(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 1 August 2017 (31.08.2017)

(10) International Publication Number
WO 2017/145047 Al

(51) International Patent Classification:
H04L 9/30 (2006.0 1) *H04L 9/32* (2006.0 1)

(21) International Application Number:
PCT/IB20 17/050978

(22) International Filing Date:
2 1 February 2017 (21 .02.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

1603 117. 1	23 February 2016 (23.02.2016)	GB
1607484. 1	29 April 2016 (29.04.2016)	GB
1619301 .3	15 November 2016 (15. 11.2016)	GB

(71) Applicant: NCHAIN HOLDINGS LIMITED [AG/AG]; Fitzgerald House, 44 Church Street, St. John's (AG).

(72) Inventors: WRIGHT, Craig Steven; c/o Urquhart-Dykes & Lord LLP, 7th Floor Churchill House, Churchill Way, Cardiff CF10 2HH (GB). SAVANAH, Stephane; c/o Urquhart-Dykes & Lord LLP, 7th Floor Churchill House, Churchill Way, Cardiff CF10 2HH (GB).

(74) Agent: JONES, Cerian; 7th Floor, Churchill House, Churchill Way, CARDIFF CF10 2HH (GB).

(81) Designated States *(unless otherwise indicated, for every kind cf national protection available):* AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, EST, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind cf regional protection available):* ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: BLOCKCHAIN-IMPLEMENTED METHOD FOR CONTROL AND DISTRIBUTION OF DIGITAL CONTENT

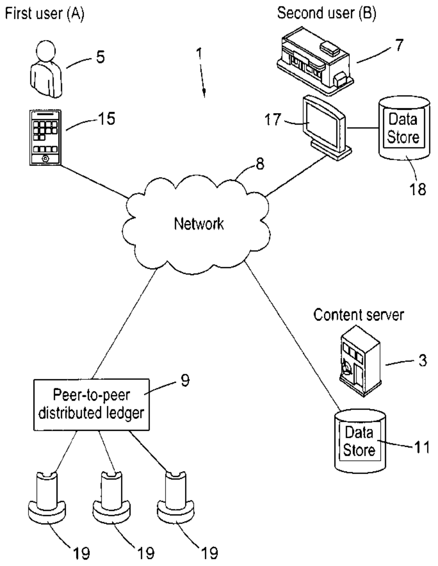


Fig. 1

(57) Abstract: The disclosure relates to a blockchain-implemented system and method of controlling the transmission and/or distribution of digital content. In an illustrative embodiment, the blockchain is the Bitcoin blockchain. The first user (5) is associated with a deposit quantity of cryptocurrency at a common address (23), wherein to spend from the common address requires signatures of both a first private key of the first user (5) and a second private key of the second user (7). The system (1) comprises a first node (15) and a second node (17).- The first node (15) is associated with a first user (5) comprising a first processing device configured to: (A) send, over a communications network (8), a request to the second node (17) to provide an episode of digital content from a series of digital content; (B) determine a payment transaction (27) to transfer from a common address (23) a payment quantity of cryptocurrency to the second user (7), wherein the payment quantity of cryptocurrency is based on a quantity of episodes of digital content in the series of digital content requested by the first user (5); and (C) sign, with the first private key (V), the payment transaction (27) and subsequently send the payment transaction (27) to the second node (17). The second node (17) is associated with the second user (7) comprising a second processing device configured to: (I) receive, over the communications network (8), the request from the first node (15) to provide the episode of digital content and the payment transaction (27), signed with the first private key; (Π) verify the payment transaction, comprising verifying that the payment transaction includes the payment quantity of cryptocurrency to the second user (7), and based on the result of verifying the second processing device is further configured to: (III) provide access, over the communications network (8), to the episode of digital content (i) to be available to the first node (15); and (IV) co-sign, with the second private key of the second user (5), the payment transaction and send the co-signed payment transaction to a distributed ledger (blockchain) (9).

"Blockchain-implemented Method for Control and Distribution of Digital Content"

Technical Field

[1] The present disclosure relates to a system and methods of payment and distribution of digital content from a series of digital content. The present disclosure may have application for digital rights management for online digital media but is not limited in this regard.

Background

[2] 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 to 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.

[3] 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 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; and ii) added to a new block built by a miner; and iii) mined, i.e. added to the public ledger of past transactions.

[4] Although blockchain technology is most widely known for the use of cryptocurrency implementation, digital entrepreneurs have begun 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.

[5] 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.

[6] 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 discernable meaning or value. The token thus serves as an identifier that allows the real-world item to be referenced from the blockchain.

[7] Digital rights management concerns controlling digital media that is subject to copyright, including control technology to restrict the use, modification and distribution of digital media. Digital media may include content that is serialised, such as sequential content like a magazine, newspaper, podcasts, soap opera, television series, etc.

[8] Implementation of digital rights management may include management of copyright work through a larger central system or multiple systems, with key exchange to create trust between nodes associated with respective users. Such systems may be hard to manage and ongoing maintenance of access rights may be difficult to achieve. In some alternatives, a trusted third party (such as certificate authorities) may be used to create hierarchies. However some of these systems may create large single points of failure that may be vulnerable to attack.

[9] In this document we use the term 'blockchain' to include all forms of electronic, computer-based, distributed ledgers. These include, but are not limited to consensus-based blockchain and transaction-chain technologies, permissioned and un-permissioned ledgers, shared ledgers 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 invention is not limited to use with the Bitcoin blockchain and alternative blockchain implementations and protocols fall within the scope of the present invention.

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

[11] Any discussion of documents, acts, materials, devices, articles or the like which has been included in the present specification is not to be taken as an admission that any or all of these matters form part of the prior art base or were common general knowledge in the field relevant to the present disclosure as it existed before the priority date of each claim of this application.

Summary

[12] The present invention provides methods and systems as defined in the appended claims.

[13] The invention may provide a control method and corresponding system, arranged to control the transmission and/or distribution of data. The transmission may be conducted via or over a computer-implemented or telecommunications network. The data may be digital content. The invention may provide a method/system which incorporates cryptographic and/or encryption techniques to secure the distribution/transmission of the data. Thus, the invention may provide an enhanced security solution for the communication of data.

[14] The term "episode" may be used interchangeably herein with the term "portion". However, the digital content that is transmitted, distributed and/or controlled by the invention may not be limited to an instalment, logical chapter or episode of broadcast media or artistic content. The term "episode" herein and in the claims simply means "portion" or "unit" or "amount" of digital content. Similarly, the term "series" is not used herein to mean simply a series in the sense of broadcast series. The series may simply be a plurality, group or association of portions of digital content. "Series" is not limited to or necessarily indicative of sequential or chronological order. In addition, the invention is not limited with regard to the nature or form of the digital content. The digital content may not be limited to entertainment media, but may relate to any type of digital content.

[15] The invention may provide a system wherein a first user is associated with a quantity of cryptocurrency at a common address. The cryptocurrency may be referred to as a "deposit quantity". The address may be an address on a network. It may be a blockchain address. It may be derived from or associated with a cryptographic key. To spend from the common address may require (digital) signatures of at least a first private key (Vi) of the first user and a second private key (V_2) of the second user. This may be specified by the use of given type of blockchain transaction. The transaction type may be part of, or defined within, a blockchain protocol.

[16] The system may comprise:

-a first node associated with a first user comprising a first processing device configured to:

(A) send, over a communications network, a request to the second node to provide an episode of digital content (i) from a series of digital content;

(B) determine and/or generate a blockchain transaction (E_i) to transfer from a common address a payment quantity of cryptocurrency (B2) to the second user, wherein the payment quantity of cryptocurrency (B2) is based on a quantity of episodes of digital content in the series of digital content requested by the first user; and

(C) sign, with the first private key (Vi), the payment transaction (Ei) and subsequently send the payment transaction (Ei) to the second node;

- a second node associated with the second user comprising a second processing device configured to:

(I) receive, over the communications network, the request from the first node to provide the episode of digital content (*i*) and the payment transaction (Ei), signed with the first private key (Vi);

(II) verify the payment transaction, comprising verifying that the payment transaction includes the payment quantity of cryptocurrency (B2) to the second user, and based on the result of verifying the second processing device is further configured to:

(III) provide access, over the communications network, to the episode of digital content (*i*) to be available to the first node; and

(IV) co-sign, with the second private key (V_2) of the second user, the payment transaction and send the co-signed payment transaction to a peer-to-peer distributed ledger.

[17] In the system, the first processing device may be further configured to request a next episode of digital content from the series of digital content by repeating steps (A) to (C). The second processing device may be further configured to receive the request and distribute the next episode of digital content by repeating steps (I) to (III), wherein the step (IV) to co-sign and send the payment transaction to the peer-to-peer distributed ledger performed on a payment transaction having a quantity of episodes of digital content that includes the next episode.

Advantageously, one of the benefits offered by the invention is that each portion of digital content is encrypted along with a cryptographic key for (or associated with) a further or subsequent portion. Use of the key provides technical evidence that the portion of digital content has been decrypted. Therefore, it can be determined that the digital content has been accessed eg viewed or somehow consumed/used.

[18] In the system, the first user may deposit the deposit quantity of cryptocurrency (B 1) at the common address with the first processing device that is configured to: send, over a communications network, a first data output (01) to record, on a peer-to-peer distributed ledger (which may hereafter be referred to simply as a "blockchain"), a first transaction of the deposit quantity of cryptocurrency (Bl) from the first user to the common address.

[19] In the system, after a specified time without a transaction of the deposit quantity of cryptocurrency from the common address, the deposit quantity of cryptocurrency (Bl) may be refunded. The first processing device may be further configured to co-sign, with a first private key (Vi) of the first user, a second transaction to transfer the deposit quantity of cryptocurrency (Bl) from the common address to the first user. The second processing device may be further configured to co-sign, with the second private key (V_2), the second transaction, wherein the co-signed second transaction with both the first private key (Vi) and the second private key (V_2) is sent to the peer-to-peer distributed ledger and is valid after the specified time to refund the deposit quantity of cryptocurrency (Bl); and send the co-signed payment transaction to the peer-to-peer distributed ledger before the specified time.

[20] In the system, the second processing device may be further configured to: send, over the communications network, an episode secret (Si) associated the episode of digital content from the series of digital content that is available to be requested by the first user. The first processing device may be further configured to: receive, over the communications network, the episode secret (Si); determine an episode secret hash (Hi) from the episode secret (Si). To determine a payment transaction (Ei) to transfer the payment quantity of cryptocurrency (B2) to the second user includes the first processing device to configured to further determine a payment redeem script (RSI) based on: the episode secret hash (Hi); and a second public key (P_2) that is a cryptographic pair with the second private key (V_2) of the second user. When the second processing device verifies the payment transaction (Ei), the second processing device is further configured to verify that the payment redeem script (RSI) is based on the episode secret hash (Hi) and the second public key (P_2).

[21] In the system, the second processing device may be further configured to: determine a next episode secret (Si_{+1}) associated with the next episode (Si_{+1}) of digital content from the series of digital content; determine a next episode secret hash (¾ $_{+1}$) from the next episode secret (Si); wherein at, or after, step (III) to send the episode of digital content, the second

processing device is further provided to send, over the communications network, a next episode secret (*Si+i)* to the first node. The first processing device may be further configured to: receive, over the communications network, the next episode secret (S_{i+I}); determine a next episode secret hash (¾ $_{+I}$) from the next episode secret (*Si+i).* A corresponding next payment transaction (E_{i+I}) includes a next payment redeem script (RS2) based on: the next episode secret hash (¾ $_{+I}$); and the second public key (P_2). When the second processing device verifies a next payment transaction (E_{i+I}), the second processing device is further configured to verify that the next payment redeem script (RS2) is based on the next episode secret hash (H_{i+I}) and the second public key (P_2).

[22] In the system, the payment transaction (E_i) may further comprise a transfer from the common address to the first user a change quantity of cryptocurrency (B3) to the first user, wherein the change quantity of cryptocurrency (B3) is based on the deposit quantity of cryptocurrency (Bl) less the payment quantity of cryptocurrency (B2).

[23] In the system, the second processing device may be further configured to determine a common secret between the first node and the second node. To provide access, over the communications network, to the episode of digital content further includes the second processing device to: encrypt one or more episode of digital content with a key based on the common secret to provide one or more encrypted episodes of digital content; and to send the one or more encrypted episodes of digital content. The first processing device may be further configured to: determine a common secret between the first node and the second node; receive, over the communications network, the one or more encrypted episodes of digital content; and decrypt the one or more encrypted episodes of digital content with the key based on the common secret to provide the one or more episodes of digital content.

[24] In the system, the second processing device may be further configured to determine an encrypted message based on the episode secret (Si), and/or the next episode secret *(Si+i)* that is encrypted with a key based on the common secret. The first processing device may be further configured to determine the episode secret (Si), and/or the next episode secret *(Si+i),* by decrypting an encrypted message with a key based on the common secret.

[25] A computer-implemented method of receiving digital content, wherein a first node associated with a first user receives digital content in return for payment to a second user

associated with a second node, wherein the first user is associated with a deposit quantity of cryptocurrency (Bl) at a common address , wherein to spend from the common address requires signatures of both a first private key (Vi) of the first user and a second private key (V_2) of the second user, the method comprising:

(A) sending, over the communications network, a request to the second node to provide an episode of digital content (i) from a series of digital content;

(B) determining a payment transaction (E_i) to transfer from the common address a payment quantity of cryptocurrency (B2) to the second user, wherein the payment quantity of cryptocurrency (B2) is based on a quantity of episodes of digital content in the series of digital content requested by the first user;

(C) signing, with the first private key (Vi), the payment transaction (E_i) and subsequently sending the payment transaction (E_i) to the second node to cause the second node to verify the payment transaction;

wherein based on the second node having verified that the payment transaction includes the payment quantity of cryptocurrency (B2), the method further comprises:

(D) accessing, over the communications network, the episode of digital content (z).

[26] The method may further comprise requesting a next episode of digital content from the series of digital content by repeating the steps (A) to (D).

[27] The method may further comprise the first user to deposit the deposit quantity of cryptocurrency (Bl) at the common address with the step of sending, over a communications network, a first data output (01) to record, on a peer-to-peer distributed ledger, a first transaction of the deposit quantity of cryptocurrency (Bl) from the first user to the common address.

[28] In a further example of the method, after a specified time without a transaction of the deposit quantity of cryptocurrency (Bl) from the common address, the deposit quantity of cryptocurrency (Bl) is refunded, and wherein the method further comprises: co-signing, with the first private key (Vi) of the first user, a second transaction to transfer the deposit quantity

of cryptocurrency (Bl) from the common address to the first user, wherein the co-signed second transaction, co-signed by the second user with the second private key (V_2), is sent to the peer-to-peer distributed ledger and is valid after the specified time to refund the deposit quantity of cryptocurrency (Bl).

[29] The method may further comprise: receiving, over the communications network, an episode secret (Si) associated with the episode of digital content from the series of digital content that is available to be requested by the first user; determining an episode secret hash (Hi) from the episode secret (Si). The payment quantity of cryptocurrency (B2) to the second user in the payment transaction (E_i) includes a payment redeem script (RSI) based on: the episode secret hash (Hi); and a second public key (P_2) that is a cryptographic pair with the second private key (V_2) of the second user.

[30] In the method at, or after, step (D), the method further may further comprise: receiving, over the communications network, a next episode secret *(S i+i)* associated with the next episode *(S i+i)* of digital content from the series of digital content. Requesting the next episode from the series of digital content comprises determining a next episode secret hash (Hi_{+1}) from the next episode secret *(S i+i),* and wherein a corresponding next payment transaction (E_{i+1}) includes a next payment redeem script (RS2) based on: the next episode secret hash (¾ $_{+1}$); and the second public key (P_2).

[31] In the method, the payment transaction (E_i) may further comprise a transfer from the common address to the first user a change quantity of cryptocurrency (B3), wherein the change quantity of cryptocurrency (B3) is based on the deposit quantity of cryptocurrency (Bl) less the payment quantity of cryptocurrency (B2).

[32] The method may further comprise: determining a common secret between the first node and the second node; and wherein accessing, over the communication network, the episode of digital content comprises: receiving, over the communications network, an encrypted episode of digital content; and decrypting the encrypted episode of digital content with a key based on the common secret to provide the episode of digital content.

[33] When receiving the episode secret (Si), and/or the next episode secret (***Si+i),*** the method may further comprise determining the episode secret (Si), and/or the next episode secret (***Si+i),*** by decrypting an encrypted message with a key based on the common secret.

[34] A computer-implemented method of distributing digital content, wherein a first node associated with a first user receives digital content in return for payment to a second user associated with a second node, wherein the first user is associated with a deposit quantity of cryptocurrency (Bl) at a common address wherein to spend from the common address requires signatures of both a first private key (Vi) of the first user and a second private key (V_2) of the second user, the method-comprising:

(I) receiving, over the communications network, a request from the first node to provide an episode of digital content (*i*) from a series of digital content;

(II) receiving a payment transaction (E_i), signed with the first private key (Vi), to transfer from the common address a payment quantity of cryptocurrency (B2) to the second user, wherein the payment quantity of cryptocurrency (B2) is based on a quantity of episodes of digital content in the series of digital content requested by the first user;

(III) verifying the payment transaction, comprising verifying that the payment transaction includes the payment quantity of cryptocurrency (B2) to the second user, wherein based on a result of verifying the method further comprises:

(IV) providing access, over the communications network, to the episode of digital content (*i*) to the first node; and

(V) co-signing, with the second private key (V_2) of the second user, the payment transaction and sending the co-signed payment transaction to the peer-to-peer distributed ledger.

[35] The method may further comprise distributing a next episode of digital content from the series of digital content by repeating steps (I) to (IV) wherein step (V) is performed on a payment transaction a quantity of episodes of digital content that includes the next episode.

[36] In one example of the method, after a specified time without a transaction of the deposit quantity of cryptocurrency from the common address, the deposit quantity of cryptocurrency (Bl) is refunded to the first user. Accordingly, the method may further comprises co-signing, with the second private key (Vi) of the second user, a second transaction to transfer the deposit quantity of cryptocurrency (Bl) from the common address to the first user, wherein the co-signed second transaction, co-signed by the first user with the first private key (Vi), is sent to the peer-to-peer distributed ledger and is valid after the specified time to refund the deposit quantity of cryptocurrency (Bl). Furthermore, the step of sending the co-signed payment transaction to the peer-to-peer distributed ledger is performed before the specified time.

[37] The method may further comprise: sending, over the communications network, an episode secret (Si) associated the episode of digital content from the series of digital content that is available to be requested by the first user; and determining an episode secret hash (Hi) from the episode secret (Si). The step of verifying the payment transaction (Ei) comprises verifying that a corresponding payment redeem script (RSI) to transfer the payment quantity of cryptocurrency (B2) to the second user is based on: the episode secret hash (Hi); and a second public key (P_2) that is a cryptographic pair with the second private key (V_2) of the second user.

[38] The method may further comprise: determining a next episode secret (Si$_{+1}$) associated with the next episode (Si$_{+1}$) of digital content from the series of digital content; and determining a next episode secret hash (¾ $_{+1}$) from the next episode secret (Si). At, or after, step (IV), the method may further comprise sending, over the communications network, a next episode secret $(Si{+}i)$ to the first node. When verifying a next payment transaction for the next episode, the method further comprises verifying that a next payment redeem script (RS2) to transfer the next payment quantity of cryptocurrency to the second user is based on: the next episode secret hash (H_{i+1}) and the second public key (P_2).

[39] In the method, the payment transaction (Ei) may further comprise a transfer from the common address to the first user a change quantity of cryptocurrency (B3) to the first user, wherein the change quantity of cryptocurrency (B3) is based on the deposit quantity of cryptocurrency (Bl) less the payment quantity of cryptocurrency (B2).

[40] The method may further comprise: determining a common secret between the first node and the second node. The step of providing access, over the communications network, to the episode of digital content may comprise: encrypting the episode of digital content with a key based on the common secret; and- sending, over the communications network, the encrypted episode of digital content.

[41] In the method, the step of sending the episode secret (Si), and/or the next episode secret (***Si+i),*** may further comprise: determining an encrypted message based on the episode secret (Si), and/or the next episode secret (***Si+i)*** that is encrypted with a key based on the common secret.

[42] Any embodiment of the invention described above may comprise a method for determining a secret common to a first and a second node, and/or a system arranged to perform such a method. The method may comprise (or the system may be operative to perform) the following steps:

determining a first node second private key based on at least a first node mater private key and a generator value;

determining a second node second private key based on at least a second node master private key and the generator value;

wherein:

determining the common secret (CS) at the first node may be based on the first node second private key and the second node second public key, and determining the common secret (CS) at the second node may be based on the second node second private key and the first node second public key;

and wherein:

the first node second public key and the second node second public key may be respectively based on at least the first/second node master key and the generator value.

The generator value may be a message, or derived from a message. It may be derived from metadata stored in a blockchain transaction (Tx).

[43] A device comprising a processing device to perform any one of the methods described above.

[44] A computer program comprising machine-readable instructions to cause a processing device to implement any one of the methods as described above.

[45] Any feature described in respect of one embodiment or aspect of the invention may also apply to one or more other embodiments/aspects of the invention. Any feature described in relation to a system of the invention may be applied to a method of the invention and vice versa.

Brief Description of Drawings

[46] Examples of the present disclosure will be described with reference to:

[47] Fig. 1 is a schematic diagram of an example system to distribute digital content;

[48] Fig. 2 is a diagram illustrating transactions between a first user, a second user, and a common address;

[49] Fig. 3 is a flow chart of computer-implemented methods for distributing and receiving digital content;

[50] Fig. 4 is a flow chart of a computer-implemented method of initialising and creating a refund transaction;

[51] Fig. 5 is a detailed flow chart of a computer-implemented method for distributing and receiving digital content according to one example; and

[52] Fig. 6 illustrates a schematic example of a processing device.

Description of Embodiments

Overview

[53] A system, devices and methods for controlling the distribution and transmission of digital content from one node and receiving the digital content at another node will now be described. Fig. 1 illustrates a system 1 that includes a first node 15 associated with a first user

5 that is in communication, over a communications network 8, with a second node 17 associated with a second user 7. In this example, the first user 5 can request to receive digital content at the first node 15 and the second user 7, via the second node 17, provides access to the digital content. The second node 17 may provide access to the digital content in a number of ways including: sending digital content from a first data store 18 to the first node 15; and making digital content at a second data store 11 associated with a content server 3 available, via the communication network 8, to the first node 15.

[54] The first node 15 and/or second node 17 are in communication, over the communications network 8, with a peer-to-peer distributed ledger (blockchain) 9. The blockchain 9 may be associated with one or more processing devices 19 to receive and record transactions. An example of a peer-to-peer distributed ledger includes the blockchain, which is a distributed ledger of transactions (Txs) based on the Bitcoin protocol. Thus the processing device 19 associated with the ledger may be processing devices used by, or associated with, "miners".

[55] Referring to Fig. 2, the first user 5 may wish to purchase an unknown number of digital content from a series of digital content from the second user 7. Before making digital content available to the first user 5, the second user 7 requires a deposit to provide confidence that the second user 7 will be paid for the digital content.

[56] To provide the deposit, the first user 5 may perform a first transaction 21 to transfer a deposit quantity of cryptocurrency (Bl) to a common address 23. The common address 23 may be a pay-to-script-hash (P2SH) address according the Bitcoin protocol, and spending from the common address 23 requires signatures of both a first private key (Vi) of the first user 5 and a second private key (V_2) of the second user 7. That is a transaction from the common address 23 must be signed by both the first user 5 and second user 7 and thereby both sides can have confidence that the deposit will not be spent without authority from both sides. It is to be appreciated that alternative multi-signature methods may be used to authorise a transaction from the common address 23.

[57] In some examples, the deposit may be time limited whereby if the first user 5 does not make a request to receive episodes of digital content within a specified time (and/or other condition), the deposit is refunded back to the first user 5. An example of this is shown in

Fig. 2 as a second transaction 25 that refunds the deposit quantity of cryptocurrency (Bl) to the first user 5. In some examples, this may be achieved by having both the first user 5 and second user 7 to co-sign a second transaction from the common address (23) to the first user 5, where the second transaction is only valid after a specified time. For examples, the specified may be d days in the future expressed in Unix time. This second transaction is then broadcast, where it will become a valid transaction after the specified time.

[58] Therefore if a competing transaction to spend the deposit quantity of cryptocurrency (Bl) from the common address is broadcast before the specified time, that competing transaction will be the valid transaction. It is in the interest of the second user 7 to broadcast a valid competing transaction before the specified time, after which the deposit quantity of cryptocurrency (B 1) will be refunded back to the first user (5). In the present example, these competing transactions are called payment transactions 27, 27', 27" as they represent transactions where the second user 7 could receive payment.

[59] A brief example of how distributing the digital content, including creating the payment transaction 27, will now be described with reference to Fig. 3 that shows the respective methods 100, 200 performed by the first node 15 and second node 17.

[60] The first user 5, upon wanting to receive an episode of digital content from a series of digital content, uses the first node 15 to make a request for digital content. The first node 15 (which may be a computer, a mobile communication device, a television, etc.,) includes a first processing device 23 that sends 110, over the communications network 8, the request to the second node 15 to provide the episode of digital content.

[61] The first node 15 also determines 120 a payment transaction (E_i) 27 to transfer from the common address (23) a payment quantity of cryptocurrency (B2) to the second user 7. The payment quantity (B2) is based on a quantity of episodes of digital content in the series of digital content requested by the first user 5. This may include the episodes that have been requested previously (and received) but where payment has not been received by the second user 7. In a simplified example, the second payment quantity (B2) may be the number of episodes requested (i) multiplied by the price of each episode (p).

[62] The first node 15 then signs 130, with the first private key (Vi), the payment transaction (Ei) 27. The payment transaction (Ei) 27 is then sent to the second node 17. Since the payment transaction (Ei) has only been signed with the first private key (Vi), this is not yet a valid transaction as it requires the second node 17 to sign with the second private key (V_2).

[63] Turning now to the second node 17 associated with the second user 7, the second node has a second processing device 23' that may include a mainframe computer, desktop computer, etc. The second processing device of the second node 17 receives 210, over the communications network 8, the request from the first node 15 to provide the episode of digital content and the payment transaction (Ei) signed with the first private key (Vi).

[64] Before the second node 17 makes the episode of digital content available to the first node 15 and first user 5, the second node 17 needs to determine that the second user 17 will be able to receive payment. Accordingly, the second node 17 then verifies 220 the payment transaction (Ei) 27, which includes verifying that the payment transaction (Ei) 27 includes the payment quantity of cryptocurrency (B2) to the second user 7. In practical examples, this may include determining the correct amount of cryptocurrency as well as the correct destination.

[65] Based on verifying the payment transaction (Ei) (i.e. in particular that the second user 7 will be paid) the second node 17 then provides access 230, over the communications network 8, the episode of digital content to be available to the first node 15. In turn, this allows the first node to access 140 the episode of digital content.

[66] To give effect to the payment transaction (Ei) 27, the second node 17 then co-signs 240, with the second private key (V_2) of the second user 5, the payment transaction (Ei) 27 and sends the co-signed payment transaction to the blockchain 9. Thus the payment quantity of cryptocurrency (B2) will be transferred from the common address (23) that had the deposit quantity of cryptocurrency (Bl).

[67] In some examples, the first user 5 may have the opportunity to request and receive further episodes. Thus the second user 17 may have the opportunity to receive more payment (from the further episodes provided to the first user 5) and may therefore defer the step of co-signing 240 and sending the co-signed payment transaction to the blockchain 9 until a time

closer to the specified time to refund the deposit of the second transaction 25. An example of distributing the next episode will now be described.

[68] The first node 15 makes a request for the next episode of digital content from the series of digital content by repeating steps 110, 120, and 130 as described above but for the next episode. Importantly, the payment quantity of cryptocurrency will be adjusted to take into account the next episode (and previous episodes in the series where payment has not been made). The second node 17 similarly receives the request and distributes the next episode of digital content by repeating steps 210 to 230 as described above.

[69] Thus the second node 17 has two payment transactions: a first payment transaction (E_i) 27 that includes payment quantity of cryptocurrency up to the episode of digital content, and a second payment transaction (E_{i+1}) 27' that includes a payment quantity of cryptocurrency up to and including the next episode of digital content. Since the second user 7 will be interested in receiving the maximum amount of payment, the second node 17 should only sign 240 and send the co-signed payment transaction 27' than includes the payment inclusive of that of the next episode - i.e. the second payment transaction (E_{i+1}) 27'. Therefore the first payment transaction (E_i) 27 may be abandoned by the second node 17.

[70] The present disclosure may provide a system of communicating, transmitting and/or distributing digital content where the level of trust may be lower. For example, the level of exposure of either the first user 5 and/or second user 7 from deceitful conduct can be minimised. In one example, if the second user 7 fails to meet their obligation, the exposure (e.g. potential loss) to the first user would be the price of one episode of digital content (since the remaining amounts will be refunded).

[71] The present disclosure may also provide a system that does not rely on other third parties, such as certificate authorities and hierarchies that may have single points of failure and vulnerable to attack. The use of cryptographic techniques enhances the security of the transmission/control arrangement provided by the invention.

[72] A detailed example will now be described for the purposes of illustration.

Initialisation - encryption protocol

[73] The first node 5 and second node 7 establish secure communication 101, 201, over the communications network 8, with one another. This may include encrypting communications with a shared symmetric encryption key (S). In some examples, the symmetric encryption key is based on a shared common secret._A technique for determining this common secret may be as follows:

determining a first node second private key based on at least a first node master private key and a generator value;

determining a second node second private key based on at least a second node master private key and the generator value;

wherein:

determining the common secret (CS) at the first node is based on the first node second private key and the second node second public key, and determining the common secret (CS) at the second node is based on the second node second private key and the first node second public key. The first node second public key and the second node second public key are respectively based on at least the first/second node master key and the generator value.

[74] A method for deriving a key based on a shared common secret is described in more detail later in this description.

Deposit of cryptocurrency to common address

[75] To make the deposit in the first transaction 21 to the common address, the first node needs to determine the common address. In a pay to script hash (P2SH) system, this may be based on the public keys (corresponding the private keys used for signing). In one example, this includes determining the first public key (Pi) corresponding the first private key (Vi) of the first user 5, which should be known to the first node 5. This also includes determining the second public key (P_2) of the second user 5, which may be determined by receiving the second public key (P_2) from the second node 17, a third party, or from a data store. The second public key (P_2) does not necessarily need to be transmitted in a secure manner, although in some examples the second public key (P_2) may be encrypted with the shared symmetric encryption key (S).

[76] The deposit quantity of cryptocurrency (B 1) may be a quantity mutually agreed upon by the first and second user 5, 7. However, the deposit quantity of cryptocurrency (Bl) may desirably be equivalent to the cost of the maximum amount of episodes of digital content in the series of digital content that can be received. This ensures that if the first user 5 decides to receive and watch all episodes, the deposit is sufficient to pay for all the episodes. Therefore if the series has a number of episodes *n*, and the price per episode is *p*, then the deposit quantity of cryptocurrency (Bl) is *n* x *p*.

[77] An example of the first transaction (Ai) 21 to transfer the deposit quantity of cryptocurrency (Bl) is shown below in Table 1 and 2.

[78] Table 1: First transaction (Ai)

Transaction identifier			A_1
Version number			
Number of inputs			1
Input (unlocking)	Previous transaction	Hash	A_0
		Output index	
	Length of signature script		
	Signature script		`<Alice’s signature> <Alice’s public key>`
	Sequence number		
Number of outputs			1
Output (locking)	Value		*np*
	Length of public key script		
	Public key script		`OP_HASH160 <hash160(redeem script)> OP_EQUAL`
Locktime			0

[79] Table 2: Redeem script for transaction (Ai)

Redeem script	**0P_2 <Alice’s public key> <3ob Js public key> 0P_2 OP_CHECKMULTISIG**

[80] In this example the first transaction (Ai) 21 has an input from a previous blockchain transaction of the first user ("Alice") 5 (that requires the first user's signature) an outputs to the common address (23). In this example, the output is to a hash that is based on a redeem script including the first user's public key (Pi, "Alice's public key") and the second user's public key (P2, "Bob's public key"). That is, redeeming the output of the first blockchain

transaction (Ai) 21 will require the signatures of both the first user 5, with the first private key (Vi), and the second user 7, with the second private key (V_2).

[81] Recording the above mentioned first transaction (Ai) 21, is shown in the method 100 performed by the first node 5 as shown in Fig. 4 where the first node where the first node 15 sends 103, over the communications network 8, a first data output (01) to record, on the blockchain 9, a first transaction of the deposit quantity of cryptocurrency from the first user 5 to the common address (23).

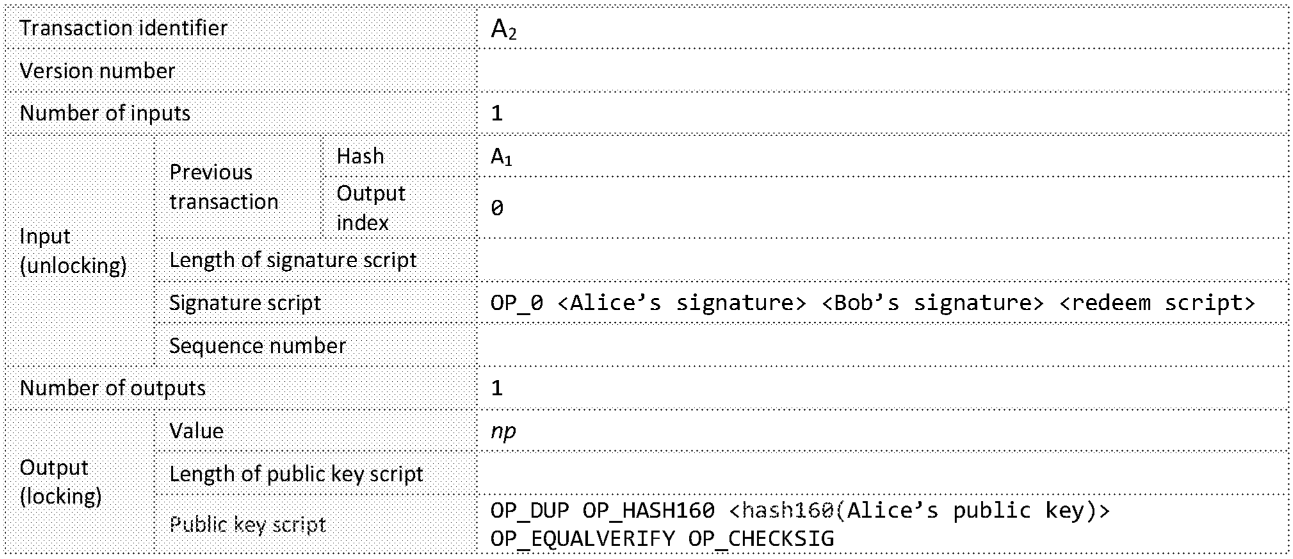
Creating a refund transaction

[82] A second blockchain transaction 25 is then created so that the deposit quantity of cryptocurrency (Bl) is refunded after an expiry of a specified time.

[83] This may include the first node 15 creating the second transaction 25 that includes spending the deposit quantity of cryptocurrency (Bl) back to the first user 5, but only after a specified time in the future. The specified time may include setting a lock time to the second transaction of ***d*** days in the future expressed in Unix time.

[84] An example of the second transaction (21) 25 to refund the deposit quantity of cryptocurrency (Bl) is shown below in Table 3.

[85] Table 3: Second transaction (A_2)



Transaction identifier			A_2
Version number			
Number of inputs			1
Input (unlocking)	Previous transaction	Hash	A_1
		Output index	0
	Length of signature script		
	Signature script		OP_0 <Alice's signature> <Bob's signature> <redeem script>
	Sequence number		
Number of outputs			1
Output (locking)	Value		*np*
	Length of public key script		
	Public key script		OP_DUP OP_HASH160 <hash160(Alice's public key)> OP_EQUALVERIFY OP_CHECKSIG

Locktime	***d*** days in the future expressed in Unix time (the number of seconds that have elapsed since 00:00:00 UTC 1 January 1970)

[86] In this example the second transaction (A_2) 25 has an input from the first transaction (Ai) 21. Unlocking the input from the common address (23) 23 requires both the first user's signature with the first private key (Vi) and the second user's signature with the second private key (V_2). In this example, the output refunds the deposit quantity of cryptocurrency (which in this case is *np)* back to the first user 5, and therefore the output is based on a hash of the the first user's public key (Pi, "Alice's public key") only. That is, redeeming the output of the first transaction (Ai) 21 will only require the signature of the first user 5, with the first private key (Vi) as the first user 5 should be free to spend their own refunded cryptocurrency.

[87] Importantly, the second transaction (A_2) 25 is only valid after a specified time, which in this case is achieved by the locktime function where the transaction is only valid after the specified time. For examples, *d* days (expressed in Unix time).

[88] Recording the second transaction (A_2) 25 is shown in Fig. 4 as steps 105, 107 performed by the first node 15 and steps 203, 205, 207 performed by the second node 17. The first node 15 co-signs 105, with the first private key (Vi) of the first user 5, the second transaction. This second transaction (A_2) 25 is then sent 107, over the communications network 8, to the second node 17 to be signed with second private key (V_2). In turn, the second node 17 receives 203 the second transaction (A_2) 25, and the second node 17 further co-signs 205 the second transaction (A_2) 25 with the second private key (V_2) of the second user 7. The second transaction (A_2) 25, now signed with both private keys is then sent 207, over the communications network 8, to the blockchain 9 where it will be valid after the specified time to refund the deposit quantity of cryptocurrency (Bl) if no other valid transactions (such as a payment transaction 27) are sent before that specified time.

[89] It is to be appreciated that these steps may be performed in other orders. For example, the second node 17 may sign the second transaction first, and send it to the first node 15 to sign second. It is to be appreciated that either nodes can create the second transaction (before signing) and either node can send the co-signed transaction to the blockchain 9. In other examples, the first and second nodes 15, 17 may send the transaction to other intermediate nodes that in turn send it to other nodes and/or the blockchain 9.

Requesting digital content and determining a payment transaction

[90] The method of requesting digital content and creating a payment transaction will now be described with reference to Fig. 5.

[91] The second node 17 determines, for each episode (z) of digital content, a corresponding episode secret (Si). The episode secret (Si) can be used to identify the episode (z) for those who know the secret, in particular the first user 5 and the second user 7. This can be useful to maintain privacy where information is sent to the blockchain 9.

[92] The second node 17 sends 208 an episode secret (Si) for a first episode of digital content in the series of digital content to the first node 17. In this example, only the episode secret of the following episode that is available to the first user 5 and first node 15 is sent. The subsequent episode secrets are withheld until the first node 15 accesses the first episode. This ensures that the episodes are accessed in order.

[93] When sending 208 the episode secret (Si), the second node 17 may create and send an encrypted message by encrypting the episode secret (Si) with the shared symmetric encryption key (S) to maintain secrecy of the episode secret (Si). The first node 15 then receives 108 the encrypted message, including the episode secret (Si), from the second node 17. The first node 15 then decrypts the encrypted message with the shared symmetric encryption key (S) to obtain the episode secret (Si).

[94] The first node 15 may store the episode secret (Si) in a data store until the first user 5 decides to access the first episode of digital content. Assuming that the specified time has not expired (i.e. it is before *d* day), the method 100 at the first node 15 includes sending 110, over a communications network 8, a request to the second node 17 to provide the first episode of digital content. This request is accompanied by a payment transaction 27 for the first episode determined 120 at the first node which will be described below.

Determining the payment transaction

[95] The payment transaction (Ei) 27, if valid, will spend from the common address (23) (and in particular the deposit quantity of cryptocurrency (Bl) therefrom) and accordingly requires the signature of both the first user 5 and second user 7. Therefore after determining

the payment transaction (Ei) 27, the first node 15 will need to sign the payment transaction (Ei) 27 and send it to the second node 17 for co-signing before sending to the blockchain 9.

[96] The first node 15 first determines 121 an episode secret hash (Hi) from the episode secret (Si). This may include using a hash function such as OP_HASH 160 (where the input is hashed twice - with SHA-256 and subsequently with RIPEMD-160). It is to be appreciated that other hash functions may also be suitable.

[97] The payment transaction (Ei) 27, in this example, is in the form of a P2SH. Therefore determining the payment transaction (Ei) 27 also includes determining a redeem script, which in this case is a payment redeem script (RSI) that is based on: the episode secret hash (Hi); and the second public key (P_2) of the second user 7. Including the episode secret hash (Hi) in the redeem script may be used as proof that this particular payment transaction is related to access of the particular episode (associated with the episode secret hash (Hi) and the episode secret (Si)). Secondly, the second public key (P_2) of the second user 7 ensures that only the second user 7, having the corresponding second private key (Vi), can spend that payment.

[98] Determining 120 the payment transaction (Ei) 27 also includes determining the payment quantity of cryptocurrency (B2) to the second user 7. In the case of the first episode, this payment quantity will be the price of that first episode. However as the first user 5 makes further requests for subsequent episodes, the payment quantity of cryptocurrency (B2) will change based on episodes that have been requested. In a simplified example, this may be the quantity of episodes multiplied by the price per episode.

[99] In addition to an output to the second user 7, the payment transaction (Ei) 27 may include another output back to the first user 5. This output back to the first user 5 may be representative of the change of the deposit quantity of cryptocurrency (Bl) back to the first user. In one example, the change quantity of cryptocurrency (B3) to the first user 5 may be based on the deposit quantity of cryptocurrency (Bl) less the payment quantity of cryptocurrency (B2).

[100] The method 100 then includes signing 130, with the first private key (Vi), the payment transaction (Ei) 27 and subsequently sending the payment transaction (Ei) 27 to the second node 17 to cause the second node 17 to verify the payment transaction.

[101] An example of the payment transaction (E_i) is shown below in Table 4 and 5.

[102] Table 4: Payment transaction (E_i)

Transaction identifier			E_i
Version number			
Number of inputs			**1**
Input (unlocking)	**Previous trans.**	Hash	Al
		Output index	**ø**
	Length of signature script		
	Signature script		**<Alice's signature> <Bob's signature> <redeem script>**
	Sequence number		
Number of outputs			**2**
Output 1 (locking)	**Value**		ip
	Length of public key script		
	Public key script		**OP_HASH160 <hashl60(redeem script)> OP_EQUAL**
Output 2 (locking)	**Value**		**$(n - i)p$**
	Length of public key script		
	Public key script		**OP_DUP OP_HASH160 <hashl60 (Alice's public key)> OP_EQUALVERIFY OP_CHECKSIG**
Locktime			8

[103] Table 5: Output 1 redeem script of payment transaction (E_i)

Redeem script	**OP_HASH160 <hi> 0P_EQUALVERIFY <Bob's public key> OP_CHECKSIG**

[104] The input to this transaction includes an unlocking script that requires the both the signatures of the first private key (Vi) of the first user 5 ("Alice's signature") and the second private key (V_2) of the second user 7 ("Bob's signature") as the payment transaction is spending from the common address (23).

[105] "Output 1" shows the output of the payment quantity of cryptocurrency (B2) to the second user 7. This output can be redeemed by payment redeem script (RS 1) shown in Table 5 which is based on the episode secret hash (Hi) and the second user public key (P_2) ("Bob's public key") as described above.

[106] "Output 2" shows the output that is the change quantity of cryptocurrency (B3) back to the second user 7. Note that the output script is based on the first user's public key Pi (Alice's public key) as the first user should be free to spend this change quantity of cryptocurrency (B3).

Verifying the payment transaction

[107] The second node 17 receives 210, over the communications network 8, the request to provide the first episode of digital content. Accordingly the second node 17 will also expect to receive the payment transaction (Ei) 27, signed with the first private key (Vi), from the first node 15.

[108] Before agreeing to the request to provide the episode of digital content, the second node will verify the payment transaction (Ei) so that the first user 7 can have confidence that they will receive payment.

[109] The second node 17 determines 121 the episode secret hash (Hi) from the episode secret (Si). This may include using a hash function in the same way as the first node 15. The second node then verifies 220 the payment transaction (Ei) that was received includes the payment quantity of cryptocurrency (B2) to the second user 7. This may include verifying the output value (such as output value in "Output 1" of Table 4) is the correct value by verifying the value is equal to the quantity of episodes request multiplied by the price.

[110] Verifying 220 may also include verifying that the payment redeem script (RS 1) is based on the episode secret hash (Hi) and the second public key (P_2). This may be achieved by comparing the output script (which is based on the redeem script) in the received payment transaction (Ei) with a corresponding hash of the known (or derivable) values of the episode secret hash (Hi) and the second public key (P_2). If this comparison shows that the output script matches the expected redeem script having the correct episode secret hash (Hi) and the second public key (P_2), then the second node 17 (and the second user 7) can have confidence of the *bona fide* of the received payment transaction (Ei).

[Ill] Although the second node 17 may sign the payment transaction (Ei) 27 and immediately send it to the blockchain 9, the second user 7 is not motivated to do so until closer towards the specified time as the first user 5 may make further requests for more episodes of digital content.

[112] After successful verification, the second node 17 then provides access to the requested episode to the first node 15 as well as the next episode secret to the first node to allow the first node to request further content (being the next episode).

Determine the next episode secret

[113] The second node 17 then determines 221 the next episode secret *(Si+i)* for the next episode i+1 (which is the episode after episode *(i)* to be provided) in the series of digital content unless there are no more episodes in the series. This may include retrieving the next episode secret *(Si+i)* from the data store 18, or generating a new secret. The next episode secret *(Si+i)* is used to determine the next episode secret hash (H_{i+1}) which in turn is used in the next payment transaction if the first user 5 decides to make a request for the next episode in the future.

[114] The next episode secret *(Si+i)* may be provided to the first node 15 at the same time the second node provides access to the present requested episode of digital content.

Providing access to digital content

[115] Once the payment transaction (E_i) 27 has been verified, the second node 17 provides access 230 to the episode of digital content to the first node 15. This may be achieved in a number of ways. In one example, the second node 17 may encrypt the episode of digital content with the shared symmetric encryption key (S) and send the encrypted episode of digital content, over the communications network 8, to the first node 15. In another example, the second node may provide the encrypted episode of digital content at a data store 11 associated with a content server 3, whereby the first node 15 may receive the encrypted episode from the data store 11 at a suitable time for the first node 15. In yet another example, the second node 15 may provide an episode specific encryption key to decrypt the episode.

[116] In one example, the episode *(i)* of digital content that was requested may be concatenated with the next episode secret *(Si+i)*. The concatenation may then be encrypted

with the shared symmetric encryption key and the second node 17 then provides access to the encrypted concatenation.

[117] The second node 17 may then send, over the communications network 8, a notification to the first node 15 indicating that the requested episode (z) of digital content is available to be accessed.

[118] In turn, the first node 15 then accesses 140 the encrypted concatenation (e.g. by downloading from the data store 11 or directly from the second node 17, etc.) and decrypts it with the shared symmetric encryption key. This provides, at the first node 15, the episode of digital content (z) as well as the next episode secret *(Si+i).* Importantly, this provides the first user the episode of digital content for consumption as well as a means (i.e. the next episode secret (S_{i+1})) to obtain the next episode. The first node 15 may store 141 the next episode secret *(Si+i)* for later use.

[119] It is to be appreciated that in some alternatives, the next episode secret may be sent 223 from the second node 17 to the first node 15 at other times and not concatenated with the episodes of digital content. This may include sending the next episode secret *(Si+i)* as a separate encrypted message over the communications network.

Requesting the next episode

[120] If the first user 5 wishes to watch the next episode ż+i, the first node 15 may then repeat the above steps of sending 110 a request for an episode of digital content, determining 120 a next payment transaction and signing 130 the next payment transaction. This can be done with the next episode secret *(Si+i)* and a corresponding determined next episode secret hash (H_{i+1}). In turn, the second node 15 will repeat the steps of receiving 210 the request and next payment transaction, verifying 220 the next payment transaction and providing access 230 to the next episode.

[121] The above can be repeated until all the episodes of digital content have been accessed by the first node 15 or when it is close to, or at, the expiry of the specified time *d* days. In these situations, the second node 15 will then perform the following steps to effect the payment to the second user 7.

Co-signing the payment transaction

[122] When all the episodes in the series of digital content have been accessed by the first node 15, the second user 7 will be motivated to co-sign the latest payment transaction (Ei) 27" to receive payment as there will be no further payment transactions 27". Alternatively, if the expiry period of the specified time is approaching, the second user 7 will be motivated to co-sign the latest payment transaction (Ei) 27" as it would be unlikely that the first user 5 will make any further requests. More importantly, the payment transaction (Ei) must be co-signed and sent to the blockchain 9 before the specified time to ensure it is recorded before the second transaction (refund transaction) is valid.

[123] Thus the method 200 includes the second node 17 co-signing 240, with the second private key (V_2), the latest payment transaction (Ei) 27" and sending the co-signed payment transaction to the blockchain 9.

[124] When the second user 7 wishes to spend the payment quantity of cryptocurrency (B2), the second node 17 will unlock the transaction by signing the redeem script shown in Table 5 by signing with the second user private key (V_2) and the episode secret (Si) corresponding to the episode secret hash (Hi) in the payment transaction (Ei). This is shown in the unlocking script in Table 6 below. Please note that the redeem script, in the format as shown in Table 5, can be determined by the second node 17 based on the second user public key (P2) and the episode secret (Si), wherein the episode secret (Si) is used to derive the episode secret hash (Hi).

[125] Table 6: The second user spending the payment quantity of cryptocurrency

Transaction identifier			B
Version number			
Number of inputs			**1**
Input (unlocking)	**Previous transaction**	**Hash**	E_i
		Output index	0
	Length of signature script		
	Signature script		**<Bob's signature>** <S_i> **<redeem script>**
	Sequence number		
Number of outputs			
	Value		i_P

Output (locking)	Length of public key script	[Dependent on how Bob decides to spend]
	Public key script	[Dependent on how Bob decides to spend]

Variations

[126] It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the above-described embodiments, without departing from the broad general scope of the present disclosure. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

[127] In one example variation, each payment transaction (E_i) may itself have a respective payment specified time before it is valid. For example, the payment specified time may be a time (e.g. *d-1* day) before the specified time (e.g. *d* days) of the second transaction (i.e. the refund transaction) so that the payment transaction (E_i) is the valid transaction before the second transaction.

[128] Therefore in this variation, the second node 17, upon verifying the payment transaction may immediately co-sign and send the payment transaction (Tx) to the blockchain 9.

[129] For subsequent payment transactions, these subsequent payment transactions have a respective specified time (e.g. *d-2* days) that is earlier than the specified time of the preceding payment transaction (e.g. *d-1* days). Thus the subsequent payment transactions, once co-signed and sent to the blockchain 9 will precede and be valid over the earlier payment transactions and the second (refund) transaction. An advantage of this variation is that if the second node 17 has a failure at a time close to the specified time for the second (refund) transaction, the second user 7 will still receive payment as the payment transactions have already been co-signed and sent to the blockchain 9.

Shared symmetric key based on a shared common secret

[130] A method of generating a common secret between two nodes is now described. The common secret can be used in the generation of a cryptographic key.

Determining a common secret

[131] The method allows for the generation of a common secret between two nodes without requiring the common secret to be sent to and/or from either one of the nodes. Each node has a respective asymmetric cryptography pair (such as an elliptic curve cryptography pair), each pair including a master private key and a master public key. For example the first node may have a master private key (Vip) and a master public key (PIP), and the second node may have a master private key (Vm) and a master public key (Pm). Respective second private and public keys of each node may be determined based on the master private key, master public key and a generator value. The generator value (or a message used to derive the generator value) is communicated to and/or from the nodes.

[132] A common secret may be determined at each of the nodes based on the second private and public keys. An example of determining a common secret between a first node and a second node will now be described. Both the first and second nodes determine a generator value that is common to both nodes. The generator value may be received by a message, or derived from a message.

[133] At the first node, the common secret (CS) is based on:

(i) a first node second private key (V_2p) based on the first node master private key (Vip) and the generator value (GV); and

(ii) a second node second public key (P_2E) based on the second node master public key (Pm) and the generator value (GV).

[134] At the second node, the same common secret (CS) can be determined based on:

(iii) a first node second public key (P_2p) based on the first node master public key (PIP) and the generator value (GV); and

(iv) a second node second private key (V_2E) based on the second node master private key (Vm) and the generator value (GV).

[135] Thus the common secret is:

[136] Common secret (CS) = $(V_{2P} \times P_{2E}) = (P_{2P} \times V_{2E})$

Securely transmitting information

[137] The common secret may be used to encrypt information for secure transmission. For example, a symmetric key may be based on the common secret. Since both nodes have the same common secret, they can determine the same symmetric key which can be used for encrypting and decrypting information transmitted (for example over an unsecure network) between the two nodes.

Processing device

[138] As noted above, the first user 5 and second user 7 are associated with respective first node 15 and second node 17. The first node 15 and second node 17 may be an electronic device, such as a computer, tablet computer, mobile communication device, computer server, computer terminal, etc. Such an electronic device may include a processing device, and accordingly, the first node 15 has a first processing device 23 and the second node 17 has a second processing device 23". The electronic device may also be associated with a data store 11, 18 and a user interface. Examples of a user interface include a keyboard, mouse, monitor, touchscreen display, etc. The blockchain 9 may also be associated with multiple processing devices 19.

[139] Fig. 6 illustrates an example of a processing device 19, 23. The processing device 19, 23 includes a processor 1510, a memory 1520 and an interface device 1540 that communicate with each other via a bus 1530. The memory 1520 stores instructions and data for implementing the method 100, 200 described above, and the processor 1510 performs the instructions (such as a computer program) from the memory 1520 to implement the methods 100, 200. The interface device 1540 may include a communications module that facilitates communication with the communications network 8 and, in some examples, with the user interface and peripherals such as data store 11, 18. It should be noted that although the processing device 1510 may be independent network elements, the processing device 1510 may also be part of another network element. Further, some functions performed by the processing device 19, 23 may be distributed between multiple network elements. For example, the first user 5 may be associated with multiple processing devices 23 (such as those

of the first user's mobile communication device, tablet, desktop computer, home media player, television,. etc.) and steps of the method 100 may be performed, and distributed, across more than one of these devices.

CLAIMS:

1. A computer-implemented system arranged to control the transmission and/or distribution of digital content, wherein a first user (5) is associated with a deposit quantity of cryptocurrency at a common address (23), wherein to spend from the common address requires signatures of both a first private key (Vi) of the first user (5) and a second private key (V_2) of the second user (7), the system comprising:

- a first node (15) associated with a first user (5) comprising a first processing device (23) configured to:

(A)- send, over a communications network (8), a request to the second node (17) to provide an episode of digital content (z) from a series of digital content;

(B)- determine a payment transaction (Ei) to transfer from a common address (23) a payment quantity of cryptocurrency (B2) to the second user (7), wherein the payment quantity of cryptocurrency (B2) is based on a quantity of episodes of digital content in the series of digital content requested by the first user (5); and

(C) - sign, with the first private key (VI), the payment transaction (Ei) and subsequently send the payment transaction (Ei) to the second node (17);

- a second node (17) associated with the second user (7) comprising a second processing device (23') configured to:

(I)- receive, over the communications network (8), the request from the first node (15) to provide the episode of digital content (z) and the payment transaction (Ei), signed with the first private key (Vi);

(II) - verify the payment transaction, comprising verifying that the payment transaction includes the payment quantity of cryptocurrency (B2) to the second user (7), and based on the result of verifying the second processing device is further configured to:

(III) - provide access, over the communications network (8), to the episode of digital content (z) to be available to the first node (15); and

(IV) - co-sign, with the second private key (V_2) of the second user (5), the payment transaction and send the co-signed payment transaction to a blockchain (9).

2. A system according to claim 1 the first processing device further configured to:

- request a next episode of digital content from the series of digital content by repeating steps (A) to (C),

wherein the second processing device is further configured to:

- receive the request and distribute the next episode of digital content by repeating steps (I) to (III); and

wherein the step (IV) to co-sign and send the payment transaction to the blockchain (9) is performed on a payment transaction having a quantity of episodes of digital content that includes the next episode.

3. A system according to any one of the preceding claims, wherein the first user (5) deposits the deposit quantity of cryptocurrency (Bl) at the common address (23) with the first processing device that is configured to:

- send, over a communications network (8), a first data output (01) to record, on a blockchain (9), a first transaction of the deposit quantity of cryptocurrency (Bl) from the first user (5) to the common address (23).

4. A system according to any one of the preceding claims wherein after a specified time without a transaction of the deposit quantity of cryptocurrency from the common address (23), the deposit quantity of cryptocurrency (Bl) is refunded, and the first processing device is further configured to:

- co-sign, with a first private key (Vi) of the first user (5), a second transaction to transfer the deposit quantity of cryptocurrency (Bl) from the common address (23) to the first user (5);

wherein the second processing device is further configured to:

- co-sign, with the second private key (V_2), the second transaction, wherein the co-signed second transaction with both the first private key (Vi) and the second private key (V_2) is sent to the blockchain (9) and is valid after the specified time to refund the deposit quantity of cryptocurrency (Bl); and

- send the co-signed payment transaction to the blockchain (9) before the specified time.

5. A system according to any one of the preceding claims wherein the second processing device is further configured to:

- send, over the communications network, an episode secret (Si) associated the episode of digital content from the series of digital content that is available to be requested by the first user (5);

wherein the first processing device is further configured to:

- receive, over the communications network, the episode secret (Si);

- determine an episode secret hash (Hi) from the episode secret (Si),

wherein to determine a payment transaction (Ei) to transfer the payment quantity of cryptocurrency (B2) to the second user (7) further includes the first processing device configured to determine a payment redeem script (RS 1) based on:

- the episode secret hash (Hi); and

- a second public key (P_2) that is a cryptographic pair with the second private key (V_2) of the second user (7),

wherein when the second processing device verifies the payment transaction (Ei), the second processing device is further configured to verify that the payment redeem script (RSI) is based on the episode secret hash (Hi) and the second public key (P_2).

6. A system according to claim 5 wherein the second processing device is further configured to:

- determine a next episode secret *(Si+i)* associated with the next episode *(Si+i)* of digital content from the series of digital content;

- determine a next episode secret hash (¾ $_{+I}$) from the next episode secret (Si);

wherein at, or after, step (III) to send the episode of digital content, the second processing device is further provided to:

- send, over the communications network (8), a next episode secret *(Si+i)* to the first node (15),

wherein the first processing device is further configured to:

- receive, over the communications network (8), the next episode secret (S$_{i+I}$);

- determine a next episode secret hash (¾ $_{+I}$) from the next episode secret *(Si+i)*, and wherein a corresponding next payment transaction (E$_{i+I}$) includes a next payment redeem script (RS2) based on:

- the next episode secret hash (H$_{i+I}$); and

- the second public key (P$_2$),

wherein when the second processing device verifies a next payment transaction (E$_{i+I}$), the second processing device is further configured to verify that the next payment redeem script (RS2) is based on the next episode secret hash (H$_{i+I}$) and the second public key (P$_2$).

7. A system according to any one of the preceding claims wherein the payment transaction (E$_{i)}$ further comprises a transfer from the common address (23) to the first user (5) a change quantity of cryptocurrency (B3) to the first user (5), wherein the change quantity of cryptocurrency (B3) is based on the deposit quantity of cryptocurrency (Bl) less the payment quantity of cryptocurrency (B2).

8. A system according to any one of the preceding wherein the second processing device is further configured to:

- determine a common secret between the first node (15) and the second node (17);

wherein to provide access, over the communications network, to the episode of digital content includes the second processing device to:

- encrypt one or more episode of digital content with a key based on the common secret to provide one or more encrypted episodes of digital content; and

to send the one or more encrypted episodes of digital content,

wherein the first processing device is further configured to:

- determine a common secret between the first node (15) and the second node (17);

- receive, over the communications network, the one or more encrypted episodes of digital content; and

- decrypt the one or more encrypted episodes of digital content with the key based on the common secret to provide the one or more episodes of digital content.

9. A system according to claim 8, when dependent on claim 5, wherein the second processing device is further configured to:

- determine an encrypted message based on the episode secret (Si), and/or the next episode secret (***Si+i)*** that is encrypted with a key based on the common secret,

wherein the first processing device is further configured to:

- determine the episode secret (Si), and/or the next episode secret (***Si+i),*** by decrypting an encrypted message with a key based on the common secret.

10. A system according to any preceding claim, wherein the system is arranged to determine a secret which is common to a first node and a second node, by:

determining a first node second private key based on at least a first node mater private key and a generator value;

determining a second node second private key based on at least a second node master private key and the generator value;

wherein:

determining the common secret (CS) at the first node may be based on the first node second private key and the second node second public key, and determining the common secret (CS) at the second node may be based on the second node second private key and the first node second public key;

and wherein:

the first node second public key and the second node second public key may be respectively based on at least the first/second node master key and the generator value.

11. A computer-implemented method of receiving digital content, wherein a first node (15) associated with a first user (5) receives digital content in return for payment to a second user (7) associated with a second node (17), wherein the first user (5) is associated with a deposit quantity of cryptocurrency (Bl) at a common address (23), wherein to spend from the common address requires signatures of both a first private key (Vi) of the first user (5) and a second private key (V_2) of the second user (7) , the method-comprising:

(A)- sending, over the communications network (8), a request to the second node (17) to provide an episode of digital content (i) from a series of digital content;

(B)- determining a payment transaction (E_i) to transfer from the common address (23) a payment quantity of cryptocurrency (B2) to the second user (7), wherein the payment quantity of cryptocurrency (B2) is based on a quantity of episodes of digital content in the series of digital content requested by the first user (5);

(C) - signing, with the first private key (VI), the payment transaction (E_i) and subsequently sending the payment transaction (E_i) to the second node (17) to cause the second node (17) to verify the payment transaction;

wherein based on the second node (17) having verified that the payment transaction includes the payment quantity of cryptocurrency (B2), the method further comprises:

(D)- accessing, over the communications network (8), the episode of digital content i.

12. A method according to claim 11 further comprising requesting a next episode of digital content from the series of digital content by repeating the steps (A) to (D).

13. A method according to either claim 11 or 12, wherein the first user (5) deposits the deposit quantity of cryptocurrency (Bl) at the common address (23) with the step of:

- sending, over a communications network (8), a first data output (01) to record, on a blockchain (9), a first transaction of the deposit quantity of cryptocurrency (Bl) from the first user (5) to the common address (23).

14. A method according to any one of claims 11 to 13 wherein after a specified time without a transaction of the deposit quantity of cryptocurrency (Bl) from the common address, the deposit quantity of cryptocurrency (B 1) is refunded, and wherein the method further comprises:

- co-signing, with the first private key (Vi) of the first user (5), a second transaction to transfer the deposit quantity of cryptocurrency (Bl) from the common address (23) to the first user (5), wherein the co-signed second transaction, co-signed by the second user (7) with the second private key (V_2), is sent to the blockchain (9) and is valid after the specified time to refund the deposit quantity of cryptocurrency (Bl).

15. A method according to any one of claims 11 to 14 further comprising:

- receiving, over the communications network, an episode secret (Si) associated with the episode of digital content from the series of digital content that is available to be requested by the first user (5);

- determining an episode secret hash (Hi) from the episode secret (Si);

wherein the payment quantity of cryptocurrency (B2) to the second user (7) in the payment transaction (Ei) includes a payment redeem script (RSI) based on:

- the episode secret hash (Hi); and

- a second public key (P_2) that is a cryptographic pair with the second private key (V_2) of the second user (7).

16. A method according to claim 15 wherein at, or after, step (D), the method further comprises:

- receiving, over the communications network (8), a next episode secret *(Si+i)* associated with the next episode *(Si+i)* of digital content from the series of digital content;

wherein requesting the next episode from the series of digital content comprises determining a next episode secret hash (H_{i+1}) from the next episode secret (Si_{+1}), and wherein a corresponding next payment transaction (E_{i+1}) includes a next payment redeem script (RS2) based on:

- the next episode secret hash (¾ $_{+1}$); and

- the second public key (P_2).

17. A method according to any one of claims 11 to 16 wherein the payment transaction (Ei) further comprises a transfer from the common address (23) to the first user (5) a change quantity of cryptocurrency (B3), wherein the change quantity of cryptocurrency (B3) is based on the deposit quantity of cryptocurrency (Bl) less the payment quantity of cryptocurrency (B2).

18. A method according to any one of claims 11 to 17 further comprising:

- determining a common secret between the first node and the second node; and

wherein accessing, over the communication network, the episode of digital content comprises:

- receiving, over the communications network, an encrypted episode of digital content; and

- decrypting the encrypted episode of digital content with a key based on the common secret to provide the episode of digital content.

19. A method according to claim 18 wherein the step of determining a common secret between the first node and the second node comprises:

determining a first node second private key based on at least a first node mater private key and a generator value;

determining a second node second private key based on at least a second node master private key and the generator value;

wherein:

determining the common secret (CS) at the first node may be based on the first node second private key and the second node second public key, and determining the common secret (CS) at the second node may be based on the second node second private key and the first node second public key;

and wherein:

the first node second public key and the second node second public key may be respectively based on at least the first/second node master key and the generator value.

20. A method according to claim 18, when dependent on claim 15, wherein receiving the episode secret (Si), and/or the next episode secret (***Si+i),*** further comprises:

- determining the episode secret (Si), and/or the next episode secret (***Si+i),*** by decrypting an encrypted message with a key based on the common secret.

21. A computer-implemented method of controlling the transmission and/or distribution of digital content, wherein a first node (15) associated with a first user (5) receives digital content in return for payment to a second user (7) associated with a second node (17), wherein the first user (5) is associated with a deposit quantity of cryptocurrency (Bl) at a common address (23) wherein to spend from the common address requires signatures of both a first private key (Vi) of the first user (5) and a second private key (V_2) of the second user (7), the method-comprising:

(I)- receiving, over the communications network (8), a request from the first node (15) to provide an episode of digital content (i) from a series of digital content;

(II)- receiving a payment transaction (E_i), signed with the first private key (Vi), to transfer from the common address (23) a payment quantity of cryptocurrency (B2) to the second user (7), wherein the payment quantity of cryptocurrency (B2) is based on a quantity of episodes of digital content in the series of digital content requested by the first user (5);

(III) - verifying the payment transaction, comprising verifying that the payment transaction includes the payment quantity of cryptocurrency (B2) to the second user (7), wherein based on a result of verifying the method further comprises:

(IV) - providing access, over the communications network (8), to the episode of digital content (i) to the first node (15); and

(V) - co-signing, with the second private key (V_2) of the second user (5), the payment transaction and sending the co-signed payment transaction to the blockchain (9).

22. A method according to 21 further comprising:

- distributing a next episode of digital content from the series of digital content by repeating steps (I) to (IV) wherein step (V) is performed on a payment transaction a quantity of episodes of digital content that includes the next episode.

23. A method according to either claims 21 or 22 wherein after a specified time without a transaction of the deposit quantity of cryptocurrency from the common address the deposit

quantity of cryptocurrency (Bl) is refunded to the first user (5), and wherein method further comprises:

- co-signing, with the second private key (Vi) of the second user (7), a second transaction to transfer the deposit quantity of cryptocurrency (Bl) from the common address (23) to the first user (5), wherein the co-signed second transaction, co-signed by the first user (5) with the first private key (Vi), is sent to the blockchain (9) and is valid after the specified time to refund the deposit quantity of cryptocurrency (Bl),

wherein sending the co-signed payment transaction to the blockchain is performed before the specified time.

24. A method according to any one of claims 21 to 23 further comprising:

- sending, over the communications network, an episode secret (Si) associated the episode of digital content from the series of digital content that is available to be requested by the first user (5);

- determining an episode secret hash (Hi) from the episode secret (Si);

wherein the step of verifying the payment transaction (Ei) comprises verifying that a corresponding payment redeem script (RSI) to transfer the payment quantity of cryptocurrency (B2) to the second user (7) is based on:

- the episode secret hash (Hi); and

- a second public key (P_2) that is a cryptographic pair with the second private key (V_2) of the second user (7).

25. A method according to claim 24 further comprising:

- determining a next episode secret (Si_{+1}) associated with the next episode (Si_{+1}) of digital content from the series of digital content;

- determining a next episode secret hash (H_{i+1}) from the next episode secret (Si);

wherein at, or after, step (IV), the method further comprises:

- sending, over the communications network (8), a next episode secret $(S i+i)$ to the first node (15),

wherein when verifying a next payment transaction for the next episode, the method further comprises verifying that a next payment redeem script (RS2) to transfer the next payment quantity of cryptocurrency to the second user (7) is based on:

- the next episode secret hash (H_{i+I}) and

- the second public key (P_2).

26. A method according to any one of claims 21 to 25 wherein the payment transaction (Ei) further comprises a transfer from the common address (23) to the first user (5) a change quantity of cryptocurrency (B3) to the first user (5), wherein the change quantity of cryptocurrency (B3) is based on the deposit quantity of cryptocurrency (Bl) less the payment quantity of cryptocurrency (B2).

27. A method according to any one of claims 21 to 26 further comprising:

- determining a common secret between the first node and the second node; and

wherein providing access, over the communications network, to the episode of digital content comprises:

- encrypting the episode of digital content with a key based on the common secret; and

- sending, over the communications network, the encrypted episode of digital content.

28. A method according to claim 27, when dependent on claim 24, wherein sending the episode secret (Si), and/or the next episode secret $(S i+i)$, further comprises:

- determining an encrypted message based on the episode secret (Si), and/or the next episode secret (***Si+i)*** that is encrypted with a key based on the common secret.

29. A method according to claim 27 or 28 wherein the step of determining a common secret between the first node and the second node comprises:

determining a first node second private key based on at least a first node mater private key and a generator value;

determining a second node second private key based on at least a second node master private key and the generator value;

wherein:

determining the common secret (CS) at the first node may be based on the first node second private key and the second node second public key, and determining the common secret (CS) at the second node may be based on the second node second private key and the first node second public key;

and wherein:

the first node second public key and the second node second public key may be respectively based on at least the first/second node master key and the generator value.

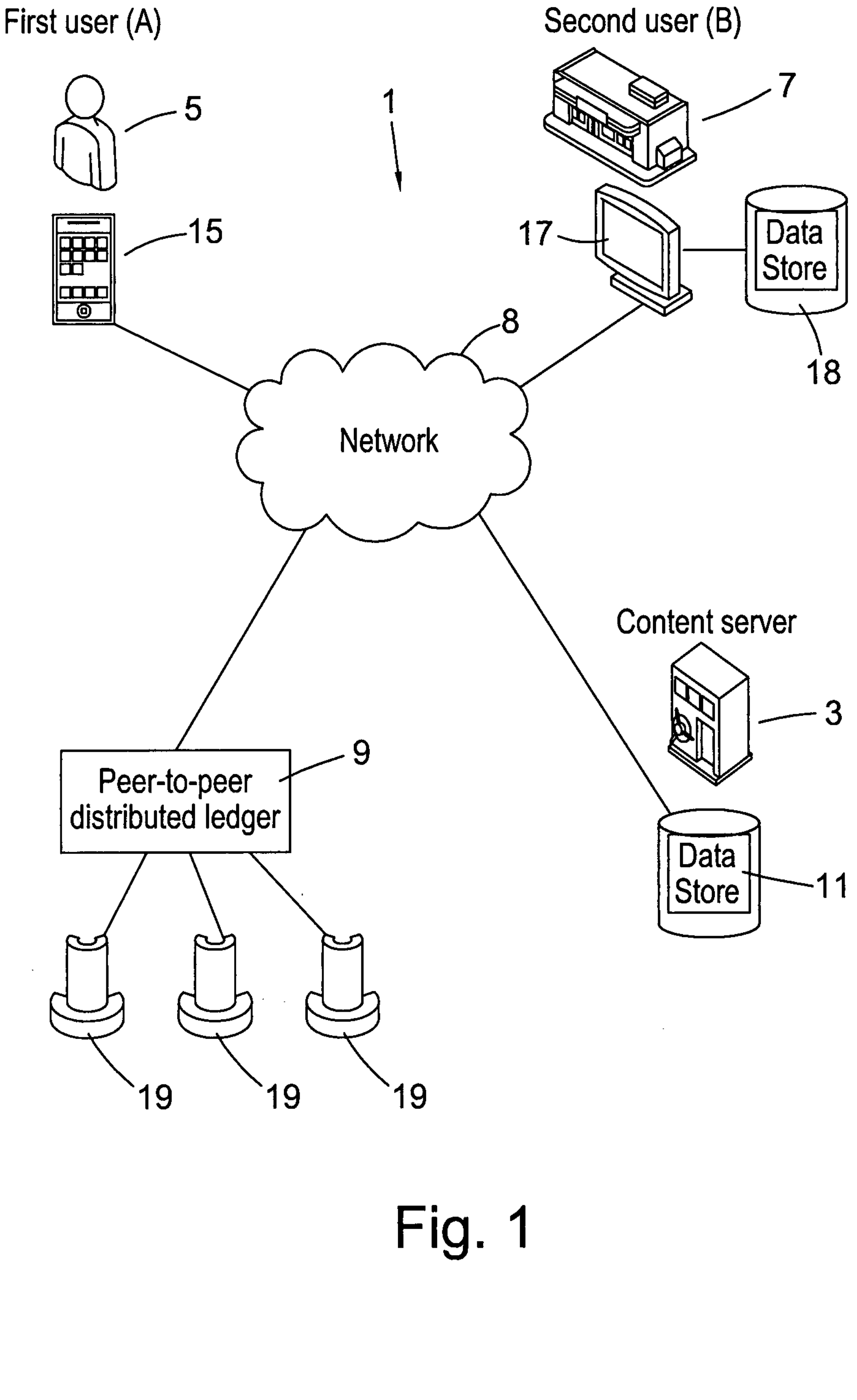
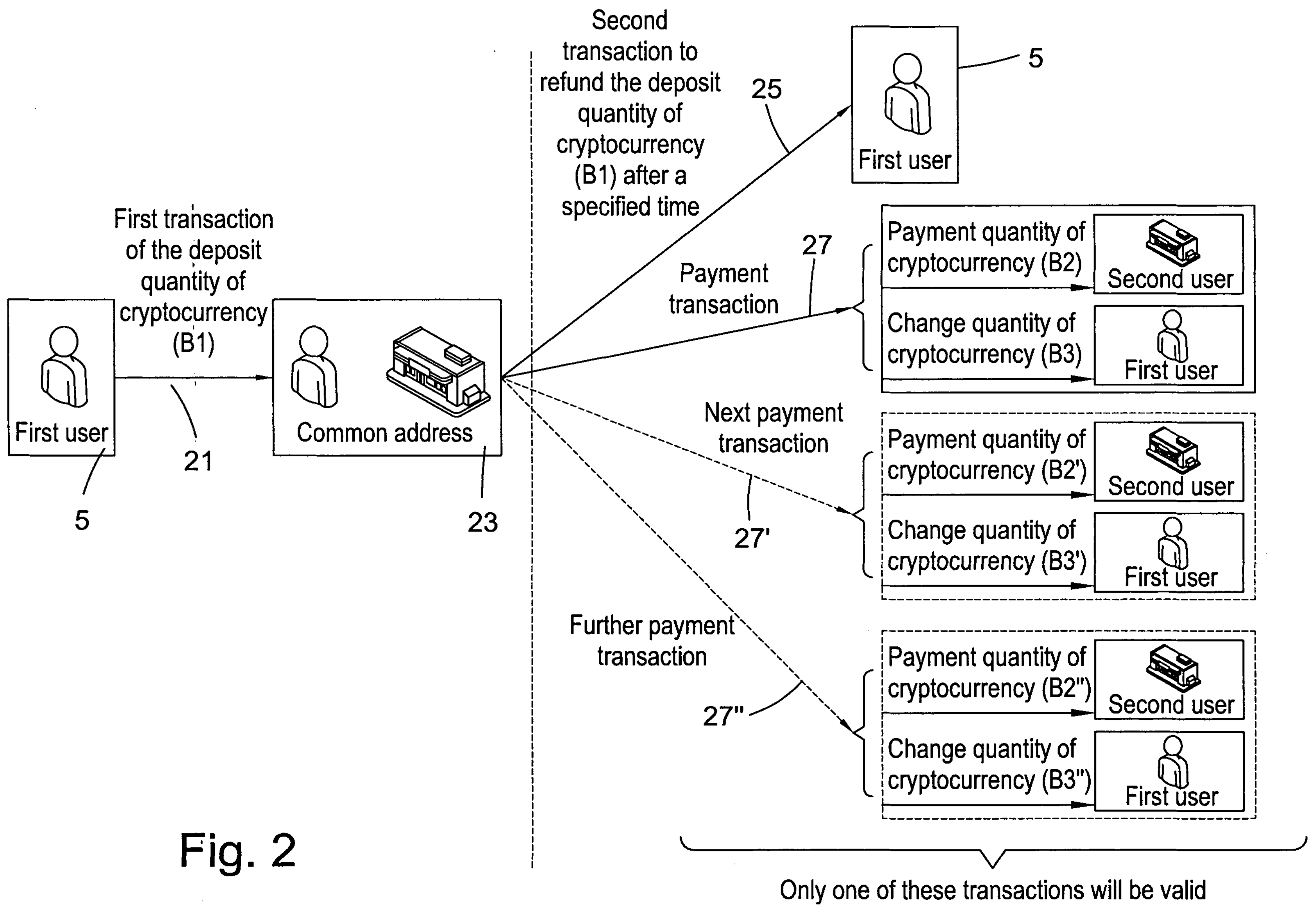

First user (A)
Second user (B)
1
5
7
15
17
Data Store
18
8
Network
Content server
3
9
Peer-to-peer distributed ledger
Data Store
11
19
19
19

Fig. 1



First user
5
First transaction of the deposit quantity of cryptocurrency (B1)
21
Common address
23
Second transaction to refund the deposit quantity of cryptocurrency (B1) after a specified time
25
First user
5
Payment transaction
27
Payment quantity of cryptocurrency (B2)
Second user
Change quantity of cryptocurrency (B3)
First user
Next payment transaction
27'
Payment quantity of cryptocurrency (B2')
Second user
Change quantity of cryptocurrency (B3')
First user
Further payment transaction
27''
Payment quantity of cryptocurrency (B2'')
Second user
Change quantity of cryptocurrency (B3'')
First user
Only one of these transactions will be valid

Fig. 2

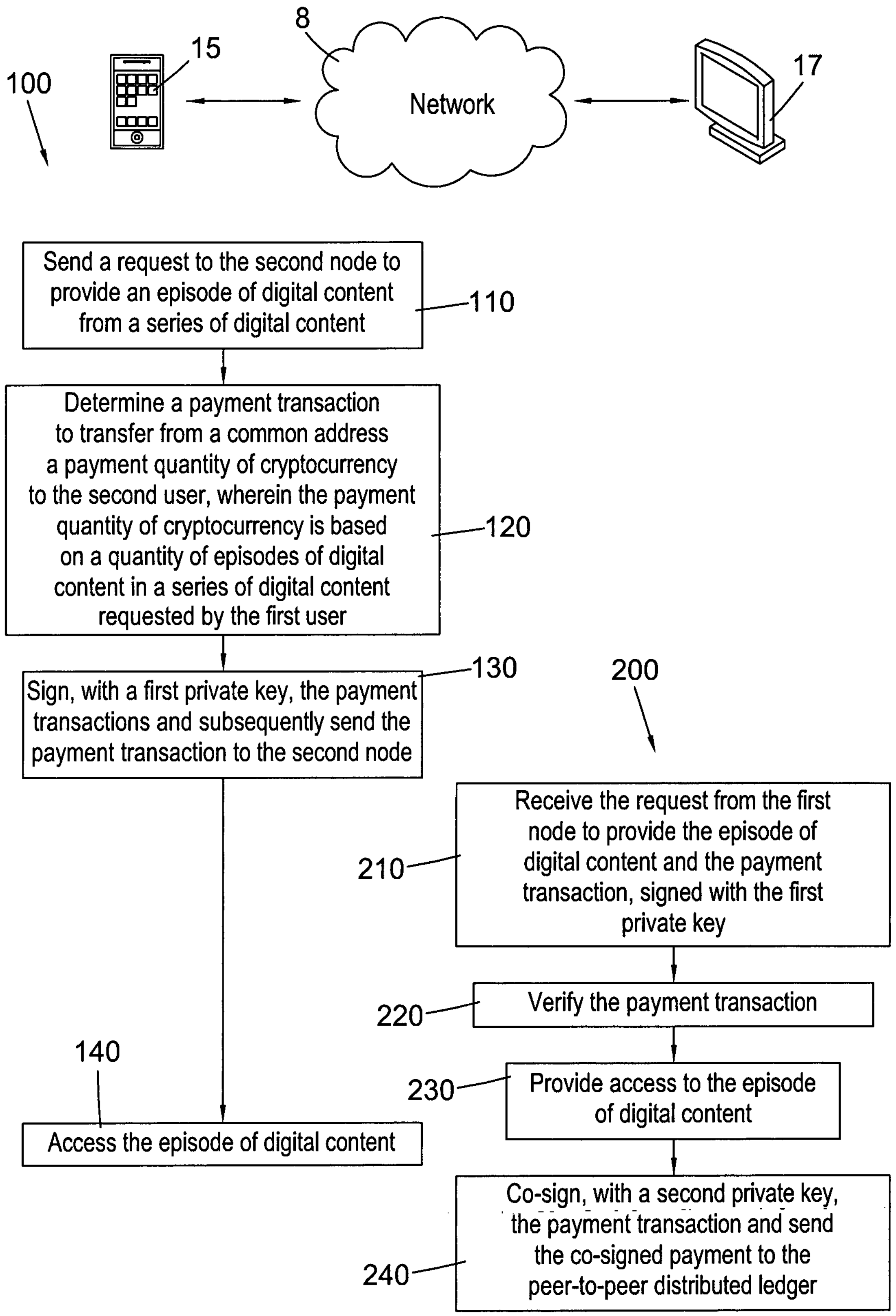

100
15
8
Network
17
Send a request to the second node to provide an episode of digital content from a series of digital content
110
Determine a payment transaction to transfer from a common address a payment quantity of cryptocurrency to the second user, wherein the payment quantity of cryptocurrency is based on a quantity of episodes of digital content in a series of digital content requested by the first user
120
Sign, with a first private key, the payment transactions and subsequently send the payment transaction to the second node
130
200
Receive the request from the first node to provide the episode of digital content and the payment transaction, signed with the first private key
210
Verify the payment transaction
220
140
Provide access to the episode of digital content
230
Access the episode of digital content
Co-sign, with a second private key, the payment transaction and send the co-signed payment to the peer-to-peer distributed ledger
240

Fig. 3

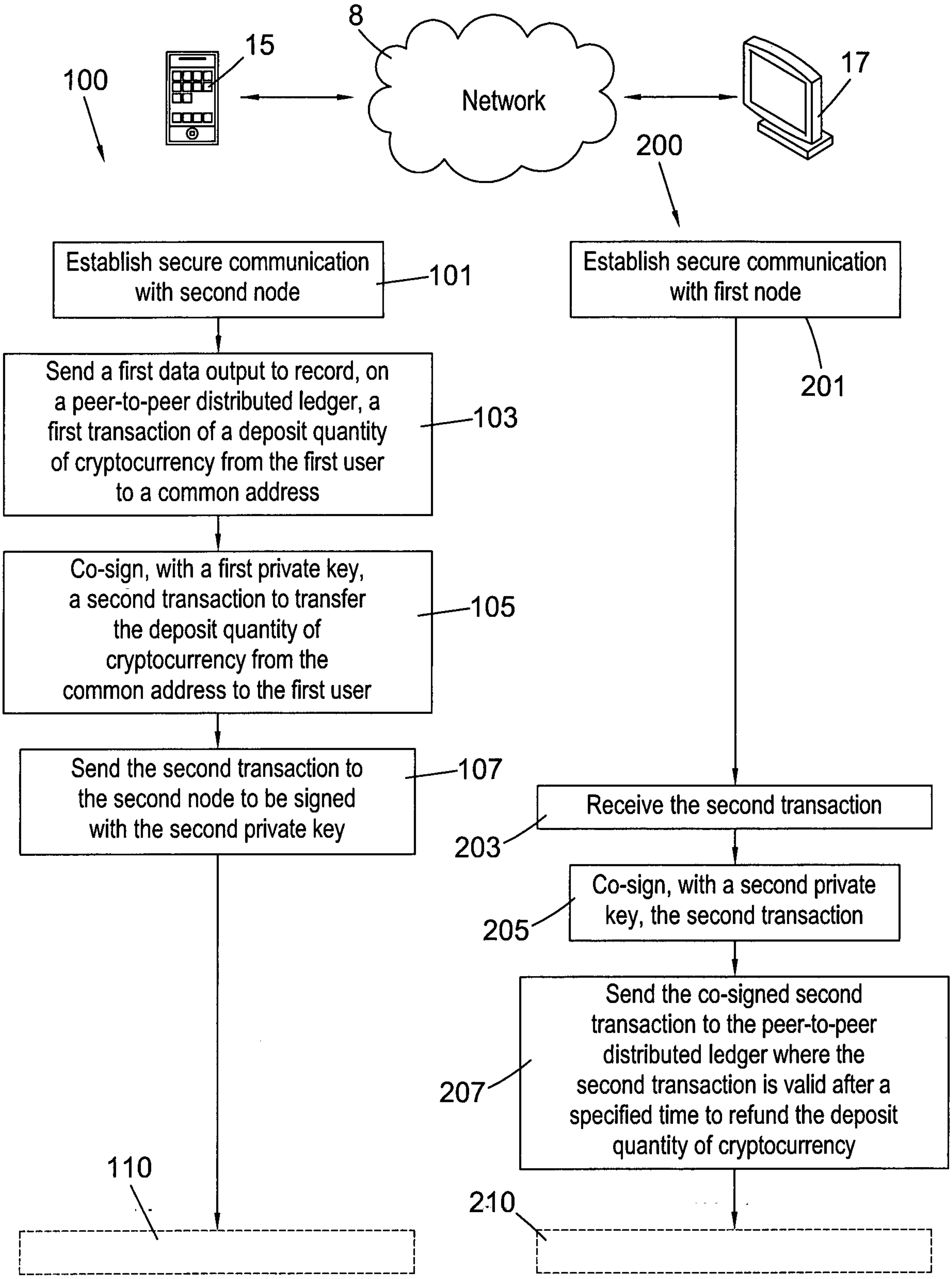

8
15
100
Network
17
200
Establish secure communication with second node
101
Establish secure communication with first node
201
Send a first data output to record, on a peer-to-peer distributed ledger, a first transaction of a deposit quantity of cryptocurrency from the first user to a common address
103
Co-sign, with a first private key, a second transaction to transfer the deposit quantity of cryptocurrency from the common address to the first user
105
Send the second transaction to the second node to be signed with the second private key
107
Receive the second transaction
203
Co-sign, with a second private key, the second transaction
205
Send the co-signed second transaction to the peer-to-peer distributed ledger where the second transaction is valid after a specified time to refund the deposit quantity of cryptocurrency
207
110
210

Fig. 4

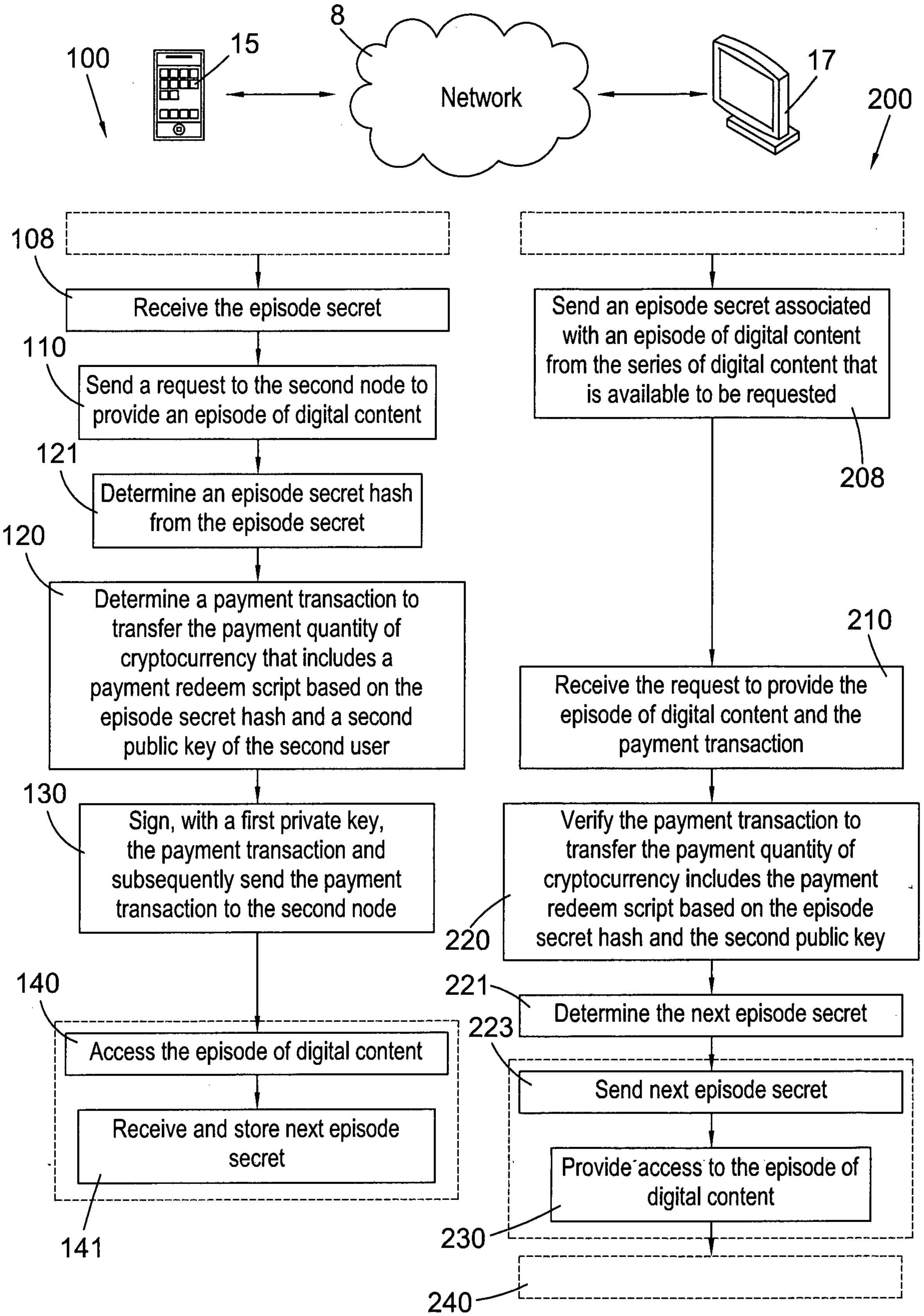

100
15
8
Network
17
200
108
Receive the episode secret
110
Send a request to the second node to provide an episode of digital content
121
Determine an episode secret hash from the episode secret
120
Determine a payment transaction to transfer the payment quantity of cryptocurrency that includes a payment redeem script based on the episode secret hash and a second public key of the second user
130
Sign, with a first private key, the payment transaction and subsequently send the payment transaction to the second node
140
Access the episode of digital content
Receive and store next episode secret
141
Send an episode secret associated with an episode of digital content from the series of digital content that is available to be requested
208
210
Receive the request to provide the episode of digital content and the payment transaction
Verify the payment transaction to transfer the payment quantity of cryptocurrency includes the payment redeem script based on the episode secret hash and the second public key
220
221
Determine the next episode secret
223
Send next episode secret
Provide access to the episode of digital content
230
240

Fig. 5

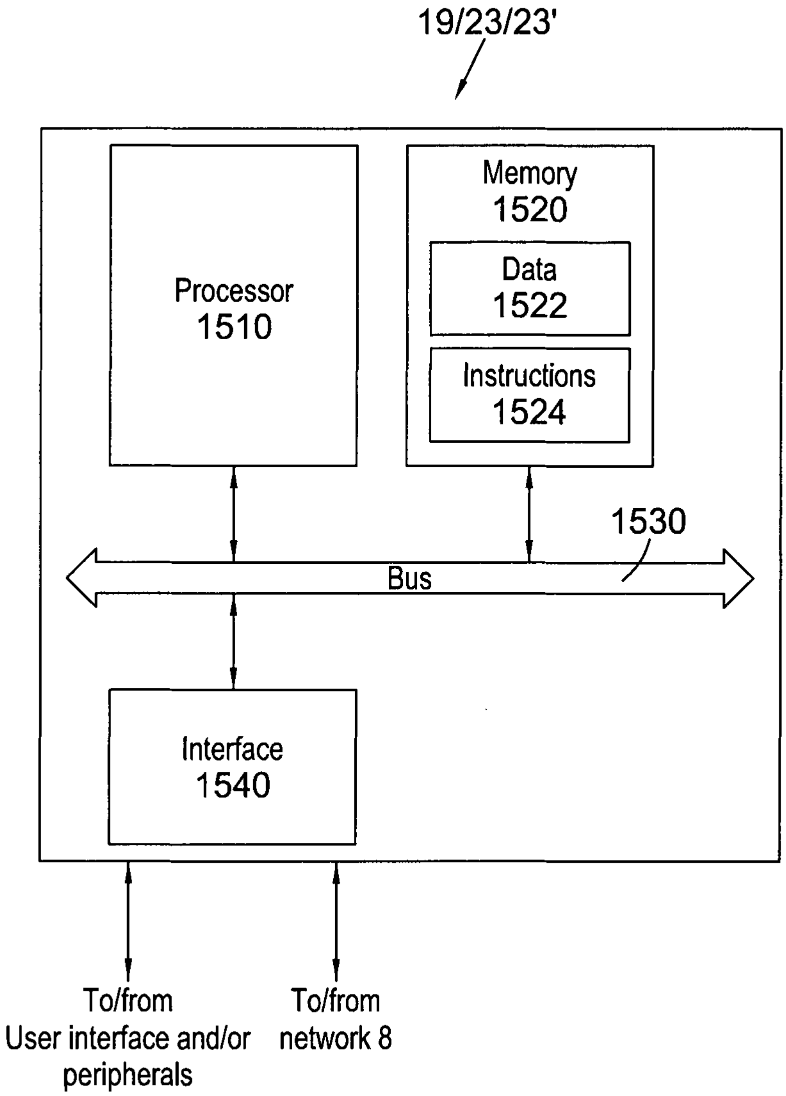

19/23/23'
Processor
1510
Memory
1520
Data
1522
Instructions
1524
1530
Bus
Interface
1540
To/from
User interface and/or
peripherals
To/from
network 8

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2017/050978

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/30 H04L9/32
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FUJIMURA SHIGERU ET AL: "BRIGHT: A concept for a decentralized rights management system based on blockchain", 2015 IEEE 5TH INTERNATIONAL CONFERENCE ON CONSUMER ELECTRONICS - BERLIN (ICCE-BERLIN), IEEE, 6 September 2015 (2015-09-06), pages 345-346, XP032855135, D0I: 10.1109/ICCE-BERLIN.2015.7391275 [retrieved on 2016-01-25] the whole document ----- -/- ·	1-29

☒ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" documentwhich may throw doubts on priority claim(s) orwhich is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 22 May 2017	Date of mailing of the international search report 31/05/2017
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Spranger, Stephanie

2

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2017/050978

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Joseph Poon ET AL: "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments", , 14 January 2016 (2016-01-14), XP055358006, Retrieved from the Internet: URL:https://lightning.network/1ightning-network-paper.pdf [retrieved on 2017-07-23] page 6, line 25 - page 42, line 7 -----	1-29
A	Gus Gutoski ET AL: "Hierarchical deterministic Bitcoin wallets that tolerate key leakage (Short paper)", , 1 February 2012 (2012-02-01), XP055369870, Retrieved from the Internet: URL:https://eprint.iacr.org/2014/998.pdf [retrieved on 2017-05-05] page 1, line 19 - page 3, line 22 page 4, line 30 - page 6, line 4 -----	1-29
A	Andreas M. Antonopoulos: "Mastering Bitcoin - Unlocking Digital Cryptocurrencies" In: "Mastering bitcoin : [unlocking digital cryptocurrencies]", 20 December 2014 (2014-12-20), O'Reilly Media, Beijing Cambridge Farnham Köln Sebastopol Tokyo, XP055306939, ISBN: 978-1-4493-7404-4 page 61, line 1 - page 138, line 13 page 161, line 1 - page 173, line 23 -----	1-29

2