating of the listing of the contingent asset for sale where, having published the availability of the updated first available contingent asset, the computing entity **21** updates the updated first available contingent asset to produce a first non-contingent asset **212** when a first asset risk level of the updated first available contingent asset is less than a contingency risk threshold level. The transitioning to the non-contingent status provides desired certainty for parties associated with ownership of the first asset during and later portion of first asset lifecycle as illustrated in FIG. 6F.

**[0098]** The updating of the updated first available contingent asset to produce the first non-contingent asset **212** by the computing entity **21** includes a series of sub-steps. In a first sub-step the asset module **30** obtains status of the first asset (e.g., interpret a first asset status update **214** from the computing entity **25-1**). In a second sub-step the asset module **30** reassesses risk information of the contingency information **202** to produce an updated probability of the payer paying the payout at the end of the asset lifecycle even when the payer has approved the payment. A third sub-step includes the asset module **30** modifying status of the record of the first asset to indicate the non-contingent status. A

fourth sub-step includes the asset module **30** repricing the first asset when the first asset is still for sale (e.g., at least the portion of the first asset is still for sale during the asset lifecycle). A fifth sub-step includes the asset module **30** republishing the record for the first non-contingent asset **212** (e.g., to the computing entities **23-1** through **23-N**) when the first asset is still available for sale.

**[0099]** The method described above in conjunction with a processing module of any computing entity of the computing system **10** can alternatively be performed by other modules of the computing system **10** of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system **10**, cause one or more computing devices of the computing system **10** to perform any or all of the method steps described above.

**[0100]** FIGS. 7A-7H are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of executing a sale of a contingent asset to a buyer from a seller.

**[0101]** The computing system includes the computing entity **20-1** of FIG. 1, the computing entity **21** of FIG. 1, the computing entity **23-1** of FIG. 1, and the computing entity **25-1** of FIG. 1.

**[0102]** FIG. 7A illustrates an example method of operation of the executing of the sale of the contingent asset to the buyer from the seller, where a first step includes the computing entity **21** indicating availability of a subset of available contingent assets of a multitude of available contingent assets to the computing entity **23-1** at **t1** of the risk chart for the asset lifecycle in FIG. 7B, based on a desired asset profile of the computing entity **23-1**. A first available contingent asset of the subset of available contingent assets assigns a potential first liability of a first payer to a first seller associated with the first available contingent asset. At least a portion of the potential first liability is to be paid by the first payer to the first seller in accordance with contingency information and subsequent to completion of a first asset lifecycle of the first available contingent asset.

**[0103]** The indicating availability of the subset of available contingent assets includes a series of sub steps. A first sub-step includes the asset module **30** identifying assets desired by the computing entity **23-1** (e.g., the buyer) as the subset of available contingent assets. For example, the asset module **30** compares the desired asset profile of the computing entity **23-1** to assets of available contingent asset information **242** to select those assets that substantially satisfy the desired asset profile. A second sub-step includes the asset module **30** generating subset of available contingent asset information **240** utilizing the selected assets. A third sub-step includes the asset module **30** sending the subset of available contingent asset information **242** the computing entity **23-1**. Alternatively, or in addition to, the asset module **30** publishes the available contingent asset information **242** on an exchange and/or sends the available contingent asset information **242** to other computing entities associated with even more buyers.

**[0104]** FIG. 7C further illustrates the example method of operation of the executing of the sale of the contingent asset to the buyer from the seller, where, having indicated the availability of the subset of available contingent assets to the buyer computing entity, in a second step the computing entity **21** obtains a set of contingent asset purchase requests **244** from the computing entity **23-1** (e.g., the buyer). The set of contingent asset purchase requests **244** includes a first contingent asset purchase request **246** with regards to a bid for the first available contingent asset. The set of contingent asset purchase requests are generated within a purchase timeframe as illustrated near **t2** of the timeline of the risk chart of the first asset lifecycle of FIG. 7D.

**[0105]** The first contingent asset purchase request **246** includes one or more of the identifier (ID) of the first asset, a buyer ID, a bid price for the first asset, a bid price range as a function of one or more conditions (e.g., higher and of the range when risk of the first asset is lower), and settlement information (e.g., an account to debit upon purchase, a credit instrument to utilize for payment, payment timing, etc.). The conditions of the bid price range include risk, number of similar assets currently available for sale, number of similar assets currently held by the buyer, number of similar assets associated with the payer that still have an active lifecycle, or any other condition that can reasonably affect pricing to create an efficient market.

**[0106]** The obtaining of the set of contingent asset purchase requests **244** by the computing entity **21** includes a variety of approaches. A first approach includes the asset module **30** issuing a request for a bid message to the computing entity **23-1** (e.g., that includes an indication that assets of the subset of available contingent asset information **240** includes assets that substantially satisfied the desired asset profile of the buyer of the computing entity **23-1**). A second approach includes the asset module **30** receiving the set of contingent asset purchase request **244** from the computing entity **23-1**.

**[0107]** A third approach includes the asset module **30** determining an auto-order outcome based on the desired asset profile of the buyer computing entity. For example, the asset module **30** interprets the desired asset profile to identify the assets to include in auto-generating the contingent asset purchase request **244** on behalf of the buyer computing entity. A fourth approach includes the asset module receiving one or more contingent asset purchase requests from one or more other computing entities.

**[0108]** FIG. 7E further illustrates the example method of operation of the executing of the sale of the contingent asset to the buyer from the seller, where, having obtained the set of contingent asset purchase requests from the buyer computing entity, a third step includes the computing entity **21** determining whether to approve the first contingent asset purchase request based on at least some of the set of contingent asset purchase requests and a risk profile during the purchase timeframe after **t2** of the risk chart for the asset lifecycle of FIG. 7F. The asset module **30** determines whether to approve the first contingent asset purchase requests based on one or more of face value of the first asset, a listed price by the seller, a minimum acceptable bid price set by the seller, a bid price from the buyer, a history of bid-ask spreads, other bid acceptances of the set of contingent asset purchase requests, a risk profile associated with the buyer, the risk level of the asset, an assessment to the

impact of the buyer's portfolio, and an assessment of the impact to the available contingent assets.

[0109] As an example of the determining whether to approve the first contingent asset purchase request, the asset module 30 indicates approval when the risk level of the asset is below a maximum desired asset risk level, the risk profile associated with the buyer is below a buyer maximum risk threshold level, and the bid price from the buyer is greater than the minimum acceptable bid price set by the seller. As another example, the asset module 30 indicates disapproval when the risk level of the buyer is greater than the buyer maximum risk threshold level. As yet another example, the asset module indicates approval when the risk level of the buyer is greater than the buyer maximum risk threshold level and the bid price from the buyer is greater than the listed price by the seller by more than a minimum difference bid-ask spread level.

[0110] When the first contingent asset purchase request is approved, a fourth step of the example method of operation to execute the sale of a contingent asset includes the computing entity 21 obtaining payment for purchase of the first available contingent asset from a first buyer associated with the first contingent asset purchase request 246. The obtaining of the payment for purchase includes a series of sub-steps. A first sub-step includes the asset module 30 determining an execution price based on the approval. The determining includes one or more of establishing a base selling price at the bid price and making an adjustment associated with risk and/or transaction fees.

[0111] A second sub-step includes the asset module 30 issuing a request for payment to the computing entity 23-1, where the request for payment includes the execution price. A third sub-step includes the asset module 30 receiving purchase information 248 from the computing entity 23-1, where the purchase information 248 includes information to execute the sale including payment (e.g., including instructions such as immediate payment and/or deducting payment from an account associated with the buyer).

[0112] FIG. 7G further illustrates the example method of operation of the executing of the sale of the contingent asset to the buyer from the seller, where, having obtained the payment for the purchase of the first available contingent asset 206, a fifth step includes the computing entity 21 facilitating seller payment utilizing the payment for purchase of the first available contingent asset to complete the purchase as illustrated in the risk chart of the asset timeline of FIG. 7H. The facilitating includes the asset module 30 determining a seller payment amount from the payment for purchase and based on the contingency information 202 (e.g., recourse, fees, etc.). The facilitating further includes the asset module 30 issuing a first available contingent asset payment 250 to the computing entity 20-1 to satisfy payment to the seller. Alternatively, or in addition to, the asset module 30 updates a seller account with a credit for the seller payment amount.

[0113] Having facilitated the seller payment, a sixth step of the example method of operation of the executing of the sale of a contingent asset to the buyer from the seller includes the computing entity 21 reassigning the potential first liability of the first available contingent asset from the first seller to an entity associated with the first buyer of the first contingent asset purchase request. For example, the asset module 30 updates the first contingent asset 206 within the contingent asset database 34 to associate an identifier of

the buyer with the first contingent asset 206. Alternatively, or in addition to, a risk level associated with the buyer is updated based on the buyer now holding the first contingent asset 206.

[0114] The method described above in conjunction with a processing module of any computing entity of the computing system 10 can alternatively be performed by other modules of the computing system 10 of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system 10, cause one or more computing devices of the computing system 10 to perform any or all of the method steps described above.

[0115] FIGS. 8A-8D are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of facilitating payment from a payer to a buyer for a contingent asset. The computing system includes the computing entity 20-1 of FIG. 1, the computing entity 21 of FIG. 1, the computing entity 23-1 of FIG. 1, and the computing entity 25-1 of FIG. 1.

[0116] FIG. 8A illustrates an example method of operation of the facilitating payment from the payer to the buyer for the contingent asset, where a first step includes the computing entity 21 obtaining a lifecycle status for a first contingent asset 206 of a multitude of contingent assets. The first contingent asset 206 assigns a potential first liability of a first payer to an owner entity associated with the first contingent asset 206. At least a portion of the potential first liability is to be paid by the first payer to the owner entity in accordance with contingency information and subsequent to completion of a first asset lifecycle of the first contingent asset 206. The lifecycle status includes pending approval, approval for payment (e.g., pending payment at 17 of FIG. 8B), and rejected.

[0117] The obtaining of the lifecycle status for the first contingent asset 206 includes a variety of approaches. A first approach includes the asset module 30 detecting a change in a risk level associated with the first contingent asset. A second approach includes the asset module 30 detecting that a transition time frame has elapsed. A third approach includes the asset module 30 receiving a request for an updated status. A fourth approach includes the asset module 30 issuing a status update to the computing entity 25-1 (e.g., the payer). A fifth approach includes the asset module 30 interpreting a first asset status update 214 from the computing entity 25-1.

[0118] Having obtained the lifecycle status for the first contingent asset, when the lifecycle status of the first contingent asset has transitioned to pending payment, a second step of the example method of operation to facilitate payment from the payer to the buyer of the contingent asset includes the computing entity 21 obtaining a payout for the first contingent asset from the first payer in accordance with the contingency information 202. The obtaining of the payout includes a series of sub-steps. A first sub-step includes the asset module 30 determining an expected payout based on the contingency information 202 and pay-

out information of the first contingent asset **206**. For example, the asset module **30** determines the expected payout to be a committed payout level from the computing entity **25-1**.

[0119] A second sub-step includes the asset module **30** issuing a payout request to the computing entity **25-1** of the payer, where the payout request includes the expected payout. A third sub-step includes the asset module **30** receiving a first contingent asset payout **260** from the computing entity **25-1**. Alternatively, or in addition to, the first contingent asset payout **260** is included in a batch payment from the computing entity **25-1** for a multitude of asset payouts.

[0120] FIG. 8C further illustrates the example method of operation of the facilitating payment from the payer to the buyer for the contingent asset, where, when the lifecycle status of the first contingent asset has transitioned to pending payment as illustrated at **17** in FIG. 8D, and having obtained the payout for the first contingent asset from the first payer, a third step includes the computing entity **21** determining a payoff for the owner entity based on the payout and the contingency information **202**. For example, when the payout is less than a face value, the asset module **30** calculates the payoff to be the payout minus any fees (e.g., a transaction fee). As another example, when the payout is greater than the face value, the asset module **30** calculates the payoff to be the payout minus the fees and further disposes of an overage (e.g., a difference between the payout and the face value) in accordance with the contingency information **202** (e.g., transfer funds to an account associated with an exchange, credit the buyer for a portion of a future purchase, credit the seller for repurchase of a future sale).

[0121] Having determined the payoff for the owner entity, a fourth step of the example method of operation of the facilitating payment from the payer to the buyer includes the computing entity **21** facilitating payment of the payoff to the owner entity. For example, the asset module **30** generates a payment message **262** that includes payment information in accordance with the first contingent asset payout **260**. The asset module **30** sends the payment message **262** to the computing entity **23-1** associated with the owner entity. Alternatively, or in addition to, the asset module **30** credits an account associated with the owner entity for the amount of the payoff.

[0122] The method described above in conjunction with a processing module of any computing entity of the computing system **10** can alternatively be performed by other modules of the computing system **10** of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system **10**, cause one or more computing devices of the computing system **10** to perform any or all of the method steps described above.

[0123] FIG. 9A is a schematic block diagram of a data structure for a smart contract **700** that includes object information **702** and. The object information **702** includes object basics (e.g., including links to blockchains and electronic assets), available purchase and/or license terms, and

available patent terms. FIG. 9A illustrates examples of each category of the object information **702**. Examples of an object of the object information **702** that are associated with contingent asset offerings include an object set identifier (e.g., of one or more contingent assets), a face value of a contingent asset, and expected payment timeframe of the contingent asset and further parameters associated with contingent assets as illustrated in FIG. 9A.

[0124] The further parameters include the environment, social, governance (ESG) information. ESG information includes negative factors caused by an entity with respect to environment, society, and entity governance. The ESG information is utilized by participants in an ESG system. The participants include investors, entities causing the negative factors, exchanges, regulatory entities, certification entities, management entities, metrics tracking entities, government entities, and ESG solution implementation entities. The ESG information further includes environment information, social information, and governance information. The ESG information broadly includes a description and metrics around the negative factors and descriptions and metrics around abatement of the negative factors.

[0125] The abatement of the negative factors includes recognizing metric levels associated with certain offsets for the negative factors. The offsetting metrics include credits from public benefit assets. Hereafter the terms public benefit assets, public benefit credits, and public benefit asset credits may be used interchangeably. In an embodiment, a public benefit asset has a net positive impact or credit (e.g., to offset a negative factor). In another embodiment, another public benefit asset has a net negative impact or debit (e.g., not a credit), where the debit actually makes the negative factor more negative. A public benefit credit includes an array of tangible offsets to abate the negative factors of any of the components of the ESG information, utilizing a public benefit asset (e.g., in a good “credit” way). For example, a carbon credit, a set of micro-carbon credits, and/or a carbon offset serves to offset a negative factor associated with the environment information. As another example, a diversity credit offsetting negative factors associated with the social information. As yet another example, a Board of Directors composition credit offsetting negative factors associated with the governance information.

[0126] As an instance of a negative environment factor, air pollution produced by a particular entity in terms of tons of carbon per year. As an associated instance of an abatement factor, a one time carbon credit granted for an environmental project to offset the air pollution where the carbon credit is associated with a metric of tons of carbon.

[0127] An instance of a negative social factor includes a low management team diversity score associated with an entity. An instance of an associated abatement factor, a one-time diversity credit to offset a negative diversity factor.

[0128] An ecosystem for creating, trading, and utilizing public benefit credits to offset the negative factors is supported by utilization of smart contracts **700**, tokens, blocks, and block chains as is further discussed. Numerous embodiments of inventions are described to support creation of digital representations of the smart contracts and tokens. Numerous inventions are further described to securely support an immutable public and/or nonpublic ledger to represent the smart contracts and tokens facilitating interest and

support of addressing the negative factors with projects and programs there are credited with offsets of the negative factors.

[0129] The license terms 704 includes owner information and agreed terms for a sale of a contingent asset associated with the smart contract. FIG. 9A further illustrates examples of each of the categories of the license terms 704. Further examples are referenced below.

[0130] FIGS. 9B and 9C are schematic block diagrams of organization of object distributed ledgers. FIG. 9B illustrates an example where a single blockchain serves as the object distributed ledger linking a series of blocks of the blockchain, where each block is associated with a different owner (e.g., different owners over time for a particular contingent asset represented by a nonfungible token). FIG. 9C illustrates another example where a first blockchain links a series of blocks of different non-fungible tokens for different sets of contingent assets. Each block forms a blockchain of its own where each further block (e.g., to the right) of its own is associated with a different owner over time for the set of contingent asset objects associated with the non-fungible token.

[0131] FIG. 9D is a schematic block diagram of an embodiment of content blockchain of an object distributed ledger, where the content includes the smart contract as previously discussed. The content blockchain includes a plurality of blocks 2-4. Each block includes a header section and a transaction section. The header section includes one or more of a nonce, a hash of a preceding block of the blockchain, where the preceding block was under control of a preceding device (e.g., a broker computing device, a user computing device, a blockchain node computing device, etc.) in a chain of control of the blockchain, and a hash of a current block (e.g., a current transaction section), where the current block is under control of a current device in the chain of control of the blockchain.

[0132] The transaction section includes one or more of a public key of the current device, a signature of the preceding device, smart contract content, change of control from the preceding device to the current device, and content information from the previous block as received by the previous device plus content added by the previous device when transferring the current block to the current device.

[0133] FIG. 9D further includes devices 2-3 to facilitate illustration of generation of the blockchain. Each device includes a hash function, a signature function, and storage for a public/private key pair generated by the device.

[0134] An example of operation of the generating of the blockchain, when the device 2 has control of the blockchain and is passing control of the blockchain to the device 3 (e.g., the device 3 is transacting a transfer of content from device 2), the device 2 obtains the device 3 public key from device 3, performs a hash function 2 over the device 3 public key and the transaction 2 to produce a hashing resultant (e.g., preceding transaction to device 2) and performs a signature function 2 over the hashing resultant utilizing a device 2 private key to produce a device 2 signature.

[0135] Having produced the device 2 signature, the device 2 generates the transaction 3 to include the device 3 public key, the device 2 signature, device 3 content request to 2 information, and the previous content plus content from device 2. The device 3 content request to device 2 information includes one or more of a detailed content request, a query request, background content, and specific instructions

from device 3 to device 2 for access to a patent license. The previous content plus content from device 2 includes one or more of content from an original source, content from any subsequent source after the original source, an identifier of a source of content, a serial number of the content, an expiration date of the content, content utilization rules, and results of previous blockchain validations.

[0136] Having produced the transaction 3 section of the block 3 a processing module (e.g., of the device 2, of the device 3, of a transaction mining server, of another server), generates the header section by performing a hashing function over the transaction section 3 to produce a transaction 3 hash, performing the hashing function over the preceding block (e.g., block 2) to produce a block 2 hash. The performing of the hashing function may include generating a nonce such that when performing the hashing function to include the nonce of the header section, a desired characteristic of the resulting hash is achieved (e.g., a desired number of preceding zeros is produced in the resulting hash).

[0137] Having produced the block 3, the device 2 sends the block 3 to the device 3, where the device 3 initiates control of the blockchain. Having received the block 3, the device 3 validates the received block 3. The validating includes one or more of verifying the device 2 signature over the preceding transaction section (e.g., transaction 2) and the device 3 public key utilizing the device 2 public key (e.g., a re-created signature function result compares favorably to device 2 signature) and verifying that an extracted device 3 public key of the transaction 3 compares favorably to the device 3 public key held by the device 3. The device 3 considers the received block 3 validated when the verifications are favorable (e.g., the authenticity of the associated content is trusted).

[0138] FIGS. 9E-9M are schematic block diagrams of another embodiment of a computing system, contingent asset risk charts, and a blockchain record illustrating an example of listing a contingent asset for sale utilizing an object distributed ledger. The computing system includes the computing entity 20-1 of FIG. 1, the computing entity 21 of FIG. 1, computing entities 23-1 through 23-N of FIG. 1, and the computing entity 25-1 of FIG. 1.

[0139] FIG. 9E illustrates an example method of operation of the listing of the contingent asset for sale utilizing the blockchain record where in a first step the asset module 30 obtains a set of asset sale requests 200-1 through 200-N from the computing entity 20-1 as depicted prior to t3 on the risk vs. time chart of FIG. 9F. A first asset of a first asset sale request of the set of asset sale requests assigns a face value level of a potential first liability of a first payer to a first seller associated with the first asset. At least a portion of the face value of the potential first liability is to be paid by the first payer to the first seller in accordance with contingency information and subsequent to completion of a first asset lifecycle of the first asset. The set of asset sale requests are generated within a sales timeframe.

[0140] The computing entity 21 obtains the asset sale request 200-1 associated with the first asset by at least one of identifying desired assets associated with the computing entity 20-1 (e.g., identify what a seller associated with the computing entity 20-1 should offer for sale), requesting that the computing entity 20-1 issue the sale request, and receiving the sale request from the computing entity 20-1. Alternatively, or in addition to, the asset sale request 200-1

includes a blockchain record associated with the first asset. In an embodiment the computing entity 20-1 is associated with a third party representing one or more sellers.

[0141] The first step further includes the computing entity 21 interpreting a set of digital records representing a multitude of contingent assets to produce a set of contingent asset sale requests. A first contingent asset of a first contingent asset sale request of the set of contingent asset sale requests assigns a potential first liability of a first payer to a first seller associated with the first contingent asset. For example, the asset module 30 interprets the digital record of asset sale request 200-1 to produce the first contingent asset sale request for the first contingent asset. The asset module 30 stores the asset sale requests in the contingent asset database 34.

[0142] Figure page further illustrates the example method of operation of the listing of the contingent asset for sale utilizing the blockchain record where, having produced the set of contingent asset sale requests, in a second step the computing entity 21 interpreting a first authenticity indicator 204 associated with the first contingent asset sale request to produce a first contingent asset risk level of the first contingent asset of the first contingent asset sale request. The interpreting of the first authenticity indicator 204 associated with the first contingent asset sale request to produce the first contingent asset risk level of the first contingent asset of the first contingent asset sale request includes a series of sub-steps.

[0143] A first sub-step includes identifying an asset authenticity computing entity based on an identifier of the first seller. For example, the asset module 30 interprets the asset sale request 200-1 to extract an identifier of the asset authenticity computing entity as computing entity 25-1.

[0144] A second sub-step includes obtaining authenticity information from the asset authenticity computing entity for the first contingent asset. For example, the asset module 30 issues a request for the authenticity information for the first contingent asset to the computing entity 25-1 and receives a response from the computing entity 25-1 that includes the first authenticity indicator 204.

[0145] A third sub-step includes the computing entity 21 indicating that the first contingent asset is valid when the authenticity information validates that the potential first liability of the first payer is to the first seller associated with the first contingent asset and that the first payer has not disapproved payment of the potential first liability. For example, the asset module 30 interprets the first authenticity indicator 204 to determine a status of the first contingent asset where the status indicates that the potential first liability of the asset sale request 200-1 is confirmed as associated with the first payer. The asset module 30 further interprets the first authenticity indicator 204 to determine that the status indicates that the potential first liability of the first payer is to be made to the first seller of the asset sale request 200-1. The asset module 30 further interprets the first authenticity indicator 204 to determine that the status indicates that the first payer has not disapproved payment of the potential first liability (e.g., status is either approved or pending approval but not denied).

[0146] When the first contingent asset is valid and the authenticity information indicates approval of the payment of the potential first liability by the first payer, a fourth sub-step includes the computing entity 21 establishing the first contingent asset risk level to be less than the contingen-

gency risk threshold level. For example, the asset module 30 updates contingency information 202 in the contingent asset database 34 to indicate that the first contingent asset risk level is less than the contingency risk threshold level since the first payer has approved the payment.

[0147] Alternatively, when the first contingent asset is valid and the authenticity information indicates pending approval of the payment of the potential first liability by the first payer, a fifth sub-step includes the computing entity 21 establishing the first contingent asset risk level to be greater than the contingency risk threshold level since the first payer has not yet approved the payment implying that it is possible that payment will never be made.

[0148] Having produced the first contingent asset risk level, a third step of the example method of operation includes the computing entity 21 determining whether the first contingent asset risk level of the first contingent asset is greater than the contingency risk threshold level as illustrated in FIG. 9H. In an embodiment, the computing entity 21 updates the first contingent asset risk level as interpreted from the first authenticity indicator 204 by obtaining risk levels of relevant attributes, re-calculating the first contingent asset risk level based on the risk levels of the relevant attributes, and comparing the first contingent asset risk level to the contingency risk threshold level. For example, the asset module 30 obtains the risk levels of the relevant attributes to include risks associated with the payer, the seller, the type of contingent asset, parameters of the sale request, and status of the first contingent asset (e.g., contingent versus noncontingent and lifecycle status). As a further example, the asset module 30 maps the risk levels of the relevant attributes to the first contingent asset risk level for comparison to the contingency risk threshold level to determine that the first contingent asset risk level is greater than the contingency risk threshold level. As yet another example, the asset module 30 indicates that the first contingent asset risk level is greater than the contingency risk threshold level when a blockchain record of the first asset (e.g., as received in the asset sale request 200-1 and/or the first authenticity indicator 204) indicates that the payer has not approved the potential liability yet.

[0149] When the first contingent asset risk level of the first contingent asset of the first contingent asset sale request is greater than a contingency risk threshold level, the third step of the example method of operation further includes the computing entity 21 establishing first available terms for the first contingent asset based on the first contingent asset sale request. The establishing the first available terms for the first contingent asset based on the first contingent asset sale request includes a series of sub-steps.

[0150] A first sub-step includes determining proposed pricing of the first contingent asset based on one or more of a desired sale price from the first seller, an estimated probability of first payer approval, an expected payment timeframe, an expected payment level, an expected rate of return for the first seller, recent bid prices for other contingent assets, and recent bid-ask spreads for the other contingent assets. For example, the asset module 30 determines the proposed pricing of the first contingent asset as the same as the desired sale price from the first seller as indicated in the asset sale request 200-1.

[0151] A second sub-step includes determining whether the proposed pricing is acceptable to the first seller. For example, the asset module 30 issues a query to the comput-

ing entity **20-1** and receives a query response indicating whether the proposed pricing is acceptable to the first seller. As another example, the asset module **30** recovers acceptable pricing range information for the first seller from the contingency information **202** and indicates whether the proposed pricing is acceptable to the first seller based on interpreting the acceptable pricing range information.

**[0152]** A third sub-step includes establishing the first available license terms to include the proposed pricing of the first contingent asset when the proposed pricing is acceptable to the first seller. For example, the asset module **30** updates the contingency information **202** for the first contingent asset to include the proposed pricing as approved by the first seller.

**[0153]** FIG. 9I further illustrates the example method of operation of the listing of the contingent asset for sale utilizing the blockchain record where, having established the first available terms for the first contingent asset, a fourth step includes the computing entity **21** generating a first smart contract to indicate availability of the first contingent asset to include the first available terms and a contingent status. For example, the asset module **30** generates the smart contract **700** as discussed previously to include an indication of availability of the first contingent asset, the first available terms, and a status indicator indicating that the payment by the first payer is still contingent (e.g., not approved yet).

**[0154]** Having generated the first smart contract, a fifth step of the example method of operation includes the computing entity **21** causing generation of a non-fungible token to represent the first smart contract in the object distributed ledger as illustrated in a publishing step along the lifecycle in FIG. 9J. The causing the generation of the non-fungible token associated with the first smart contract in the object distributed ledger includes determining whether to indirectly or directly update the object distributed ledger. For example, the computing entity **21** determines to indirectly update the object distributed ledger when the computing entity **21** does not have a satisfactory direct access to the object distributed ledger (e.g., the computing entity **21** does not serve as a blockchain node). As another example, the computing entity **21** determines to directly update the object distributed ledger when a predetermination stored in the contingent asset database **34** indicates to directly access the object distributed ledger when possible (e.g., a copy of the blockchain is stored in the contingent asset database **34** of the computing entity **21**).

**[0155]** When indirectly updating the object distributed ledger, the causing the generation includes the computing entity **21** issuing a non-fungible token generation request to an object ledger computing device serving as a blockchain node of the object distributed ledger. The non-fungible token generation request includes the first smart contract. For example, the computing entity **21** issues a first contingent asset blockchain record **300** to the computing entity **23-1**, where the contingent asset blockchain record **300** includes the request and the first smart contract. In response, the computing entity **23-1** adds a new non-fungible token listing to the object distributed ledger (e.g., as illustrated by FIGS. 9B and 9C).

**[0156]** When directly updating the object distributed ledger, the causing the generation includes the computing entity **21** performing a series of sub-steps previously discussed in FIG. 9D and as also discussed in FIG. 9K. A first sub-step includes obtaining a copy of the object distributed ledger.

For example, the computing entity **21** extracts the object distributed ledger from a message from computing entity **23-1**. As another example, the computing entity **21** recovers the object distributed ledger from the contingent asset database **34**.

**[0157]** A second sub-step includes hashing the first smart contract utilizing a receiving public key of the object distributed ledger to produce a next transaction hash value. For example, the computing entity **21** obtains a suitable receiving public key (e.g., from a current version of the blockchain, from a blockchain node, from the computing entity **23-1**) and performs the hashing function to produce the next transaction hash value.

**[0158]** A third sub-step includes encrypting the next transaction hash value utilizing a private key of the computing entity **21** to produce a next transaction signature. For example, the computing entity **21** recovers a private key associated with the computing entity **21** and utilizes the recovered private key to encrypt the next transaction hash value to produce the next transaction signature.

**[0159]** A fourth sub-step includes generating a next block of a blockchain of the object distributed ledger to include the first smart contract and the next transaction signature. For example, the computing entity **21** generates the next block as previously discussed with regards to FIG. 9D to include the first smart contract and the next transaction signature.

**[0160]** A fifth sub-step includes causing inclusion of the next block as the non-fungible token in the object distributed ledger. For example, the computing entity **21** appends the next block of the blockchain in the object distributed ledger as previously discussed with reference to FIG. 9D to update the object distributed ledger as illustrated in FIGS. 9B and 9C.

**[0161]** Alternatively, when the first contingent asset risk level of the first contingent asset of the first contingent asset sale request is less than the contingency risk threshold level, the example method of operation includes the computing entity **21** establishing the first available terms for the first contingent asset based on the first contingent asset sale request. The example method of operation further includes the computing entity **21** generating first smart contract to indicate the availability of the first contingent asset to include the first available terms and a non-contingent status (e.g., the first payer has approved the payment). The example method of operation further includes the computing entity **21** causing generation of the non-fungible token to represent the first smart contract in the object distributed ledger as previously discussed.

**[0162]** FIG. 9K illustrates an example of generating a contingent asset blockchain record (e.g., for the first contingent asset blockchain record **300**) where, blockchain-encoded records are utilized to securely represent contingent assets through the contingent asset lifecycle of FIG. 5B. In particular, a blockchain of blockchain-encoded records is utilized to record transactions and updates associated with a particular contingent asset. For instance, a new blockchain is created when a contingent asset is created by an associated computing entity on behalf of an initial owner. As another instance, the blockchain is updated when the contingent asset is sold by the original owner to a buyer. As yet another instance, the blockchain is updated when the contingent asset is sold by the buyer to another buyer. As a still further instance, the blockchain is updated when a liability of the contingent asset is paid by a payer to a current owner.

[0163] Each block of the blockchain includes various fields associated with the blockchain and a transaction field that includes content associated with the corresponding contingent asset as previously discussed. The content includes anything related to the contingent asset including contingency information and transaction information associated with a current event prompting updating of the blockchain.

[0164] The example blockchain includes blocks 2-4. Each block includes a header section and a transaction section. The header section includes one or more of a nonce, a hash of a preceding block of the blockchain, where the preceding block was under control of a preceding computing device (e.g., a computing device of a seller) in a chain of control of the blockchain, and a hash of a current block (e.g., a current transaction section). The current block is under control of a current computing device in the chain of control of the blockchain.

[0165] The transaction section includes one or more of a public key of the current computing device, a signature of the preceding computing device, request information regarding a record request and change of control from the preceding computing device to the current computing device, and content information from the previous block as received by the previous computing device plus content added by the previous computing device when transferring the current block to the current computing device.

[0166] The example further includes computing devices 2-3 (e.g., devices #2 and #3) to facilitate illustration of generation of the blockchain. Each computing device includes a hash function, a signature function, and storage for a public/private key pair generated by the device.

[0167] In an example of operation of the generating of the blockchain, when the device 2 has control of the blockchain and is passing control of the blockchain to the device 3 (e.g., the device 3 is transacting a transfer of content from device 2), the device 2 obtains the device 3 public key from device 3, performs a hash function 2 over the device 3 public key and the transaction 2 to produce a hashing resultant (e.g., preceding transaction to device 2) and performs a signature function 2 over the hashing resultant utilizing a device 2 private key to produce a device 2 signature.

[0168] Having produced the device 2 signature, the device 2 generates the transaction 3 to include the device 3 public key, the device 2 signature, device 3 record request to device 2 information, and the previous content plus content from device 2. The device 3 record request to device 2 information includes one or more of the actual record request, a query request, background content, and routing instructions from device 3 to device 2 for access to the content. The previous content plus content from device 2 includes one or more of content from an original source, content from any subsequent source after the original source, an identifier of a source of content, a serial number of the content, an expiration date of the content, content utilization rules, and results of previous blockchain validations.

[0169] Having produced the transaction 3 section of the block 3 a processing module (e.g., of the device 2, of the device 3, of a transaction mining computing entity, of a computing device), generates the header section by performing a hashing function over the transaction section 3 to produce a transaction 3 hash, performing the hashing function over the preceding block (e.g., block 2) to produce a block 2 hash. The performing of the hashing function may

include generating a nonce such that when performing the hashing function to include the nonce of the header section, a desired characteristic of the resulting hash is achieved (e.g., a desired number of zero's).

[0170] Having produced the block 3, the device 2 sends the block 3 to the device 3, where the device 3 initiates control of the blockchain. Having received the block 3, the device 3 validates the received block 3. The validating includes one or more of verifying the device 2 signature over the preceding transaction section (e.g., transaction 2) and the device 3 public key utilizing the device 2 public key (e.g., a re-created signature function result compares favorably to device 2 signature) and verifying that an extracted device 3 public key of the transaction 3 compares favorably to the device 3 public key held by the device 3. The device 3 considers the received block 3 validated when the verifications are favorable (e.g., the authenticity of the associated content is trusted). For instance, the device considers the records intact, valid, and usable to facilitate listing, selling, buying, and paying off the contingent asset of the contingent asset blockchain record.

[0171] FIG. 9L further illustrates the example method of operation of the listing of the contingent asset for sale utilizing the blockchain record where, having published availability of the first contingent asset utilizing the first contingent asset blockchain encoded record and a nonfungible token, and when subsequent to the generation of the non-fungible token that represents the first smart contract in the object distributed ledger, a sixth step includes the computing entity 21, when the first contingent asset risk level of the first contingent asset of the first contingent asset sale request is less than the contingency risk threshold level (e.g., the first payer approves payment), establishing updated first available terms for the first contingent asset based on the first contingent asset risk level. For example, the asset module 30 redetermines the first contingent asset risk level and establishes repricing information for the smart contract (e.g., a higher price since the risk is lower from the payment approval).

[0172] The re-determining of the first contingent asset risk level includes one or more of interpreting a first asset status update 214 from the computing entity 25-1 (e.g., indicating one of a payment approval status, approval pending, or approval rejected), reassess the risk information associated with the first asset including updating a probability that the payer will pay at the end of the asset lifecycle, and interpreting risk information of the content of the blockchain record. In an embodiment, the first asset status update 214 includes a status blockchain. The asset module 30 indicates the first contingent asset risk level to be less than the contingency risk threshold level when the status blockchain from the first asset status update 214 indicates that the payer has approved the potential liability of the first asset when the status blockchain has been verified as previously discussed. The new lowered risk level along the lifecycle is indicated in FIG. 9M.

[0173] The sixth step further includes the computing entity 21 generating an updated first smart contract to indicate the availability of the first contingent asset to include the updated first available terms and a non-contingent status (e.g., to include the re-pricing information). The sixth step further includes the computing entity 21 causing modifica-

tion of the non-fungible token to represent the updated first smart contract in the object distributed ledger and/or updating of the blockchain record.

**[0174]** The updating of the blockchain record associated with the first contingent asset includes one or more of changing a status from contingent to non-contingent, determining an updated price (e.g., raising the price when the asset is unsold and the payer has approved a subsequent payout), and generating the first noncontingent asset blockchain record **302** to include the updated record. Alternatively, or in addition to, the asset module **30** further publishes the updated record by sending the first noncontingent asset blockchain record **302** to the computing entities **23-1** through **23-N** when the first asset has not been sold and the computing entities **23-1** through **23-N** are associated with potential buyers of the first contingent asset.

**[0175]** The method described above in conjunction with a processing module of any computing entity of the computing system **10** can alternatively be performed by other modules of the computing system **10** of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system **10**, cause one or more computing devices of the computing system **10** to perform any or all of the method steps described above.

**[0176]** FIGS. 10A-10F are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of updating a listing for a contingent asset for sale utilizing a blockchain record. The computing system includes the computing entity **20-1** of FIG. 1, the computing entity **21** of FIG. 1, computing entities **23-1** through **23-N** of FIG. 1, and the computing entity **25-1** of FIG. 1.

**[0177]** FIG. 10A illustrates an example method of operation of the updating of the listing of the contingent asset for sale utilizing the blockchain record where a first step includes the computing entity **21** determining to update a first available contingent asset blockchain encoded record **320** representing the first available contingent asset of a multitude of available contingent assets. The first available contingent asset assigns a potential first liability of a first payer to a first seller associated with the first available contingent asset. At least a portion of the potential first liability is to be paid by the first payer to the first seller in accordance with contingency information **202** and subsequent to completion of a first asset lifecycle, as illustrated in FIG. 10B, of the first available contingent asset.

**[0178]** The determining to update the first available contingent asset blockchain encoded record includes a variety of approaches. A first approach includes the asset module **30** detecting that an update time frame has elapsed. A second approach includes the asset module **30** interpreting a first asset status update **214** from the computing entity **25-1** (e.g., from the payer). In an embodiment, the first asset status update to **14** includes a status blockchain. A third approach includes the asset module **30** interpreting first available contingent asset pricing update information **222** from the

computing entity **20-1** (e.g., from the seller). For instance, the seller requests a higher asking price and more time to sell the first asset.

**[0179]** A fourth approach includes the asset module **30** detecting that value has changed on a pool of related assets. A fifth approach includes the asset module **30** determining that a price change for the first asset is required to hit a desired rate of return. A sixth approach includes the asset module **30** detecting that bids for the first asset are over the asking price by more than a maximum overage threshold level (e.g., suggesting the first asset has been underpriced).

**[0180]** Having determined to update the first available contingent asset blockchain encoded record, a second step of the example method of operation of the updating of the listing of a contingent asset for sale utilizing the blockchain record includes the computing entity **21** determining an updated valuation of the first available contingent asset as depicted at **t2** on the risk chart of FIG. 10B to produce an updated first available contingent asset. The determining includes the asset module **30** reassessing the risk associated with the first asset and recalculating the value of the first available contingent asset based on one or more of a new estimate of the probability of payer approval, an updated expected payment, updated expected payment timing, an updated expected rate of return, recent bid prices for the first asset, and recent bid-ask spreads for other pools of similar assets.

**[0181]** FIG. 10C further illustrates the example method of operation of the updating of the listing of the contingent asset for sale utilizing the blockchain record where, having determined the updated valuation of the first available contingent asset, the computing entity **21** updates the first available contingent asset to produce an updated first available contingent asset blockchain record **322** based on the updated valuation of the first available contingent asset. For example, the asset module **30** updates the blockchain record, as discussed with reference to FIG. 9K, of the first available contingent asset to produce the updated first available contingent asset blockchain record **322** utilizing the updated valuation. Alternatively, or in addition to, the asset module **30** updates aspects of the contingency information **202** as a function of the updated valuation.

**[0182]** Having updated the first available contingent asset blockchain encoded record, a fourth step of the example method of operation of the updating of the listing of the contingent asset for sale utilizing the blockchain record includes the computing entity **21** publishing availability of the updated first available contingent asset to a plurality of other computing entities **23-1** through **23-N** (e.g., to buyers) as illustrated in FIG. 10D utilizing the updated first available contingent asset blockchain record **322**. The publishing includes the asset module **30** performing one or more of generating an exchange listing utilizing that includes the updated first available contingent asset blockchain record **322**, posting the exchange listing on an exchange, and sending the updated first available contingent asset blockchain record **322** to a plurality of other computing entities (e.g., to the computing entities **23-1** through **23-N**).

**[0183]** FIG. 10E further illustrates the example method of operation of the updating of the listing of the contingent asset for sale utilizing the blockchain record where, having published the availability of the updated first available contingent asset, the computing entity **21** updates the updated first available contingent asset blockchain record to

produce a first non-contingent asset blockchain record **324** when a first asset risk level of the updated first available contingent asset is less than a contingency risk threshold level. The transitioning to the non-contingent status provides desired certainty for parties associated with ownership of the first asset during and later portion of first asset lifecycle as illustrated in FIG. 10F.

**[0184]** The updating of the updated first available contingent asset to produce the first non-contingent asset blockchain record **324** by the computing entity **21** includes a series of sub-steps. In a first sub-step the asset module **30** obtains status of the first asset (e.g., interpret a first asset status update **214** from the computing entity **25-1**). In a second sub-step the asset module **30** reassesses risk information of the contingency information **202** to produce an updated probability of the payer paying the payout at the end of the asset lifecycle even when the payer has approved the payment. A third sub-step includes the asset module **30** modifying status of the blockchain record, as discussed with reference to FIG. 9K, of the first asset to indicate the non-contingent status. A fourth sub-step includes the asset module **30** repricing the first asset when the first asset is still for sale (e.g., at least the portion of the first asset is still for sale during the asset lifecycle). A fifth sub-step includes the asset module **30** publishing a first noncontingent asset blockchain record **302** (e.g., to the computing entities **23-1** through **23-N**) when the first asset is still available for sale.

**[0185]** The method described above in conjunction with a processing module of any computing entity of the computing system **10** can alternatively be performed by other modules of the computing system **10** of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system **10**, cause one or more computing devices of the computing system **10** to perform any or all of the method steps described above.

**[0186]** FIGS. 11A-11H are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of executing a sale of a contingent asset to a buyer from a seller utilizing a blockchain record. The computing system includes the computing entity **20-1** of FIG. 1, the computing entity **21** of FIG. 1, computing entities **23-1** through **23-N** of FIG. 1, and the computing entity **25-1** of FIG. 1.

**[0187]** FIG. 11A illustrates an example method of operation of the executing of the sale of the contingent asset to the buyer from the seller utilizing the blockchain record, where a first step includes the computing entity **21** indicating availability of a subset of available contingent assets of a multitude of available contingent assets to the computing entity **23-1** at **t1** of the risk chart for the asset lifecycle in FIG. 11B, based on a desired asset profile of the computing entity **23-1** and utilizing a subset of available contingent asset blockchain encoded records that represent the subset of available contingent assets. A first available contingent asset of the subset of available contingent assets assigns a potential first liability of a first payer to a first seller associated with the first available contingent asset. At least a portion of

the potential first liability is to be paid by the first payer to the first seller in accordance with contingency information and subsequent to completion of a first asset lifecycle of the first available contingent asset.

**[0188]** The indicating availability of the subset of available contingent assets includes a series of sub steps. A first sub-step includes the asset module **30** identifying assets desired by the computing entity **23-1** (e.g., the buyer) as the subset of available contingent assets. For example, the asset module **30** compares the desired asset profile of the computing entity **23-1** to assets of available contingent asset information **242** to select those assets that substantially satisfy the desired asset profile. A second sub-step includes the asset module **30** generating available contingent asset blockchain records **330** utilizing the selected assets (e.g., recovering individual blockchain records for each of the subset of available contingent assets from the contingent asset database **34**). A third sub-step includes the asset module **30** sending the available contingent asset blockchain records **330** to the computing entity **23-1**. Alternatively, or in addition to, the asset module **30** publishes the available contingent asset blockchain records **330** on an exchange and/or sends the available contingent asset blockchain records **330** to other computing entities associated with even more buyers.

**[0189]** FIG. 11C further illustrates the example method of operation of the executing of the sale of the contingent asset to the buyer from the seller utilizing the blockchain record, where, having indicated the availability of the subset of available contingent assets using the available contingent asset blockchain records **330** to the buyer computing entity, in a second step the computing entity **21** obtains a set of contingent asset purchase requests **244** from the computing entity **23-1** (e.g., the buyer). The set of contingent asset purchase requests **244** includes a first contingent asset purchase request **246** with regards to a bid for the first available contingent asset. The set of contingent asset purchase requests are generated within a purchase timeframe as illustrated near **t2** of the timeline of the risk chart of the first asset lifecycle of FIG. 11D.

**[0190]** The first contingent asset purchase request **246** includes one or more of the identifier (ID) of the first asset, an identifier for a corresponding blockchain record, a buyer ID, a bid price for the first asset, a bid price range as a function of one or more conditions (e.g., higher and of the range when risk of the first asset is lower), and settlement information (e.g., an account to debit upon purchase, a credit instrument to utilize for payment, payment timing, etc.). In an embodiment, the contingent asset purchase request **244** includes modified blockchain records for corresponding contingent assets (e.g., to include purchase request content). The conditions of the bid price range include risk, a blockchain record verification requirement (e.g., bid only valid when a corresponding blockchain record can be verified), number of similar assets currently available for sale, number of similar assets currently held by the buyer, number of similar assets associated with the payer that still have an active lifecycle, or any other condition that can reasonably affect pricing to create an efficient market.

**[0191]** The obtaining of the set of contingent asset purchase requests **244** by the computing entity **21** includes a variety of approaches. A first approach includes the asset module **30** issuing a request for a bid message to the computing entity **23-1** (e.g., that includes an indication that

assets of the subset of available contingent asset includes assets that substantially satisfies the desired asset profile of the buyer of the computing entity 23-1). A second approach includes the asset module 30 receiving the set of contingent asset purchase request 244 from the computing entity 23-1. [0192] A third approach includes the asset module 30 determining an auto-order outcome based on the desired asset profile of the buyer computing entity. For example, the asset module 30 interprets the desired asset profile to identify the assets to include in auto-generating the contingent asset purchase requests 244 on behalf of the buyer computing entity. A fourth approach includes the asset module receiving one or more contingent asset purchase requests from one or more other computing entities.

[0193] FIG. 11E further illustrates the example method of operation of the executing of the sale of the contingent asset to the buyer from the seller utilizing the blockchain record, where, having obtained the set of contingent asset purchase requests from the buyer computing entity, a third step includes the computing entity 21 determining whether to approve the first contingent asset purchase request 246 based on at least some of the set of contingent asset purchase requests and a risk profile during the purchase timeframe after t2 of the risk chart for the asset lifecycle of FIG. 11F. The asset module 30 determines whether to approve the first contingent asset purchase request 246 based on one or more of verification of a blockchain record associated with the first contingent asset purchase request, face value of the first asset, a listed price by the seller, a minimum acceptable bid price set by the seller, and a bid price from the buyer, a history of bid-ask spreads. The approval determination is further based on one or more of other bid acceptances of the set of contingent asset purchase requests, a risk profile associated with the buyer, the risk level of the asset, an assessment to the impact of the buyer's portfolio, and an assessment of the impact to the available contingent assets.

[0194] As an example of the determining whether to approve the first contingent asset purchase request 246, the asset module 30 indicates approval when the risk level of the asset is below a maximum desired asset risk level in the blockchain record has been verified, the risk profile associated with the buyer is below a buyer maximum risk threshold level, and the bid price from the buyer is greater than the minimum acceptable bid price set by the seller. As another example, the asset module 30 indicates disapproval when the risk level of the buyer is greater than the buyer maximum risk threshold level and/or when the blockchain record does not verify. As yet another example, the asset module indicates approval when the risk level of the buyer is greater than the buyer maximum risk threshold level and the bid price from the buyer is greater than the listed price by the seller by more than a minimum difference bid-ask spread level.

[0195] When the first contingent asset purchase request is approved, a fourth step of the example method of operation to execute the sale of the contingent asset to the buyer from the seller utilizing the blockchain record includes the computing entity 21 obtaining payment for purchase of the first available contingent asset from a first buyer associated with the first contingent asset purchase request 246. The obtaining of the payment for purchase includes a series of sub-steps. A first sub-step includes the asset module 30 determining an execution price based on the approval. The determining includes one or more of establishing a base

selling price at the bid price and making an adjustment associated with risk and/or transaction fees.

[0196] A second sub-step includes the asset module 30 issuing a request for payment to the computing entity 23-1, where the request for payment includes the execution price within the blockchain record for the first asset. A third sub-step includes the asset module 30 receiving purchase information 248 from the computing entity 23-1, where the purchase information 248 includes an updated blockchain record including information to execute the sale including payment (e.g., including instructions such as immediate payment and/or deducting payment from an account associated with the buyer).

[0197] FIG. 11G further illustrates the example method of operation of the executing of the sale of the contingent asset to the buyer from the seller utilizing the blockchain record, where, having obtained the payment for the purchase of the first available contingent asset, a fifth step includes the computing entity 21 facilitating seller payment utilizing the payment for purchase of the first available contingent asset to complete the purchase as illustrated in the risk chart of the asset timeline of FIG. 11H. The facilitating includes the asset module 30 determining a seller payment amount from the payment for purchase and based on the contingency information 202 (e.g., recourse, fees, etc.). The facilitating further includes the asset module 30 issuing a first available contingent asset payment 250 to the computing entity 20-1 to satisfy payment to the seller. In an embodiment, the first available contingent asset payment 250 includes the blockchain record associated with the first asset to provide payment. Alternatively or in addition to, the asset module 30 updates a seller account with a credit for the seller payment amount.

[0198] Having facilitated the seller payment, a sixth step of the example method of operation of the executing of the sale of a contingent asset to the buyer from the seller utilizing the blockchain record includes the computing entity 21 updating the first available contingent asset blockchain encoded record of the subset of available contingent asset blockchain encoded records that corresponds to the first available contingent asset to indicate reassignment the potential first liability of the first available contingent asset from the first seller to an entity associated with the first buyer of the first contingent asset purchase request. For example, the asset module 30 updates the first available contingent asset blockchain record 332 as illustrated in FIG. 9K within the contingent asset database 34 to associate an identifier of the buyer with the first contingent asset. Alternatively, or in addition to, a risk level associated with the buyer is updated within the blockchain record based on the buyer now holding the first contingent asset.

[0199] The method described above in conjunction with a processing module of any computing entity of the computing system 10 can alternatively be performed by other modules of the computing system 10 of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system 10, cause one or more

computing devices of the computing system 10 to perform any or all of the method steps described above.

[0200] FIGS. 12A-12D are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of facilitating payment from a payer to a buyer for a contingent asset utilizing a blockchain record. The computing system includes the computing entity 20-1 of FIG. 1, the computing entity 21 of FIG. 1, computing entities 23-1 through 23-N of FIG. 1, and the computing entity 25-1 of FIG. 1.

[0201] FIG. 12A illustrates an example method of operation of the facilitating payment from the payer to the buyer for the contingent asset utilizing the blockchain record, where a first step includes the computing entity 21 obtaining a lifecycle status for a first contingent asset of a multitude of contingent assets. The first contingent asset assigns a potential first liability of a first payer to an owner entity associated with the first contingent asset. At least a portion of the potential first liability is to be paid by the first payer to the owner entity in accordance with contingency information and subsequent to completion of a first asset lifecycle of the first contingent asset as illustrated in FIG. 12B. The lifecycle status includes pending approval, approval for payment (e.g., pending payment at (7 of FIG. 12B), and rejected.

[0202] The obtaining of the lifecycle status for the first contingent asset includes a variety of approaches. A first approach includes the asset module 30 detecting a change in a risk level associated with the first contingent asset. A second approach includes the asset module 30 detecting that a transition time frame has elapsed. A third approach includes the asset module 30 receiving a request for an updated status. A fourth approach includes the asset module 30 issuing a status update request to the computing entity 25-1 (e.g., the payer). A fifth approach includes the asset module 30 interpreting a first asset status update 214 from the computing entity 25-1. In an embodiment the first asset status update to 14 includes a blockchain record associated with the first contingent asset.

[0203] Having obtained the lifecycle status for the first contingent asset, when the lifecycle status of the first contingent asset has transitioned to pending payment, a second step of the example method of operation to facilitate payment from the payer to the buyer of the contingent asset utilizing the blockchain record includes the computing entity 21 updating a first contingent asset blockchain encoded record 340 to indicate the lifecycle status of the first contingent asset has transitioned to pending payment. The updating includes the asset module 30 modifying the content of the blockchain record as discussed in FIG. 9K.

[0204] Having updated the first contingent asset blockchain encoded record 340, a third step of the example method of operation to facilitate payment from the payer to the buyer of the contingent asset utilizing the blockchain record includes the computing entity 21 obtaining a payout for the first contingent asset from the first payer in accordance with the contingency information 202 an utilizing the first contingent asset blockchain encoded record 340. The obtaining of the payout includes a series of sub-steps. A first sub-step includes the asset module 30 determining an expected payout based on the contingency information 202 and payout information of content of the first contingent asset blockchain record 340. For example, the asset module 30 determines the expected payout to be a committed payout level from the computing entity 25-1.

[0205] A second sub-step includes the asset module 30 issuing a payout request to the computing entity 25-1 of the payer, where the asset module 30 modifies the first contingent asset blockchain record 340 to include the expected payout and includes the first contingent asset blockchain record 340 in the payout request. A third sub-step includes the asset module 30 receiving a first contingent asset payout 260 from the computing entity 25-1. In an embodiment, the first contingent asset payout 260 includes a further updated first contingent asset blockchain record that includes payout information. Alternatively, or in addition to, the first contingent asset payout 260 is included in a batch payment from the computing entity 25-1 for a multitude of asset payouts, where a multitude of contingent asset blockchain records include a multitude of payouts.

[0206] FIG. 12C further illustrates the example method of operation of the facilitating payment from the payer to the buyer for the contingent asset utilizing the blockchain record, where, when the lifecycle status of the first contingent asset has transitioned to pending payment as illustrated at t7 in FIG. 12D, and having obtained the payout for the first contingent asset from the first payer, a fourth step includes the computing entity 21 determining a payoff for the owner entity based on the payout and the contingency information 202. For example, when the payout is less than a face value, the asset module 30 calculates the payoff to be the payout minus any fees (e.g., a transaction fee). As another example, when the payout is greater than the face value, the asset module 30 calculates the payoff to be the payout minus the fees and further disposes of an overage (e.g., a difference between the payout and the face value) in accordance with the contingency information 202 (e.g., transfer funds to an account associated with an exchange, credit the buyer for a portion of a future purchase, credit the seller for repurchase of a future sale).

[0207] Having determined the payoff for the owner entity, a fifth step of the example method of operation of the facilitating payment from the payer to the buyer utilizing the blockchain record includes the computing entity 21 facilitating payment of the payoff to the owner entity. For example, the asset module 30 generates a payment message 262 that includes payment information in accordance with the first contingent asset payout 260. In an embodiment, the asset module 30 generates the payment message 262 to include the first contingent asset blockchain record 340, where the first contingent asset blockchain record 340 includes the payment information. The asset module 30 sends the payment message 262 to the computing entity 23-1 associated with the owner entity. Alternatively, or in addition to, the asset module 30 credits an account associated with the owner entity for the amount of the payoff.

[0208] The method described above in conjunction with a processing module of any computing entity of the computing system 10 can alternatively be performed by other modules of the computing system 10 of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system 10, cause one or more

computing devices of the computing system 10 to perform any or all of the method steps described above.

[0209] FIGS. 13A-13F are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of updating a listing for a contingent asset for sale utilizing a split blockchain record. The computing system includes the computing entity 20-1 of FIG. 1, the computing entity 21 of FIG. 1, computing entities 23-1 through 23-N of FIG. 1, and the computing entity 25-1 of FIG. 1.

[0210] A split blockchain record enables ownership and transfer of ownership transactions to occur for two or more portions (e.g., sub-assets) of a common contingent asset throughout the lifecycle of the contingent asset. For example, a split blockchain record supports two ownership entities. As another example, another split blockchain record supports 1,000 ownership entities of the common contingent asset.

[0211] A split blockchain record includes several approaches. A first approach includes utilizing one blockchain record for a corresponding contingent asset, where different content portions of the blockchain record correspond to the different ownership entities. A second approach includes generating a separate new blockchain record for each ownership entity to accompany the original blockchain record for the contingent asset, where content of all of the blockchain records includes references to all other blockchain records associated with the original blockchain record. A third approach includes replacing the original blockchain record with a separate new blockchain record for each ownership entity, where content from the original blockchain record is transferred to each of the separate new blockchain records. A fourth approach includes utilizing the original blockchain record for a first ownership entity and creating a separate new blockchain record for each ownership entity beyond the first ownership entity of a multitude of ownership entities. As is further discussed below, use of the term split blockchain record may refer to any of the approaches.

[0212] FIG. 13A illustrates an example method of operation of the updating of the listing of the contingent asset for sale utilizing the split blockchain record where a first step includes the computing entity 21 determining to update a first available contingent asset blockchain encoded record set 400 corresponding to a set of first available contingent sub-assets of a first available contingent asset of a multitude of available contingent assets. The first available contingent asset assigns a potential first liability of a first payer to a first seller associated with the first available contingent asset. At least a portion of the potential first liability is to be paid by the first payer to the first seller in accordance with contingency information 202 and subsequent to completion of a first asset lifecycle, as illustrated in FIG. 13B, of the first available contingent asset. Each first available contingent asset blockchain encoded record of the first available contingent asset blockchain encoded record set 400 is mapped to a corresponding first available contingent sub-asset of the set of first available contingent sub-assets of the first available contingent asset.

[0213] The determining to update the first available contingent asset blockchain encoded record set 400 includes a variety of approaches. A first approach includes the asset module 30 detecting that an update time frame has elapsed. A second approach includes the asset module 30 interpreting

a first asset status update 214 from the computing entity 25-1 (e.g., from the payer). In an embodiment, the first asset status update to 14 includes a status blockchain. A third approach includes the asset module 30 interpreting first available contingent asset pricing update information 222 from the computing entity 20-1 (e.g., from the seller). For instance, the seller requests a higher asking price for each sub-asset. As another instance, the seller requests that more sub-assets be created.

[0214] A fourth approach includes the asset module 30 detecting that value has changed on a pool of related assets. A fifth approach includes the asset module 30 determining that a price change for the first asset is required to hit a desired rate of return. A sixth approach includes the asset module 30 detecting that bids for a majority of the sub-assets are under corresponding asking prices by more than a maximum underage threshold level (e.g., suggesting the set of first available contingent sub-assets has been overpriced).

[0215] Having determined to update the first available contingent asset blockchain record set 400, a second step of the example method of operation of the updating of the listing of a contingent asset for sale utilizing the split blockchain record includes the computing entity 21 determining an updated valuation of each first available contingent sub-asset of the set of first available contingent sub-assets of the first available contingent asset to produce an updated set of first available contingent sub-assets and an updated first available contingent asset as depicted at t2 on the risk chart of FIG. 13B. The determining includes the asset module 30 reassessing the risk associated with the first asset and recalculating the value of each sub-asset based on one or more of a percentage of the sub-assets that have been sold, a new estimate of the probability of payer approval, an updated expected payment, updated expected payment timing, an updated expected rate of return, recent bid prices for the first asset, and recent bid-ask spreads for other pools of similar assets.

[0216] FIG. 13C further illustrates the example method of operation of the updating of the listing of the contingent asset for sale utilizing the split blockchain record where, having produced the updated set of first available contingent sub-assets and the updated first available contingent asset, a third step includes the computing entity 21 updating the first available contingent asset blockchain encoded record set to produce an updated first available contingent asset blockchain encoded record set 402 based on the updated valuation of each first available contingent sub-asset of the set of first available contingent sub-assets. For example, the asset module 30 updates the first available contingent asset blockchain record set 400, as discussed with reference to FIG. 9K, to modify content of each record to indicate the updated valuation of each first available contingent sub-asset. Alternatively, or in addition to, the asset module 30 updates aspects of the contingency information 202 as a function of the updated valuations.

[0217] Having produced the updated first available contingent asset blockchain record set 402, a fourth step of the example method of operation of the updating of the listing of the contingent asset for sale utilizing the split blockchain record includes the computing entity 21 publishing availability of the updated first available contingent asset to a plurality of other computing entities 23-1 through 23-N (e.g., to buyers) as illustrated in FIG. 13D utilizing the updated first available contingent asset blockchain record set

**402.** The publishing includes the asset module **30** performing one or more of generating an exchange listing utilizing that includes the updated first available contingent asset blockchain record set **402**, posting the exchange listing on an exchange, and sending the updated first available contingent asset blockchain record set **402** to a plurality of other computing entities (e.g., to the computing entities **23-1** through **23-N**).

**[0218]** FIG. 13E further illustrates the example method of operation of the updating of the listing of the contingent asset for sale utilizing the split blockchain record where, having published the availability of the updated first available contingent asset, the computing entity **21** updates the updated first available contingent asset blockchain encoded record set to produce a first non-contingent asset blockchain encoded record set **404** when a first asset risk level of the updated first available contingent asset is less than a contingency risk threshold level. The transitioning to the non-contingent status provides desired certainty for parties associated with ownership of the portions of the first asset throughout the first asset lifecycle as illustrated in FIG. 13F.

**[0219]** The updating of the updated first available contingent asset to produce the first non-contingent asset blockchain record set **404** by the computing entity **21** includes a series of sub-steps. In a first sub-step the asset module **30** obtains status of the first asset (e.g., interpret a first asset status update **214** from the computing entity **25-1**). In a second sub-step the asset module **30** reassesses risk information of the contingency information **202** to produce an updated probability of the payer paying the payout at the end of the asset lifecycle even when the payer has approved the payment. A third sub-step includes the asset module **30** modifying status of the blockchain record, as discussed with reference to FIG. 9K, of the first asset (e.g., and sub-assets) to indicate the non-contingent status. A fourth sub-step includes the asset module **30** repricing at least some of the sub-assets of the first asset when the first asset is still for sale (e.g., at least the portion of the first asset is still for sale during the asset lifecycle, setting a proportionally higher price for larger portions). A fifth sub-step includes the asset module **30** publishing the first non-contingent asset blockchain record set **404** (e.g., to the computing entities **23-1** through **23-N**) when at least some of the first asset is still available for sale.

**[0220]** The method described above in conjunction with a processing module of any computing entity of the computing system **10** can alternatively be performed by other modules of the computing system **10** of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system **10**, cause one or more computing devices of the computing system **10** to perform any or all of the method steps described above.

**[0221]** FIGS. 14A-14H are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of executing a sale of a portion of a contingent asset to a buyer from a seller utilizing a split blockchain record. The computing system

includes the computing entity **20-1** of FIG. 1, the computing entity **21** of FIG. 1, computing entities **23-1** through **23-N** of FIG. 1, and the computing entity **25-1** of FIG. 1.

**[0222]** FIG. 14A illustrates an example method of operation of the executing the sale of the portion of the contingent asset to the buyer from the seller utilizing the split blockchain record, where a first step includes the computing entity **21** indicates availability of a subset of available contingent assets of a multitude of available contingent assets to the computing entity **23-1** at **t1** of the risk chart for the asset lifecycle in FIG. 14B, based on a desired asset profile of the computing entity **23-1** and utilizing a plurality of available contingent asset blockchain encoded record sets **500** that represent the subset of available contingent assets. Each available contingent asset blockchain encoded record of a corresponding available contingent asset blockchain encoded record set is mapped to a corresponding available contingent sub-asset of an available contingent asset of the subset of available contingent assets.

**[0223]** A first available contingent asset of the subset of available contingent assets assigns a potential first liability of a first payer to a first seller associated with the first available contingent asset. At least a portion of the potential first liability is to be paid by the first payer to the first seller in accordance with contingency information and subsequent to completion of a first asset lifecycle of the first available contingent asset. Each first available contingent asset blockchain encoded record of a first available contingent asset blockchain encoded record set is mapped to a corresponding first available contingent sub-asset of a set of first available contingent sub-assets of a first available contingent asset.

**[0224]** The indicating availability of the subset of available contingent assets includes a series of sub-steps. A first sub-step includes the asset module **30** identifying assets desired by the computing entity **23-1** (e.g., the buyer) as the subset of available contingent assets. For example, the asset module **30** compares the desired asset profile of the computing entity **23-1** to assets of the available contingent asset blockchain record sets **500** and/or of assets listed in the contingent asset database **34** to select those assets that substantially satisfy the desired asset profile. A second sub-step includes the asset module **30** generating the available contingent asset blockchain record sets **500** utilizing the selected assets (e.g., recovering individual blockchain records for each of the subset of available contingent assets from the contingent asset database **34**). A third sub-step includes the asset module **30** sending the available contingent asset blockchain record sets **500** to the computing entity **23-1**. Alternatively, or in addition to, the asset module **30** publishes the available contingent asset blockchain record sets **500** on an exchange and/or sends the available contingent asset blockchain record sets **500** to other computing entities associated with even more buyers as illustrated at **t1** of the risk chart for the asset lifecycle in FIG. 14B.

**[0225]** FIG. 14C further illustrates the example method of operation of the executing of the sale of the portion of the contingent asset to the buyer from the seller utilizing the split blockchain record, where, having indicated the availability of the subset of available contingent assets using the available contingent asset blockchain record sets **500** to the buyer computing entity, in a second step the computing entity **21** obtains a set of contingent asset purchase requests **244** from the computing entity **23-1** (e.g., the buyer). The set of contingent asset purchase requests **244** includes a first

contingent asset purchase request 246 with regards to a bid for a portion of the first available contingent asset. The set of contingent asset purchase requests are generated within a purchase timeframe as illustrated near 12 of the timeline of the risk chart of the first asset lifecycle of FIG. 14D.

[0226] The first contingent asset purchase request 246 includes one or more of the identifier (ID) of the first asset, an identifier of the portion of the first asset, an identifier for a corresponding blockchain record, a buyer ID, a bid price for the portion of the first asset, the bid price for combinations of two or more portions, a bid price in a strike price for a first right purchase option on one or more portions, a bid price and a strike price for at least one put option on the portion if purchased, a bid price range as a function of one or more conditions (e.g., higher and of the range when risk of the first asset is lower), and settlement information (e.g., an account to debit upon purchase, a credit instrument to utilize for payment, payment timing, etc.). In an embodiment, the contingent asset purchase request 244 includes modified blockchain records for portions of corresponding contingent assets (e.g., to include purchase request content). The conditions of the bid price range include risk, a blockchain record verification requirement (e.g., bid only valid when a corresponding blockchain record can be verified), number of portions of similar assets currently available for sale, number of portions of similar assets currently held by the buyer, number portions of similar assets associated with the payer that still have an active lifecycle, or any other condition that can reasonably affect pricing to create an efficient market.

[0227] The obtaining of the set of contingent asset purchase requests 244 by the computing entity 21 includes a variety of approaches. A first approach includes the asset module 30 issuing a request for a bid message to the computing entity 23-1 (e.g., that includes an indication that assets of the subset of available contingent asset includes portions of assets that substantially satisfies the desired asset profile of the buyer of the computing entity 23-1). A second approach includes the asset module 30 receiving the set of contingent asset purchase request 244 from the computing entity 23-1.

[0228] A third approach includes the asset module 30 determining an auto-order outcome based on the desired asset profile of the buyer computing entity. For example, the asset module 30 interprets the desired asset profile to identify the portions of assets to include in auto-generating the contingent asset purchase requests 244 on behalf of the buyer computing entity. A fourth approach includes the asset module receiving one or more contingent asset purchase requests from one or more other computing entities.

[0229] FIG. 14E further illustrates the example method of operation of the executing of the sale of the portion of the contingent asset to the buyer from the seller utilizing the split blockchain record, where, having obtained the set of contingent asset purchase requests from the buyer computing entity, a third step includes the computing entity 21 determining whether to approve the first contingent asset purchase request 246 based on at least some of the set of contingent asset purchase requests and a risk profile during the purchase timeframe after 12 of the risk chart for the asset lifecycle of FIG. 14F. The asset module 30 determines whether to approve the first contingent asset purchase request 246 based on one or more of verification of a blockchain record associated with the portion of the first

contingent asset purchase request, face value of the first asset, a listed price by the seller for the portion, a minimum acceptable bid price set by the seller, and a bid price from the buyer, a history of bid-ask spreads. The approval determination is further based on one or more of other bid acceptances of the set of contingent asset purchase requests, a risk profile associated with the buyer, the risk level of the asset, an assessment to the impact of the buyer's portfolio, and an assessment of the impact to the available contingent assets.

[0230] As an example of the determining whether to approve the first contingent asset purchase request 246, the asset module 30 indicates approval when the risk level of the asset is below a maximum desired asset risk level in the corresponding blockchain record has been verified, the risk profile associated with the buyer is below a buyer maximum risk threshold level, and the bid price from the buyer is greater than the minimum acceptable bid price set by the seller for the portion. As another example, the asset module 30 indicates disapproval when the risk level of the buyer is greater than the buyer maximum risk threshold level and/or when the corresponding blockchain record does not verify. As yet another example, the asset module indicates approval when the risk level of the buyer is greater than the buyer maximum risk threshold level and the bid price from the buyer is greater than the listed price by the seller by more than a minimum difference bid-ask spread level.

[0231] When the first contingent asset purchase request 246 is approved for the portion, a fourth step of the example method of operation to execute the sale of the portion of the contingent asset to the buyer from the seller utilizing the split blockchain record includes the computing entity 21 obtaining payment for purchase of the portion of the first available contingent asset from a first buyer associated with the first contingent asset purchase request 246. The obtaining of the payment for purchase includes a series of sub-steps. A first sub-step includes the asset module 30 determining an execution price based on the approval. The determining includes one or more of establishing a base selling price at the bid price and making an adjustment associated with risk and/or transaction fees.

[0232] A second sub-step includes the asset module 30 issuing a request for payment to the computing entity 23-1, where the request for payment includes the execution price within the blockchain record for the portion of the first asset. A third sub-step includes the asset module 30 receiving purchase information 248 from the computing entity 23-1, where the purchase information 248 includes an updated blockchain record including information to execute the sale including payment for the portion (e.g., including instructions such as immediate payment and/or deducting payment from an account associated with the buyer).

[0233] FIG. 14G further illustrates the example method of operation of the executing of the sale of the portion of the contingent asset to the buyer from the seller utilizing the split blockchain record, where, having obtained the payment for the purchase of the portion of the first available contingent asset, a fifth step includes the computing entity 21 facilitating seller payment utilizing the payment for purchase of the portion of the first available contingent asset to complete the purchase as illustrated in the risk chart of the asset timeline of FIG. 14H. The facilitating includes the asset module 30 determining a seller payment amount from the payment for purchase and based on the contingency information 202 (e.g., recourse, fees, etc.). The facilitating

further includes the asset module **30** issuing a payment for portion of first available contingent asset **502** to the computing entity **20-1** to satisfy payment to the seller. In an embodiment, the payment for portion of first available contingent asset **502** includes the corresponding split blockchain record associated with the portion of the first asset to provide payment. Alternatively, or in addition to, the asset module **30** updates a seller account with a credit for the seller payment amount.

**[0234]** Having facilitated the seller payment, a sixth step of the example method of operation of the executing of the sale of the portion of the contingent asset to the buyer from the seller utilizing the split blockchain record includes the computing entity **21** identifying a selected first available contingent asset blockchain encoded record of the first available contingent asset blockchain encoded record set **500** that corresponds to the portion of the first available contingent asset. For example, the asset module **30** selects a split blockchain record of the available contingent asset blockchain record sets **500** that maps to the portion of the first available contingent asset.

**[0235]** Having identified the first available contingent asset blockchain encoded record that corresponds to the portion, a seventh step of the example method of operation of the executing of the sale of the portion of the contingent asset to the buyer from the seller utilizing the split blockchain record includes the computing entity **21** updating at least some of the first available contingent asset blockchain encoded record set **500** based on the portion of the first available contingent asset to indicate reassignment of at least a portion of the potential first liability of the first available contingent asset from the first seller to an entity associated with the first buyer of the first contingent asset purchase request. For example, the asset module **30** updates the identified first available contingent asset blockchain encoded record (e.g., split blockchain record) as illustrated in FIG. 9K, within the contingent asset database **34** to associate an identifier of the buyer with the first contingent asset. Alternatively, or in addition to, a risk level associated with the buyer is updated within the blockchain record based on the buyer now holding the first contingent asset.

**[0236]** The method described above in conjunction with a processing module of any computing entity of the computing system **10** can alternatively be performed by other modules of the computing system **10** of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system **10**, cause one or more computing devices of the computing system **10** to perform any or all of the method steps described above.

**[0237]** FIGS. 15A-15H are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of listing a contingent asset for sale utilizing a split blockchain record. The computing system includes the computing entity **20-1** of FIG. 1, the computing entity **21** of FIG. 1, computing entities **23-1** through **23-N** of FIG. 1, and the computing entity **25-1** of FIG. 1.

**[0238]** FIG. 15A illustrates an example method of operation of the listing of the contingent asset for sale utilizing the split blockchain record where a first step includes the computing entity **21** interpreting a multitude of digital records representing a multitude of contingent assets to produce a first digital record of the multitude of digital records. The first digital record of the multitude of digital records represents a first contingent asset (e.g., a first asset) of the multitude of contingent assets and assigns a potential first liability of a first payer identifier to a first seller identifier associated with the first contingent asset. For example, the asset module **30** obtains a set of asset sale requests **200-1** through **200-N** from the computing entity **20-1** as depicted prior to t3 on the risk vs. time chart of FIG. 15B. At least a portion of the face value of the potential first liability is to be paid by a first payer associated with the first payer identifier to a first seller associated with the first seller identifier in accordance with contingency information **202** and subsequent to completion of a first asset lifecycle of the first asset. The set of asset sale requests are generated within a sales timeframe.

**[0239]** The computing entity **21** produces the first digital record of the asset sale request **200-1** associated with the first asset by at least one of identifying desired assets associated with the computing entity **20-1** (e.g., identify what a seller associated with the computing entity **20-1** should offer for sale), requesting that the computing entity **20-1** issue the sale request, and receiving the sale request from the computing entity **20-1**. Alternatively, or in addition to, the asset sale request **200-1** includes a blockchain record associated with the first asset. In an embodiment the computing entity **20-1** is associated with a third party representing one or more sellers.

**[0240]** FIG. 15C further illustrates the example method of operation of the listing of the contingent asset for sale utilizing the split blockchain record where, having obtained the set of asset sale requests and produced the first digital record, a second step includes the computing entity **21** interpreting a first authenticity indicator associated with the first digital record to produce a first contingent asset risk level of the first contingent asset. The interpreting the first authenticity indicator associated with the first digital record that represents the first contingent asset to produce the first contingent asset risk level of the first contingent asset includes a series of sub-steps.

**[0241]** A first sub-step includes the asset module **30** extracting an identifier of an asset authenticity computing entity from the first digital record that represents the first contingent asset based on the first seller identifier. For example, the asset module **30** extracts the identifier of the computing entity **25-1** from the asset sale request **200-1**.

**[0242]** A second sub-step includes the asset module **30** obtaining authenticity information from the asset authenticity computing entity for the first contingent asset utilizing the identifier of the asset authenticity computing entity. For example, the asset module **30** receives the authenticity information from the computing entity **25-1** (e.g., via a first authenticity indicator **204**).

**[0243]** A third sub-step includes the asset module **30** indicating that the first contingent asset is valid when the authenticity information validates that the potential first liability of the first payer identifier is to the first seller identifier associated with the first contingent asset and indicates that the first payer identifier has not disapproved

payment of the potential first liability. For example, the asset module **30** interprets the first authenticity indicator **204** to determine a status of the first contingent asset where the status indicates that the potential first liability of the asset sale request **200-1** is confirmed as associated with the first payer. The asset module **30** further interprets the first authenticity indicator **204** to determine that the status indicates that the potential first liability of the first payer is to be made to the first seller of the asset sale request **200-1**. The asset module **30** further interprets the first authenticity indicator **204** to determine that the status indicates that the first payer has not disapproved payment of the potential first liability (e.g., status is either approved or pending approval but not denied).

[0244] When the first contingent asset is valid and the authenticity information indicates approval of the payment of the potential first liability, a fourth sub-step includes the computing entity **21** establishing the first contingent asset risk level to be less than a contingency risk threshold level. For example, the asset module **30** updates the contingency information **202** in the contingent asset database **34** to indicate that the first contingent asset risk level is less than the contingency risk threshold level since the first payer has approved the payment.

[0245] Alternatively, when the first contingent asset is valid and the authenticity information indicates pending approval of the payment of the potential first liability, a fifth sub-step includes the computing entity **21** establishing the first contingent asset risk level to be greater than the contingency risk threshold level since the first payer has not yet approved the payment implying that it is possible that payment will never be made. For example, the asset module **30** updates the contingency information **202** to indicate that the first contingent asset risk level is greater than the contingency risk threshold level as illustrated in FIG. **15D**.

[0246] Having produced the first contingent asset risk level, when the first contingent asset risk level of the first contingent asset is greater than a contingency risk threshold level, a third step of the example method of operation includes the computing entity **21** establishing a set of first contingent asset available terms for a corresponding set of portions of the first contingent asset based on the first contingent asset risk level.

[0247] The establishing the set of first contingent asset available terms for the corresponding set of portions of the first contingent asset based on the first contingent asset risk level includes a series of sub-steps. A first sub-step includes the asset module **30** determining proposed pricing of the portions of the first contingent asset based on one or more of a desired set of sale prices from the first seller associated with the first seller identifier, an estimated probability of first payer approval, an expected payment timeframe, an expected payment level, an expected rate of return for the first seller, recent bid prices for other contingent assets, and recent bid-ask spreads for the other contingent assets. For example, the asset module **30** determines the proposed pricing of the set of portions of the first contingent asset as the same as the desired set of sale prices from the first seller as indicated in the asset sale request **200-1**.

[0248] A second sub-step includes the asset module **30** determining whether the proposed pricing is acceptable to the first seller. For example, the asset module **30** issues a query to the computing entity **20-1** and receives a query response that includes a first contingent asset pricing

approval indicator **208** indicating whether the proposed pricing of the set of portions is acceptable to the first seller. As another example, the asset module **30** recovers acceptable pricing range information for the first seller from the contingency information **202** and indicates whether the proposed pricing of the set of portions is acceptable to the first seller based on interpreting the acceptable pricing range information.

[0249] A third sub-step includes establishing the set of first contingent asset available terms to include the proposed pricing of the portions of the first contingent asset when the proposed pricing is acceptable to the first seller. For example, the asset module **30** updates the contingency information **202** for the first contingent asset to include the proposed pricing of the set of portions as approved by the first seller.

[0250] FIG. **15E** further illustrates the example method of operation of the listing of the contingent asset for sale utilizing the split blockchain record where, having determined that the first contingent asset risk level is greater than the contingency risk threshold level as illustrated in FIG. **15F**, in a fourth step, when the first asset risk level of the first contingent asset is greater than the contingency risk threshold level, the computing entity **21** generates a set of first smart contracts to represent the set of portions of the first contingent asset to include the set of first contingent asset available terms and a contingent status. Each first smart contract of the set of first smart contracts includes a corresponding first contingent asset available terms of a corresponding portion of the set of portions of the first contingent asset. For example, the asset module **30** generates the set of smart contracts as discussed previously for smart contract **700** to include an indication of availability of a portion of the first contingent asset, first available terms, and a status indicator indicating that the payment by the first payer is still contingent (e.g., not approved yet).

[0251] Having generated the set of first smart contracts, a fifth step of the example method of operation includes the computing entity **21** causing generation of a non-fungible token (NFT) to represent the set of first smart contracts in the object distributed ledger. The generating of the NFT to represent the set of first smart contracts in the object distributed ledger includes determining whether to indirectly or directly update the object distributed ledger. For example, the computing entity **21** determines to indirectly update the object distributed ledger when the computing entity **21** does not have a satisfactory direct access to the object distributed ledger (e.g., the computing entity **21** does not serve as a blockchain node). As another example, the computing entity **21** determines to directly update the object distributed ledger when a predetermination stored in the contingent asset database **34** indicates to directly access the object distributed ledger when possible (e.g., a copy of the blockchain is stored in the contingent asset database **34** of the computing entity **21**).

[0252] When indirectly updating the object distributed ledger, the causing the generation includes the computing entity **21** issuing a non-fungible token generation request to an object ledger computing device serving as a blockchain node of the object distributed ledger. The non-fungible token generation request includes the set of first smart contracts. For example, the computing entity **21** issues a first available contingent asset blockchain record set **301** to the computing entity **23-1**, where the first available contingent asset block-

chain record set **301** includes the request and the set of first smart contracts. In response, the computing entity **23-1** adds a new non-fungible token listing to the object distributed ledger (e.g., as illustrated by FIGS. 9B and 9C).

[0253] When directly updating the object distributed ledger, the causing the generation includes the computing entity **21** performing a series of sub-steps previously discussed in FIG. 9D and as also discussed in FIG. 9K. A first sub-step includes obtaining a copy of the object distributed ledger. For example, the computing entity **21** extracts the object distributed ledger from a message from computing entity **23-1**. As another example, the computing entity **21** recovers the object distributed ledger from the contingent asset database **34**.

[0254] A second sub-step includes hashing the set of first smart contracts utilizing a receiving public key of the object distributed ledger to produce a next transaction hash value. For example, the computing entity **21** obtains a suitable receiving public key (e.g., from a current version of the blockchain, from a blockchain node, from the computing entity **23-1**) and performs the hashing function to produce the next transaction hash value.

[0255] A third sub-step includes encrypting the next transaction hash value utilizing a private key of the computing entity **21** to produce a next transaction signature. For example, the computing entity **21** recovers a private key associated with the computing entity **21** and utilizes the recovered private key to encrypt the next transaction hash value to produce the next transaction signature.

[0256] A fourth sub-step includes generating a next block of a blockchain of the object distributed ledger to include the set of first smart contracts and the next transaction signature. For example, the computing entity **21** generates the next block as previously discussed with regards to FIG. 9D to include the set of first smart contracts and the next transaction signature.

[0257] A fifth sub-step includes causing inclusion of the next block as the non-fungible token in the object distributed ledger. For example, the computing entity **21** appends the next block of the blockchain in the object distributed ledger as previously discussed with reference to FIG. 9D to update the object distributed ledger as illustrated in FIGS. 9B and 9C.

[0258] Alternatively, when the first contingent asset risk level of the first contingent asset is less than the contingency risk threshold level, the example method of operation includes the computing entity **21** establishing the set of first contingent asset available terms for the corresponding set of portions of the first contingent asset to include the set of first contingent asset available terms and a non-contingent status. The example method of operation further includes the computing entity **21** causing generation of the non-fungible token to represent the set of first smart contracts in the object distributed ledger as previously discussed.

[0259] Having generated the first contingent asset blockchain record set **301** as the NFT, the example method further includes the computing entity **21** publishing availability of the portions of first available contingent asset utilizing the first available contingent asset blockchain record set **301** to a plurality of other computing entities (e.g., to a plurality of potential buyers). The publishing includes one or more of generating a message that includes the first available contingent asset blockchain record set **301**, posting the message on an exchange (e.g., storing the blockchain record set in the

contingent asset database **34** and making that portion of the database available to potential buyers), and sending the message to at least some of the computing entities **23-1** through **23-N** to reach buyers with the listing as illustrated in the risk versus time chart of FIG. 15F.

[0260] FIG. 15G further illustrates the example method of operation of the listing of the contingent asset for sale utilizing the split blockchain record where, having published availability of the first available contingent asset utilizing the first available contingent asset blockchain encoded record set, in a sixth step the computing entity **21** updates the first available contingent asset blockchain encoded record set to produce a first non-contingent asset blockchain encoded record set **303** as a modification to the NET as illustrated on the risk chart of FIG. 15H, subsequent to the generation of the non-fungible token that represents the set of first smart contracts in the object distributed ledger when the first contingent asset risk level of the first contingent asset is greater than the contingency risk threshold level.

[0261] The producing of the modification of the NFT includes a series of sub-steps. A first sub-step includes the computing entity **21** detecting that an updated first contingent asset risk level of the first contingent asset is less than the contingency risk threshold level. For example, the asset module **30** obtains status of the first contingent asset by interpreting a first asset status update **214** from the computing entity **25-1** (indicating one of a payment approval status, approval pending, or approval rejected), reassess the risk information associated with the portions of the first contingent asset including updating a probability that the payer will pay at the end of the asset lifecycle, and interpreting risk information of the content of the blockchain record set. In an embodiment, the first asset status update **214** includes a status blockchain. The asset module **30** indicates the first asset risk level to be less than the contingency risk threshold level when the status blockchain from the first asset status update **214** indicates that the payer has approved the potential liability of the first asset when the status blockchain has been verified as previously discussed.

[0262] A second sub-step includes establishing an updated set of first contingent asset available terms for the corresponding set of portions of the first contingent asset based on the updated first contingent asset risk level. For example, the asset module **30** changes a status from contingent to non-contingent, determines an updated price and/or set of prices for the portions (e.g., raising prices when the portions are unsold and the payer has approved a subsequent payout).

[0263] A third sub-step includes generating an updated set of first smart contracts to represent the set of portions of the first contingent asset to include the updated set of first contingent asset available terms and a non-contingent status. A fourth sub-step includes causing modification of the non-fungible token to represent the updated set of first smart contracts in the object distributed ledger. Alternatively, or in addition to, the asset module **30** further publishes the updated records by sending the first noncontingent asset blockchain record set **303** to the computing entities **23-1** through **23-N** when at least one portion of the first contingent asset is still available.

[0264] The method described above in conjunction with a processing module of any computing entity of the computing system **10** can alternatively be performed by other modules of the computing system **10** of FIG. 1 or by other devices. In addition, at least one memory section that is

non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system 10, cause one or more computing devices of the computing system 10 to perform any or all of the method steps described above.

**[0265]** FIGS. 16A-16D are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of facilitating payment from a payer to a buyer for a contingent asset utilizing a split blockchain record. The computing system includes the computing entity 20-1 of FIG. 1, the computing entity 21 of FIG. 1, computing entities 23-1 through 23-N of FIG. 1, and the computing entity 25-1 of FIG. 1. In an embodiment, the buyer includes a plurality of owner entities.

**[0266]** FIG. 16A illustrates an example method of operation of the facilitating payment from the payer to the buyer for the contingent asset utilizing the split blockchain record, where a first step includes the computing entity 21 obtaining a lifecycle status for a first contingent asset of a multitude of contingent assets. The first contingent asset assigns a potential first liability of a first payer to an owner entity associated with the first contingent asset. At least a portion of the potential first liability is to be paid by the first payer to the owner entity in accordance with contingency information and subsequent to completion of a first asset lifecycle of the first contingent asset as illustrated in FIG. 16B. The lifecycle status includes pending approval, approval for payment (e.g., pending payment at (7 of FIG. 16B), and rejected.

**[0267]** The obtaining of the lifecycle status for the first contingent asset includes a variety of approaches. A first approach includes the asset module 30 detecting a change in a risk level associated with the first contingent asset. A second approach includes the asset module 30 detecting that a transition time frame has elapsed. A third approach includes the asset module 30 receiving a request for an updated status. A fourth approach includes the asset module 30 issuing a status update request to the computing entity 25-1 (e.g., the payer). A fifth approach includes the asset module 30 interpreting a first asset status update 214 from the computing entity 25-1. In an embodiment the first asset status update 214 includes a blockchain record associated with the first contingent asset.

**[0268]** Having obtained the lifecycle status for the first contingent asset, when the lifecycle status of the first contingent asset has transitioned to pending payment, a second step of the example method of operation to facilitate payment from the payer to the buyer of the contingent asset utilizing the split blockchain record includes the computing entity 21 updating a first contingent asset blockchain encoded record set 341 to indicate the lifecycle status of the first contingent asset has transitioned to pending payment.

**[0269]** The first contingent asset blockchain-encoded record set 341 corresponds to a set of first contingent sub-assets of the first contingent asset. Each first contingent asset blockchain-encoded record of the first contingent asset blockchain-encoded record set is mapped to a corresponding first contingent sub-asset of the set of first contingent sub-assets of the first contingent asset. The updating further

includes the asset module 30 modifying the content of each blockchain record of the blockchain record set as discussed in FIG. 9K.

**[0270]** Having updated the first contingent asset blockchain encoded record set 341, a third step of the example method of operation to facilitate payment from the payer to the buyer of the contingent asset utilizing the split blockchain record includes the computing entity 21 obtaining a payout for the first contingent asset from the first payer in accordance with the contingency information 202 an utilizing the first contingent asset blockchain encoded record set 341. The obtaining of the payout includes a series of sub-steps. A first sub-step includes the asset module 30 determining an expected payout based on the contingency information 202 and payout information of content of the first contingent asset blockchain record set 341. For example, the asset module 30 determines the expected payout to be a committed payout level from the computing entity 25-1.

**[0271]** A second sub-step includes the asset module 30 issuing a payout request to the computing entity 25-1 of the payer, where the asset module 30 modifies the first contingent asset blockchain record set 341 to include the expected payout and includes the first contingent asset blockchain record set 341 in the payout request. A third sub-step includes the asset module 30 receiving a first contingent asset payout 260 from the computing entity 25-1. In an embodiment, the first contingent asset payout 260 includes a further updated first contingent asset blockchain record set that includes payout information. Alternatively, or in addition to, the first contingent asset payout 260 is included in a batch payment from the computing entity 25-1 for a multitude of asset payouts, where a multitude of contingent asset blockchain records include a multitude of payouts associated with at least the set of first contingent sub-assets of the first contingent asset.

**[0272]** FIG. 16C further illustrates the example method of operation of the facilitating payment from the payer to the buyer for the contingent asset utilizing the blockchain record, where, when the lifecycle status of the first contingent asset has transitioned to pending payment as illustrated at t7 in FIG. 16D, and having obtained the payout for the first contingent asset from the first payer, a fourth step includes the computing entity 21 determining a payoff for each owner entity of a set of owner entities based on the payout, the contingency information 202, and the first contingent asset blockchain encoded record set 341. For example, when the payout is less than a face value, the asset module 30 calculates the payoff to be a total payout minus any fees (e.g., a transaction fee). As another example, when the payout is greater than the face value, the asset module 30 calculates the total payoff to be the payout minus the fees and further disposes of an overage (e.g., a difference between the payout and the face value) in accordance with the contingency information 202 (e.g., transfer funds to an account associated with an exchange, credit the buyer for a portion of a future purchase, credit the seller for repurchase of a future sale). As yet another example, the asset module 30 calculates each payout for each owner based on ownership levels indicated by the first contingent asset blockchain record set 341.

**[0273]** Having determined the payoff for the set of owner entities, a fifth step of the example method of operation of the facilitating payment from the payer to the buyer utilizing

the split blockchain record includes the computing entity 21 facilitating payment of the payoff to the set of owner entities. For example, the asset module 30 generates a payment message 262 for each owner entity that includes corresponding payment information in accordance with the first contingent asset payout 260 and the first contingent asset blockchain record set 341. In an embodiment, the asset module 30 generates a first payment message 262 for an owner entity associated with the computing entity 23-1 to include a corresponding record of the first contingent asset blockchain record set 341, where the corresponding record of the first contingent asset blockchain record set 341 includes the payment information. The asset module 30 sends the payment message 262 to the computing entity 23-1 associated with the owner entity. Alternatively, or in addition to, the asset module 30 credits an account associated with the owner entity for the amount of the payoff.

[0274] The method described above in conjunction with a processing module of any computing entity of the computing system 10 can alternatively be performed by other modules of the computing system 10 of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system 10, cause one or more computing devices of the computing system 10 to perform any or all of the method steps described above.

[0275] FIGS. 17A-17F are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of creating a contingent asset for conversion into an instant asset at a point of purchase. The computing system includes computing entities 20-1 through 20-N of FIG. 1, the computing entity 21 of FIG. 1, computing entities 23-1 through 23-N of FIG. 1, and the computing entity 25-1 of FIG. 1. In an embodiment, the computing entities 20-1 through 20-N are associated with a multitude of consumers in a point of purchase scenario. For example, computing entity 20-1 is associated with retail processing for a first retailer of a multitude of retailers (e.g., at a point of sale terminal, on a smart phone of the consumer, on a home computer associated with the consumer). As another example, computing entity 20-2 is associated with a first consumer of the multitude of consumers. As yet another example, computing entity 20-3 is associated with a first merchant bank of a multitude of merchant banks (e.g., a debit or credit processing facility).

[0276] FIG. 17A illustrates an example method of operation of the creating the contingent asset for conversion into the instant asset at the point of purchase, where a first step includes the computing entity 21 obtaining, from a requesting computing entity of the computing system in accordance with a securely passing process, control over a secure first pending transaction associated with a transaction item. The secure first pending transaction includes identity of the transaction item (e.g., identity of a good, identity of a service, an element of an agreement, etc.), identity of the requesting computing entity (e.g., computing entity 20-1), identity of the computing entity (e.g., computing entity 21),

and an authenticated value of the transaction item (e.g., a purchase price associated with the good).

[0277] Only a device possessing control over the secure first pending transaction may modify the secure first pending transaction. The secure first pending transaction includes a header section and a transaction section. The header section includes routing identifiers and common information for a block of the transaction (e.g., security information, a hash of the block, etc.). The transaction section includes specific content associated with unique aspects of the secure first pending transaction (e.g., the identity of the transaction item, the authenticated value of the transaction item, and security information for the transaction). The security information for the transaction includes a signature over the transaction section utilizing a private key of the device in control of the transaction and a public key of a next designated device to have the control over the transaction. In an embodiment, the header section and the transaction section for the block is arranged as previously discussed with reference to FIG. 9D.

[0278] The securely passing process includes obtaining control as either an originator of the first pending transaction and being authorized as to possess control from a current entity that possesses the control. The current owner includes a public key of the next owner in the transaction section of the block and generates the signature over the transaction section utilizing both the private key of the current owner device and the public key of the next owner device as discussed in greater detail with reference to FIG. 9D.

[0279] The obtaining, in accordance with the securely passing process, the control over the secure first pending transaction includes a series of sub-steps. A first sub-step includes the asset module 30 of the computing entity 21 receiving an indication of the control over the secure first pending transaction from the requesting computing entity. For example, the asset module 30 receives a purchase adjustment request 600-1 from the computing entity 20-1, where the purchase adjustment request 600-number one includes the secure first pending transaction that includes the private key associated with the computing entity 20-1.

[0280] A second sub-step includes establishing the identity of the computing entity to have control over the secure first pending transaction. For example, the asset module 30 modifies the secure first pending transaction to include the identity of the computing entity 21 as having the control over the secure first pending transaction.

[0281] In another embodiment, the asset module 30 selects the first purchase adjustment request 600-1 of a multitude of purchase adjustment requests 600-1 through 600-N with regards to the secure first pending transaction associated with a first consumer of a multitude of consumers. The first purchase adjustment request 600-1 includes first preliminary adjustment option selections (e.g., simple rebate in 90 days, a desired discount level, a desired payment scheme). A first payer of a multitude of payers is associated with at least one component of the first pending purchase transaction. For example, a big-ticket item (e.g., as indicated by the identity of the transaction item) of the first pending purchase transaction is an item provided by the first payer to the associated retailer for sale to the first consumer.

[0282] The asset module 30 selects the first purchase adjustment request 600-1 based on one or more of matching the big-ticket item of the first pending purchase transaction to the first payer, determining that the big-ticket item is associated with a purchase price greater than a minimum

purchase price wrestled level, and determining that the big-ticket item is likely to be eligible for a purchase adjustment. The purchase adjustment includes one or more of a rebate (e.g., a portion of the purchase price is returned to the first consumer), an instant discount (e.g., the price of the big-ticket item is reduced right away), and a custom payment plan (e.g., four equal payments over 4 time periods, ramping payments over several time periods, etc.).

[0283] The purchase adjustment request 600-1 further includes one or more of an identifier of the point of purchase provider (e.g., retailer, etc.), an identifier of the consumer, and a list of items and quantities associated with the purchase request. In an embodiment, the purchase adjustment request further includes an identifier of one or more payers known to be associated with one or more of the items of the list of items, indications of specific items of the list of items that are known to be eligible for a purchase adjustment, and an indication of a desired purchase adjustment (e.g., rebate versus discount now versus a custom payment plan, or a combination thereof).

[0284] Having selected the first purchase adjustment request, the example of operation of the creating the contingent asset for conversion into the instant asset at the point of purchase further includes a second step where the computing entity 21 determines a set of candidate contingent assets for the secure first pending transaction based the identity of the transaction item, the identity of the requesting computing entity, and the authenticated value of the transaction item. Each candidate contingent asset of the set of candidate contingent assets includes a proposed unique smart contract between the identifier of the requesting computing entity and an identifier of a provider of the proposed unique smart contract.

[0285] The determining the set of candidate contingent assets for the secure first pending transaction based the identity of the transaction item, the identity of the requesting computing entity, and the authenticated value of the transaction item includes a variety of approaches. A first approach includes, when utilizing the identity of the transaction item, identifying a subset of the set of candidate contingent assets based on the identity of the transaction item and the authenticated value of the transaction item. For example, the asset module 30 of the computing entity 21 interprets an asset establishment message 602 from the computing entity 25-1 (e.g., a payer associated with the transaction item) to identify one or more candidate contingent assets associated with the transaction item. For instance, the asset module 30 identifies one or more rebate programs from the manufacturer of a refrigerator when the refrigerator is the transaction item and stores such information as contingency information 202 and the contingency asset database 34.

[0286] A second approach includes, when utilizing the identity of the requesting computing entity, a first sub-step that includes the asset module 30 determining a transaction profile for the identity of the requesting computing entity. The transaction profile includes, for the identity of the requesting computing entity, a history of purchases, a participation history in previous rebate programs, overall purchasing patterns, and demographics of an individual associated with the identity of the requesting computing entity.

[0287] A second sub-step of the second approach includes the asset module 30 identifying another subset of the set of candidate contingent assets based on the profile for the identity of the requesting computing entity. For example, the

asset module 30 matches characteristics of the profile for the identity of the requesting computing entity to characteristics of the other subset of the set of candidate contingent assets from further asset establishment message is 602 from the computing entity 25-1.

[0288] Alternatively, or in addition to, when determining the set of candidate contingent assets, the asset module 30 establishes a first contingent asset 604 with the first payer in accordance with the first preliminary adjustment option selections as illustrated in the risk chart of FIG. 17B. The first contingent asset 604 assigns a potential first liability of the first payer to the first consumer associated with the first purchase adjustment request. At least a portion of the potential first liability is to be paid by the first payer to the first consumer in accordance with contingency information of the first contingent asset and subsequent to completion of a first asset lifecycle of the first contingent asset as illustrated in FIG. 17B.

[0289] The establishing of the first contingent asset 604 includes exchanging asset establishment message 602 with the computing entity 25-1 associated with the first payer. For example, the asset module 30 issues a first asset establishment message to the computing entity 25-1 that includes the first purchase adjustment request 600-1. The computing entity 25-1 issues a second asset establishment message to the computing entity 21 that includes the first contingent asset 604. For instance, the computing entity 25-1 temporarily assigns the first consumer as the recipient of a 90 day rebate associated with the big-ticket item of the purchase adjustment request when the big-ticket item is associated with the first payer and is eligible for the rebate. The computing entity 20-1 and/or the computing entity 21 may place a temporary hold on a credit card associated with the first consumer to guarantee completion of the rebate process. In an embodiment, the computing entity that creates the first contingent asset also creates the blockchain record for the first contingent asset.

[0290] FIG. 17C further illustrates the example method of operation of the creating the contingent asset for conversion into the instant asset at the point of purchase, where, having established the set of candidate contingent assets, a third step of the example method includes the computing entity 21 facilitating selection of at least one candidate contingent asset of the set of candidate contingent assets utilizing an asset selection approach to produce a set of selected contingent assets. The facilitating the selection of the at least one candidate contingent asset of the set of candidate contingent assets utilizing the asset selection approach to produce the set of selected contingent assets includes a variety of approaches.

[0291] A first approach includes, when the asset selection approach includes a user selection, a first sub-step that includes ranking an estimated benefit to an entity associated with the identity of the requesting computing entity for each candidate contingent asset of the set of candidate contingent assets to produce an estimated benefit ranking. For example, the asset module 30 of the computing entity 21 analyzes each contingent asset to determine the estimated benefit (e.g., overall value) for an individual associated with the identity of the requesting computing entity. For instance, when Fred is buying a new refrigerator and there are two rebate programs for that refrigerator, the benefit is estimated for each rebate program for Fred based on peculiarities of

the rebate programs with regards to Fred (e.g., affinity award points for Fred, an extra amount included in the rebate since it is Fred, etc.).

[0292] A second sub-step of the first approach includes obtaining the user selection of the at least one candidate contingent asset in response to the estimated benefit ranking to produce the set of selected contingent assets. For example, the asset module 30 of the computing entity 21 receives a first authenticity indicator 204 from the computing entity 25-1 to verify rebate programs associated with the secure first pending transaction that are available. The asset module 30 interprets a user selection 205 from the computing entity 20-1 to identify the at least one candidate contingent asset in response to a selection request from the asset module 30 that includes the estimated benefit ranking.

[0293] A first sub-step of a second approach includes, when the asset selection approach includes a ranked evaluation, evaluating a potential for each candidate contingent asset of the set of candidate contingent assets to produce a potential ranking. For example, the asset module 30 of the computing entity 21 computes the potential for each candidate contingent asset more broadly for any individual that may utilize each contingent asset to produce the potential ranking (e.g., by value of the candidate contingent asset).

[0294] A second sub-step of the second approach includes selecting the at least one candidate contingent asset based on the potential ranking to produce the set of selected contingent assets. For example, the asset module 30 automatically selects a top-ranked (e.g., most value) candidate asset from the set of candidate contingent assets to identify the at least one candidate contingent asset.

[0295] Alternatively, or in addition to, the facilitating of the selection of the at least one candidate contingent asset further includes basing the selection on asset risk level. The utilization of the asset risk level includes the asset module 30 determining whether a first asset risk level of a first contingent asset is greater than a contingency risk threshold level. The determining includes one or more of obtaining risk levels of relevant attributes, calculating the first asset risk level based on the risk levels of the relevant attributes, and comparing the first asset risk level to the contingency risk threshold level. For example, the asset module 30 obtains the risk levels of the relevant attributes to include risks associated with the payer, the consumer, the type of asset, parameters of the purchase request, and status of the contingent asset by interpreting a first authenticity indicator 204 from the computing entity 25-1 on behalf of the payer (e.g., contingent versus noncontingent and lifecycle status as illustrated in FIG. 17D).

[0296] As a further example, the asset module 30 maps the risk levels of the relevant attributes to the first asset risk level for comparison to the contingency risk threshold level to determine that the first asset risk level is greater than the contingency risk threshold level. As yet another example, the asset module 30 indicates that the first asset risk level is greater than the contingency risk threshold level when the blockchain record of the first contingent asset indicates that the payer has not approved the potential liability yet.

[0297] When the first asset risk level of the first contingent asset is greater than the contingency risk threshold level, the alternative example method of operation further includes the computing entity 21 determining first preliminary instant asset terms 606 for utilization of the first contingent asset 604 as a first instant asset to support the secure first pending

transaction based on the first preliminary adjustment options, the first contingent asset, and the first asset risk level. The first preliminary instant asset terms 606 includes one or more of an instant discount level, a payment scheme (e.g., payment time periods, payment levels), expected contingency asset payout information, and contingency information 202 of the first contingent asset 604. For example, the asset module 30 generates the first preliminary instant asset terms 606 to include a maximum instant discount when the first preliminary adjustment options of the purchase adjustment request indicated a desire for an instant discount.

[0298] FIG. 17E further illustrates the example method of operation of the creating the contingent asset for conversion into the instant asset at the point of purchase, where, having selected the at least one candidate contingent asset, the method further includes the computing entity 21 generating a non-fungible token (NFT) in accordance with the securely passing process to represent a corresponding set of smart contracts of the set of selected contingent assets in the object distributed ledger. The NET includes the secure first pending transaction.

[0299] The generating the NFT in accordance with the securely passing process to represent the corresponding set of smart contracts of the set of selected contingent assets in the object distributed ledger includes determining whether to indirectly or directly update the object distributed ledger. For example, the computing entity 21 determines to indirectly update the object distributed ledger when the computing entity 21 does not have a satisfactory direct access to the object distributed ledger (e.g., the computing entity 21 does not serve as a blockchain node). As another example, the computing entity 21 determines to directly update the object distributed ledger when a predetermination stored in the contingent asset database 34 indicates to directly access the object distributed ledger when possible (e.g., a copy of the blockchain is stored in the contingent asset database 34 of the computing entity 21).

[0300] When indirectly updating the object distributed ledger, the causing the generation includes the computing entity 21 issuing a non-fungible token generation request to an object ledger computing entity of the computing system serving as a blockchain node of the object distributed ledger. The non-fungible token generation request includes the set of smart contracts of the set of selected contingent assets. For example, the computing entity 21 issues a first contingent asset blockchain record 300 to the computing entity 23-1, where the first contingent asset blockchain record 300 includes the original request and the set of smart contracts. In response, the computing entity 23-1 adds a new non-fungible token listing to the object distributed ledger (e.g., as illustrated by FIGS. 9B and 9C).

[0301] When directly updating the object distributed ledger, the causing the generation includes the computing entity 21 performing a series of sub-steps previously discussed in FIG. 9D and as also discussed in FIG. 9K. A first sub-step includes obtaining a copy of the object distributed ledger. For example, the computing entity 21 extracts the object distributed ledger from a message from computing entity 23-1 (e.g., acting as a blockchain node). As another example, the computing entity 21 recovers the object distributed ledger from the contingent asset database 34.

[0302] A second sub-step includes hashing the set of smart contracts utilizing a receiving public key of the object distributed ledger to produce a next transaction hash value.

For example, the computing entity **21** obtains a suitable receiving public key (e.g., from a current version of the blockchain, from a blockchain node, from the computing entity **23-1**, from a computing entity to be next in control) and performs the hashing function to produce the next transaction hash value.

**[0303]** A third sub-step includes encrypting the next transaction hash value utilizing a private key of the computing entity **21** to produce a next transaction signature. For example, the computing entity **21** recovers a private key associated with the computing entity **21** and utilizes the recovered private key to encrypt the next transaction hash value to produce the next transaction signature.

**[0304]** A fourth sub-step includes generating a next block of a blockchain of the object distributed ledger to include the set of smart contracts and the next transaction signature. For example, the computing entity **21** generates the next block as previously discussed with regards to FIG. 9D to include the set of smart contracts and the next transaction signature.

**[0305]** A fifth sub-step includes causing inclusion of the next block as the non-fungible token in the object distributed ledger. For example, the computing entity **21** appends the next block of the blockchain in the object distributed ledger as previously discussed with reference to FIG. 9D to update the object distributed ledger as illustrated in FIGS. 9B and 9C.

**[0306]** Alternatively, when the first contingent asset risk level of the first contingent asset is less than the contingency risk threshold level, the example method of operation includes the computing entity **21** establishing the set of contingent asset available terms for the corresponding set of portions of the first contingent asset to include the set of first contingent asset available terms and a non-contingent status. The example method of operation further includes the computing entity **21** causing generation of the non-fungible token to represent the set of first smart contracts in the object distributed ledger as previously discussed.

**[0307]** Having generated the first contingent asset blockchain record **300** as the NFT, a fifth step of the example method further includes the computing entity **21** securely passing control over the NFT via the object distributed ledger when the NFT is selected to complete the secure first pending transaction. For example, the computing entity **21** receives an indication that the contingent asset of the newly created NFT on the blockchain is to be utilized for conversion into an instant asset to facilitate completion of the secure first pending transaction. After receiving the indication, the computing entity **21** identifies a computing entity associated with the completion of the transaction to turnover control of the NFT. The computing entity **21** generates another block for the blockchain as discussed with reference to FIG. 9D to complete passing of the control to the identified computing entity associated with the completion of the transaction.

**[0308]** In an alternative embodiment, the computing entity **21** determines first preliminary instant asset terms and generates the first contingent asset blockchain record **300** for the first contingent asset to be utilized as the first instant asset in accordance with first preliminary instant asset terms. For example the asset module **30** generates instant asset content to include the first preliminary instant asset terms and generates the first contingent asset blockchain record **300** as described in FIG. 9K for the instant asset content.

**[0309]** Having generated the first contingent asset blockchain encoded record for the first contingent asset to be utilized as the first instant asset, the example of operation of the creating the contingent asset for conversion into the instant asset at the point of purchase further includes the computing entity **21** publishing availability of the first contingent asset utilizing the first contingent asset blockchain record **300** as illustrated in FIG. 17F. For example, the asset module **30** sends the first contingent asset blockchain encoded record **300** to a plurality of other computing entities **23-1** through **23-N**. As another example, the asset module **30** sends the first contingent asset blockchain record **300** to another process within the computing entity **21** (e.g., where an exchange process subsequently purchases the contingent asset for supporting utilization of the instant asset).

**[0310]** The method described above in conjunction with a processing module of any computing entity of the computing system **10** can alternatively be performed by other modules of the computing system **10** of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system **10**, cause one or more computing devices of the computing system **10** to perform any or all of the method steps described above.

**[0311]** FIGS. 18A-18F are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of executing a sale of a contingent asset for conversion into an instant asset at a point of purchase. The computing system includes computing entities **20-1** through **20-N** of FIG. 1, the computing entity **21** of FIG. 1, computing entities **23-1** through **23-N** of FIG. 1, and the computing entity **25-1** of FIG. 1. In an embodiment, the computing entities **20-1** through **20-N** are associated with a multitude of consumers in a point of purchase scenario.

**[0312]** FIG. 18A illustrates an example method of operation of the executing the sale of the contingent asset for conversion into the instant asset at the point of purchase, where a first step includes the computing entity **21** indicating availability of a first contingent asset for subsequent utilization as a first instant asset to one or more other computing entities utilizing a first contingent asset blockchain encoded record **300** for the first contingent asset. The subsequent utilization as the first instant asset supports a first purchase adjustment request of a multitude of purchase adjustment requests with regards to a first pending purchase transaction associated with a first consumer of a multitude of consumers. A first payer of a multitude of payers is associated with at least one component of the first pending purchase transaction. The first contingent asset assigns a potential first liability of the first payer to the first consumer associated with the first contingent asset. At least a portion of the potential first liability is to be paid by the first payer to the first consumer in accordance with contingency information **202** of the first contingent asset and subsequent to completion of a first asset lifecycle of the first contingent asset as illustrated with regards to FIG. 18B. First preliminary instant asset terms of the first contingent asset blockchain

encoded record specify the subsequent utilization of the first contingent asset as the first instant asset to support the first pending purchase transaction.

[0313] The indicating of the availability of the first contingent asset includes the asset module 30 sending the first contingent asset blockchain record 300 to the computing entities 23-1 through 23-N (e.g., buyers). The indicating of the availability of the first contingent asset further includes identifying one or more computing entities to target solicitation of purchasing the first contingent asset. For example, identifying computing entity 23-1 as a most likely computing entity to purchase the first contingent asset when the computing entity 23-1 has historically purchased contingent assets for conversion to instant assets.

[0314] Having indicated the availability of the first contingent asset, a second step of the example method of operation of the executing the sale of the contingent asset for conversion into the instant asset at the point of purchase includes the computing entity 21 obtaining a set of contingent asset purchase requests 244 from one or more of the other computing entities. The set of contingent asset purchase requests 244 includes a first contingent asset purchase request 246 with regards a bid for the first contingent asset. A bid includes first offered instant asset terms based on the first preliminary instant asset terms. The set of contingent asset purchase requests are generated within a purchase timeframe as illustrated in FIG. 18B. The first offered instant asset terms includes one or more of a discount range, a payment plan approach, payment plan values (e.g., how much to be paid when), guarantees required (e.g., a hold on a credit card of the consumer for an amount comparable to value of the instant asset), and a time frame of validity of the purchase request.

[0315] FIG. 18C further illustrates the example method of operation of the executing the sale of the contingent asset for conversion into the instant asset at the point of purchase, where, having obtained the first contingent asset purchase request 246, a third step of the example method includes the computing entity 21 determining whether to approve the first contingent asset purchase request 246 based on a comparison of the first offered instant asset terms to the first preliminary instant asset terms and a first asset risk level of the first contingent asset as illustrated in FIG. 18D. The determining whether to approve the first contingent asset purchase request is based on one or more of identifying a difference in terms, a listed price, a bid price, a history of bid-ask spreads, a history of other acceptances of a set of purchase requests, a comparison to other instant assets of a buyer associated with the purchase request, and an impact to one or more contingent asset portfolios. For example, the asset module 30 determines to approve the first contingent asset purchase request 246 when the bid price for the first contingent asset for conversion is greater than a minimum required bid price and an assessment of the risk is less than a maximum risk threshold level for conversion.

[0316] Having determined to approve the first contingent asset purchase request, a fourth step of the example method of operation of the executing the sale of the contingent asset for conversion into the instant asset at the point of purchase includes the computing entity 21 obtaining payment for purchase of the first contingent asset from the first buyer associated with the first contingent asset purchase request 246. For example, the asset module 30 obtains purchase information 248 from the computing entity 23-1, where the

purchase information 248 includes payment enabling information. For instance, the purchase information 248 includes a blockchain payment message including information to complete payment.

[0317] FIG. 18E further illustrates the example method of operation of the executing the sale of the contingent asset for conversion into the instant asset at the point of purchase, where, having obtained the payment for the purchase of the first contingent asset, a fifth step of the example method includes the computing entity 21 determining first final instant asset terms 620 for utilization of the first contingent asset as the first instant asset. The asset module 30 determines the first final instant asset terms 620 based on one or more of the first offered instant asset terms and the first preliminary instant asset terms and utilizing a terms rationalization approach. The terms rationalization approach includes, selecting one term or another, averaging terms, and ranking terms for selection of terms ranked high or low. For example, the asset module 30 determines the first final instant asset terms 620 to include exactly the terms offered by the buyer when the terms rationalization approach indicates to utilize offered terms when the offer terms are within acceptable ranges included in the first preliminary instant asset terms.

[0318] Having determined the first final instant asset terms 620, a sixth step of the example method of operation of the executing the sale of the contingent asset for conversion into the instant asset at the point of purchase includes the computing entity 21 updating first contingent asset blockchain encoded record 300 to indicate reassignment of the potential first liability of the first contingent asset from the first consumer to an entity associated with the first buyer of the first contingent asset purchase request and to indicate availability for the subsequent utilization of the first contingent asset as the first instant asset by the first consumer in accordance with the first final instant asset terms 620 as illustrated in FIG. 18F. For example, the asset module 30 modifies the content and security aspects of the first contingent asset blockchain record 300 as discussed with reference to FIG. 9K. In an example, the entity associated with the first buyer is the first computing entity 23-1. In another example, the entity associated with the first buyer is the computing entity 21 when the exchange is to purchase the first contingent asset for conversion to the instant access.

[0319] The method described above in conjunction with a processing module of any computing entity of the computing system 10 can alternatively be performed by other modules of the computing system 10 of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system 10, cause one or more computing devices of the computing system 10 to perform any or all of the method steps described above.

[0320] FIGS. 18G-18H are schematic block diagrams of an embodiment of a computing system illustrating an example of securely converting a contingent asset into an instant asset at a point of purchase. The computing system includes computing entities 20-1 through 20-N of FIG. 1, the

computing entity 21 of FIG. 1, computing entities 23-1 through 23-N of FIG. 1, and the computing entity 25-1 of FIG. 1. In an embodiment, the computing entities 20-1 through 20-N are associated with a multitude of consumers in a point of purchase scenario.

[0321] FIG. 18G illustrates an example method of operation of the securely converting the contingent asset into the instant asset at the point of purchase, where a first step includes the computing entity 21 generating a secure first token 802 in accordance with a securely passing process to represent utilization of a selected contingent asset for a first pending transaction associated with a transaction item. For example, the asset module 30 of the computing entity 21, in response to point of purchase information 804 from the computing entity 20-1 (e.g., in an example where the computing entity 20-1 is utilized by a first consumer performing a point of purchase of the transaction item within the first pending transaction), wraps a contingent asset (e.g., a rebate offered by a payer associated with the computing entity 25-1) into a block of a blockchain, stored, from time to time, as blockchain information 800 in the contingent asset database 34, as discussed with reference to FIG. 9K. In an embodiment, block of the blockchain is securely stored in an object distributed ledger maintained by one or more of the computing entities 23-1 through 23-N as illustrated in FIG. 18G as block 1.

[0322] The point of purchase information 804 includes one or more of a first pending transaction identifier, a secure first token identifier, a selected contingent asset identifier, identity of the computing entity 20-1 (e.g., a requesting computing entity), and an identity of the transaction item. The selection and generation of the contingent asset is discussed in greater detail with reference to FIGS. 17A-17F.

[0323] Having generated the secure first token, either currently as described above or previously and placed on the blockchain, a second step of the example method of operation includes the computing entity 21 obtaining, in accordance with a securely passing process, control over the secure first token 802 representing a first pending transaction associated with the transaction item. The secure first token 802 includes a set of smart contracts of the first pending transaction (e.g., rebate terms between parties as previously discussed). The set of smart contracts pertains to a selected contingent asset of a set of candidate contingent assets for the first pending transaction. The secure first pending transaction includes identity of the transaction item, identity of a requesting computing entity, identity of the computing entity, and an authenticated value of the transaction item. The selected contingent asset assigns a potential first liability of a first payer identifier (ID) to a first owner ID associated with the selected contingent asset. Only a device possessing control over the secure first token may modify the secure first token.

[0324] The obtaining, in accordance with the securely passing process, the control over the secure first token includes a series of sub-steps. A first sub-step includes receiving an indication of the control over the secure first token from the requesting computing entity. For example, the computing entity 21 receives the secure first token 802 from the computing entity 23-1 with an indication that the computing entity 21 is to take control of the secure first token. A second sub-step includes establishing the identity of the computing entity to have control over the secure first token. For example, the computing entity 21 notifies the

computing entity 23-1 to establish the control with computing entity 21 as discussed in greater detail with reference to FIG. 9K.

[0325] FIG. 18H further illustrates the example method of operation of the securely converting the contingent asset into the instant asset at the point of purchase, where, having obtained control over the secure first token, a third step of the example method includes the computing entity 21 obtaining, in accordance with an instant asset selection approach, a selection of a first instant asset of a set of candidate instant assets that may be utilized to subsequently provide conversion of the selected contingent asset to complete the first pending transaction. At least one candidate instant asset of the set of candidate instant assets pertains to satisfying a portion of another liability associated with a delinquently paying consumer to the first payer ID (e.g., the purchaser has an option to donate a portion of rebate value associated with the contingent asset to an anonymous person that is behind in paying their electric bill when the first payer ID is the electric company).

[0326] The instant asset selection approach includes a user selection and a rank evaluation. The user selection allows the purchaser to select from a series of alternatives to convert the contingent asset to an instant asset. Examples of the set of candidate instant assets includes an instant rebate now, a gift card, an extended warranty from a manufacturer associated with the transaction item, affinity points with a retail chain associated with the purchase or with the manufacturer of the transaction item, a donation to one or more individuals or entities (e.g., the anonymous person behind in paying their electric bill), and a combination of any selections.

[0327] The obtaining the selection of the first instant asset of the set of candidate instant assets includes a series of sub-steps for the selection approach scenarios of the user selection and the rank evaluation. When the instant asset selection approach includes the user selection, a first sub-step includes ranking an estimated benefit to an entity associated with the identity of the requesting computing entity for each candidate instant asset of the set of candidate instant assets to produce an estimated benefit ranking. For example, the asset module 30 of the computing entity 21 identifies the set of candidate instant assets (e.g., a list, receive, determine for the purchaser, etc.) and evaluates upside for the purchaser for each of the candidate instant assets.

[0328] A second sub-step includes identifying the at least one candidate instant asset of the set of candidate instant assets that pertains to satisfying a portion of another liability associate with a delinquently paying consumer to the first payer ID. For example, the asset module 30 of the computing entity 21 obtains candidate instant asset 806 that includes a list of consumers that are behind in paying their electric bill from the computing entity 25-1.

[0329] A third sub-step includes obtaining the user selection of the first instant asset in response to at least one of the estimated benefit ranking and the identifying of the at least one candidate instant asset of the set of candidate instant assets that pertains to satisfying the portion of another liability associated with the delinquently paying consumer to the first payer ID to produce the selection of the first instant asset of the set of candidate instant assets. For example, the asset module 30 receives a user selection 808 that includes identification of the first instant asset.

[0330] When the instant asset selection approach includes the rank evaluation, a first sub-step includes evaluating a potential for each candidate instant asset of the set of candidate instant assets to produce a potential ranking. For example, the asset module 30 of the computing entity 21 calculates a benefit for the purchaser for each of the candidate instant assets.

[0331] A second sub-step includes selecting the first instant asset based on the potential ranking to produce the selection of the first instant asset of the set of candidate instant assets. For example, the asset module 30 selects a candidate instant asset associated with the best benefit to the purchaser.

[0332] Having selected the first instant asset, a fourth step of the example method of operation includes generating an updated secure first token 810 in accordance with the securely passing process, as discussed with reference to FIG. 9K, to represent the selection of the first instant asset to subsequently provide the conversion of the selected contingent asset to complete the first pending transaction. The generating the updated secure first token in accordance with the securely passing process to represent the selection of the first instant asset includes a series of sub-steps.

[0333] A first sub-step includes determining whether to indirectly or directly update an object distributed ledger as previously discussed (e.g., directly update the blockchain or request that the computing entity 23-1 update the blockchain). When indirectly updating the object distributed ledger, a second sub-step includes issuing a secure first token update request to an object ledger computing entity of the computing system serving as a blockchain node of the object distributed ledger. The secure first token update request includes an updated set of smart contracts of the first pending transaction based on the first instant asset. For example, the asset module 30 of the computing entity 21 issues the secure first token update request to the computing entity 23-1 that is serving as the blockchain node.

[0334] When directly updating the object distributed ledger, the second sub-step includes obtaining a copy of the object distributed ledger (e.g., the asset module 30 recovers blockchain information 800 from the contingent asset database 34). A third sub-step includes hashing the updated set of smart contracts utilizing a receiving public key of the object distributed ledger to produce a next transaction hash value. For example, the asset module 30 hashes the updated set of smart contracts utilizing a public key of the computing entity 23-1 to produce the next transaction hash value. A fourth sub-step includes encrypting the next transaction hash value utilizing a private key of the computing entity to produce a next transaction signature. For example, the asset module 30 encrypts the next transaction hash value utilizing the private key of the computing entity 21 to produce the next transaction signature. A fifth sub-step includes generating a next block of a blockchain of the object distributed ledger to include the updated set of smart contracts and the next transaction signature. For example, the asset module 30 generates the updated secure first token 810 to include the updated set of smart contracts and the next transaction signature. A sixth sub-step includes causing inclusion of the next block as the updated secure first token in the object distributed ledger. For example, the asset module 30 updates the blockchain as discussed with reference to FIG. 9K to include the updated secure token 810 represented in FIG. 18H as block 1-1.

[0335] Having generated the updated secure first token, a fifth step of the example method of operation includes securely passing control over the updated secure first token via the object distributed ledger when the secure first token is processed to complete the first pending transaction.

[0336] For example, the asset module 30 modifies the content and security aspects of updated secure first token 810 as discussed with reference to FIG. 9K. The method described above in conjunction with a processing module of any computing entity of the computing system 10 can alternatively be performed by other modules of the computing system 10 of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system 10, cause one or more computing devices of the computing system 10 to perform any or all of the method steps described above.

[0337] FIGS. 19A-19D are schematic block diagrams of another embodiment of a computing system and a contingent asset risk chart illustrating an example of utilizing a contingent asset for conversion into an instant asset at a point of purchase. The computing system includes computing entities 20-1 through 20-N of FIG. 1, the computing entity 21 of FIG. 1, computing entities 23-1 through 23-N of FIG. 1, and the computing entity 25-1 of FIG. 1. In an embodiment, the computing entities 20-1 through 20-N are associated with a multitude of consumers in a point of purchase scenario.

[0338] FIG. 19A illustrates an example method of operation of the utilizing the contingent asset for conversion into the instant asset at the point of purchase, where a first step includes the computing entity 21 validating a first contingent asset blockchain encoded record 300 for utilization of a first contingent asset as a first instant asset to support a first purchase adjustment request of a multitude of purchase adjustment requests with regards to a first pending purchase transaction associated with a first consumer of a multitude of consumers. A first payer of a multitude of payers is associated with at least one component of the first pending purchase transaction. The first contingent asset assigns a potential first liability of the first payer to an owner entity currently associated with the first contingent asset. At least a portion of the potential first liability is to be paid by the first payer to the owner entity in accordance with contingency information of the first contingent asset and subsequent to completion of a first asset lifecycle of the first contingent asset as illustrated with regards to FIG. 19B. First final instant asset terms 620 of the first contingent asset blockchain encoded record 300 specify the subsequent utilization of the first contingent asset as the first instant asset to support the first pending purchase transaction.

[0339] The validating of the first contingent asset blockchain encoded record 300 includes the asset module 30 validating security aspects of the blockchain itself as discussed with FIG. 9K. The validating further includes verifying that the owner entity owns the first contingent asset (e.g., validating an ownership portion of the first contingent asset blockchain encoded record 300). The validating further

includes verifying that the first final instant asset terms comply with an instant asset utilization approach (e.g., terms are within acceptable ranges for all parties).

[0340] Having determined the first final instant asset terms **620**, a second step of the example method of operation of the utilizing the contingent asset for conversion into the instant asset at the point of purchase includes the computing entity **21** updating the first final instant asset terms based on the first final instant asset terms **620** and an instant asset utilization approach as illustrated in FIG. 19B. For example, the asset module **30** queries the first consumer to obtain any final allowed changes to the first final instant asset terms. As another example, the asset module **30** applies a final application of the instant asset to a discount and/or one or more payments of the terms.

[0341] FIG. 19C further illustrates the example method of operation of the utilizing the contingent asset for conversion into the instant asset at the point of purchase, where, having updated the first final instant asset terms **620**, a third step of the example method includes the computing entity **21** updating the first contingent asset blockchain encoded record **300** with the first final instant asset terms **620** utilizing updated first final instant asset terms when the updated first final instant asset terms are different than the first final instant asset terms as illustrated in FIG. 19D. For example, the asset module **30** extracts terms content from the first contingent asset blockchain encoded record **300**, modifies the content in accordance with the updated first final instant asset terms, and recalculates security aspects of the blockchain to update the first contingent asset blockchain record **300**.

[0342] Having updated the first contingent asset blockchain record **300**, a second step of the example method of operation of the utilizing the contingent asset for conversion into the instant asset at the point of purchase includes the computing entity **21** facilitating completion of the first pending purchase transaction utilizing the first instant asset of the first contingent asset blockchain encoded record. The first pending purchase transaction is executed in accordance with the first final instant asset terms. The facilitating completion of the first pending purchase transaction includes exchanging transaction completion message **640** with the computing entity **20-1** associated with the first purchaser. For example, the asset module **30** applies a discount to the pending purchase transaction when a discount is included in the first final instant asset terms and sends an associated transaction completion message **640** to the computing entity **20-1**. As another example, the asset module **30** establishes a payment plan that includes payments and payment dates associated with the payments in accordance with the first final instant asset terms and issues a corresponding transaction completion message **640** to the computing entity **20-1**.

[0343] The method described above in conjunction with a processing module of any computing entity of the computing system **10** can alternatively be performed by other modules of the computing system **10** of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system **10**, cause one or more

computing devices of the computing system **10** to perform any or all of the method steps described above.

[0344] FIGS. 19E-19F are schematic block diagrams of an embodiment of a computing system illustrating an example of updating a secure token of a contingent asset in accordance with the present invention. The computing system includes computing entities **20-1** through **20-N** of FIG. 1, the computing entity **21** of FIG. 1, computing entities **23-1** through **23-N** of FIG. 1, and the computing entity **25-1** of FIG. 1. In an embodiment, the computing entities **20-1** through **20-N** are associated with a multitude of consumers in a point of purchase scenario.

[0345] FIG. 19E illustrates an example method of operation of the updating the secure token of the contingent asset, where a first step includes the computing entity **21** generating a secure first token **802** in accordance with a securely passing process to represent utilization of a selected contingent asset for a first pending transaction associated with a transaction item. For example, the asset module **30** of the computing entity **21**, in response to point of purchase information **804** from the computing entity **20-1** (e.g., in an example where the computing entity **20-1** is utilized by a first consumer performing a point of purchase of the transaction item within the first pending transaction), wraps a contingent asset (e.g., a rebate offered by a payer associated with the computing entity **25-1**) into a block of a blockchain, stored, from time to time, as blockchain information **800** in the contingent asset database **34**, as discussed with reference to FIG. 9K. In an embodiment, a block of the blockchain is securely stored in an object distributed ledger maintained by one or more of the computing entities **23-1** through **23-N** as illustrated in FIG. 19E as block **1**.

[0346] The point of purchase information **804** includes one or more of a first pending transaction identifier, a secure first token identifier, a selected contingent asset identifier, identity of the computing entity **20-1** (e.g., a requesting computing entity), and an identity of the transaction item. The selection and generation of the contingent asset is discussed in greater detail with reference to FIGS. 17A-17F.

[0347] Having generated the secure first token, either currently as described above or previously and placed on the blockchain, a second step of the example method of operation includes the computing entity **21** obtaining, in accordance with a securely passing process, control over the secure first token **802** representing a first pending transaction associated with the transaction item. The secure first token **802** includes a set of smart contracts of the first pending transaction (e.g., rebate terms between parties as previously discussed). The set of smart contracts pertains to a selected contingent asset of a set of candidate contingent assets for the first pending transaction. The secure first pending transaction includes identity of the transaction item, identity of a requesting computing entity, identity of the computing entity, and an authenticated value of the transaction item. The selected contingent asset assigns a potential first liability of a first payer identifier (ID) to a first owner ID associated with the selected contingent asset. Only a device possessing control over the secure first token may modify the secure first token.

[0348] The obtaining, in accordance with the securely passing process, the control over the secure first token includes a series of sub-steps. A first sub-step includes receiving an indication of the control over the secure first token from the requesting computing entity. For example,

the computing entity **21** receives the secure first token **802** from the computing entity **23-1** with an indication that the computing entity **21** is to take control of the secure first token. A second sub-step includes establishing the identity of the computing entity to have control over the secure first token. For example, the computing entity **21** notifies the computing entity **23-1** to establish the control with computing entity **21** as discussed in greater detail with reference to FIG. 9K.

[0349] FIG. 19F further illustrates the example method of operation of the updating the secure token of the contingent asset, where, having obtained control over the secure first token, a third step of the example method includes the computing entity **21** determining, in accordance with an instant asset determination approach, a set of candidate instant assets that may be utilized to subsequently provide conversion of the selected contingent asset to complete the first pending transaction. The determining, in accordance with the instant asset determination approach, the set of candidate instant assets that may be utilized to subsequently provide conversion of the selected contingent asset to complete the first pending transaction includes a series of sub-steps. A first sub-step includes, when the instant asset determination approach includes a ranked evaluation, identifying potential candidate instant assets based on the secure first token. The potential candidate instant assets includes one or more of an instant rebate now, a gift card, an extended warranty from a manufacturer associated with the transaction item, affinity points with a retailer associated with the pending first transaction, other affinity points with the manufacturer associated with the transaction item, a donation to one or more individuals, a donation to one or more entities, and a payment to satisfy a portion of another liability associated with a delinquent paying consumer to the first payer ID.

[0350] For example, the asset module **30** of the computing entity **21** interprets candidate instant assets **806** from the computing entity **25-1** to produce the potential candidate instant assets. As another example, the asset module **30** recovers contingency information **202** from the contingent asset database **34** to produce the potential candidate instant assets. As yet another example, the asset module **30** identifies candidate instant assets associated with the identifier of the requesting entity (e.g., affinity programs for the consumer at the point of sale).

[0351] A second sub-step includes ranking an estimated benefit to an entity associated with the identity of the requesting computing entity for each potential candidate instant asset of the potential candidate instant assets to produce an estimated benefit ranking of a set of estimated benefit rankings. For example, the asset module **30** produces estimated benefits for each of the potential candidate instant assets as associated with the consumer and rank orders the estimated benefits to produce the set of estimated benefit rankings.

[0352] A third sub-step includes selecting the set of candidate instant assets of the potential candidate instant assets based on the estimated benefit ranking of the set of estimated benefit rankings. For example, the asset module **30** identifies potential candidate instant assets that are ranked the highest (e.g., most beneficial to the consumer) to produce the set of candidate instant assets.

[0353] Having determined the set of candidate instant assets, a fourth step of the example method of operation

includes obtaining, in accordance with an instant asset selection approach, a selection of a first subset of instant assets of the set of candidate instant assets to be utilized to subsequently provide the conversion of the selected contingent asset to complete the first pending transaction. For example, the asset module **30** of the computing entity **21** selects the subset of instant assets that are potentially the most beneficial to the consumer. As another example, the asset module **30** interprets user selection **808** to identify the subset of instant assets as selected by the consumer.

[0354] Having selected the first subset of instant assets of the set of candidate instant assets, a fifth step of the example method of operation includes generating an updated secure first token **810** in accordance with the securely passing process, as discussed with reference to FIG. 9K, to represent the selection of the first subset of instant assets to subsequently provide the conversion of the selected contingent asset to complete the first pending transaction. The generating the updated secure first token in accordance with the securely passing process to represent the selection of the first subset of instant assets includes a series of sub-steps.

[0355] A first sub-step includes determining whether to indirectly or directly update an object distributed ledger as previously discussed (e.g., directly update the blockchain or request that the computing entity **23-1** update the blockchain). When indirectly updating the object distributed ledger, a second sub-step includes issuing a secure first token update request to an object ledger computing entity of the computing system serving as a blockchain node of the object distributed ledger. The secure first token update request includes an updated set of smart contracts of the first pending transaction based on the first subset of instant assets. For example, the asset module **30** of the computing entity **21** issues an updated secure first token **810** as the secure first token update request to the computing entity **23-1** that is serving as the blockchain node.

[0356] When directly updating the object distributed ledger, the second sub-step includes obtaining a copy of the object distributed ledger (e.g., the asset module **30** recovers blockchain information **800** from the contingent asset database **34**). A third sub-step includes hashing the updated set of smart contracts utilizing a receiving public key of the object distributed ledger to produce a next transaction hash value. For example, the asset module **30** hashes the updated set of smart contracts utilizing a public key of the computing entity **23-1** to produce the next transaction hash value. A fourth sub-step includes encrypting the next transaction hash value utilizing a private key of the computing entity **21** to produce a next transaction signature. For example, the asset module **30** encrypts the next transaction hash value utilizing the private key of the computing entity **21** to produce the next transaction signature.

[0357] A fifth sub-step includes generating a next block of a blockchain of the object distributed ledger to include the updated set of smart contracts and the next transaction signature. For example, the asset module **30** generates the updated secure first token **810** to include the updated set of smart contracts and the next transaction signature. A sixth sub-step includes causing inclusion of the next block as the updated secure first token in the object distributed ledger. For example, the asset module **30** updates the blockchain as discussed with reference to FIG. 9K to include the updated secure token **810** represented in FIG. 19F as block **1-1**.

[0358] Having generated the updated secure first token, a sixth step of the example method of operation includes securely passing control over the updated secure first token via the object distributed ledger when the secure first token is processed to complete the first pending transaction.

[0359] For example, the asset module 30 modifies the content and security aspects of updated secure first token 810 as discussed with reference to FIG. 9K.

[0360] The method described above in conjunction with a processing module of any computing entity of the computing system 10 can alternatively be performed by other modules of the computing system 10 of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system 10, cause one or more computing devices of the computing system 10 to perform any or all of the method steps described above.

[0361] FIGS. 20A-20B are schematic block diagrams of an embodiment of a computing system illustrating an example of updating a secure token of a carbon credit asset. The computing system includes computing entities 20-1 through 20-N of FIG. 1, the computing entity 21 of FIG. 1, computing entities 23-1 through 23-N of FIG. 1, and the computing entity 25-1 of FIG. 1. In an embodiment, the computing entities 20-1 through 20-N are associated with a multitude of consumers in a point of purchase scenario.

[0362] The carbon credit asset represents a tradable certificate or permit representing the right to emit a set amount of carbon dioxide or the equivalent amount of a different greenhouse gas (GHG). Carbon credits and carbon markets are a component of national and international attempts to mitigate the growth in concentrations of GHGs. 1 carbon credit=1 ton of carbon dioxide or carbon dioxide equivalent gases.

[0363] FIG. 20A illustrates an example method of operation of the updating the secure token of the carbon credit asset, where a first step includes the computing entity 21 generating a secure first token 802 in accordance with a securely passing process to represent utilization of a selected carbon credit asset for a first pending transaction associated with a transaction item. The generating the secure first token includes a series of sub-steps.

[0364] A first sub-step includes determining a first credit level of the selected carbon credit based on the identity of a transaction item. For example, the computing entity 21 determines the first credit level (e.g., energy savings) for an appliance when the appliance is the transaction item (e.g., interpret a query response, perform a lookup, etc.). As another example, the computing entity 21 determines the first credit level for a banked carbon credit (e.g., acquired previously and saved) and/or a new carbon credit based on the transaction item.

[0365] A second sub-step includes generating the selected carbon credit asset to assign the first credit level of from the first payer ID to the first owner ID associated with the selected carbon credit asset. For example, the computing entity 21 exchanges asset establishment messages 602 with computing entity 25-1 to obtain approval and issuance of the

carbon credit for the first credit level from the first payer ID (e.g., an entity desiring to pay for the energy efficiency) to the first owner ID (e.g., an entity performing the transaction) when the computing entity 25-1 is associated with issuing and/or exchanging digital representations of carbon credits.

[0366] A third sub-step includes generating the secure token itself. For example, the asset module 30 of the computing entity 21, in response to point of purchase information 804 from the computing entity 20-1 (e.g., in an example where the computing entity 20-1 is utilized by a first consumer performing a point of purchase of the transaction item within the first pending transaction), wraps the carbon credit asset into a block of a blockchain, stored, from time to time, as blockchain information 800 in the contingent asset database 34, as discussed with reference to FIG. 9K. In an embodiment, a block of the blockchain is securely stored in an object distributed ledger maintained by one or more of the computing entities 23-1 through 23-N as illustrated in FIG. 20A as block 1.

[0367] The point of purchase information 804 includes one or more of a first pending transaction identifier, a secure first token identifier, a selected carbon credit asset identifier, identity of the computing entity 20-1 (e.g., a requesting computing entity), and an identity of the transaction item.

[0368] Having generated the secure first token, either currently as described above or previously and placed on the blockchain, a second step of the example method of operation includes the computing entity 21 obtaining, in accordance with a securely passing process, control over the secure first token 802 representing a first pending transaction associated with the transaction item. The secure first token 802 includes a set of smart contracts of the first pending transaction. The set of smart contracts pertains to the selected carbon credit asset of a set of candidate contingent assets (e.g., amongst rebates and other carbon credits not affiliated with the transaction item, etc.) for the first pending transaction. The secure first pending transaction includes identity of the transaction item, identity of a requesting computing entity, identity of the computing entity, and an authenticated value of the transaction item. The selected carbon credit asset assigns the first credit level of the first payer identifier (ID) to a first owner ID associated with the selected carbon credit asset. Only a device possessing control over the secure first token may modify the secure first token.

[0369] The obtaining, in accordance with the securely passing process, the control over the secure first token includes a series of sub-steps. A first sub-step includes receiving an indication of the control over the secure first token from the requesting computing entity. For example, the computing entity 21 receives the secure first token 802 from the computing entity 23-1 with an indication that the computing entity 21 is to take control of the secure first token. A second sub-step includes establishing the identity of the computing entity to have control over the secure first token. For example, the computing entity 21 notifies the computing entity 23-1 to establish the control with computing entity 21 as discussed in greater detail with reference to FIG. 9K.

[0370] FIG. 20B further illustrates the example method of operation of the updating the secure token of the carbon credit asset, where, having obtained control over the secure first token, a third step of the example method includes the computing entity 21 determining, in accordance with an

instant asset determination approach, a set of candidate instant assets that may be utilized to subsequently provide conversion of the selected carbon credit asset to complete the first pending transaction. The determining, in accordance with the instant asset determination approach, the set of candidate instant assets that may be utilized to subsequently provide conversion of the selected carbon credit asset to complete the first pending transaction includes a series of sub-steps. A first sub-step includes, when the instant asset determination approach includes a ranked evaluation, identifying potential candidate instant assets based on the secure first token. The potential candidate instant assets includes one or more of an instant rebate now, a gift card, an extended warranty from a manufacturer associated with the transaction item, affinity points with a retailer associated with the pending first transaction, other affinity points with the manufacturer associated with the transaction item, a donation to one or more individuals, a donation to one or more entities, a lottery ticket, and a payment to satisfy a portion of another liability associated with a delinquent paying consumer to the first payer ID.

[0371] For example, the asset module 30 of the computing entity 21 interprets candidate instant assets 806 from the computing entity 25-1 to produce the potential candidate instant assets. As another example, the asset module 30 recovers contingency information 202 from the contingent asset database 34 to produce the potential candidate instant assets. As yet another example, the asset module 30 identifies candidate instant assets associated with the identifier of the requesting entity (e.g., affinity programs for the consumer at the point of sale).

[0372] A second sub-step includes ranking an estimated benefit to an entity associated with the identity of the requesting computing entity for each potential candidate instant asset of the potential candidate instant assets to produce an estimated benefit ranking of a set of estimated benefit rankings. For example, the asset module 30 produces estimated benefits for each of the potential candidate instant assets as associated with the consumer and rank orders the estimated benefits to produce the set of estimated benefit rankings.

[0373] A third sub-step includes selecting the set of candidate instant assets of the potential candidate instant assets based on the estimated benefit ranking of the set of estimated benefit rankings. For example, the asset module 30 identifies potential candidate instant assets that are ranked the highest (e.g., most beneficial to the consumer) to produce the set of candidate instant assets.

[0374] Having determined the set of candidate instant assets, a fourth step of the example method of operation includes obtaining, in accordance with an instant asset selection approach, a selection of a first subset of instant assets of the set of candidate instant assets to be utilized to subsequently provide the conversion of the selected carbon credit asset to complete the first pending transaction. For example, the asset module 30 of the computing entity 21 selects the subset of instant assets that are potentially the most beneficial to the consumer. As another example, the asset module 30 interprets user selection 808 to identify the subset of instant assets as selected by the consumer.

[0375] Having selected the first subset of instant assets of the set of candidate instant assets, a fifth step of the example method of operation includes generating an updated secure first token 810 in accordance with the securely passing

process, as discussed with reference to FIG. 9K, to represent the selection of the first subset of instant assets to subsequently provide the conversion of the selected carbon credit asset to complete the first pending transaction. The generating the updated secure first token in accordance with the securely passing process to represent the selection of the first subset of instant assets includes a series of sub-steps.

[0376] A first sub-step includes determining whether to indirectly or directly update an object distributed ledger as previously discussed (e.g., directly update the blockchain or request that the computing entity 23-1 update the blockchain). When indirectly updating the object distributed ledger, a second sub-step includes issuing a secure first token update request to an object ledger computing entity of the computing system serving as a blockchain node of the object distributed ledger. The secure first token update request includes an updated set of smart contracts of the first pending transaction based on the first subset of instant assets. For example, the asset module 30 of the computing entity 21 issues an updated secure first token 810 as the secure first token update request to the computing entity 23-1 that is serving as the blockchain node.

[0377] When directly updating the object distributed ledger, the second sub-step includes obtaining a copy of the object distributed ledger (e.g., the asset module 30 recovers blockchain information 800 from the contingent asset database 34). A third sub-step includes hashing the updated set of smart contracts utilizing a receiving public key of the object distributed ledger to produce a next transaction hash value. For example, the asset module 30 hashes the updated set of smart contracts utilizing a public key of the computing entity 23-1 to produce the next transaction hash value. A fourth sub-step includes encrypting the next transaction hash value utilizing a private key of the computing entity 21 to produce a next transaction signature. For example, the asset module 30 encrypts the next transaction hash value utilizing the private key of the computing entity 21 to produce the next transaction signature.

[0378] A fifth sub-step includes generating a next block of a blockchain of the object distributed ledger to include the updated set of smart contracts and the next transaction signature. For example, the asset module 30 generates the updated secure first token 810 to include the updated set of smart contracts and the next transaction signature. A sixth sub-step includes causing inclusion of the next block as the updated secure first token in the object distributed ledger. For example, the asset module 30 updates the blockchain as discussed with reference to FIG. 9K to include the updated secure token 810 represented in FIG. 20B as block 1-1.

[0379] Having generated the updated secure first token, a sixth step of the example method of operation includes securely passing control over the updated secure first token via the object distributed ledger when the secure first token is processed to complete the first pending transaction.

[0380] For example, the asset module 30 modifies the content and security aspects of updated secure first token 810 as discussed with reference to FIG. 9K.

[0381] The method described above in conjunction with a processing module of any computing entity of the computing system 10 can alternatively be performed by other modules of the computing system 10 of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory

organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system 10, cause one or more computing devices of the computing system 10 to perform any or all of the method steps described above.

[0382] FIGS. 21A-21B are schematic block diagrams of an embodiment of a computing system illustrating an example of updating a secure token of a set of public benefit credit assets. The computing system includes computing entities 20-1 through 20-N of FIG. 1, the computing entity 21 of FIG. 1, computing entities 23-1 through 23-N of FIG. 1, and the computing entity 25-1 of FIG. 1. In an embodiment, the computing entities 20-1 through 20-N are associated with a multitude of consumers in a point of purchase scenario.

[0383] The set of public benefit credit assets represents a set of tradable certificates or permits representing the right to continue to do deeds of negative factors in one area but yet be offset by facilitating abatement in another area. For example, when the public benefit credit is associated with a carbon credit, the public benefit credit asset represents the right to emit a set amount of carbon dioxide or the equivalent amount of a different greenhouse gas (GHG). Carbon credits and carbon markets are a component of national and international attempts to mitigate the growth in concentrations of GHGs. 1 carbon credit=1 ton of carbon dioxide or carbon dioxide equivalent gases. The set of carbon credit assets includes micro-carbon credits (e.g., household) and/or a portion of one or more of voluntary carbon credits and certified carbon credits (e.g., vetted through a registration entity and process).

[0384] FIG. 21A illustrates an example method of operation of the updating the secure token of the set of public benefit credit assets, where a first step includes the computing entity 21 generating a secure first token 802 in accordance with a securely passing process to represent utilization of the set of public benefit credit assets for a first pending transaction associated with a transaction item. The generating of the secure first token includes a series of sub-steps.

[0385] A first sub-step includes determining a first credit level of the set of public benefit credit assets based on the identity of the transaction item. For example, the computing entity 21 determines the first credit level (e.g., energy savings) for an appliance when the appliance is the transaction item (e.g., interpret a query response, perform a lookup, etc.) and the set of public benefit credit assets (e.g., carbon credits) shall include a micro carbon credit due to the appliance when the public benefit credit includes a micro carbon credit category. As another example, the computing entity 21 determines the first credit level for a banked carbon credit (e.g., acquired previously and saved for numerous micro carbon credits) and/or a new carbon credit based on the transaction item.

[0386] A second sub-step includes generating the set of public benefit credit assets to assign a first credit level of from a first payer identifier (ID) to a first owner ID associated with the set of public benefit credit assets. For example, the computing entity 21 exchanges public benefit credit establishment messages 603 with computing entity 25-1 to obtain approval and issuance of micro carbon credits as part of the environment information 609 of ESG information 607

stored within a memory module 102 of the computing entity 25-1. A first credit level is established by the environment information 609 from the first payer ID (e.g., an entity desiring to pay for the energy efficiency) to the first owner ID (e.g., an entity performing the transaction) when the computing entity 25-1 is associated with issuing and/or exchanging digital representations of carbon credits (e.g., a vetting agency). Another embodiment includes trading in abatements associated with social factors as part of social information 611. A yet another embodiment includes trading in abatements associated with governance factors as part of governance information 613.

[0387] A third sub-step includes generating the secure first token 802 in accordance with a securely passing process to represent utilization of the set of selected public benefit credit assets for the first pending transaction associated with the transaction item. For example, the asset module 30 of the computing entity 21, in response to point of purchase information 804 from the computing entity 20-1 (e.g., in an example where the computing entity 20-1 is utilized by a first consumer performing a point of purchase of the transaction item within the first pending transaction), wraps the public benefit credit asset into a block of a blockchain, stores, from time to time, as blockchain information 800 in the contingent asset database 34, as discussed with reference to FIG. 9K. In an embodiment, a block of the blockchain is securely stored in an object distributed ledger maintained by one or more of the computing entities 23-1 through 23-N as illustrated in FIG. 21A as block 1 (secure first token 802).

[0388] The point of purchase information 804 includes one or more of a first pending transaction identifier, a secure first token identifier, a set of public benefit credit asset identifiers, identity of the computing entity 20-1 (e.g., a requesting computing entity), and an identity of the transaction item. In an embodiment, the point of purchase information 804 further includes an authenticated value of the transaction item (e.g., a hash over the value is verified).

[0389] Having generated the secure first token, either currently as described above or previously and placed on the blockchain, a second step of the example method of operation includes the computing entity 21 obtaining, in accordance with a securely passing process, control over the secure first token 802 representing the first pending transaction associated with the transaction item. The secure first token 802 includes a set of smart contracts of the first pending transaction. The set of smart contracts pertains to the set of public benefit credit assets (e.g., amongst rebates and other public benefit credits not affiliated with the transaction item, etc.) for the first pending transaction. The secure first pending transaction includes identity of the transaction item, identity of a requesting computing entity, identity of the computing entity 21, and the authenticated value of the transaction item. A particular public benefit credit asset of the set of selected public benefit credit assets assigns a corresponding credit level from a corresponding payer identifier (ID) to a corresponding owner ID associated with the particular public benefit credit asset. Only a device possessing control over the secure first token may modify the secure first token.

[0390] The obtaining, in accordance with the securely passing process, the control over the secure first token includes a series of sub-steps. A first sub-step includes receiving an indication of the control over the secure first token from the requesting computing entity. For example,

the computing entity **21** receives the secure first token **802** from the computing entity **23-1** with an indication that the computing entity **21** is to take control of the secure first token. A second sub-step includes establishing the identity of the computing entity to have control over the secure first token. For example, the computing entity **21** notifies the computing entity **23-1** to establish the control with computing entity **21** as discussed in greater detail with reference to FIG. 9K.

**[0391]** FIG. 21B further illustrates the example method of operation of the updating the secure token of the public benefit credit asset, where, having obtained control over the secure first token, a third step of the example method includes the computing entity **21** determining, in accordance with an instant asset determination approach, a set of candidate instant assets that may be utilized to subsequently provide conversion of the set of public benefit credit assets to complete the first pending transaction. The determining, in accordance with the instant asset determination approach, the set of candidate instant assets that may be utilized to subsequently provide conversion of the set of public benefit credit assets to complete the first pending transaction includes a series of sub-steps. A first sub-step includes, when the instant asset determination approach includes a ranked evaluation, identifying potential candidate instant assets based on the secure first token. The potential candidate instant assets includes one or more of an instant rebate now, a gift card, an extended warranty from a manufacturer associated with the transaction item, affinity points with a retailer associated with the pending first transaction, other affinity points with the manufacturer associated with the transaction item, a donation to one or more individuals, a donation to one or more entities, a lottery ticket, and a payment to satisfy a portion of another liability associated with a delinquent paying consumer to the first payer ID.

**[0392]** For example, the asset module **30** of the computing entity **21** interprets candidate instant assets **806** from the memory module **102** of the computing entity **25-1** to produce the potential candidate instant assets from ESG information **607** (e.g., public benefit credits associated with one or more of the environment information **609**, the social information **611**, and the governance information **613**). As another example, the asset module **30** recovers contingency information **202** from the contingent asset database **34** to produce the potential candidate instant assets. As yet another example, the asset module **30** identifies candidate instant assets associated with the identifier of the requesting entity (e.g., affinity programs for the consumer at the point of sale).

**[0393]** A second sub-step includes ranking an estimated benefit to an entity associated with the identity of the requesting computing entity for each potential candidate instant asset of the potential candidate instant assets to produce an estimated benefit ranking of a set of estimated benefit rankings. For example, the asset module **30** produces estimated benefits for each of the potential candidate instant assets as associated with the consumer and rank orders the estimated benefits to produce the set of estimated benefit rankings.

**[0394]** A third sub-step includes selecting the set of candidate instant assets of the potential candidate instant assets based on the estimated benefit ranking of the set of estimated benefit rankings. For example, the asset module **30** identifies

potential candidate instant assets that are ranked the highest (e.g., most beneficial to the consumer) to produce the set of candidate instant assets.

**[0395]** Having determined the set of candidate instant assets, a fourth step of the example method of operation includes obtaining, in accordance with an instant asset selection approach, a selection of a first subset of instant assets of the set of candidate instant assets to be utilized to subsequently provide the conversion of the set of public benefit credit assets to complete the first pending transaction. For example, the asset module **30** of the computing entity **21** selects the subset of instant assets that are potentially the most beneficial to the consumer. As another example, the asset module **30** interprets user selection **808** to identify the subset of instant assets as selected by the consumer.

**[0396]** Having selected the first subset of instant assets of the set of candidate instant assets, a fifth step of the example method of operation includes generating an updated secure first token **810** in accordance with the securely passing process, as discussed with reference to FIG. 9K, to represent the selection of the first subset of instant assets to subsequently provide the conversion of the set of public benefit credit assets to complete the first pending transaction. The generating the updated secure first token in accordance with the securely passing process to represent the selection of the first subset of instant assets includes a series of sub-steps.

**[0397]** A first sub-step includes determining whether to indirectly or directly update an object distributed ledger as previously discussed (e.g., directly update the blockchain or request that the computing entity **23-1** update the blockchain). When indirectly updating the object distributed ledger, a second sub-step includes issuing a secure first token update request to an object ledger computing entity of the computing system serving as a blockchain node of the object distributed ledger. The secure first token update request includes an updated set of smart contracts of the first pending transaction based on the first subset of instant assets. For example, the asset module **30** of the computing entity **21** issues an updated secure first token **810** as the secure first token update request to the computing entity **23-1** that is serving as the blockchain node.

**[0398]** When directly updating the object distributed ledger, the second sub-step includes obtaining a copy of the object distributed ledger (e.g., the asset module **30** recovers blockchain information **800** from the contingent asset database **34**). A third sub-step includes hashing the updated set of smart contracts utilizing a receiving public key of the object distributed ledger to produce a next transaction hash value. For example, the asset module **30** hashes the updated set of smart contracts utilizing a public key of the computing entity **23-1** to produce the next transaction hash value. A fourth sub-step includes encrypting the next transaction hash value utilizing a private key of the computing entity **21** to produce a next transaction signature. For example, the asset module **30** encrypts the next transaction hash value utilizing the private key of the computing entity **21** to produce the next transaction signature.

**[0399]** A fifth sub-step includes generating a next block of a blockchain of the object distributed ledger to include the updated set of smart contracts and the next transaction signature. For example, the asset module **30** generates the updated secure first token **810** to include the updated set of smart contracts and the next transaction signature. A sixth

sub-step includes causing inclusion of the next block as the updated secure first token in the object distributed ledger. For example, the asset module **30** updates the blockchain as discussed with reference to FIG. 9K to include the updated secure token **810** represented in FIG. 21B as block **1-1** for the updated secure first token **810**.

**[0400]** Having generated the updated secure first token, a sixth step of the example method of operation includes securely passing control over the updated secure first token via the object distributed ledger when the secure first token is processed to complete the first pending transaction. For example, the asset module **30** modifies the content and security aspects of updated secure first token **810** as discussed with reference to FIG. 9K.

**[0401]** The method described above in conjunction with a processing module of any computing entity of the computing system **10** can alternatively be performed by other modules of the computing system **10** of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system **10**, cause one or more computing devices of the computing system **10** to perform any or all of the method steps described above.

**[0402]** FIGS. 22A-22B are schematic block diagrams of an embodiment of a computing system illustrating an example of utilizing a secure token of a set of public benefit credit assets. The computing system includes computing entities **20-1** through **20-N** of FIG. 1, the computing entity **21** of FIG. 1, computing entities **23-1** through **23-N** of FIG. 1, and the computing entity **25-1** of FIG. 1. In an embodiment, the computing entities **20-1** through **20-N** are associated with a multitude of consumers in a point of purchase scenario.

**[0403]** The set of public benefit credit assets represents a set of tradable certificates or permits representing the right to continue to do deeds of negative factors in one area but yet be offset by facilitating abatement in another area. The negative factors include associations with one or more of environmental factors, social factors, and governance factors. For example, when the public benefit credit is associated with a carbon credit, the public benefit credit asset represents the right to emit a set amount of carbon dioxide or the equivalent amount of a different greenhouse gas (GHG). Carbon credits and carbon markets are a component of national and international attempts to mitigate the growth in concentrations of GHGs. 1 carbon credit=1 ton of carbon dioxide or carbon dioxide equivalent gases. The set of carbon credit assets includes micro-carbon credits (e.g., household) and/or a portion of one or more of voluntary carbon credits and certified carbon credits (e.g., vetted through a registration entity and process).

**[0404]** FIG. 22A illustrates an example method of operation of the utilizing the secure token of the set of public benefit credit assets, where a first step includes the computing entity **21** obtaining a secure first token **802** for a first pending transaction. The obtaining includes interpreting point of purchase information **804** received from the com-

puting entity **20-1** to identify a transaction item associated with the first pending transaction.

**[0405]** The obtaining further includes selecting the set of selected public benefit credit assets from a group of candidate public benefit credit assets based on the identity of the transaction item and an associated credit level of each candidate public benefit credit asset of the group of candidate public benefit credit assets. For example, the asset module **30** interprets public benefit credit establishment messages **603** from the computing entity **25-1** to identify candidate public benefit credit assets associated with the identity of the transaction item. For instance, the asset module **30** identifies environment information **609** to locate an environment public benefit credit such as a carbon credit when the identity of the transaction item is associated with machinery within improved energy efficiency level) and that have desirable associated credit levels. The asset module **30** further selects those associated candidate public benefit credit assets that have sufficient associated credit levels.

**[0406]** Having selected the set of selected public benefit credit assets, the obtaining of the secure first token further includes generating the secure first token in accordance with a securely passing process to represent utilization of the set of selected public benefit credit assets for the pending first transaction associated with the transaction item. For example, the asset module **30** of the computing entity **21** establishes a set of smart contracts that includes a portion of the point of purchase information **804** and contingency information **202** that includes a portion of the selected assets from the public benefit credit establishment message is **603**. Having established the smart contracts, the asset module **30** generates the secure first token **802** to include the set of smart contracts as previously discussed.

**[0407]** Having obtained the secure first token for the first pending transaction, a second step of the example method of operation includes obtaining, in accordance with the securely passing process, control over the secure first token representing the first pending transaction associated with the transaction item. The secure first token includes a set of smart contracts of the first pending transaction. The set of smart contracts shall pertain to the set of selected public benefit credit assets for the first pending transaction. The first pending transaction includes identity of the transaction item, identity of a requesting computing entity, identity of the computing entity, and an authenticated value of the transaction item. A particular public benefit credit asset of the set of selected public benefit credit assets assigns a corresponding credit level from a corresponding payer identifier (ID) to a corresponding owner ID associated with the particular public benefit credit asset. Only a device possessing control over the secure first token may modify the secure first token.

**[0408]** The asset module **30** of the computing entity **21** obtains and/or maintains control over the secure first token of a first pending transaction as previously discussed. For instance, the computing entity **21** sends the secure first token **802** to the computing entity **23-1** that is serving as a blockchain node associated with an object distributed ledger utilizing a blockchain. For instance, the asset module **30** of the computing entity **21** utilizes blockchain information **800** recovered from the contingent asset database **34** associated with the blockchain accessed via the computing entity **23-1**

to place the secure first token **802** on the blockchain as an object nonfungible token block **1** as depicted in FIG. 22A as previously discussed.

**[0409]** FIG. 22B further illustrates the example method of operation of the utilizing the secure token of the set of public benefit credit assets, where a third step includes the computing entity **21** determining a set of instant assets. For example, the asset module **30** of the computing entity **21** interprets candidate instant asset information **806** from the computing entity **25-1** to produce the set of instant assets. Having produced the set of instant assets, a fourth step of the example method of operation includes the asset module **30** selecting a first subset of instant assets. For instance, the asset module **30** selects the first subset of instant assets based on smart contract content of the first pending transaction (e.g., selects assets to meet a purchase price of the transaction item).

**[0410]** Having selected the first subset of instant assets, a fifth step of the example method of operation includes generating an updated secure first token **810** in accordance with the securely passing process to represent the selection of the selected public benefit credit assets to subsequently provide the conversion of the set of selected public benefit credit assets to complete the first pending transaction. For example, the asset module **30** updates the smart contract of the secure first token **802** to include the selected first subset of instant assets and generates the updated secure first token **810** to include updated smart contracts as previously discussed.

**[0411]** Having generated the updated secure first token **810**, a sixth step of the example method of operation includes the computing entity **21** passing control over the further updated secure first token to complete the first pending transaction. For example, the asset module **30** issues the updated secure first token **810** to the computing entity **23-1** to facilitate placing a block **1-1** on the object distributed ledger utilizing the blockchain information **800**. The block **1-1** includes ESG information **607** associated with the updated smart contracts (e.g., to include environment information **609** and/or social information **611**).

**[0412]** The method described above in conjunction with a processing module of any computing entity of the computing system **10** can alternatively be performed by other modules of the computing system **10** of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system **10**, cause one or more computing devices of the computing system **10** to perform any or all of the method steps described above.

**[0413]** FIGS. 23A-23B are schematic block diagrams of an embodiment of a computing system illustrating an example of generating a secure token of a set of public benefit credit assets. The computing system includes computing entities **20-1** through **20-N** of FIG. 1, the computing entity **21** of FIG. 1, computing entities **23-1** through **23-N** of FIG. 1, and the computing entity **25-1** of FIG. 1. In an

embodiment, the computing entities **20-1** through **20-N** are associated with a multitude of consumers in a point of purchase scenario.

**[0414]** The set of public benefit credit assets represents a set of tradable certificates or permits representing the right to continue to do deeds of negative factors in one area but yet be offset by facilitating abatement in another area. The negative factors include associations with one or more of environmental factors, social factors, and governance factors. For example, when the public benefit credit is associated with a carbon credit, the public benefit credit asset represents the right to emit a set amount of carbon dioxide or the equivalent amount of a different greenhouse gas (GHG). Carbon credits and carbon markets are a component of national and international attempts to mitigate the growth in concentrations of GHGs. 1 carbon credit=1 ton of carbon dioxide or carbon dioxide equivalent gases. The set of carbon credit assets includes micro-carbon credits (e.g., household) and/or a portion of one or more of voluntary carbon credits and certified carbon credits (e.g., vetted through a registration entity and process).

**[0415]** FIG. 23A illustrates an example method of operation of the generating the secure token of the set of public benefit credit assets, where a first step includes the computing entity **21** establishing a set of authenticated public benefit asset information for a set of public benefit credit assets of a set of candidate public benefit credit assets of a request to generate the set of public benefit credit assets. A particular public benefit credit asset of the set of public benefit credit assets assigns a corresponding credit level from a corresponding payer identifier (ID) to a corresponding owner ID associated with the particular public benefit credit asset. For example, the computing entity **21** interprets unauthenticated public benefit asset information **902** from the computing entity **20-1** to produce the request to generate the set of public benefit credit assets. For example, an individual makes a request to apply for environmental carbon credits associated with a set of more energy-efficient appliances being installed at a residence.

**[0416]** Having produced the request, the asset module **30** exchanges public benefit establishment message is **603** with the computing entity **25-1** to verify and validate the request (e.g., matching to categories of the ESG information **607**, and/or matching to public or private registries utilized to eliminate duplication of credits granted for similar abatements and to enter the requested assets into an associated registry). When verified and validated, the computing entity **21** produces the set of public benefit credit assets associated with the unauthenticated public benefit asset information **902**.

**[0417]** Having established the authenticated public benefit asset information, a second step of the example method of operation includes the computing entity **21** generating, in accordance with a securely passing process, a secure first token **802** representing the set of public benefit credit assets based on the set of authenticated public benefit asset information. The asset module **30** of the computing entity **21** generates the secure first token **802** to include a smart contract associated with the set of public benefit credit assets as previously discussed.

**[0418]** FIG. 23B further illustrates the example method of operation of the generating the secure token of the set of public benefit credit assets, where a third step includes the computing entity **21** establishing, in accordance with the

securely passing process, control over the secure first token representing the set of public benefit credit assets on an object distributed ledger. Only a device possessing control over the secure first token may modify the secure first token.

[0419] For example, the asset module 30 of the computing entity 21 issues the secure first token 802 to the computing entity 23-1 serving as an object node of the object distributed ledger to facilitate placing the secure first token 802 on the blockchain of the object is committed ledger as block 1 that includes a nonfungible token 1 (NFT 1) as previously discussed. For instance, the smart contract of the secure first token 802 includes the ESG information 607 associated with the set of public benefit credit assets that were selected in the request.

[0420] The method described above in conjunction with a processing module of any computing entity of the computing system 10 can alternatively be performed by other modules of the computing system 10 of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system 10, cause one or more computing devices of the computing system 10 to perform any or all of the method steps described above.

[0421] FIGS. 24A-24B are schematic block diagrams of an embodiment of a computing system illustrating an example of identifying a secure token of a set of public benefit credit assets. The computing system includes computing entities 20-1 through 20-N of FIG. 1, the computing entity 21 of FIG. 1, computing entities 23-1 through 23-N of FIG. 1, and the computing entity 25-1 of FIG. 1. In an embodiment, the computing entities 20-1 through 20-N are associated with a multitude of consumers in a point of purchase scenario.

[0422] The set of public benefit credit assets represents a set of tradable certificates or permits representing the right to continue to do deeds of negative factors in one area but yet be offset by facilitating abatement in another area. The negative factors include associations with one or more of environmental factors, social factors, and governance factors. For example, when the public benefit credit is associated with a carbon credit, the public benefit credit asset represents the right to emit a set amount of carbon dioxide or the equivalent amount of a different greenhouse gas (GHG). Carbon credits and carbon markets are a component of national and international attempts to mitigate the growth in concentrations of GHGs. 1 carbon credit=1 ton of carbon dioxide or carbon dioxide equivalent gases. The set of carbon credit assets includes micro-carbon credits (e.g., household) and/or a portion of one or more of voluntary carbon credits and certified carbon credits (e.g., vetted through a registration entity and process).

[0423] FIG. 24A illustrates an example method of operation of the identifying the secure token of the set of public benefit credit assets, where a first step includes the computing entity 21 establishing a set of required public benefit asset information 906 for subsequent acquisition of a set of candidate public benefit credit assets based on a request to acquire the set of public benefit credit assets. A particular

public benefit credit asset of the set of public benefit credit assets assigns a corresponding credit level from a corresponding payer identifier (ID) to a corresponding owner ID associated with the particular public benefit credit asset. For example, the asset module 30 of the computing entity 21 interprets a public benefit credit asset request 904 from the computing entity 20-1 with regards to acquiring the set of public benefit credit assets to produce the set of required benefit asset information (e.g., identity of the assets, parameters of the assets).

[0424] Having produced the set of required benefit asset information, the asset module 30 of the computing entity 21 exchanges public benefit credit establishment message is 603 with the computing entity 25-1 to interpret ESG information 607 to validate the set of required benefit asset information (e.g., valid asset categories, valid asset value ranges, etc.). When valid, the asset module 30 indicates that the set of required benefit asset information is valid.

[0425] Having established the set of required benefit asset information mental 6, a second step of the example method of operation includes identifying, in accordance with a securely passing process, a secure first token 802 on an object distributed ledger representing the set of public benefit credit assets based on the set of required public benefit asset information. For example, the asset module 30 of the computing entity 21 interprets the secure first token 802 received from the computing entity 23-1 that serves as a node of the object distributed ledger to access the secure first token 802 stored as one or more of a block 1 and a nonfungible token 1 (NFT 1), where, a smart contract of the secure first token 802 includes the ESG information 607 for the set of public benefit credit assets that substantially aligns with the set of required benefit asset information.

[0426] FIG. 24B further illustrates the example method of operation of the identifying the secure token of the set of public benefit credit assets, where a third step includes the computing entity 21 establishing, in accordance with the securely passing process, control over the secure first token 802 representing the set of public benefit credit assets to produce an updated secure first token 10.

[0427] Only a device possessing control over the secure first token may modify the secure first token. For example, the asset module 30 of the computing entity 21 facilitates acquisition of the set of public benefit credit assets and updates the smart contract of the secure first token 802 to produce the updated secure first token 810 to include ESG information 607 (e.g., environment information 609 associated with a group of micro-carbon credits matching the public benefit credit asset request). Having produced the updated secure first token 810 the asset module 30 of the computing entity 21 utilizes the blockchain information 800 and sends the updated secure first token 810 to the computing entity 23-1 that facilitates storage of the updated secure first token 810 as a block 1-1 on the object distributed ledger as previously discussed.

[0428] The method described above in conjunction with a processing module of any computing entity of the computing system 10 can alternatively be performed by other modules of the computing system 10 of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section,

a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system 10, cause one or more computing devices of the computing system 10 to perform any or all of the method steps described above.

[0429] FIGS. 25A-25B are schematic block diagrams of an embodiment of a computing system illustrating an example of identifying a secure token of a set of public benefit credit assets. The computing system includes computing entities 20-1 through 20-N of FIG. 1, the computing entity 21 of FIG. 1, computing entities 23-1 through 23-N of FIG. 1, and the computing entity 25-1 of FIG. 1. In an embodiment, the computing entities 20-1 through 20-N are associated with a multitude of consumers, including, in a point of purchase scenario.

[0430] The set of public benefit credit assets represents a set of tradable certificates or permits representing the right to continue to do deeds of negative factors in one area but yet be offset by facilitating abatement in another area. The negative factors include associations with one or more of environmental factors, social factors, and governance factors. For example, when the public benefit credit is associated with a carbon credit, the public benefit credit asset represents the right to emit a set amount of carbon dioxide or the equivalent amount of a different greenhouse gas (GHG). Carbon credits and carbon markets are a component of national and international attempts to mitigate the growth in concentrations of GHGs. 1 carbon credit=1 ton of carbon dioxide or carbon dioxide equivalent gases. The set of carbon credit assets includes micro-carbon credits (e.g., household) and/or a portion of one or more of voluntary carbon credits and certified carbon credits (e.g., vetted through a registration entity and process).

[0431] As a high-level point-of-purchase example, a consumer obtains a public benefit credit asset that has a type or geographic location affinity with the consumer will to bolster impact at a local level. A type includes a direct power association (e.g., purchasing a new appliance that saves energy, or adding home insulation to save heating and cooling energy) and others like helping with regards to social and diversity topics (e.g., buying from a veteran or minority-owned business, etc.). A geographic location affinity includes economic help for a business that is within a geographic proximal distance to the consumer to help the local ecosystem. For example, bolstering credit for simply buying local.

[0432] FIG. 25A illustrates an example method of operation of the identifying the secure token of the set of public benefit credit assets, where a first step includes the computing entity 21 determining selection criteria for the token utilizing one or more of a variety of approaches. The determining the selection criteria includes establishing buyer affinity information for a set of public benefit credit assets. A first approach includes identifying a buyer entity type affinity of a buyer entity (e.g., a consumer desiring to buy a public benefit asset at least temporarily) to a public benefit project type. For example, the asset module 30 interprets a public benefit credit asset request 904 from the computing entity 20-1 (e.g., from a buyer) to identify the public benefit project type (e.g., environment, social, governance).

[0433] A second approach includes extracting the selection criteria from a secure first token associated with the

buyer entity. The association with the buyer includes tokens that are presented to the buyer, buyer identified tokens, and third-party suggested tokens. For example, the asset module 30 extracts the selection criteria from a particular (e.g., secure first token) token recovered from one or more of a public benefit credit exchange, a verification server, a computing entity affiliated with a public ledger that includes a blockchain to list public benefit assets. The recovery of the token is discussed with greater detail below.

[0434] A third approach includes identifying a buyer entity geographic location affinity to the public benefit project geographic location. For example, the asset module 30 extracts buyer entity geographic location parameters from the public benefit credit asset request 904 (e.g., location within 50 miles of a city).

[0435] A fourth approach includes extracting the selection criteria from a secure second token associated with the buyer entity. For example, the asset module 30 extracts the selection criteria from another secure token as is discussed in greater detail below.

[0436] Having established the buyer affinity information (e.g., geographic location, type), a second step of the example method of operation includes the computing entity 21 identifying, in accordance with a securely passing process and based on at least one of the public benefit project type and the public benefit project geographic location of selection criteria for a set of public benefit credit assets, the secure first token on an object distributed ledger representing the set of public benefit credit assets. A particular public benefit credit asset of the set of public benefit credit assets includes a smart contract that assigns a corresponding credit level from a corresponding payer identifier (ID) to a corresponding owner ID associated with the particular public benefit credit asset.

[0437] The identifying the secure first token includes a series of sub-steps. A first sub-step includes the asset module 30 obtaining the secure first token 802 from at least one of the contingent asset database 34 the computing entity 21, recovering the secure first token 802 from the computing entity 23-1 that serves as a blockchain node, and interpreting public benefit credit establishment message is 603 from the computing entity 25-1 that includes the secure first token 802 and/or verification of authenticity of the secure first token 802. For example, the asset module 30 receives the secure first token 802 via the computing entity 23-1 from the blockchain, where the secure first token 802 includes a block that includes the ESG information 607. The ESG information 607 includes the environment information 609 in the social information 611 associated with the secure first token as previously discussed. Alternatively or in addition to, the asset module 30 applies the securely passing process, as described with reference to FIG. 9D, to validate content of the secure first token.

[0438] A second sub-step of the identifying the secure first token includes determining whether an aspect of the selection criteria for the set of public benefit credit assets matches a corresponding portion of the secure first token representing the set of public benefit credit assets. For example, the asset module 30 matches a power savings type of a purchase by the buyer to the energy type of the secure first token. As another example, the asset module 30 matches a social impact type of a purchase from a minority-owned store to the social type of the secure first token. As yet another example, the asset module 30 matches the buyer entity

geographic location affinity (e.g., 25 miles within the buyer's home) to the public benefit project geographic location of the secure first token (e.g., local business).

[0439] A third sub-step of the identifying the secure first token includes indicating selection of the secure first token when the aspect of the selection criteria for the set of public benefit credit assets matches the corresponding portion of the secure first token representing the set of public benefit credit assets. For example, the asset module 30 indicates the selection of the secure first token when the local businesses within 25 miles of the buyer's home. As another example, the asset module 30 indicates the selection of the secure first token when the green energy type of the secure first token matches the energy savings purchased type of the buyer.

[0440] FIG. 25B further illustrates the example method of operation of the identifying the secure token of the set of public benefit credit assets, where a third step includes the computing entity 21 establishing, in accordance with the securely passing process, control over the secure first token representing the set of public benefit credit assets. Only device possessing control over the secure first token may modify the secure first token. Establishing the control over the secure first token includes a series of sub-steps. A first sub-step includes determining whether to indirectly or directly update the object distributed ledger as previously discussed.

[0441] When indirectly updating the object distributed ledger, a second sub-step includes issuing a secure first token update request to an object ledger computing entity of the computing system serving as a blockchain node of the object distributed ledger. The secure first token update request includes an identifier of the computing entity establishing the control over the secure first token. For example, the asset module 30 of the computing entity 21 accesses the computing entity 23-1 with the secure first token update request that includes an ID of the computing entity 21.

[0442] Alternatively, when directly updating the object distributed ledger, a second sub-step includes obtaining a copy of the object distributed ledger. For example, the asset module 30 recovers the secure first token 802 from the contingent asset database 34 (e.g., after receiving the secure first token 802 from the computing entity 23-1). The asset module 30 hashes the identifier of the computing entity utilizing a receiving public key of the object distributed ledger to produce a next transaction hash value. For example, the asset module 30 hashes the ID of the computing entity 21 utilizing a receiving public key of the computing entity 23-1 to produce the next transaction hash value. The asset module 30 encrypts the next transaction hash value utilizing a private key of the computing entity 21 to produce a next transaction signature. The asset module 30 generates a next block of a blockchain of the object distributed ledger to include the identifier of the computing entity 21 and the next transaction signature. The asset module 30 causes inclusion of the next block as an updated secure first token in the object distributed ledger. For example, the asset module sends an updated secure first token 810 to the computing entity 23-1 to include as either a replacement for block 1 or as a block 1-1 on the blockchain.

[0443] Having established the control over the secure first token, a fourth step of the example method of operation includes generating the updated secure first token 810 in accordance with the securely passing process to represent selection of the set of public benefit credit assets. The

generating the updated secure first token includes a series of sub-steps. A first sub-step includes determining whether to indirectly or directly update the object distributed ledger as previously discussed.

[0444] A second sub-step includes, when indirectly updating the object distributed ledger, issuing a secure first token update request to an object ledger computing entity of the computing system serving as a blockchain node of the object distributed ledger a secure first token update request includes an updated smart contract to represent assignment of a corresponding credit level from a corresponding buyer identifier (ID) to a corresponding current owner ID associated with the set of public benefit credit assets. For example, the asset module 30 updates the smart contract portion of the secure first token 802 to produce the updated secure first token 810 to indicate that the present buyer is obtaining the public benefit credit asset. The asset module 30 further issues the updated secure first token 810 to the computing entity 23-1 for placement of the block 1-1 on the blockchain, where the updated secure first token 810 includes ESG information 607 including the environmental information 609 in the energy savings example as previously discussed.

[0445] Alternatively, the second sub-step includes, when directly updating the object distributed ledger, the asset module 30 obtaining a copy of the object distributed ledger (e.g., from the contingent asset database 34) and hashing the updated smart contract utilizing a receiving public key of the object distributed ledger of the computing entity 23-1) to produce the next transaction hash value. The asset module 30 encrypts the next transaction hash value utilizing the private key of the computing entity 21 to produce the next transaction signature. The asset module 30 generates the next block (e.g., 1-1) of the blockchain of the object distributed ledger to include the updated smart contract and the next transaction signature. The asset module 30 causes inclusion of the next block as the updated secure first token in the object distributed ledger. For example, the block 1-1 is linked to the block 1 on the blockchain as discussed with reference to FIG. 9D.

[0446] The method described above in conjunction with a processing module of any computing entity of the computing system 10 can alternatively be performed by other modules of the computing system 10 of FIG. 1 or by other devices. In addition, at least one memory section that is non-transitory (e.g., a non-transitory computer readable storage medium, a non-transitory computer readable memory organized into a first memory element, a second memory element, a third memory element, a fourth element section, a fifth memory element, a sixth memory element, etc.) that stores operational instructions can, when executed by one or more processing modules of the one or more computing entities of the computing system 10, cause one or more computing devices of the computing system 10 to perform any or all of the method steps described above.

[0447] It is noted that terminologies as may be used herein such as bit stream, stream, signal sequence, etc. (or their equivalents) have been used interchangeably to describe digital information whose content corresponds to any of a number of desired types (e.g., data, video, speech, text, graphics, audio, etc. any of which may generally be referred to as 'data').

[0448] As may be used herein, the terms "substantially" and "approximately" provides an industry-accepted tolerance for its corresponding term and/or relativity between

items. For some industries, an industry-accepted tolerance is less than one percent and, for other industries, the industry-accepted tolerance is 10 percent or more. Other examples of industry-accepted tolerance range from less than one percent to fifty percent. Industry-accepted tolerances correspond to, but are not limited to, component values, integrated circuit process variations, temperature variations, rise and fall times, thermal noise, dimensions, signaling errors, dropped packets, temperatures, pressures, material compositions, and/or performance metrics. Within an industry, tolerance variances of accepted tolerances may be more or less than a percentage level (e.g., dimension tolerance of less than  $\pm 1\%$ ). Some relativity between items may range from a difference of less than a percentage level to a few percent. Other relativity between items may range from a difference of a few percent to magnitude of differences.

[0449] As may also be used herein, the term(s) “configured to”, “operably coupled to”, “coupled to”, and/or “coupling” includes direct coupling between items and/or indirect coupling between items via an intervening item (e.g., an item includes, but is not limited to, a component, an element, a circuit, and/or a module) where, for an example of indirect coupling, the intervening item does not modify the information of a signal but may adjust its current level, voltage level, and/or power level. As may further be used herein, inferred coupling (i.e., where one element is coupled to another element by inference) includes direct and indirect coupling between two items in the same manner as “coupled to”.

[0450] As may even further be used herein, the term “configured to”, “operable to”, “coupled to”, or “operably coupled to” indicates that an item includes one or more of power connections, input(s), output(s), etc., to perform, when activated, one or more its corresponding functions and may further include inferred coupling to one or more other items. As may still further be used herein, the term “associated with”, includes direct and/or indirect coupling of separate items and/or one item being embedded within another item.

[0451] As may be used herein, the term “compares favorably”, indicates that a comparison between two or more items, signals, etc., provides a desired relationship. For example, when the desired relationship is that signal 1 has a greater magnitude than signal 2, a favorable comparison may be achieved when the magnitude of signal 1 is greater than that of signal 2 or when the magnitude of signal 2 is less than that of signal 1. As may be used herein, the term “compares unfavorably”, indicates that a comparison between two or more items, signals, etc., fails to provide the desired relationship.

[0452] As may be used herein, one or more claims may include, in a specific form of this generic form, the phrase “at least one of a, b, and c” or of this generic form “at least one of a, b, or c”, with more or less elements than “a”, “b”, and “c”. In either phrasing, the phrases are to be interpreted identically. In particular, “at least one of a, b, and c” is equivalent to “at least one of a, b, or c” and shall mean a, b, and/or c. As an example, it means: “a” only, “b” only, “c” only, “a” and “b”, “a” and “c”, “b” and “c”, and/or “a”, “b”, and “c”.

[0453] As may also be used herein, the terms “processing module”, “processing circuit”, “processor”, “processing circuitry”, and/or “processing unit” may be a single processing device or a plurality of processing devices. Such a process-

ing device may be a microprocessor, micro-controller, digital signal processor, microcomputer, central processing unit, field programmable gate array, programmable logic device, state machine, logic circuitry, analog circuitry, digital circuitry, and/or any device that manipulates signals (analog and/or digital) based on hard coding of the circuitry and/or operational instructions. The processing module, module, processing circuit, processing circuitry, and/or processing unit may be, or further include, memory and/or an integrated memory element, which may be a single memory device, a plurality of memory devices, and/or embedded circuitry of another processing module, module, processing circuit, processing circuitry, and/or processing unit. Such a memory device may be a read-only memory, random access memory, volatile memory, non-volatile memory, static memory, dynamic memory, flash memory, cache memory, and/or any device that stores digital information. Note that if the processing module, module, processing circuit, processing circuitry, and/or processing unit includes more than one processing device, the processing devices may be centrally located (e.g., directly coupled together via a wired and/or wireless bus structure) or may be distributedly located (e.g., cloud computing via indirect coupling via a local area network and/or a wide area network). Further note that if the processing module, module, processing circuit, processing circuitry and/or processing unit implements one or more of its functions via a state machine, analog circuitry, digital circuitry, and/or logic circuitry, the memory and/or memory element storing the corresponding operational instructions may be embedded within, or external to, the circuitry comprising the state machine, analog circuitry, digital circuitry, and/or logic circuitry. Still further note that, the memory element may store, and the processing module, module, processing circuit, processing circuitry and/or processing unit executes, hard coded and/or operational instructions corresponding to at least some of the steps and/or functions illustrated in one or more of the Figures. Such a memory device or memory element can be included in an article of manufacture.

[0454] One or more embodiments have been described above with the aid of method steps illustrating the performance of specified functions and relationships thereof. The boundaries and sequence of these functional building blocks and method steps have been arbitrarily defined herein for convenience of description. Alternate boundaries and sequences can be defined so long as the specified functions and relationships are appropriately performed. Any such alternate boundaries or sequences are thus within the scope and spirit of the claims. Further, the boundaries of these functional building blocks have been arbitrarily defined for convenience of description. Alternate boundaries could be defined as long as the certain significant functions are appropriately performed. Similarly, flow diagram blocks may also have been arbitrarily defined herein to illustrate certain significant functionality.

[0455] To the extent used, the flow diagram block boundaries and sequence could have been defined otherwise and still perform the certain significant functionality. Such alternate definitions of both functional building blocks and flow diagram blocks and sequences are thus within the scope and spirit of the claims. One of average skill in the art will also recognize that the functional building blocks, and other illustrative blocks, modules, and components herein, can be implemented as illustrated or by discrete components, appli-

cation specific integrated circuits, processors executing appropriate software and the like or any combination thereof.

[0456] In addition, a flow diagram may include a "start" and/or "continue" indication. The "start" and "continue" indications reflect that the steps presented can optionally be incorporated in or otherwise used in conjunction with one or more other routines. In addition, a flow diagram may include an "end" and/or "continue" indication. The "end" and/or "continue" indications reflect that the steps presented can end as described and shown or optionally be incorporated in or otherwise used in conjunction with one or more other routines. In this context, "start" indicates the beginning of the first step presented and may be preceded by other activities not specifically shown. Further, the "continue" indication reflects that the steps presented may be performed multiple times and/or may be succeeded by other activities not specifically shown. Further, while a flow diagram indicates a particular ordering of steps, other orderings are likewise possible provided that the principles of causality are maintained.

[0457] The one or more embodiments are used herein to illustrate one or more aspects, one or more features, one or more concepts, and/or one or more examples. A physical embodiment of an apparatus, an article of manufacture, a machine, and/or of a process may include one or more of the aspects, features, concepts, examples, etc. described with reference to one or more of the embodiments discussed herein. Further, from figure to figure, the embodiments may incorporate the same or similarly named functions, steps, modules, etc. that may use the same or different reference numbers and, as such, the functions, steps, modules, etc. may be the same or similar functions, steps, modules, etc. or different ones.

[0458] Unless specifically stated to the contra, signals to, from, and/or between elements in a figure of any of the figures presented herein may be analog or digital, continuous time or discrete time, and single-ended or differential. For instance, if a signal path is shown as a single-ended path, it also represents a differential signal path. Similarly, if a signal path is shown as a differential path, it also represents a single-ended signal path. While one or more particular architectures are described herein, other architectures can likewise be implemented that use one or more data buses not expressly shown, direct connectivity between elements, and/or indirect coupling between other elements as recognized by one of average skill in the art.

[0459] The term "module" is used in the description of one or more of the embodiments. A module implements one or more functions via a device such as a processor or other processing device or other hardware that may include or operate in association with a memory that stores operational instructions. A module may operate independently and/or in conjunction with software and/or firmware. As also used herein, a module may contain one or more sub-modules, each of which may be one or more modules.

[0460] As may further be used herein, a computer readable memory includes one or more memory elements. A memory element may be a separate memory device, multiple memory devices, or a set of memory locations within a memory device. Such a memory device may be a read-only memory, random access memory, volatile memory, non-volatile memory, static memory, dynamic memory, flash memory, cache memory, a quantum register or other quan-

tum memory and/or any other device that stores data in a non-transitory manner. Furthermore, the memory device may be in a form of a solid-state memory, a hard drive memory or other disk storage, cloud memory, thumb drive, server memory, computing device memory, and/or other non-transitory medium for storing data. The storage of data includes temporary storage (i.e., data is lost when power is removed from the memory element) and/or persistent storage (i.e., data is retained when power is removed from the memory element). As used herein, a transitory medium shall mean one or more of: (a) a wired or wireless medium for the transportation of data as a signal from one computing device to another computing device for temporary storage or persistent storage; (b) a wired or wireless medium for the transportation of data as a signal within a computing device from one element of the computing device to another element of the computing device for temporary storage or persistent storage; (c) a wired or wireless medium for the transportation of data as a signal from one computing device to another computing device for processing the data by the other computing device; and (d) a wired or wireless medium for the transportation of data as a signal within a computing device from one element of the computing device to another element of the computing device for processing the data by the other element of the computing device. As may be used herein, a non-transitory computer readable memory is substantially equivalent to a computer readable memory. A non-transitory computer readable memory can also be referred to as a non-transitory computer readable storage medium.

[0461] While particular combinations of various functions and features of the one or more embodiments have been expressly described herein, other combinations of these features and functions are likewise possible. The present disclosure is not limited by the particular examples disclosed herein and expressly incorporates these other combinations.

What is claimed is:

1. A computer-implemented method, the method comprises:

determining, by a computing entity of a computing system, selection criteria for a set of public benefit credit assets represented by a secure first token on an object distributed ledger, wherein a particular public benefit credit asset of the set of public benefit credit assets includes a smart contract that assigns a corresponding credit level from a corresponding payer identifier (ID) to a corresponding owner ID associated with the particular public benefit credit asset, wherein the determining the selection criteria includes one or more of: identifying, for a buyer ID, a buyer entity type affinity with a public benefit project type of the set of public benefit credit assets as a portion of the selection criteria,

identifying, for the buyer ID, a buyer entity geographic location affinity with a public benefit project geographic location of the set of public benefit credit assets as another portion of the selection criteria, and extracting the selection criteria from a secure buyer token associated with the buyer entity;

indicating, by the computing entity, selection of the secure first token to produce a selected secure first token when at least one of the portion of the selection criteria for the set of public benefit credit assets and the another portion of the selection criteria for the set of public

- benefit credit assets matches a corresponding portion of the secure first token representing the set of public benefit credit assets;
- updating, by the computing entity, the smart contract of the selected secure first token to produce an updated smart contract to represent assignment of a new corresponding credit level from the buyer ID to the corresponding current owner ID associated with the particular public benefit credit asset;
- obtaining, by the computing entity, a copy of the object distributed ledger,
- hashing, by the computing entity, the updated smart contract utilizing a receiving public key of the object distributed ledger to produce a next transaction hash value;
- encrypting, by the computing entity, the next transaction hash value utilizing a private key of the computing entity to produce a next transaction signature;
- generating, by the computing entity, a next block of a blockchain of the object distributed ledger to include the updated smart contract and the next transaction signature; and
- causing, by the computing entity, inclusion of the next block as an updated secure first token of the selected secure first token in the object distributed ledger.
- 2.** The method of claim 1 further comprises:
- issuing, by the computing entity, a secure first token update request to an object ledger computing entity of the computing system serving as a blockchain node of the object distributed ledger a secure first token update request that includes the updated smart contract to facilitate the inclusion the updated secure first token in the object distributed ledger.
- 3.** The method of claim 1, wherein the extracting the selection criteria from the secure buyer token associated with the buyer entity comprises:
- identifying the secure buyer token based on an association with the buyer ID; and
- recovering the secure buyer token from at least one of the object distributed ledger, a second object distributed ledger, a verification server, and another computing entity affiliated with at least one of the object distributed ledger and the second object distributed ledger.
- 4.** The method of claim 1, wherein the indicating selection of the secure first token to produce the selected secure first token further comprises at least one of:
- determining whether a power savings aspect of a purchase of the selection criteria for the set of public benefit credit assets matches an energy type of the secure first token representing the set of public benefit credit assets; and
- determining whether a social impact type aspect of the purchase of the selection criteria for the set of public benefit credit assets matches a social impact type aspect of the secure first token representing the set of public benefit credit assets.
- 5.** The method of claim 1, wherein the updating the smart contract of the selected secure first token to produce the updated smart contract further comprises:
- modifying the smart contract to indicate that the buyer ID is associated with control of the particular public benefit credit asset and the corresponding current owner ID is disassociated with the control of the particular public benefit credit asset.
- 6.** The method of claim 1, wherein the hashing the updated smart contract utilizing the receiving public key of the object distributed ledger to produce the next transaction hash value further comprises one of:
- obtaining the receiving public key from the blockchain of the object distributed ledger;
  - receiving the receiving public key from a blockchain node of the object distributed ledger; and
  - determining the receiving public key to be associated with the computing entity.
- 7.** A computing entity of a computing system comprises:
- an interface;
- a local memory; and
- a processor operably coupled to the interface and the local memory, wherein the processor performs functions stored by the local memory to:
- determine selection criteria for a set of public benefit credit assets represented by a secure first token on an object distributed ledger, wherein a particular public benefit credit asset of the set of public benefit credit assets includes a smart contract that assigns a corresponding credit level from a corresponding payer identifier (ID) to a corresponding owner ID associated with the particular public benefit credit asset, wherein the processor determines the selection criteria by one or more of:
- identifying, for a buyer ID, a buyer entity type affinity with a public benefit project type of the set of public benefit credit assets as a portion of the selection criteria,
  - identifying, for the buyer ID, a buyer entity geographic location affinity with a public benefit project geographic location of the set of public benefit credit assets as another portion of the selection criteria, and
  - extracting the selection criteria from a secure buyer token associated with the buyer entity;
- indicate selection of the secure first token to produce a selected secure first token when at least one of the portion of the selection criteria for the set of public benefit credit assets and the another portion of the selection criteria for the set of public benefit credit assets matches a corresponding portion of the secure first token representing the set of public benefit credit assets;
- update the smart contract of the selected secure first token to produce an updated smart contract to represent assignment of a new corresponding credit level from the buyer ID to the corresponding current owner ID associated with the particular public benefit credit asset;
- obtain, via the interface, a copy of the object distributed ledger;
- hash the updated smart contract utilizing a receiving public key of the object distributed ledger to produce a next transaction hash value;
- encrypt the next transaction hash value utilizing a private key of the computing entity to produce a next transaction signature;
- generate a next block of a blockchain of the object distributed ledger to include the updated smart contract and the next transaction signature; and

cause, via the interface, inclusion of the next block as an updated secure first token of the selected secure first token in the object distributed ledger.

**8.** The computing entity of claim 7, wherein the processor performs further functions to:

issue a secure first token update request to an object ledger computing entity of the computing system serving as a blockchain node of the object distributed ledger a secure first token update request that includes the updated smart contract to facilitate the inclusion of the updated secure first token in the object distributed ledger.

**9.** The computing entity of claim 7, wherein the processor performs functions to extract the selection criteria from the secure buyer token associated with the buyer entity by:

identifying the secure buyer token based on an association with the buyer ID; and recovering, via the interface, the secure buyer token from at least one of the object distributed ledger, a second object distributed ledger, a verification server, and another computing entity affiliated with at least one of the object distributed ledger and the second object distributed ledger.

**10.** The computing entity of claim 7, wherein the processor performs functions to indicate selection of the secure first token to produce the selected secure first token by at least one of:

determining whether a power savings aspect of a purchase of the selection criteria for the set of public benefit credit assets matches an energy type of the secure first token representing the set of public benefit credit assets; and

determining whether a social impact type aspect of the purchase of the selection criteria for the set of public benefit credit assets matches a social impact type aspect of the secure first token representing the set of public benefit credit assets.

**11.** The computing entity of claim 7, wherein the processor performs functions to update the smart contract of the selected secure first token to produce the updated smart contract further by:

modifying the smart contract to indicate that the buyer ID is associated with control of the particular public benefit credit asset and the corresponding current owner ID is disassociated with the control of the particular public benefit credit asset.

**12.** The computing entity of claim 7, wherein the processor performs functions to hash the updated smart contract utilizing the receiving public key of the object distributed ledger to produce the next transaction hash value by one of:

obtaining, via the interface, the receiving public key from the blockchain of the object distributed ledger;

receiving, via the interface, the receiving public key from a blockchain node of the object distributed ledger; and

determining the receiving public key to be associated with the computing entity.

**13.** A non-transitory computer readable memory of a computing system that comprises:

a first memory element that stores operational instructions that, when executed by a processing module of a computing entity of a computing system, causes the processing module to:

determine selection criteria for a set of public benefit credit assets represented by a secure first token on an

object distributed ledger, wherein a particular public benefit credit asset of the set of public benefit credit assets includes a smart contract that assigns a corresponding credit level from a corresponding payer identifier (ID) to a corresponding owner ID associated with the particular public benefit credit asset, wherein the processing module determines the selection criteria by one or more of:

identifying, for a buyer ID, a buyer entity type affinity with a public benefit project type of the set of public benefit credit assets as a portion of the selection criteria,

identifying, for the buyer ID, a buyer entity geographic location affinity with a public benefit project geographic location of the set of public benefit credit assets as another portion of the selection criteria, and

extracting the selection criteria from a secure buyer token associated with the buyer entity;

a second memory element that stores operational instructions that, when executed by the processing module, causes the processing module to:

indicate selection of the secure first token to produce a selected secure first token when at least one of the portion of the selection criteria for the set of public benefit credit assets and the another portion of the selection criteria for the set of public benefit credit assets matches a corresponding portion of the secure first token representing the set of public benefit credit assets, and

update the smart contract of the selected secure first token to produce an updated smart contract to represent assignment of a new corresponding credit level from the buyer ID to the corresponding current owner ID associated with the particular public benefit credit asset; and

a third memory element that stores operational instructions that, when executed by the processing module, causes the processing module to:

obtain a copy of the object distributed ledger; hash the updated smart contract utilizing a receiving public key of the object distributed ledger to produce a next transaction hash value;

encrypt the next transaction hash value utilizing a private key of the computing entity to produce a next transaction signature;

generate a next block of a blockchain of the object distributed ledger to include the updated smart contract and the next transaction signature; and

cause inclusion of the next block as an updated secure first token of the selected secure first token in the object distributed ledger.

**14.** The non-transitory computer readable memory of claim 13 further comprises:

a fourth memory element that stores operational instructions that, when executed by the processing module, causes the processing module to:

issue a secure first token update request to an object ledger computing entity of the computing system serving as a blockchain node of the object distributed ledger a secure first token update request that includes the updated smart contract to facilitate the inclusion of the updated secure first token in the object distributed ledger.

**15.** The non-transitory computer readable memory of claim **13**, wherein the processing module functions to execute the operational instructions stored by the first memory element to cause the processing module to extract the selection criteria from the secure buyer token associated with the buyer entity by:

identifying the secure buyer token based on an association with the buyer ID; and

recovering the secure buyer token from at least one of the object distributed ledger, a second object distributed ledger, a verification server, and another computing entity affiliated with at least one of the object distributed ledger and the second object distributed ledger.

**16.** The non-transitory computer readable memory of claim **13**, wherein the processing module functions to execute the operational instructions stored by the second memory element to cause the processing module to indicate selection of the secure first token to produce the selected secure first token by at least one of:

determining whether a power savings aspect of a purchase of the selection criteria for the set of public benefit credit assets matches an energy type of the secure first token representing the set of public benefit credit assets; and

determining whether a social impact type aspect of the purchase of the selection criteria for the set of public

benefit credit assets matches a social impact type aspect of the secure first token representing the set of public benefit credit assets.

**17.** The non-transitory computer readable memory of claim **13**, wherein the processing module functions to execute the operational instructions stored by the second memory element to cause the processing module to update the smart contract of the selected secure first token to produce the updated smart contract by:

modifying the smart contract to indicate that the buyer ID is associated with control of the particular public benefit credit asset and the corresponding current owner ID is disassociated with the control of the particular public benefit credit asset.

**18.** The non-transitory computer readable memory of claim **13**, wherein the processing module functions to execute the operational instructions stored by the third memory element to cause the processing module to hash the updated smart contract utilizing the receiving public key of the object distributed ledger to produce the next transaction hash value by one of:

obtaining the receiving public key from the blockchain of the object distributed ledger;

receiving the receiving public key from a blockchain node of the object distributed ledger; and

determining the receiving public key to be associated with the computing entity.

\* \* \* \* \*