

Event Streams for a Sequence of Events associated with a Blockchain

Technical Field

This disclosure relates generally to methods and systems for implementing a platform of one or more services associated with a distributed ledger, i.e. a blockchain, for one or more clients. Particularly, the present disclosure relates, but is not limited to, the provision of access to a plurality functions and applications associated with a blockchain for one or more clients, such as the implementation of event streams or machine-readable contracts.

Background

In this document we use the term 'blockchain' to include all forms of electronic, computer-based, distributed ledgers. These include consensus-based blockchain and transaction-chain technologies, permissioned and un-permissioned ledgers, shared ledgers, public and private blockchains, and variations thereof. The most widely known application of blockchain technology is the Bitcoin ledger, although other blockchain implementations have been proposed and developed. While Bitcoin may be referred to herein for the purpose of convenience and illustration, it should be noted that the disclosure is not limited to use with the Bitcoin blockchain, and alternative blockchain implementations and protocols associated with any kind of digital asset or a representation of a digital asset fall within the scope of the present disclosure. The terms "client", "entity", "node", "user", "sender", "recipient", "payer", "payee" may refer herein to a computing or processor-based resource. The term "Bitcoin" is used herein to include any version or variation that derives from or is based on the Bitcoin protocol. The term "digital asset" may refer to any transferrable asset, such as cryptocurrency, tokens representing at least a part of a property, a smart contract, a license, i.e. software licence, or DRM contracts for media content, etc. It will be understood that the term "digital asset" is used throughout this document to represent a commodity that may be associated with a value, which may be transferred to or provided as a payment in a transaction from one entity to another.

A blockchain is a peer-to-peer, electronic ledger, which is implemented as a computer-based, decentralised, distributed system made up of blocks, which in turn are made up of transactions. Each transaction is a data structure that encodes the transfer of control of a digital asset between participants in the blockchain system and includes at least one input and

at least one output. Each block contains a hash of the previous block so that blocks become chained together to create a permanent, unalterable record of all transactions which have been written to the blockchain since its inception. Transactions contain small programs known as scripts, embedded into their inputs and outputs, which specify how and by whom the outputs of the transactions can be accessed. On the Bitcoin platform, these scripts are written using a stack-based scripting language.

In order for a transaction to be written to the blockchain it must be “validated”. Network nodes (miners) perform work to ensure that each transaction is valid, with invalid transactions rejected from the network. Software clients installed on the nodes perform this validation work on an unspent transaction (UTXO) by executing its locking and unlocking scripts. If execution of the locking and unlocking scripts evaluate to TRUE, the transaction is valid, and the transaction is then written to the blockchain. Thus, in order for a transaction to be written to the blockchain, it must be i) validated by the first node that receives the transaction – if the transaction is validated, the node relays it to the other nodes in the network; ii) added to a new block built by a miner; and iii) mined, i.e. added to the public ledger of past transactions.

It will be appreciated that the nature of the work performed by miners will depend on the type of consensus mechanism used to maintain the blockchain. While proof of work (PoW) is associated with the original Bitcoin protocol, it will be appreciated that other consensus mechanisms, such as, proof of stake (PoS), delegated proof of stake (DPoS), proof of capacity (PoC), proof of elapsed time (PoET), proof of authority (PoA) etc. may be used. Different consensus mechanisms vary in how mining is distributed between nodes, with the odds of successfully mining a block depending on e.g. a miner’s hashing power (PoW), an amount of cryptocurrency held by a miner (PoS), an amount of cryptocurrency staked on a delegate miner (DPoS), a miner’s ability to store pre-determined solutions to a cryptographic puzzle (PoC), a wait time randomly assigned to a miner (PoET), etc. Typically, miners are provided with an incentive or reward for mining a block. The Bitcoin blockchain, for example, rewards miners with newly issued cryptocurrency (Bitcoin) and fees associated with transactions in the block (transaction fees). For the Bitcoin blockchain, the amount of cryptocurrency issued diminishes with time, with the incentive eventually consisting of transaction fees only. It will be appreciated, therefore, that the handling of transaction fees is a part of the underlying mechanism for committing data to public blockchains such as the Bitcoin blockchain.

As mentioned previously, each transaction in a given block encodes the transfer of control of a digital asset between participants in the blockchain system. The digital asset need not

necessarily correspond to a cryptocurrency. For example, the digital asset may pertain to a digital representation of a document, image, physical object, etc. The payment of cryptocurrency and / or transaction fees to miners may simply act as an incentive to maintain the validity of the blockchain by performing the necessary work. It may be that the cryptocurrency associated with the blockchain acts as a security for miners, with the blockchain itself being a ledger for transactions that predominantly relate to digital assets other than cryptocurrency. In some cases, it may be that the transfer of cryptocurrency between participants is handled by an entity that is different from and / or independent of the entity using the blockchain to maintain a ledger of transactions.

Once stored in the blockchain as a UTXO, a user can transfer control of the associated resource to another address associated with an input in another transaction. This transfer is usually, but not essentially, done using a digital wallet. This digital wallet may be a device; physical medium; program; application (app) on a computing device such as a desktop, laptop or a mobile terminal; or a remotely-hosted service, associated with a domain on a network, such as the Internet. The digital wallet stores public and private keys and can be used to track ownership of resources; tokens and assets etc., that are associated with a user; receive or spend digital assets; transfer tokens which may relate to digital assets, such as cryptocurrencies, licences, property, or other types of resource.

Although blockchain technology is most widely known for the use of cryptocurrency implementation, digital entrepreneurs are exploring the use of both the cryptographic security system Bitcoin is based on, and the data that can be stored on the Blockchain to implement new systems. It would be highly advantageous if the blockchain could be used for automated tasks and processes which are not limited to the realm of cryptocurrency. Such solutions would be able to harness the benefits of the blockchain (e.g. a permanent, tamper-proof records of events, distributed processing etc.) while being more versatile in their applications.

One area of current research is the use of the blockchain for the implementation of “smart contracts”. These are computer programs designed to automate the execution of the terms of a machine-readable contract or agreement. Unlike a traditional contract which would be written in natural language, a smart contract is a machine-executable program, which comprises rules that can process inputs in order to produce results, which can then cause actions to be performed dependent upon those results. Another area of blockchain-related interest is the use of ‘tokens’ (or ‘coloured coins’) to represent and transfer real-world entities via the blockchain. A potentially sensitive or secret item can be represented by the token, which has

no discernible meaning or value. The token thus serves as an identifier that allows the real-world item to be referenced from the blockchain.

The above-mentioned examples or scenarios, whilst making use of the advantages of the blockchain to provide a permanent, tamper-proof record of events; requires a client, client entity, computing devices, or a terminal associated with a client, to include or implement software and/or hardware, or a processor/module, such as a digital wallet for implementing functionality for managing digital assets, managing cryptographic keys for Elliptic Curve Digital Signature Algorithm (ECDSA) that are used, for example, by the BSV (Bitcoin Satoshi's Vision) Blockchain. In addition, there is also a requirement for the client device to be able to implement blockchain transaction construction and have access to BSV libraries. Thus, not only do clients need to include processing to implement such functionality, but they also need to ensure that appropriate security measures are implemented for such processes before they can make use of a blockchain network to send, receive, and view data, and/or digital assets, which relate to a smart contract or a token representing a real world asset transaction.

Accordingly, there is a desire to implement secure, low-complexity, user-friendly, efficient, and robust techniques, that will allow any client, whether computationally sophisticated or not, to be able to instantaneously access and interact with useful applications associated with the blockchain, in a simple, fast, accurate, reliable, and secure manner, that is computationally and functionally less onerous. More particularly, there is a desire to make use of distributed ledger (blockchain) technology, and the advantages of increased security, transparency, and reliability of records, to provide a common platform or interface for a plurality of blockchain related services or applications, that enable any client computing device to ensure any data, event, or digital asset associated with the client, can be instantaneously and securely mined, or written into the blockchain easily, thereby providing a lasting, tamper-proof, and auditable record of it, which can be created, written, updated, read, or viewed as required.

Such an improved solution has now been devised. The present disclosure addresses the above technical concerns by proposing one or more techniques, whereby data, or information associated with a client, may be simply, securely, and instantaneously written into, or obtained from the blockchain, by methods, devices, and systems which provide an application programming interface (API) for one or more services associated with a blockchain, without such clients needing to implement any processing or functionality for using the blockchain, while still being able to avail all advantages associated with the blockchain.

Summary

The present disclosure proposes methods, devices, and systems, for providing, creating, updating, and/or terminating an event stream that is implemented using the blockchain, and creating a tamper-proof log or record of events associated with the event chain. An event E_n for the event stream ES is identified in the received request and represents the current length of the event stream ES. If $n = 0$, so that E_n is the first event to create the event stream ES, then a blockchain transaction is created, including an unspent output that is a dust output. If $0 < n \leq N$, where N is the final or maximum value for n , so that E_n is an event to amend the event stream ES, then a blockchain transaction is created including a first input, spending a dust output associated with a previous transaction for the event stream; an unspent transaction output being a dust output for the current transaction; and an unspent transaction output being associated with event data representing the current event E_n . If $n=N$, so that E_n is an event to terminate the event stream ES, then a blockchain transaction is created including a first input, spending a dust output associated with a previous transaction for the event stream; an unspent transaction output being associated with a digital asset that is above a defined dust output limit. Once the created transaction is accepted and/or submitted to the blockchain, a result associated with the transaction is provided in the HTTP transmission protocol format. In some embodiments one or more transactions in the event stream, while being accepted or being a valid transaction for a given event stream, are not submitted to the blockchain immediately. For instance, the transactions in an event stream will be submitted to a block after a given number of transactions or time has elapsed, i.e. after 25 or so transactions in an event stream have taken place, for example. The transactions may be held in a mempool until the number or time has elapsed. In other embodiments, it is possible that a transaction in an event stream is submitted to the blockchain instantaneously.

Throughout this specification the word "comprise", or variations such as "includes", "comprises", or "comprising", will be understood to imply the inclusion of a stated element, integer, step, or group of elements, integers, or steps, but not the exclusion of any other element, integer, step, or group of elements, integers, or steps.

Brief Description of the Drawings

Aspects and embodiments of the present disclosure will now be described, by way of example only, and with reference to the accompany drawings, in which:

Figure 1 is a schematic diagram, depicting an overview of a platform for a plurality of services associated with a blockchain, according to a first aspect.

Figure 2a is a flowchart, depicting a method for providing a platform of a plurality of services that are associated with a blockchain, according to the first aspect, as implemented by one or more processors associated with the platform.

Figure 2b is a flowchart, depicting a method for accessing a platform of a plurality of services that are associated with a blockchain, according to the first aspect, as implemented by one or more processors associated with a client.

Figure 3 is a schematic diagram, depicting the components of the platform of a plurality of services that are associated with a blockchain, according to the first aspect.

Figure 4 is a flowchart, depicting a method for implementing a data-writing service for transactions associated with a blockchain, according to a second aspect, as implemented by one or more processors associated with a platform service.

Figure 5 is a flowchart, depicting a method for creating an event stream associated with a blockchain, according to a third aspect, as implemented by one or more processors associated with a platform service.

Figure 6 is a flowchart, depicting a method for updating an event stream associated with a blockchain, according to the third aspect, as implemented by one or more processors associated with a platform service.

Figure 7 is a flowchart, depicting a method for terminating an event stream associated with a blockchain, according to the third aspect, as implemented by one or more processors associated with a platform service.

Figure 8 is a flowchart, depicting a method for accessing a data-writing service for transactions associated with a blockchain, according to a second or third aspect, as implemented by one or more processors associated with a client.

Figure 9 is a schematic diagram, illustrating a computing environment in which various aspects and embodiments of the present disclosure can be implemented.

Detailed Description

While the appended claims are in relation to a third aspect of the present disclosure described in detail below, a detailed discussion in detailed to the first and second aspects are provided herein to provide a reader with a full and complete understanding of the claimed aspects and related embodiments of the present disclosure.

In accordance with a first aspect, the present disclosure provides a computer implemented method for providing a platform of a plurality of services that are associated with a blockchain, the platform being provided for a plurality of clients, the method implemented by a platform processor associated with an application programming interface (API).

Advantageously, the platform processor API allows for web-based interaction interface, i.e. it may in some embodiments be implemented as a web service for the one or more clients, such that communication may take place over the Internet using standard Internet communication protocols for web-based services. For instance, in some embodiments, whereby HTTP messages or requests in an application level, or layer between a client and a server (the platform service in this case), such as HTTP, HTTPS etc. may be transmitted and received based on transport layer protocols, such as TCP/IP etc. The reference to HTTP transmission protocols, or HTTP API, herein also encapsulates all standard Internet communication protocols, such as TCP/IP, UDP, HTTPS, etc.

In some embodiments the platform processor is implemented as an HTTP API endpoint. In some embodiments the platform processor is implemented as a Representational State Transfer (REST) endpoint. Advantageously, the API may be implemented as a REST endpoint, thereby also allowing the client to communicate using standard Internet or web-based protocols, such as HTTP or HTTPS.

The method of the first aspect comprises the steps of receiving a request from a given client among the plurality of clients, the request pertaining to a given service among the plurality of services, and from the given client being based on a Hypertext Transfer Protocol (HTTP) transmission protocol format. Then, based on a determination that the client identity and/or request(s) is/are valid, the method includes obtaining a destination address associated with the given service. In some embodiments, the destination address may be an IP address or a network address endpoint. For example, this may be an endpoint universal resource identifier

(URI) and may include the universal resource location (URL) of a web server, from where the requested service may be accessed by the payment processor or one or more other entities (including the client) for the requested service.

In some embodiments, this destination address may be the same endpoint as the platform API endpoint. This may be the case if the platform offers such a requested service as that of a main or core service. In other embodiments, where there are multiple different types of services offered by the platform, each implemented by different processors or web servers, then the destination address may be different to the platform API, which may act as a host server for other processor and web servers that are associated with the platform. In this case, a platform processor comprises or is associated with a plurality of processors, each configured for implementing a given service among the plurality of services on the blockchain, and each being associated with a specific destination address or endpoint that is unique to the respective processor.

The method of the first aspect further includes the step of processing the request for the given service, based on at least one blockchain transaction corresponding to the obtained destination address to obtain an output script. In some embodiments, the output script is associated with data relating to the requested service, or the result of the service requested is included in a UTXO and includes such data or digital asset for the transaction.

In the first aspect, this result associated with the output script is then sent to the given (requesting) client in the HTTP or similar transmission protocol format.

Advantageously, the method of the first aspect of the present disclosure, by implementing a platform that is provided as an API for one or more clients, allows one or more processor associated with a client to sign-up, or use a web service provided by the platform processor to write or access data into a blockchain. The one or more processors associated with the platform can implement one or more of the services being offered, using a standards-based interface design, such as, but not limited to, the REST (Representational State Transfer) – which is an architectural style for developing web services and web-based interactions. A resource, in the context of REST API, can be defined as an object with a type, associated data, relationships to other resources, and a set of methods that operate on it. Thus, the platform or services implemented by the platform processor of the first aspect is advantageously provided as an API implementation, to access the (state of a) blockchain or distributed ledger, such as the Bitcoin SV (BSV) blockchain, and to trigger operations or functions that can alter that state, via an application interface, and expose it as a REST API.

In other words, one or more servers or processors associated with the platform may be considered as a REST endpoint for one or more clients that choose to use such service. Advantageously, the client can thus communicate with the platform service via HTTP or similar Internet commands. More advantageously, no BSV, Bitcoin, blockchain knowledge, ECDSA, or other cryptographic key-management libraries, or transaction construction software, such as digital wallet software etc., needs to be implemented by the client for any of the services offered. The client using one or more processing resources or user terminals can simply register to use the platform via some known authentication techniques, such as password protection authorisation or standard public key infrastructure (PKI) for verifying client identity. The client should then simply be able to communicate with the platform service via basic HTTP or similar.

In some embodiments, some examples of the services associated with the blockchain that can be provided via the platform are:

- data services, for writing/submitting data into the blockchain to alter a state of the blockchain;
- data services, for reading/obtaining data reflecting the current state of the blockchain;
- services associated with simplified payment verification, for transactions associated with the blockchain;
- services associated with the management of one or more event streams and/or machine-readable contracts associated with the blockchain;
- services associated with the management of a digital wallet framework, for a plurality of clients.

In the embodiments, where there are multiple processors or web servers associated with the platform processor of the first aspect, the method of the first aspect further comprises the step of providing an application programming interface (API) converter, for performing the steps of: receiving the request from the client in the HTTP transmission protocol format, converting a received request to a Remote Procedure Call (RPC) format, and sending the RPC request to a given processor among the plurality of processors, that is configured to implement the service identified in the received request. In a reverse flow path this embodiment includes receiving a response associated from the given processor in an RPC format, and converting the respective response to be sent to the client using the HTTP, or a similar transmission protocol.

This is advantageous as it allows the client to communicate requests that are associated with the blockchain via simple HTTP, using a web-based platform API, and seamlessly providing interoperability with any of the nodes or servers that implement the above described services, but that do not communicate using Internet protocol communication standards for web services. The API convertor implemented in this embodiment is not limited to HTTPS to RPC and vice versa conversion, or for that matter other web-based protocols to alternative communication protocols that are supported by the platform processors implementing one or more of the above services, networks for a given cryptocurrency, or digital assets that can otherwise be envisaged. In the reverse flow path, the method of the first aspect also includes receiving responses associated with the corresponding blockchain transaction from a respective processor in an RPC format, and accordingly, converting the respective responses using HTTP for sending on to the client. Thus, advantageously implementing the proposed interface by the platform processor enables seamless communication, for submitting transactions to the blockchain when the clients (payees) and miners use different wireless data communication protocols and mechanisms.

In some embodiments of the first aspect, the received request from the client is an HTTP GET or HTTP POST or HTTP PUT or HTTP PATCH request that includes or is associated with a client identifier, specific to a given client, as well as a service identifier for the given service requested among the plurality of services that are offered by the platform, as mentioned above. In some embodiments, the result sent to the client is an HTTP POST request based on the client identifier.

In some embodiments, to make client addressing for blockchain transactions simpler, there already exist mechanisms where a memorable and more user-friendly alias is used instead of the complicated public address for one or more client entities. Such a solution is proposed in US patent application no. 16/384696 and UK patent application number 1907180.2, both in the name of nChain Holdings Limited. These documents set out an alias-based payment service and associated protocols, referred to as bsvalias payment service, where an alias is used for destination addressing instead of the public address of a client entity. The alias in such a system is usually associated with a domain name of a sending/receiving client entity and may be a URI or an email address. Thus, as long as a sender or entity is aware of, or is provided with the alias, this is sufficient for the bsvalias payment system or an alias based addressing mechanism. Messages may be sent to the alias of a client, for instance, using instructions provided in a machine-readable resource, such as a JavaScript Object Notation JSON document, saved in a well-known URI or location for the bsvalias or other payment

service. In some embodiments of the present disclosure, one or more of the plurality of clients may have an alias such as the above to identify the respective client.

In related embodiments, the method of the first aspect comprises validating the client based on the client identifier and a record corresponding to the client identifier, the record associated with the platform processor. For example, such record may have been created and stored in or associated with the platform processor at the time of client sign-up or registration. Then, based on a successful validation of the client, the method includes determining if the received request from the client is valid, based on the service identifier and an attribute or setting included in the respective record. In some embodiments, said attribute or setting may indicate whether or not a given client is allowed access to all or part of the requested service. For instance, one or more levels of permission associated with the client identifier may be provided in the attribute or setting. For example, a given client may be allowed to request services to read data that is on a blockchain for a specific event, but may not be allowed to modify, delete or terminate such event, whereas another client may have permission for all action pertaining to one or more services.

In some embodiments, the step of verifying the identity of a given client may be based on a digital signature associated with the client. Cryptographic key pairs, including a private key and a public key (or public address) associated with each client, may be used for verifying that a request made for a service did indeed originate from the given client, i.e. where data signed by a private key can only be recovered or validated using the corresponding public key. Standard public key infrastructure (PKI) techniques may be used and implemented if verification is based on a digital signature.

In some embodiments of the first aspect, a computer implemented method for accessing the platform of a plurality of services, as implemented by one or more processors of a given client among the plurality of clients, comprising the steps of obtaining or identifying an application programming interface (API) endpoint associated with one or more processors, associated with the platform, and sending a request pertaining to a given service among the plurality of services, the request including or associated with a client identifier for the given client, and a service identifier for the given service requested. As mentioned above, the request is sent using a Hypertext Transfer Protocol (HTTP) or similar transmission protocol format. The method also includes receiving a result pertaining to an output script of a blockchain transaction associated with the request, said result being provided to the client in the HTTP transmission protocol format.

In a second aspect, the present disclosure provides a computer-implemented method for implementing a data-writing service, for transactions associated with a blockchain, the method being implemented by a platform processor associated with an application programming interface (API), to enable clients to access the service to write data into a blockchain. The method of the second aspect comprises the steps of receiving a request from a client, the request relating to an event stream ES implemented using the blockchain, the request from the client being based on a Hypertext Transfer Protocol (HTTP) transmission protocol format. In some embodiments, the event stream may track or represent as a Finite State Machine (FSM), such as a Deterministic Finite Automaton (DFA), which is a well-known computing term, representing a system having a finite number of states, and which may be in only one state at a given time, with a transition function or a trigger event for transitioning from one stage to the next. In some embodiments such event stream is useful to represent a control means or technique of a technical process. In some embodiments, the event stream may represent or track the inputs, states and/or events associated with a machine-readable contract or smart contract on the blockchain, where, advantageously, an immutable record of the past and current state of the contract is recorded. In some embodiments, the request received from the client includes a trigger event, to enable a state transition to take place in a smart contract associated with the event stream.

The method of the second aspect comprises the step of determining a current state of the event Stream $ES_{i=n}$, wherein i is an integer from 0 to N , each integer i representing a given state of the event stream ES, whereby $i = 0$ represents the created event stream ES, $i = n$ represents the event stream ES in a current state in the blockchain, and $i = N$ represents a final state of the event stream ES. In some embodiments, the determination of the current state may be an indication of the present state based on a most recent result associated with the event stream, said result stored on the blockchain or in one or more separate off-chain storage resources for event stream. This may be based on an identifier of an earlier or previous blockchain transaction associated with the event stream. If there is no previous state identified for the event stream then this will result in a determination that the current state is $n=0$, i.e. a new event stream is to be created. In some embodiments, the current state may also be retrieved or read from the blockchain. This may be performed by a data reader as explained above, which may be a service among the plurality of services provided by the platform processor.

In the method of the second aspect, processing a new event E_{n+1} for the event stream ES, based on the received request, includes the step of creating a blockchain transaction TX_{n+1} , the blockchain transaction TX_{n+1} including an input associated with a transaction output (TXO_n) from a previous transaction TX_n , and an unspent output ($UTXO_{n+1}$), associated with event data representing the new event E_n . In some embodiments, where $n=0$, no input that spends a previous output will exist. There may however be other inputs that represent digital assets associated with the event stream ES. The method then includes submitting the transaction TX_{n+1} to the blockchain.

Once submitted, the current state of the event stream is updated to be based on the submitted blockchain transaction, i.e. the state will be updated to be $ES_{i=n+1}$ based on the newly created event E_{n+1} , such that $ES_{i=n} = ES_{n+1}$. In some embodiments, the updated state is based on data present in $UTXO_{n+1}$, the unspent output of the latest transaction in the event stream. The method then includes sending a result, based on the updated current state of the event stream ES_{n+1} , the result being provided based on the HTTP transmission protocol format.

The second aspect of the present disclosure discusses the implementation of a data-writing service implemented by a platform processor, or in other words, the implementation enables the functionality of writing data associated with a real world process, such as controlling the states of a smart contract. The platform processor of the second aspect is associated to that discussed in the first aspect, wherein the second aspect discusses one of a plurality of blockchain services, i.e. for writing data into the blockchain to change its current state. As the request and the respect is received and provided using an API for the platform, the second aspect provides all the advantages associated with the first aspect. In addition, the data-writing service advantageously allows one or more clients to enable a transaction of state of a blockchain-implemented smart contract, by simply extracting the triggers or events from the effect. Thus, an immutable record of the various stages of the smart contract may be provided by the data writing service of the second aspect.

The third aspect of the present disclosure is related to the data-writing service of the second aspect, as discussed above for service provided in relation to event streams. In this aspect, a technique for establish a tamper-proof record or log, or a certificate confirming the sequential occurrence of events associated with an event stream. Thus, in the third aspect the method of the present disclosure proposes methods, devices, and systems for providing a creating, updating and/or terminating event stream, that is implemented using the blockchain and automatically creates a tamper-proof log or record of events associated with the event chain.

In the third aspect, the present disclosure provides a computer - implemented method for implementing a data-writing service, for transactions associated with a blockchain, the method being implemented by a platform processor associated with an application programming interface (API), to enable clients to access the service to write data into a blockchain. The method of the third aspect comprises the steps of receiving a request from a client, the request relating to an event stream ES on the blockchain, the request from the client being based on a Hypertext Transfer Protocol (HTTP) transmission protocol format.

An event E_n for the event stream ES is then identified in the received request from a client. For the event stream ES, n represents the current length of the event stream ES. If $n = 0$, so that E_n is the first event to create the event stream ES, then a first blockchain transaction is created for the event stream ES, including a first unspent output that is a dust output. Blockchain transaction dust or simply "dust" in the context of blockchain transaction for the present disclosure is understood to be a spendable transaction for a digital asset or cryptocurrency that has an output of low or minuscule value, i.e. the value may be much less than fees for mining the output in the blockchain. This dust output may be a minimum value of cryptocurrency or digital asset output that can be spent. In some embodiments, the digital asset or crypto current funds associated with such dust transactions, i.e. those handling the transfer of minimum value of a digital asset in its output, may be provided or managed by the platform processor. In other words, the dust output referred to in the present disclosure for the blockchain transaction is associated with a digital asset having a value that is below a value limit for a transaction", i.e. perhaps the value of the dust output is lower than for instance the mining fee that may be required to spend such transaction.

If $0 < n < N$, where N is the final or maximum value for n , so that E_n is an event to amend the event stream ES, then a current blockchain transaction is created including a first input spending a dust output, associated with a previous transaction for the same event stream; a first unspent transaction output being a dust output for the current transaction, and a final unspent transaction output being associated with event data, representing the current event E_n . In some embodiments, the event data is included in a data carrier element. This may be an un-spendable OP-RETURN output of the transaction. In some embodiments, the event data for the event E_n in the final unspent transaction output for the current blockchain transaction includes a hash of the event data. This advantageously keeps the event data contents of the event stream ES private. In some embodiments, a salt, which is a unique value that may be randomly generated by the platform processor for each transaction associated

with an event stream, may also be included. In some embodiments, the hash of said event data is applied by the platform processor, thereby advantageously allowing the platform service or processors to hold such event data privately. In other embodiments, the hash of said event data is applied by the client device prior to being included in the request that is received by the platform processor. This advantageously enables the client to hold the event or data associated with the event in the request privately, not even sharing it with the platform. In other embodiments, the event data for the event E_n in the final unspent transaction output includes raw event data, which is public on the blockchain, once written or submitted to it.

If $n=N$, so that E_n is an event to terminate the event stream ES, then a blockchain transaction is created including a first input, spending a dust output associated with a previous transaction for the event stream; a first unspent transaction output associated with a digital asset that is above a defined dust output limit, i.e. above the defined or minimum value of digital asset or cryptocurrency. Advantageously, the absence of a dust output signifies the termination of the event stream in this case, as this represents that there is nothing more in the event stream to track, i.e. no more events in the sequence. The provision that the first output being above the dust limit is to signal the end of the chain. Further, the final blockchain transaction does not have any event data output, i.e. there is no data carrier element present, which advantageously signals that this is not a data event to alter the event stream, but to terminate it.

In either of the three cases for n discussed above, the transaction is submitted to the blockchain and a result associated with the transaction is provided based on the HTTP transmission protocol format. In some embodiments, the event associated with the request, i.e. either E_0 , E_n or E_N , may be a single event or two or more events, relating to the respective request. For example, the request may include a data set of two or more sub-events for each E_0 , E_n or E_N . In some embodiments, the result is based on the event data output of the transaction or the event associated with the respective transaction. In some embodiments, any result or event data that is returned may be held in an un-spensible OP_RETURN output of the transaction. This is a Script opcode which can be used to write arbitrary data on blockchain and also to mark a transaction output as invalid. As another example, OP_RETURN is an opcode of the Script language for creating an unspendable output of a transaction that can store data and/or metadata within the transaction, and thereby record the metadata immutably in the blockchain. Metadata could comprise a log or time entry or a document which is desired to be stored in the blockchain. The event data or result may in some embodiments be considered to be a payload comprised in the unspendable output of

the respective transaction. Such an output may be made unspendable by means of an opcode that terminates the locking script of that output, e.g. OP_RETURN mentioned above. However in other embodiments, the payload or event data may be included in other ways.

The use of dust outputs in the transaction is advantageous and key for maintaining an immutable sequential record of all transactions as they occur for an event stream ES. This is because, although by posting transactions to the blockchain all blockchain transactions would be time-stamped and remain in order in the blockchain, this does not guarantee preservation of their sequential order. This is because transactions might be mined into blocks at different times. Therefore, only the ordering of the blocks in the chain follows chronologically in a blockchain, and not individual transactions. Whereas, to track, record, and audit the exact sequential order of events for an event stream that may be a smart contract, advantageously, the use of dust outputs that must be spent by the first input of the next transaction in the sequence ensures that the order of the transaction is chronologically tracked and a tamper-proof record is created. This is because once mined into a block, the payment of dust from a previous transaction to a next one in the sequence ensures that, in alignment with Bitcoin protocol rules, the sequence of embedded data carrier elements (which are the final outputs in each transaction) cannot be reordered, and no insertions or deletions may occur, which could change it without it being immediately obvious that the event stream has been compromised. In some embodiments, a double spend prevention inherent to the Bitcoin protocol ensures that the movement of cryptocurrency (e.g. dust) between different addresses, and therefore associated events, remains in chronological order. Thus, this improves the security of smart contracts on the blockchain as well as the log, a copy or a replication of the series of event occurrences.

In some embodiments, a hierarchical deterministic key chain K , to be used for a request associated with the event stream ES, is determined. Such key chain is unique to the given event stream. The cryptographic private/public key pairs, from the seed or parent, or master key pair K , may then be derived for each event associated, such that $K = K_{n=0 \text{ to } N}$, where n is an integer from 0 to N , each integer n representing a current length or current number of events associated with the event stream ES, where N represents a maximum or final value of n . This advantageously ensures that the keys derived for a particular event stream are related to a common master or seed key and can be derived for processing each respective event. This way, advantageously, a locking script associated with the dust outputs are secured with a derived key K_n for the current event, and the first inputs each spend the dust outputs from

the previous transactions, using the previous key pair K_{n-1} . This ensures that the outputs can only be spent with a corresponding key pair, specific to the respective previous transactions.

In some embodiments, the result associated with the event stream ES includes a certificate confirming at least one of the following:

- a transaction identifier within which the event E_n was submitted to the blockchain
- a Merkle inclusion proof of the transaction to a header in the blockchain
- a copy of the block header in which said transaction was included

In some embodiments, each of the transactions created, as discussed above for the third aspect, may further comprise other inputs associated with a digital asset. This may be provided based on an operational float, managed by the platform processor. In some embodiments, this may be associated with a digital asset or cryptocurrency resource or fund maintained or controlled by the payment processor to cover transacting mining fees and one or more other operations for the blockchain etc. The transactions may also have one or more change outputs associated with the digital asset. As mentioned above, the final transaction has all change outputs.

In some embodiments, the event stream ES may be identified based on a transaction identifier associated with the submitted blockchain transaction. In some embodiments, a state associated with the event stream ES may also be identified based on a transaction identifier associated with the most recently submitted blockchain transaction.

In some embodiments, the method includes storing a copy of a record, or a log that is based on the result(s) for each event of the event stream ES, in an off-chain storage resource. This storage resource may be associated with the platform processor, or in a different device, database, or service from which it may be requested or retrieved when requested by a client. Advantageously, storage of the log associated with the results of the event stream are stored separately, to avoid a requirement to download an entire blockchain and sift through the data for any queries associated with the event stream. The blockchain itself implementing the event stream, could be checked in circumstances during audits or data verification. The back-up or separate copy could then be used for quick queries.

Some specific embodiments are now described by way of illustration with reference to the accompanying drawings, in which like reference numerals refer to like features.

First aspect – Platform API for a plurality of services associated with a blockchain

The platform processor for providing a plurality of services described above for the first aspect may be Platform as a Service (PaaS) and Software as a service (SaaS) offering that advantageously enables rapid delivery of useful real-world business and technical applications, such as management of software controlled technical systems or smart contracts, using a blockchain network such as the BSV blockchain. An overview of the platform services can be seen in Figure 1 that shows a high-level schematic of the system. The platform services has a platform processor 100 that provides an API 108, via which the services may be accessed by one or more clients.

Platform Services 100 as shown in this Figure are made up of three families of services and is aimed at allowing users and organisations to easily and securely make use of the advantages offered by the unique properties of a blockchain, without actually implementing any blockchain based software, knowledge or libraries at the client end. These services are:

- Data Services 102 that aim to simplify the usage of the chain as a commodity data ledger.
- Compute Services 104 that aim to provide a generalised compute framework backed by a digital asset such as Bitcoin SV.
- Commerce Services 106 that provide enterprise-class capabilities for transacting using a digital asset such as Bitcoin SV

As mentioned above, requests may be received via or using the HTTPS protocol from a client at the API, as the API is implemented as a web service. The requested services are then implemented by the one or more service modules or processing resources 102 -106 using underlying software 110, such underlying software 110 being associated with the blockchain, i.e. to implement resources, libraries and/or key-management wallet implementations for creating, processing and submitting transactions associated with the blockchain. Once processed, transactions can be submitted to the blockchain network 112 (instead of the client implementing any such functionality or transaction libraries). At most, the client may or can implement a digital wallet or the like associated with cryptocurrency or some other digital asset, but this is not essential as the platform service 100 may also be able to provide and manage the digital asset for the client.

Figure 2a relates to the first aspect of the present disclosure and depicts a computer implemented method for providing a platform of a plurality of services that are associated with a blockchain, such as the platform 100 shown in Figure 1. The method of Figure 2a is implemented by a platform processor associated with an application programming interface (API).

Step 202a depicts receiving a request from a given client among the plurality of clients. In some embodiments, the client may be one or more computing devices, resources or processors associated with a client, said client having signed up or registered to access the plurality of services that are provided by the platform processor. As mentioned above, the platform processor may be one or more processors, each offering a different type of function or service to be implemented using a blockchain, such as the Bitcoin SV blockchain (such as a processor for the data, compute and commerce services seen in Figure 1). It is also possible for there to be just one processor for a single service. As the platform processor is associated with an API endpoint, such as a URI for the platform, the request from the given client can be based on a standard Internet protocol such as the Hypertext Transfer Protocol (HTTP) transmission protocol format. In some embodiments, the request may include an identifier for the client as well as an identifier for the service requested.

In step 204a the identity of the client is checked to see if the client is a valid client registered to use the platform processor and the functionality offered by it. In some embodiments, this may be based on known authentication methods such as password protected login authentication or the like. In this case, a record may be created for the given client based on a client identifier or alias included in the request, and a password. Validation may be based on a password received at the API matching the password in the record. In other embodiments, standard PKI techniques based on cryptographic private/public key pairs may also be used to validate a digital signature that is present in the request received from the client in step 202a. In this case, the identity of the client can be verified by checking if request signed by the private key can be successfully recovered or validated using the public key.

If the client identity cannot be verified or verification fails, then in step 206a the request is not processed any further.

If the client is validated successfully, then in step 208a, the validity of the request for the service in step 202a is then checked. This step is to ensure that the given client is indeed authorised to avail the service requested. The permission or attributes for this may be present

in the record for the client, to indicate one or more types of access levels or service that can be provided or not to a respective client.

If the request is found to be disallowed or invalid for the requesting client, then in step 210a the request is not processed any further.

It is to be understood that the embodiments of validating the client and/or service set out above are not essential for the operation of the first aspect, although it is useful. In some cases only the validation in steps 204a or 208a may be performed. In some cases no validation is performed. In this case, any client, whether registered or not, can use the service or platform upon appropriate payment for such access.

In step 212a, a destination address, which may be an endpoint URI for a server or processor that is responsible for implementing the requested service in step 202a, is obtained. In some embodiments, where there are a plurality of platform processors, a host server or platform API may convert the received request to a Remote Procedure Call (RPC) format to be sent to the destination address associated with the processor that is configured to implement the service identified.

In step 214a, the service requested is processed by the respective platform processor responsible for it. A blockchain transaction is either obtained or read or generated by the platform processor based on destination address/endpoint of the responsible processor, and an output script for this transaction is obtained. While Figure 2a refers to generating a blockchain transaction in this step, it will be understood that the first aspect of the present disclosure is not so limited. If the request in step 202a is to read or get data from the blockchain, then a transaction may not be generated, it can simply be read or obtained from the blockchain. There may be a plurality of blockchain transactions or multiple output scripts for one or more of the blockchain transactions generated.

In step 216a the output scripts may include data outputs as the result (for instance there may be a data carrier UTXO), or the result may be obtained based on the transaction identifiers or remaining outputs of the transaction. There may also be a non-spendable OP-RETURN output that is associated with the transaction from which the result can be obtained.

In step 218a, the result associated with the output script is provided to the given client in a HTTP or similar transmission protocol format. In some embodiments, if the responsible

processor for the service is located remotely to the host platform API, then the platform processor receives the response associated with the blockchain transaction(s) from the responsible processor in an RPC format. An API converter then converts this to a message that can be sent based on the HTTP format, before sending it to the client. As mentioned above, if the client used an alias addressing service, such as bsvalias, then the result is sent in a HTTP message addressed to the alias for the client in a format that is dictated by the bsvalias machine readable resource.

Figure 2b relates to the first aspect of the present disclosure and depicts a computer implemented method for accessing a platform of a plurality of services that are associated with a blockchain, such as the platform 100 shown in Figure 1. The method of Figure 2b is implemented by one or more processors associated with a client.

In step 202b, the application programming interface (API) endpoint associated with the platform is identified. As mentioned before, this may be the API associated with a host platform processor, and there may be one or more further processors responsible for implementing the service - each with their own service endpoint or a destination address.

In step 204b, the client prepares a request for a service, such as the data writing service 102 in Figure 1. The client in some embodiment includes a client alias or identifier and/or a service identifier in the request, so that it can be routed to the correct service endpoint. This is useful for checks by the platform processor regarding the validity of the requesting client and the client's permission to use the requested service.

In step 206b, the request prepared in step 204b is sent using a Hypertext Transfer Protocol (HTTP) or similar transmission protocol format, as the platform processor is implemented as a HTTP or REST API.

In step 208b, the result that pertains to an output script of a blockchain transaction associated with the request is provided from the platform processor. This result is provided to the client in the HTTP transmission protocol format.

Advantageously, with the methods of the first aspect, a request for blockchain based services is sent and received by the client in the HTTP transmission protocol format, and therefore the client can make use of all advantages and services unique to a blockchain, without having to implement any transaction capability or blockchain libraries. This is because the service is

offered via a platform API, which may be a HTTP or REST API endpoint. For example, REST API design standards can process HTTP requests and communication using the following HTTP commands over the Internet – and this is all the functionality that is required by the client, i.e. to be able to send and receive messages over the Internet. The platform processor(s) implement the commands remotely, or separately for the client.

Commands	GET	POST	PUT	DELETE	PATCH
Resource	read	create	update or create	delete	partial update

Figure 3 provides a more granular schematic view of the plurality of services associated with a blockchain, and which can be implemented by the platform 300 that is associated with an API via which any one or more of the offered services can be accessed. As seen in this Figure, the data services 302 may include a data writer 302a and a data reader service 302b. The implementation of event streams using the data writer service 302a will be explained in detail in Figures 4 to 8, to enable clients to write data into the blockchain in a simple, secure and optimised manner. The data reader service 302b enables the clients to send queries, which returns data that is stored in the blockchain. This may be using Filtered streams in which the client may pre-define the type of data that they wish to read from the blockchain on an ad hoc or periodic basis, i.e. within certain timeframe, or those associated with a set of related or unrelated events or documents that are processed in the blockchain 310. The data archive feature allows access to logs of previous transaction for a specified event or contract.

The compute services 306 of the platform 300 includes an application 306a and framework 306b associated with smart contracts, which in some embodiments may be represented as a state machine in the blockchain 310. The compute services 306 interacts with the data services 302 as data will need to be input and results provided to a client for any such computation.

Commerce services 304 are responsible for provision of enterprise-class capabilities via enterprise wallets 304a for transacting over the blockchain 310, based on best-in-class security practices and technologies. For example, in some embodiments enterprise wallets may implement functionality to enable blockchain transaction processing when more than one person or user or account may need to sign off on a transaction meeting a defined criterion.

i.e. associated with cryptocurrency of a large value above a certain predefined limit. An enterprise wallet may also include functionality to implement a threshold number and/or type of signatures to move large amounts of digital assets such as cryptocurrency or tokens representing another resource. The movement of these assets can then be represented on the blockchain following processing based on the criteria applied by such enterprise wallet implementation.

The SPV services 308 (simplified payment verification) are applications that require information from the blockchain but do not include direct links to it, as they do not run a miner node. Such SPV service 308 allows a lightweight client to verify that a transaction is included in a blockchain, without downloading the entire blockchain 310.

Second aspect – a Platform providing a data writing service associated with a blockchain

Figure 4 relates to a second aspect of the present disclosure and depicts a computer implemented method for providing a data writing service for transactions that are associated with a blockchain, such as the data writer 302a seen in Figure 3 of the first aspect. The method of Figure 3 is implemented by a platform processor associated with an application programming interface (API) for the service.

Step 402 depicts receiving a request from a client, the request relating to an event stream ES implemented using a blockchain. The request from the client being in a Hypertext Transfer Protocol (HTTP) transmission protocol format, as with the first aspect. In some embodiments, the event stream relates to a state machine, and represents a machine-readable contract or smart contract that is implemented as a finite state machine in the blockchain. A Finite state Machine (FSM) is a well-known mathematical model of computation. It is an abstract machine that can be in exactly one of a finite number of states at any given time. The FSM can change from one state to another in response to some external inputs - the change from one state to another is called a transition. An FSM may be defined by a list of its states, its initial state, and the conditions for each transition. In the Bitcoin SV Blockchain the UTXO set can be thought of as a state machine, with a given output's spent state being a function of previous inputs to the transaction (the machine). Thus, by replaying all transactions, the current spend state of any output, and the current contents of the UTXO set, can be established deterministically using the blockchain. Thus, in the embodiment of Figure 4, the request can be considered as

a request to alter a current state of a smart contract, implemented as an event stream ES in the blockchain.

Step 404 depicts determining a current state of the event Stream $ES_{i=n}$, by the data writer or a platform processor for implementing the data writing service. Let us consider that i is an integer from 0 to N , each integer i representing a given state of the event stream ES having a finite number of states, whereby $i = 0$ represents the created event stream ES, $i = n$ represents the event stream ES in a current state in the blockchain, and $i = N$ represents a final state of the event stream ES. Thus the current state of the event stream ES would be E_n .

Step 406 depicts identifying or obtaining data associated with a next or new event E_{n+1} for the event stream ES based on the received request in step 402. In this embodiment, the new event may be data or a function to trigger an alteration of a state so that the event stream transitions to the next state.

Step 408 depicts the step of creating a blockchain transaction TX_{n+1} for a next event E_{n+1} by one or more processors associated with the platform processor implementing the data writer. The blockchain transaction TX_{n+1} includes at least:

- an input associated with a transaction output (TXO_n) from a previous transaction TX_n . This input spends the TXO_n output from the previous transaction.
- an unspent output ($UTXO_{n+1}$) associated with event data representing the new event E_{n+1} . In some embodiments this is a data output, i.e. representing a data carrier element of the transaction.

There may be additional inputs, such as fund inputs to cover network mining fees as appropriate, and there also may be other outputs, such as change outputs for the transaction.

Step 410 depicts submitting the transaction TX_{n+1} created in step 408 to the blockchain. Here the transaction may be submitted to the blockchain, such as the Bitcoin SV network for inclusion in a subsequent block by a miner node or BSV node software associated with the platform processor.

Step 412 depicts updating the current state of the event stream ES to now be $ES_{i=n+1}$ based on the newly created event E_{n+1} , such that $ES_{i=n} = ES_{n+1}$. This corresponds to the latest transaction TX_{n+1} submitted to the blockchain for ES. In some embodiments, the new state is identified and updated based on the event data output in the final transaction output $UTXO_{n+1}$.

Step 414 depicts sending a result based on the updated current state ES_{n+1} in step 412, the result being provided based on the HTTP transmission protocol format to the client.

Third aspect – a Platform providing a data writing service for recording an event stream associated with a blockchain

Figures 5, 6 and 7 discuss an application associated with implementing event streams, such as those discussed in relation to figure 4 of the second aspect. The third aspect relates to a technique for establishing an immutable sequential log or record of the event stream ES up to its current state on the blockchain. In some embodiments, the log in addition to being stored on the blockchain, can also be provided or stored off-chain. As the state of the event stream is based on inputs and outputs associated with transactions, the techniques described below for the third aspect set out a method for establishing an immutable chronological log of all transactions associated with an event stream on the blockchain. The event stream may represent sequential inputs that are applied to a smart contract that is implemented using an FSM, DFA etc.

Figure 5 relates to the second aspect of the present disclosure and depicts a computer implemented method for providing a data writing service for transactions that are associated with a blockchain, such as the data writer 302a seen in Figure 3 of the first aspect. The method of Figure 5 is implemented by a platform processor associated with an application programming interface (API). The method relates to creating a new event stream.

Step 502 depicts receiving a request from a client, the request being to create a new event stream ES using the blockchain. The request from the client is in a Hypertext Transfer Protocol (HTTP) transmission protocol format, as with the first and second aspects.

Step 504 depicts the step of determining a hierarchical deterministic (HD) key chain K to be used with a new event stream ES to be created. In some embodiments, this may be implemented by a HD wallet implementation associated with the platform processor to generate a hierarchical tree-like structure of keys which start from the seed or parent or master key based on the known BIP 21 Protocol. The HD key creation and transfer protocol greatly simplifies key generation and permits creation of child accounts which can operate independently, gives each parent account the ability to monitor or control its children even if the child account is compromised. The HD protocol uses a single root seed to create a hierarchy of child, grandchild, and other descended keys with separate deterministically-

generated integer values. Each child key also gets a deterministically-generated seed from its parent, called a chain code. This way, any compromising of one chain code doesn't necessarily compromise the integer sequence for the whole hierarchy. In addition to the above advantages, in the present aspect, this key generation is carried out by the platform processor, therefore removing the resource and functionality of this generated from the client. No HD wallet therefore needs to be implemented by the client. In step 504, key chain K includes a series of private/public key pairs derived from a selected parent key pair, such that:

$K = K_{n=0 \text{ to } N}$, whereby n is an integer from 0 to N, each integer n representing a current length or current number of events associated with event stream ES, and N represents a maximum or final value of n.

Step 506 depicts identifying or obtaining data associated with a first event E_0 , this being for the new event stream ES to be created in the blockchain based on event data in the received request in step 502.

Step 508 depicts creating a first blockchain transaction TX_0 for the new event stream ES where $n = 0$ by one or more processors associated with the platform processor implementing the data writer.

Step 510 depicts that the output of the blockchain transaction TX_0 created in step 508 includes at least a first unspent transaction output ($UTXO_{0_dust}$) being a dust output, said dust output associated with a locking script secured with a first derived key pair K_0 in the series of keys derived from the HD key chain K in step 504. A dust output is associated with a (digital asset) value that is below a defined limit for a transaction or having a defined minimum value, i.e. lower than a mining fee that would be required to spend such transaction. There may also be other inputs associated with digital assets associated with an operational float or digital asset or cryptocurrency fund that is maintained or associated with the payment processor. It is also possible to have other outputs in the transaction that are digital asset change outputs.

Thus, in some embodiments, a Create template for a blockchain transaction to create an event stream as per the present embodiment is one where the first input must be greater than dust. This is to advantageously indicate that there is no previous entry in the event stream, and this is the first entry. The Create template also specifies that first output of the template is dust, and that there is no data carrier or data output (so no `OP_RETURN`), as there is no event data associated with the Create state – other than the creation of a new event stream ES. In some embodiments, an `OP_RETURN` is included for the create frame, but this does not hold

any event data. It may hold metadata describing the parameters of the newly created stream. Examples of metadata examples may include details such as publicise or notarise properties, write to blockchain time, time when events will first be accepted, time when events will no longer be accepted, geo-region where backing or related data will be stored, maximum size of acceptable data, sequence number and more.

Step 512 depicts submitting the transaction TX_0 to the blockchain. Here, the transaction may be submitted to the blockchain, such as the Bitcoin SV network for inclusion in a subsequent block by a miner node or BSV node software associated with the platform processor. In some embodiments, once mined, the transaction identifier TX_0 may be used to uniquely identify the newly created event stream ES.

Step 514 depicts sending a result associated with the created event stream ES in TX_0 to the client, the result being provided in the HTTP transmission protocol format. The result relating to the event stream may be copied or saved separately from the blockchain.

In some embodiments, the creation of the event stream may be decoupled from the submission to the blockchain for on-chain settlement. In this case, an event stream id that is unique to a respective event stream may also be used, and may be provided in the result to the client instead.

Figure 6 relates to the third aspect of the present disclosure and depicts a computer implemented method for providing a data writing service for transactions that are associated with a blockchain, such as the data writer 302a seen in Figure 3 of the first aspect. The method of Figure 6 is implemented by a platform processor associated with an application programming interface (API). This figure is related to a request to append a new event to an existing event stream ES on the blockchain.

Step 602 depicts receiving a request from a client, the request being to amend an existing stream ES identified in the request and implemented in the blockchain. The request from the client is in a Hypertext Transfer Protocol (HTTP) transmission protocol format, as with the first and second aspects. As discussed in relation to step 504 of Figure 5, the event stream ES on the blockchain is associated with a key chain K such that $K = K_{n=0 \text{ to } N}$, where n is an integer from 0 to N , each integer n representing a current length or current number of events associated with the event stream ES, where N represents a maximum or final value of n . In

some embodiments, authentication and authorization checks are performed, which may be a test for the presence of an API access token, or a session check or a password /digital signature test, or some other appropriate method to validating the client or the service request made.

In step 604, the current length n of the event stream ES is determined.

Step 606 depicts identifying or obtaining data associated with an event E_n , this being the event to be currently added or appended to the event stream ES on the blockchain based on event data in the received request in step 602.

In step 608, a previous blockchain transaction TX_{n-1} associated with the event stream ES is identified. Once identified, a key pair K_{n-1} associated with the identified previous transaction TX_{n-1} is then determined. As mentioned above, this is based on the same seed key pair K set out in step 602.

In step 610 a key pair K_n for the current event E_n is derived from the seed key pair K .

Step 612 depicts creating a current blockchain transaction TX_n for the new event stream ES where $0 < n < N$ by one or more processors associated with the platform processor implementing the data writer. The blockchain transaction TX_n created for the current event E_n to be appended to the event stream ES includes:

- a first input spending a dust output associated with the previous transaction TX_{n-1} , said spend authorised with the obtained key pair K_{n-1} for the previous transaction obtained in step 608;
- a first unspent transaction output ($UTXO_{n_dust}$) being a dust output for the current transaction TX_n , said dust output associated with a locking script secured with the derived key pair K_n from step 610; and
- a final unspent transaction output ($UTXO_{n_data}$) associated with event data representing the current event E_n .

As mentioned above, A dust output is associated with a (digital asset) value that is below a defined limit for a transaction or having a defined minimum value. There may also be other inputs associated with digital assets based on an operational float. This float may be controlled by the platform processor. It is also possible to have other outputs in the transaction that are digital asset change outputs.

Thus, in some embodiments, an Update template for a blockchain transaction to update an event stream as per the present embodiment is one where the first input must be dust and the first output must be dust. This is to advantageously indicate the presence of a previous entry in the event stream. This also indicates that the event in question E_n (the present or current event data) comes after the previous transaction or state. Thus, the transaction advantageously follows the dust chain and comes before the next state. The Update template includes a data carrier, i.e. a data output that carries the event data or a result associated with the current event or state. This may be an un-spensible OP_RETURN output.

The use of dust outputs in the transaction is advantageous for maintaining an immutable sequential record of all transactions as they occur for an event stream ES in the blockchain. This is because, although by posting transactions to the blockchain all blockchain transactions would be time-stamped and remain in order in the blockchain, this does not guarantee preservation of their sequential order. This is because transactions might be mined into blocks at different times. The use of a dust output of a previous transaction being spent as the first input of a current transaction, where the spend is based on respective unique keys pertaining to the locking/unlocking scripts of each transaction ensures a clear, sequential tamper proof record of the event stream in chronological order.

Step 614 depicts submitting the transaction TX_n to the blockchain. Here the transaction may be submitted to the blockchain, such as the Bitcoin SV network for inclusion in a subsequent block by a miner node or BSV node software associated with the platform processor. In some embodiments, once mined, the transaction identifier may be used to uniquely identify the event stream ES.

Step 616 depicts sending a result associated with the created event stream ES in TX_n to the client, the result being provided in the HTTP transmission protocol format. The result may be copied or saved separately to the blockchain. In some embodiments, this may be based on the event data in the final unspent transaction output ($UTXO_{n_data}$). In some embodiments, the event data for the event E_n in ($UTXO_{n_data}$) includes a hash of said event data, thereby ensuring that this is kept private by the platform processor. The hash may be applied by the platform processor or be applied by the client, i.e. applied in some embodiments prior to generating the event data pertaining to the request that is received at the platform processor in step 602 for the event E_n . In the case of it being applied by the client, the event data in the request is private even before it reaches the platform processor. In other embodiments, the event data may be provided as raw data, publicly available from the blockchain.

Figure 7 relates to the third aspect of the present disclosure and depicts a computer implemented method for providing a data writing service for transactions that are associated with a blockchain, such as the data writer 302a seen in Figure 3 of the first aspect. The method of Figure 7 is implemented by a platform processor associated with an application programming interface (API). The request in Figure 7 is to terminate an existing event stream on the blockchain.

Step 702 depicts receiving a request from a client, the request relating to the termination of an existing event stream ES implemented using the blockchain. The request from the client being in a Hypertext Transfer Protocol (HTTP) transmission protocol format, as with the first and second aspects. As discussed in relation to step 504 of Figure 5, the event stream ES on the blockchain is associated with a key chain K such that $K = K_{n=0 \text{ to } N}$, where n is an integer from 0 to N , each integer n representing a current length or current number of events associated with the event stream ES, where N represents a maximum or final value of n . In some embodiments, authentication and authorization checks are performed, which may be a test for the presence of an API access token, or a session check or a password /digital signature test, or some other appropriate method to validating the client or the request made.

In step 704, the current length N of the event stream ES is determined.

Step 706 depicts identifying or obtaining data associated with a final event E_N , this being for the event to be currently added or appended to the event stream ES on the blockchain based on event data in the request received in step 702.

In step 708, a previous blockchain transaction TX_{N-1} associated with the event stream ES is identified. Once identified, a key pair K_{N-1} associated with the identified previous transaction TX_{N-1} is then determined. As mentioned above, this is based on the same seed key pair K set out in step 702.

In step 710 a key pair K_N for the current event E_N is derived from the seed key pair K .

Step 712 depicts creating a current blockchain transaction TX_N for the new event stream ES where $n=N$ by one or more processors associated with the platform processor implementing the data writer. The blockchain transaction TX_N created for the current event E_N to terminate the event stream ES includes:

- a first input spending a dust output associated with the previous transaction TX_{N-1} , said spend authorised with the obtained key pair K_{N-1} for the previous transaction obtained in step 708;
- a first unspent transaction output ($UTXO_N$) associated with a digital asset that is above a defined dust output limit.

For the final event, all transaction outputs return change. There is no dust output as there is no requirement or need to track the next stage of the terminated event stream. Thus, no dust output is provided by the platform processor when $n=N$. In other words, the outputs may be considered as a change output (digital asset payment) associated with the event stream ES. This advantageously marks or indicates the final terminated state of the event stream being tracked. In some embodiments, there is also no event data or data carrier element, i.e. no OP_RETURN for event data, for the output as the event or contract is in a terminated state. Thus, separate dust and data carrier outputs are not generated to terminate the event stream ES and the first output is above the dust limit to signal that this is the end of the event stream on the blockchain, along with the absence of an event data output which also indicates termination. In embodiments where there is metadata in the OP_RETURN instead of event data, this metadata may be helpful to a verifying entity. There may be other inputs or change outputs associated with a digital asset from an operational float. In some embodiments, the value of the digital asset associated with the dust set out in relation to Figures 5 and 6 may simply be added to the one or more other outputs.

Thus, in some embodiments, a Close template for a blockchain transaction to terminate an event stream as per the present embodiment is one where the first input must be dust, like the first input of the Update template in Figure 6. The first output must not be dust, and this advantageously acts as an end-of-ledger marker and furthermore distinguishes the Close template from the Update template. Like the Create template in Figure 5, there may be no data carrier for event data, but the OP_RETURN may include metadata in the Close template.

Step 714 depicts submitting the transaction TX_N to the blockchain. Here the transaction may be submitted to the blockchain, such as the Bitcoin SV network for inclusion in a subsequent block by a miner node or BSV node software associated with the platform processor.

Step 716 depicts sending a result associated with the created event stream ES in TX_N to the client, the result being provided in the HTTP transmission protocol format.

Figure 8 relates to the third aspect of the present disclosure and depicts a computer implemented method for accessing a platform or a data writing service for writing data into an

event stream associated with a blockchain, such as the platform 100 shown in Figure 1 or platform 300 in Figure 3. The method of Figure 8 is implemented by one or more processors associated with a client.

In step 802, the application programming interface (API) endpoint associated with the platform is identified. As mentioned before, this may be the API associated with a host platform processor, and there may be one or more further processors responsible for implementing the service, that each have a service endpoint or a destination address.

In step 804, the client prepares a request for a service, such as the data writing service 302 in Figure 3. The request is associated with one or more events E_n pertaining to an event stream ES in the blockchain. The client in some embodiment includes a client alias or identifier and/or a service identifier in the request, so that the request can be routed to the correct service endpoint, and so that the platform processor can check the validity of the requesting client and the client's permission to use the requested service.

In step 806, the request prepared in step 804 is sent using a Hypertext Transfer Protocol (HTTP) or similar transmission protocol format, as the platform processor is implemented as a HTTP or REST API.

In step 808, a result is received that pertains to an output script of a blockchain transaction associated with the event E_n in the request. This result is provided to the client in the HTTP transmission protocol format. In some embodiments, the result may be saved in a log separately to the blockchain, either in or associated with the platform processor.

Advantageously, the implementation of an event stream and its sequential log associated with the blockchain as implemented by the methods of the third aspect of the present disclosure offers guarantees relating to immutability of events and immutability of event sequencing. Once written, any attempt to tamper with the event stream in any of the following ways is either prevented or made evident:

- Changing the contents of an event
- Re-ordering events
- Inserting events at the start or middle of a stream
- Removing events from anywhere in the stream

In other words, the methods according to the third aspect makes the following attributes relating to the event stream provable:

- Individual entries in the event stream have not been modified since they were written
- No entries have been inserted between previously contiguous entries
- No entries have been removed
- No entries have been re-ordered

These properties and advantages have many practical applications, from audit/compliance logs, to state machine replication, to more efficient, tamper resistance and accurate methods for reading from and writing data into the blockchain for all clients.

An example for an event stream for which capture of an event log would be useful is an application to track and record the event of a game, such as Noughts O and Crosses X using the blockchain.

For instance, consider the game up to $n=4$ (5 states from 0 to 4) is in the following state:

	A	B	C
1	O		O
2		O	
3	X		X

As the game proceeds, by the method of the third aspect, a log based on the output of the blockchain transactions may be recorded as follows:

0	B2
1	A3
2	A1
3	C3
4	C1

Consider that there is an attempt to tamper with or change a copy of a log this is maintained for this sequence, such as insert a different entry for the result when $n=4$ so that the log does not reflect the actual state of the game – as given below:

0	B2
1	A3
2	A1
3	C3
4	B3
4	C1

This will be immediately identified from a check or audit of the automatically generated sequential log of the event stream on the blockchain, as the input of the transaction that spends the dust output for a transaction where $n=3$ will not be validated. It will be appreciated that where such games involve financial transactions (e.g. pay to play), there may be a desire from players to check the veracity of their game logs and whether or not a given games provider is adhering to the odds or difficulty that they are advertising. By storing individual game entries (or hashes thereof) for a given game in an event stream as described above, players can be assured that in-game events can be checked and verified independently of any internal system maintained by the games provider.

It will be further appreciated that each event in a given event stream need not correspond to individual events occurring within a gaming session. An event stream may be defined for any log of events where an accurate, sequential, tamper-proof log of said events is desirable. Examples of events in a given event stream may include, e.g. inputs and / or outputs of a given smart-contract being executed locally or remotely (preferably off-chain); messages sent between two or more participants of a given online messaging conversation; physical measurements performed by sensors or IoT devices for measuring e.g. weather, locations of e.g. vehicles, goods, people, etc.; drug / medicine tracking— including e.g. source of manufacture, transportation, dispenser location, prescribed dosage, recipient information, etc.; financial transactions, such as e.g. an amount an account is credited and / or debited (regardless of whether the account is credited with cryptocurrency or fiat), changes in exchange rate, execution of trades, requests for the purchasing of goods or shares, etc. Ultimately, the context in which the event stream is generated and used will be at the leisure of the party using the platform processor to generate such an event stream.

Turning now to Figure 9, there is provided an illustrative, simplified block diagram of a computing device 2600 that may be used to practice at least one embodiment of the present disclosure. In various embodiments, the computing device 2600 may be used to implement any of the systems illustrated and described above. For example, the computing device 2600 may be configured to be used as one or more components of DBMS of figure, or the computing device 2600 may be configured to be a client entity that is associated with a given user, the client entity making database requests for a database that is managed by the DBMS of Figure 9. Thus, computing device 2600 may be a portable computing device, a personal computer, or any electronic computing device. As shown in Figure 9, the computing device 2600 may include one or more processors with one or more levels of cache memory and a memory controller (collectively labelled 2602) that can be configured to communicate with a storage subsystem 2606 that includes main memory 2608 and persistent storage 2610. The main memory 2608 can include dynamic random-access memory (DRAM) 2618 and read-only memory (ROM) 2620 as shown. The storage subsystem 2606 and the cache memory 2602 and may be used for storage of information, such as details associated with transactions and blocks as described in the present disclosure. The processor(s) 2602 may be utilized to provide the steps or functionality of any embodiment as described in the present disclosure.

The processor(s) 2602 can also communicate with one or more user interface input devices 2612, one or more user interface output devices 2614, and a network interface subsystem 2616.

A bus subsystem 2604 may provide a mechanism for enabling the various components and subsystems of computing device 2600 to communicate with each other as intended. Although the bus subsystem 2604 is shown schematically as a single bus, alternative embodiments of the bus subsystem may utilise multiple buses.

The network interface subsystem 2616 may provide an interface to other computing devices and networks. The network interface subsystem 2616 may serve as an interface for receiving data from, and transmitting data to, other systems from the computing device 2600. For example, the network interface subsystem 2616 may enable a data technician to connect the device to a network such that the data technician may be able to transmit data to the device and receive data from the device while in a remote location, such as a data centre.

The user interface input devices 2612 may include one or more user input devices such as a keyboard; pointing devices such as an integrated mouse, trackball, touchpad, or graphics

tablet; a scanner; a barcode scanner; a touch screen incorporated into the display; audio input devices such as voice recognition systems, microphones; and other types of input devices. In general, use of the term “input device” is intended to include all possible types of devices and mechanisms for inputting information to the computing device 2600.

The one or more user interface output devices 2614 may include a display subsystem, a printer, or non-visual displays such as audio output devices, etc. The display subsystem may be a cathode ray tube (CRT), a flat-panel device such as a liquid crystal display (LCD), light emitting diode (LED) display, or a projection or other display device. In general, use of the term “output device” is intended to include all possible types of devices and mechanisms for outputting information from the computing device 2600. The one or more user interface output devices 2614 may be used, for example, to present user interfaces to facilitate user interaction with applications performing processes described and variations therein, when such interaction may be appropriate.

The storage subsystem 2606 may provide a computer-readable storage medium for storing the basic programming and data constructs that may provide the functionality of at least one embodiment of the present disclosure. The applications (programs, code modules, instructions), when executed by one or more processors, may provide the functionality of one or more embodiments of the present disclosure, and may be stored in the storage subsystem 2606. These application modules or instructions may be executed by the one or more processors 2602. The storage subsystem 2606 may additionally provide a repository for storing data used in accordance with the present disclosure. For example, the main memory 2608 and cache memory 2602 can provide volatile storage for program and data. The persistent storage 2610 can provide persistent (non-volatile) storage for program and data and may include flash memory, one or more solid state drives, one or more magnetic hard disk drives, one or more floppy disk drives with associated removable media, one or more optical drives (e.g. CD-ROM or DVD or Blue-Ray) drive with associated removable media, and other like storage media. Such program and data can include programs for carrying out the steps of one or more embodiments as described in the present disclosure as well as data associated with transactions and blocks as described in the present disclosure.

The computing device 2600 may be of various types, including a portable computer device, tablet computer, a workstation, or any other device described below. Additionally, the computing device 2600 may include another device that may be connected to the computing device 2600 through one or more ports (e.g., USB, a headphone jack, Lightning connector,

etc.). The device that may be connected to the computing device 2600 may include a plurality of ports configured to accept fibre-optic connectors. Accordingly, this device may be configured to convert optical signals to electrical signals that may be transmitted through the port connecting the device to the computing device 2600 for processing. Due to the ever-changing nature of computers and networks, the description of the computing device 2600 depicted in Figure 9 is intended only as a specific example for purposes of illustrating the preferred embodiment of the device. Many other configurations having more or fewer components than the system depicted in Figure 9 are possible.

Enumerated Example Embodiments

The present disclosure is hereby discussed based on the following clauses that are related to the above aspects, which are provided herein as exemplary embodiments for better explaining, describing and understanding the claimed aspects and embodiments.

1. A computer implemented method for providing a platform of a plurality of services that are associated with a blockchain, the platform being provided for a plurality of clients, the method implemented by a platform processor associated with an application programming interface (API), the method comprising the steps of:
receiving a request from a given client among the plurality of clients, the request pertaining to a given service among the plurality of services, the request from the given client being based on a Hypertext Transfer Protocol (HTTP) transmission protocol format;
based on a determination that the client identity and/or request is/are valid, obtaining a destination address associated with the given service;
processing the request for the given service based on at least one blockchain transaction corresponding to the obtained destination address to obtain an output script; and
sending a result associated with the output script to the given client, the result being provided based on the HTTP transmission protocol format.
2. The method as set out in clause 1 wherein platform processor is implemented as an HTTP API endpoint.
3. The method as set out in clause 2 wherein the platform processor is implemented as a Representational State Transfer (REST) endpoint.

4. The method as set out in any preceding clause wherein the platform processor comprises or is associated with a plurality of processors, each configured for implementing a given service among the plurality of services on the blockchain, and each associated with a specific destination address or endpoint that is unique to the respective processor.
5. The method as set out in any preceding wherein the platform processor is associated with an API converter, the API converter is configured for performing the steps of:
 - receiving the request from the given client in the HTTP transmission protocol format;
 - converting a received request to a Remote procedure Call (RPC) format, and sending the RPC request to a given processor among the plurality of processors that is configured to implement the given service identified in the received request;
 - receiving a response associated with at least one blockchain transaction from the given processor in an RPC format; and
 - converting the respective response to be sent to the client using the HTTP transmission protocol.
6. The method as set out in any preceding clause wherein the received request is a HTTP GET or POST or PUT or PATCH request that includes or is associated with a client identifier for the given client and a service identifier for the given service requested, and wherein the result sent to the client is a HTTP POST request based on the client identifier for the given client.
7. The method as set out in clause 6 comprising validating the client based on the client identifier and a record corresponding to the client identifier, the record associated with the platform processor; and
based on a successful validation of the client, determining if the received request from the client is valid based on the service identifier and an attribute or setting included in the respective record.
8. The method as set out in clauses 6 or 7 wherein the client identifier is an alias that is provided for a given client, the alias being specific to the given client and provided by an alias-based addressing service, the addressing service having a machine readable resource that is accessible from a defined or well-known location, the machine readable resource including one or more capabilities pertaining to the given client.

9. The method as set out in clause 8 wherein the alias is associated with a domain name for the given client.

10. The method as set out in any preceding clause wherein the platform includes at least one or more of the following services implemented using the blockchain:

data services for writing/submitting data into the blockchain to alter a state of the blockchain;

data services for reading/obtaining data reflecting the current state of the blockchain;

services associated with simplified payment verification for transactions associated with the blockchain;

services associated with the management of one or more event streams and/or smart contracts associated with the blockchain;

services associated with the management of a digital wallet framework for a plurality of clients associated with the blockchain.

11. A computer implemented method for accessing a platform of a plurality of services that are associated with a blockchain, the platform being provided for a plurality of clients, the method implemented by one or more processors of a given client among the plurality of clients, the method comprising the steps of:

obtaining or identifying an application programming interface (API) endpoint associated with one or more processors associated with the platform;

sending a request pertaining to a given service among the plurality of services, the request including associated with a client identifier for the given client and a service identifier for the given service requested, wherein the request is sent based on a Hypertext Transfer Protocol (HTTP) transmission protocol format; and

receiving a result pertaining to an output script of a blockchain transaction associated with the request, said result being provided to the client based on the HTTP transmission protocol format.

12. A computer implemented method for implementing a data writing service for transactions associated with a blockchain, the method implemented by a platform processor associated with an application programming interface (API), the method comprising the steps of:

receiving a request from a client, the request relating to an event stream ES implemented using the blockchain, the request from the client being based on a Hypertext Transfer Protocol (HTTP) transmission protocol format;

determining a current state of the event Stream $ES_{i=n}$, wherein i is an integer from 0 to N , each integer i representing a given state of the event stream ES , whereby $i = 0$ represents the created event stream ES , $i = n$ represents the event stream ES in a current state in the blockchain, and $i = N$ represents a final state of the event stream ES ;

processing a new event E_{n+1} for the event stream ES based on the received request by the steps of:

creating a blockchain transaction TX_{n+1} , the blockchain transaction TX_{n+1} including:

an input associated with a transaction output (TXO_n) from a previous transaction TX_n ; and

an unspent output ($UTXO_{n+1}$) associated with event data representing the new event E_{n+1} ;

submitting the transaction TX_{n+1} to the blockchain;

wherein, responsive to said submission the method includes updating the current state of the event stream to be $ES_{i=n+1}$ based on the newly created event E_{n+1} , such that $ES_{i=n} = ES_{n+1}$; and

sending a result based on the updated current state ES_{n+1} , the result being provided based on the HTTP transmission protocol format.

13. A computer implemented method for implementing an event stream associated with a blockchain, the method implemented by a platform processor associated with an application programming interface (API), the method comprising the steps of:

receiving a request from a client relating to an event stream ES , the request received based on a Hypertext Transfer Protocol (HTTP) transmission protocol format;

determine a current length n of the event stream E ;

wherein if $n = 0$, then the method comprises:

identifying an event E_n for the event stream in the received request as a first event to create the event stream ES ;

processing the received event E_n by creating a blockchain transaction including a first unspent output $UTXO_{0_dust}$ that is a dust output;

wherein if $0 < n < N$, where N is the final or maximum value for, then the method comprises:

identifying an event E_n for the event stream in the received request a current event to amend the event stream ES ;

processing the received event E_n by creating a blockchain transaction including:

a first input spending a dust output associated with a previous transaction for the event stream ES ;

a first unspent transaction output $UTXO_{n_dust}$ being a dust output; and

a final unspent transaction output $UTXO_{n_data}$ associated with event data representing the current event E_n ;

wherein if $n = N$, then the method comprises:

identifying an event E_n for the event stream in the received request as a final event to create the terminate the stream ES; and

processing the received event E_n by creating a blockchain transaction including:

a first input spending a dust output associated with a previous transaction for the event stream ES; and

a final unspent output $UTXO_N$ that is associated with a digital asset that more than a defined dust output value;

the method comprising:

submitting the created transaction to the blockchain; and

sending a result associated with the event stream ES in TX_0 to the client, the result being provided based on the HTTP transmission protocol format.

14. A computer implemented method for creating an event stream associated with a blockchain, the method implemented by a platform processor associated with an application programming interface (API), the method comprising the steps of:

receiving a request from a client relating to a new event stream ES, the request received based on a Hypertext Transfer Protocol (HTTP) transmission protocol format;

determining a hierarchical deterministic key chain K to be used with the new event stream ES, wherein the key chain K includes a series of private/public key pairs derived from a selected parent key pair, such that $K = K_{n=0 \text{ to } N}$, whereby n is an integer from 0 to N, each integer n representing a current length or current number of events associated with event stream ES, and N represents a maximum or final value of n;

creating a first blockchain transaction TX_0 for the new event stream ES where $n = 0$, the blockchain transaction including:

a first unspent transaction output ($UTXO_{0_dust}$) being a dust output, said dust output associated with a locking script secured with a first derived key pair K_0 from the key chain K;

submitting the transaction TX_0 to the blockchain; and

sending a result associated with the created event stream ES in TX_0 to the client, the result being provided based on the HTTP transmission protocol format.

15. A computer implemented method for updating an event stream associated with a blockchain, the method implemented by a platform processor associated with an application programming interface (API), the method comprising the steps of:

receiving a request from a client to update an existing event stream ES associated with the blockchain, the request received based on a Hypertext Transfer Protocol (HTTP) transmission protocol format, and wherein the event stream ES is associated with a key chain K such that $K = K_{n=0 \text{ to } N}$, where n is an integer from 0 to N, each integer n representing a current length or current number of events associated with the event stream ES, where N represents a maximum or final value of n;

determining a current length n of the event stream ES;

from the request, obtaining a current event E_n to be appended to the event stream ES;

identifying a previous blockchain transaction TX_{n-1} associated with the event stream ES;

obtaining a key pair K_{n-1} associated with the identified previous transaction TX_{n-1} ;

deriving a key pair K_n for the current event E_n ;

creating a current blockchain transaction TX_n for the current event E_n to be appended to the event stream ES where $0 < n < N$, the current blockchain transaction including:

a first input spending a dust output associated with the previous transaction TX_{n-1} , said spend authorised with the obtained key pair K_{n-1} for the previous transaction;

a first unspent transaction output ($UTXO_{n_dust}$) being a dust output for the current transaction TX_n , said dust output associated with a locking script secured with the derived key pair K_n ; and

a final unspent transaction output ($UTXO_{n_data}$) associated with event data representing the current event E_n ;

submitting the transaction TX_n to the blockchain; and

sending a result associated with the updated event stream ES to the client, the result being provided based on the HTTP transmission protocol format.

16. The method as set out in clause 15 where the event data for the event E_n in the final unspent transaction output ($UTXO_{n_data}$) for the current blockchain transaction TX_n includes a hash of said event data.

17. The method as set out in clause 16 where the hash of said event data is applied by the platform processor.

18. The method as set out in clause 16 where the hash of said event data is applied by the client device prior to being included in the request that is received by the platform processor.

19. The method as set out in clause 15 where the event data for the event E_n in the final unspent transaction output ($UTXO_{n_data}$) for the current blockchain transaction TX_n includes raw event data.

20. A computer implemented method for terminating an event stream associated with a blockchain, the method implemented by a platform processor associated with an application programming interface (API), the method comprising the steps of:

receiving a request from a client to terminate an existing event stream ES associated with the blockchain, the request received based on a Hypertext Transfer Protocol (HTTP) transmission protocol format, and wherein the event stream ES is associated a key chain K such that $K = K_{n=0 \text{ to } N}$, where n is an integer from 0 to N, each integer n representing a current length or current number of events associated with the event stream ES, where N represents a maximum or final value of n;

determining a current length $n = N$ of the event stream ES;

from the request, obtaining a final event E_N to be appended to the event stream ES;

identifying a previous blockchain transaction TX_{N-1} associated with the event stream ES;

obtaining a key pair K_{N-1} associated with the previous transaction TX_{N-1} ;

deriving a key pair K_N for the final event E_N ;

creating a final blockchain transaction TX_N for the final event E_N to be appended to the event stream ES, the final blockchain transaction including:

a first input spending a dust output associated with the previous transaction TX_{N-1} , said spend authorised with the obtained key pair K_{N-1} for the previous transaction;

a first unspent transaction output ($UTXO_N$) associated with a digital asset that is above a defined dust output limit;

submitting the transaction TX_N to the blockchain; and

sending a result associated with the terminated event stream ES to the client, the result being provided based on the HTTP transmission protocol format.

21. The method as set out in any one of clauses 12 to 19 wherein the result associated with the event stream ES includes a certificate confirming at least one of the following :

- a transaction identifier within which the event E_n was submitted to the blockchain;
- a Merkle inclusion proof of the transaction to a header in the blockchain
- a copy of the block header in which said transaction was included

22. The method as set out in any one of clauses 12 to 21 wherein the step of submitting comprises including the created transaction in a subsequent block associated with the blockchain to be mined.

23. The method as set out in any one of clauses 12 to 22 wherein the created blockchain transaction further comprises
an input associated with a digital asset; and
one or more change outputs associated with the digital asset.

24. The method as set out in clause 23 wherein the digital asset is associated with an operational float.

25. The method as set out in any one of clauses 12 to 24 comprising the step of identifying the event stream ES based on a transaction identifier associated with the submitted blockchain transaction.

26. The method as set out in any one of clauses 12 to 25 comprising the step of identifying a state associated with the event stream ES based on a transaction identifier associated with the submitted blockchain transaction.

27. The method as set out in any one of clauses 12 to 26 wherein the event stream is used to represent a smart contract on the blockchain.

28. The method as set out in clause 27 wherein the smart contract is implemented as a Finite State Machine(FSM).

29. The method as claimed in any one of clauses 13 to 28 comprising storing a copy or a record or a log that is based on the result(s) for each event of the event stream in an off-chain storage resource.

30. A computer implemented method for writing data associated with an event stream in a blockchain, the method implemented by one or more processors of a given client among a plurality of clients, the method comprising the steps of:
obtaining or identifying an application programming interface (API) endpoint associated with one or more processors associated with a platform for providing a data writing service;

sending a request for one or more events E_n pertaining to an event stream, wherein the request is sent based on a Hypertext Transfer Protocol (HTTP) transmission protocol format; and

receiving a result associated with an output script of a blockchain transaction pertaining to the requested event E_n , said result being received based on the HTTP transmission protocol format.

31. The method as set out in clause 30 comprising applying a hash function to event data for the event E_n , such that the request includes the hashed event data for the event E_n .

32. A computing device comprising a processor and memory, the memory including executable instructions that, as a result of execution by the processor, causes the device to perform the computer-implemented method as set out in any one of clauses 1 to 10 and 12 to 29, the computing device pertaining to a platform processor.

33. A computing device comprising a processor and memory, the memory including executable instructions that, as a result of execution by the processor, causes the device to perform the computer-implemented method as set out in any one of clauses 11, 30 or 31, wherein the computing device is pertaining to a client.

34. A computer system comprising:

at least one platform processor communicatively coupled to at least one client via a wireless communication network, the at least one platform processor associated with an application programming interface(API) endpoint for processing HTTP requests from the at least one client, the at least one platform processor implemented in accordance with the computing device as set out in clause 32 ; and the at least one client being implemented in accordance with the computing device as set out in clause 33.

35. A computer-readable storage medium having stored thereon executable instructions that, as a result of being executed by a processor of a computer, cause the computer to perform the method of any one of clauses 1 to 31.

It should be noted that the above-mentioned aspects and embodiments illustrate rather than limit the disclosure, and that those skilled in the art will be capable of designing many alternative embodiments without departing from the scope of the disclosure as defined by the appended claims. In the claims, any reference signs placed in parentheses shall not be

construed as limiting the claims. The word "comprising" and "comprises", and the like, does not exclude the presence of elements or steps other than those listed in any claim or the specification as a whole. In the present specification, "comprises" means "includes or consists of" and "comprising" means "including or consisting of". The singular reference of an element does not exclude the plural reference of such elements and vice-versa. The disclosure may be implemented by means of hardware comprising several distinct elements, and by means of a suitably programmed computer. In a device claim enumerating several means, several of these means may be embodied by one and the same item of hardware. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.

Claims:

1. A computer implemented method for implementing an event stream associated with a blockchain, the method implemented by a platform processor associated with an application programming interface (API), the method comprising the steps of:

receiving a request from a client relating to an event stream ES, the request received based on a Hypertext Transfer Protocol (HTTP) transmission protocol format;

determine a current length n of the event stream E;

wherein if $n = 0$, then the method comprises:

identifying an event E_n for the event stream in the received request as a first event to create the event stream ES;

processing the received event E_n by creating a blockchain transaction including a first unspent output $UTXO_{0_dust}$ that is a dust output;

wherein if $0 < n < N$, where N is the final or maximum value for, then the method comprises:

identifying an event E_n for the event stream in the received request a current event to amend the event stream ES;

processing the received event E_n by creating a blockchain transaction including:

a first input spending a dust output associated with a previous transaction for the event stream ES;

a first unspent transaction output $UTXO_{n_dust}$ being a dust output; and

a final unspent transaction output $UTXO_{n_data}$ associated with event data representing the current event E_n ;

wherein if $n = N$, then the method comprises:

identifying an event E_n for the event stream in the received request as a final event to create the terminate the stream ES; and

processing the received event E_n by creating a blockchain transaction including:

a first input spending a dust output associated with a previous transaction for the event stream ES; and

a final unspent output $UTXO_N$ that is associated with a digital asset that more than a defined dust output value;

the method comprising:

submitting the created transaction to the blockchain; and

sending a result associated with the event stream ES in TX_0 to the client, the result being provided based on the HTTP transmission protocol format.

2. A computer implemented method for creating an event stream associated with a blockchain, the method implemented by a platform processor associated with an application programming interface (API), the method comprising the steps of:

receiving a request from a client relating to a new event stream ES, the request received based on a Hypertext Transfer Protocol (HTTP) transmission protocol format;

determining a hierarchical deterministic key chain K to be used with the new event stream ES, wherein the key chain K includes a series of private/public key pairs derived from a selected parent key pair, such that $K = K_{n=0 \text{ to } N}$, whereby n is an integer from 0 to N, each integer n representing a current length or current number of events associated with event stream ES, and N represents a maximum or final value of n;

creating a first blockchain transaction TX_0 for the new event stream ES where $n = 0$, the blockchain transaction including:

a first unspent transaction output ($UTXO_{0_dust}$) being a dust output, said dust output associated with a locking script secured with a first derived key pair K_0 from the key chain K;

submitting the transaction TX_0 to the blockchain; and

sending a result associated with the created event stream ES in TX_0 to the client, the result being provided based on the HTTP transmission protocol format.

3. A computer implemented method for updating an event stream associated with a blockchain, the method implemented by a platform processor associated with an application programming interface (API), the method comprising the steps of:

receiving a request from a client to update an existing event stream ES associated with the blockchain, the request received based on a Hypertext Transfer Protocol (HTTP) transmission protocol format, and wherein the event stream ES is associated with a key chain K such that $K = K_{n=0 \text{ to } N}$, where n is an integer from 0 to N, each integer n representing a current length or current number of events associated with the event stream ES, where N represents a maximum or final value of n;

determining a current length n of the event stream ES;

from the request, obtaining a current event E_n to be appended to the event stream ES;

identifying a previous blockchain transaction TX_{n-1} associated with the event stream ES;

obtaining a key pair K_{n-1} associated with the identified previous transaction TX_{n-1} ;

deriving a key pair K_n for the current event E_n ;

creating a current blockchain transaction TX_n for the current event E_n to be appended to the event stream ES where $0 < n < N$, the current blockchain transaction including:

a first input spending a dust output associated with the previous transaction TX_{n-1} , said spend authorised with the obtained key pair K_{n-1} for the previous transaction;
 a first unspent transaction output ($UTXO_{n_dust}$) being a dust output for the current transaction TX_n , said dust output associated with a locking script secured with the derived key pair K_n ; and
 a final unspent transaction output ($UTXO_{n_data}$) associated with event data representing the current event E_n ;
 submitting the transaction TX_n to the blockchain; and
 sending a result associated with the updated event stream ES to the client, the result being provided based on the HTTP transmission protocol format.

4. The method as claimed in claim 3 where the event data for the event E_n in the final unspent transaction output ($UTXO_{n_data}$) for the current blockchain transaction TX_n includes a hash of said event data.

5. The method as claimed in claim 4 where the hash of said event data is applied by the platform processor.

6. The method as claimed in claim 4 where the hash of said event data is applied by the client device prior to being included in the request that is received by the platform processor.

7. The method as claimed in claim 3 where the event data for the event E_n in the final unspent transaction output ($UTXO_{n_data}$) for the current blockchain transaction TX_n includes raw event data.

8. A computer implemented method for terminating an event stream associated with a blockchain, the method implemented by a platform processor associated with an application programming interface (API), the method comprising the steps of:

receiving a request from a client to terminate an existing event stream ES associated with the blockchain, the request received based on a Hypertext Transfer Protocol (HTTP) transmission protocol format, and wherein the event stream ES is associated a key chain K such that $K = K_{n=0 \text{ to } N}$, where n is an integer from 0 to N, each integer n representing a current length or current number of events associated with the event stream ES, where N represents a maximum or final value of n;

determining a current length $n = N$ of the event stream ES;

from the request, obtaining a final event E_N to be appended to the event stream ES;

identifying a previous blockchain transaction TX_{N-1} associated with the event stream ES;

obtaining a key pair K_{N-1} associated with the previous transaction TX_{N-1} ;

deriving a key pair K_N for the final event E_N ;

creating a final blockchain transaction TX_N for the final event E_N to be appended to the event stream ES, the final blockchain transaction including:

a first input spending a dust output associated with the previous transaction TX_{N-1} , said spend authorised with the obtained key pair K_{N-1} for the previous transaction;

a first unspent transaction output ($UTXO_N$) associated with a digital asset that is above a defined dust output limit;

submitting the transaction TX_N to the blockchain; and

sending a result associated with the terminated event stream ES to the client, the result being provided based on the HTTP transmission protocol format.

9. The method as claimed in any one of claims 1 to 8 wherein the result associated with the event stream ES includes a certificate confirming at least one of the following :

- a transaction identifier within which the event E_n was submitted to the blockchain;
- a Merkle inclusion proof of the transaction to a header in the blockchain
- a copy of the block header in which said transaction was included

10. The method as claimed in any one of claims 1 to 9 wherein the step of submitting comprises including the created transaction in a subsequent block associated with the blockchain to be mined.

11. The method as claimed in any one of claims 1 to 10 wherein the created blockchain transaction further comprises
an input associated with a digital asset; and
one or more change outputs associated with the digital asset.

12. The method as claimed in claim 11 wherein the digital asset is associated with an operational float.

13. The method as claimed in any one of claims 1 to 12 comprising the step of identifying the event stream ES based on a transaction identifier associated with the submitted blockchain transaction.

14. The method as claimed in any one of claims 1 to 13 comprising the step of identifying a state associated with the event stream ES based on a transaction identifier associated with the submitted blockchain transaction.
15. The method as claimed in any one of claims 1 to 14 wherein the event stream is used to represent a smart contract on the blockchain.
16. The method as claimed in claim 15 wherein the smart contract is implemented as a Finite State Machine(FSM).
17. The method as claimed in any one of claims 1 to 16 comprising storing a copy or a record or a log that is based on the result(s) for each event of the event stream in an off-chain storage resource.
18. A computer implemented method for writing data associated with an event stream in a blockchain, the method implemented by one or more processors of a given client among a plurality of clients, the method comprising the steps of:
obtaining or identifying an application programming interface (API) endpoint associated with one or more processors associated with a platform for providing a data writing service;
sending a request for one or more events E_n pertaining to an event stream, wherein the request is sent based on a Hypertext Transfer Protocol (HTTP) transmission protocol format;
and
receiving a result associated with an output script of a blockchain transaction pertaining to the requested event E_n , said result being received based on the HTTP transmission protocol format.
19. The method as claimed in claim 18 comprising applying a hash function to event data for the event E_n , such that the request includes the hashed event data for the event E_n .
20. A computing device comprising a processor and memory, the memory including executable instructions that, as a result of execution by the processor, causes the device to perform the computer-implemented method as claimed in any one of claims 1 to 17, the computing device pertaining to a platform processor.

21. A computing device comprising a processor and memory, the memory including executable instructions that, as a result of execution by the processor, causes the device to perform the computer-implemented method as claimed in any one of claims 18 or 19, wherein the computing device is pertaining to a client.

22. A computer system comprising:

at least one platform processor communicatively coupled to at least one client via a wireless communication network, the at least one platform processor associated with an application programming interface(API) endpoint for processing HTTP requests from the at least one client, the at least one platform processor implemented in accordance with the computing device as claimed in claim 20 ; and the at least one client being implemented in accordance with the computing device as claimed in claim 21.

23. A computer-readable storage medium having stored thereon executable instructions that, as a result of being executed by a processor of a computer, cause the computer to perform the method of any one of claims 1 to 19.