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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 May 2021 (27.05.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/102041 A1

(51) International Patent Classification:
G06Q 20/38 (2012.01)

(21) International Application Number:
PCT/US2020/061111

(22) International Filing Date:
18 November 2020 (18.11.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/939,501 22 November 2019 (22.11.2019) US
16/951,747 18 November 2020 (18.11.2020) US

(71) Applicant: **CONIO INC.** [US/US]; c/o The Orrick Building, 405 Howard Street, San Francisco, California 94105 (US).

(72) Inventors: **DI NICOLA, Vincenzo**; Conio Inc., c/o The Orrick Building, 405 Howard Street, San Francisco, California 94105 (US). **SALA, Massimiliano**; Conio Inc., c/o The Orrick Building, 405 Howard Street, San Francisco, California 94105 (US). **MENEGHETTI, Alessio**; Conio Inc., c/o The Orrick Building, 405 Howard Street, San Francisco, California 94105 (US). **LONGO, Riccardo**; Conio Inc., c/o The Orrick Building, 405 Howard Street, San Francisco, California 94105 (US).

(74) Agent: **BATHURST, K. Brian** et al.; Carr & Ferrell LLP, 120 Constitution Drive, Menlo Park, California 94025 (US).

(81) Designated States *(unless otherwise indicated, for every kind of 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, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN,

(54) Title: METHOD AND APPARATUS FOR A BLOCKCHAIN-AGNOSTIC SAFE MULTI-SIGNATURE DIGITAL ASSET MANAGEMENT

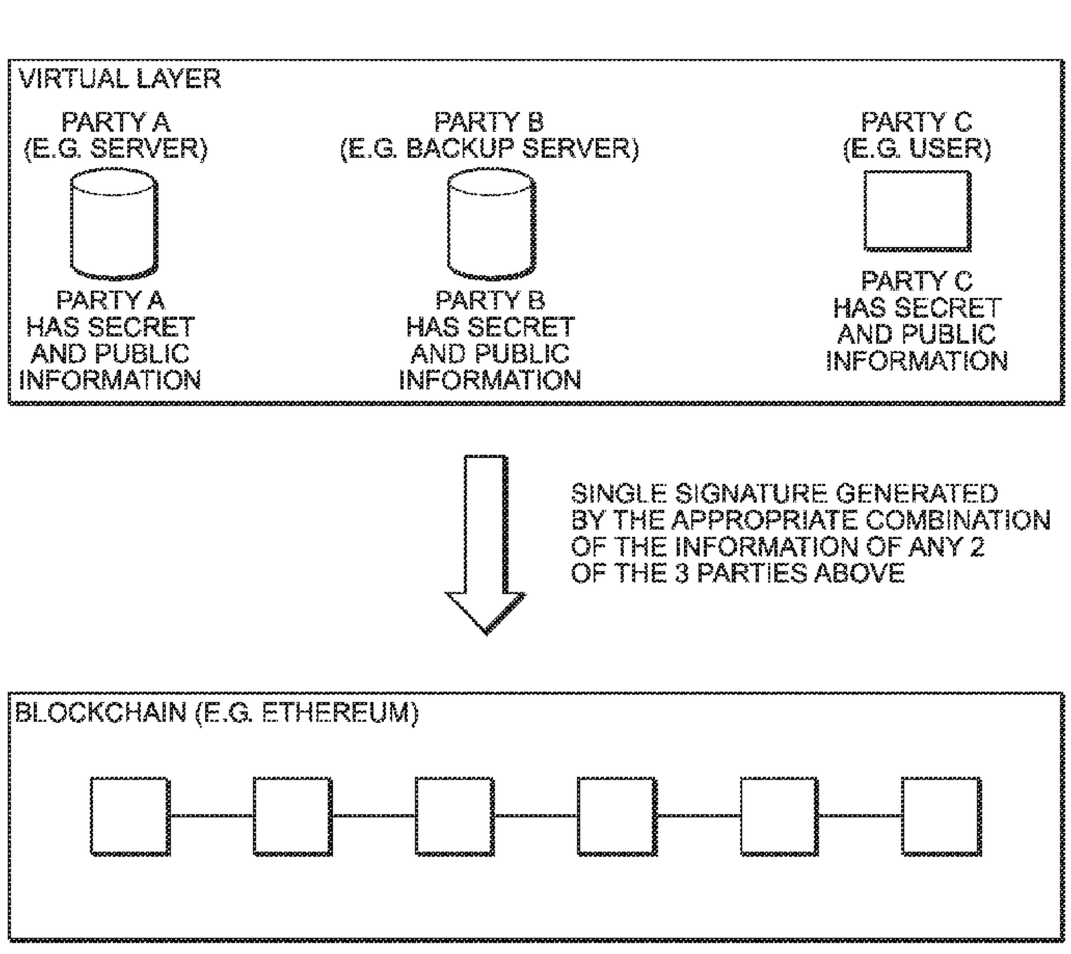

FIG. 1

(57) Abstract: Exemplary embodiments provided herein include a method for safe creation, custody, recovery and management of a digital asset, agnostic to an underlying blockchain technology, the method including establishing a virtual layer where three private keys are generated, transacting the digital asset by using two of three of the private keys and multi-party computation techniques, abstracting interactions between the three private keys from the underlying blockchain technology, having a digital asset transaction considered as a single-signature by the underlying blockchain technology, and recovering the digital asset if any of the three private keys is no longer available. Additionally, the digital asset may be a cryptocurrency, and a party may be disconnected from any network during the normal user operation phases. Furthermore, the digital asset transaction may be considered as a single-signature, as seen by the underlying blockchain technology, and is associated to a public key PK_ABC.

[Continued on next page]

WO 2021/102041 A1

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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of 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))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

METHOD AND APPARATUS FOR A BLOCKCHAIN-AGNOSTIC SAFE MULTI-SIGNATURE DIGITAL ASSET MANAGEMENT

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims the priority benefit of U.S. Provisional Patent Application Serial No. 62/939,501 filed on November 22, 2019 titled "Method and Apparatus for a Blockchain-Agnostic Safe Multi-Signature Digital Asset Management," which is hereby incorporated by reference in its entirety.

FIELD OF INVENTION

[0002] The present technology pertains to a method and apparatus for digital asset management independent of the type of blockchain employed.

SUMMARY OF EXEMPLARY EMBODIMENTS

[0003] The exemplary embodiments provided herein include a method for safe creation, custody, recovery and management of a digital asset, agnostic to an underlying blockchain technology, the method including establishing a virtual layer where three private keys are generated, transacting the digital asset by using two of three of the private keys and multi-party computation techniques, abstracting interactions between the three private keys from the underlying blockchain technology, having a digital asset transaction considered as a single-signature by the underlying blockchain technology, and recovering the digital asset if any of the three private keys is no longer available. Additionally, the digital asset may be a cryptocurrency, and a party may be disconnected from any network during the normal user operation phases.

[0004] The digital asset transaction, according to various exemplary embodiments, may be considered as a single-signature, as seen by the underlying blockchain technology, and associated to a public key PK_ABC that is created and used to verify the transaction. Additionally, the digital asset may be transacted and recovered through derived keys.

[0005] In further exemplary embodiments, a first party [B] may generate a private and public information pair (sk_B; pk_B) and transmit the public information (pk_B) to a second party [A]. The first party [B] may keep the private information sk_B secret and never reveal it. A third party [C] may initiate communication with the second party [A] and transmit the public information pk_B to the third party [C] and the second party [A] may generate a secret s_A and two shards σ_AB and σ_AC. Additionally, the third party [C] may generate a secret s_C and two shards σ_CA and σ_CB, the second party [A] may generate a shard σ_BA, and the third party [C] may generate a shard σ_BC. The second party [A] may encrypt shard σ_AB and shard σ_BA with the public information

pk_B, getting rec_AB, and the third party [C] may encrypt shard σ_CB and shard σ_BC with the public information pk_B, getting rec_CB.

[0006] Additionally, the second party [A], according to many exemplary embodiments, may send (σ_AC; rec_AB) to the third party [C] and the third party [C] may send (σ_CA; rec_CB) to the second party [A]. The second party [A] may compute the private key SK_A, generated by using s_A, σ_BA and σ_CA, and the third party [C] may compute the private key SK_C, by using s_C, σ_BC and σ_AC. By combining a signature of private keys (SK_A, SK_C) a digital asset may be transacted. Furthermore, the second party [A] and the third party [C] may compute a public key PK_ABC. The public key PK_ABC may be communicated to a blockchain underneath the virtual layer, and the blockchain underneath the virtual layer may use the public key PK_ABC to verify that a signature is valid. In various exemplary embodiments, the signature may be created on the virtual layer by multiple private keys and the blockchain underneath the virtual layer may have access only to the public key PK_ABC and the signature. The blockchain underneath the virtual layer may not have access to the multiple private keys on the virtual layer. Additionally, the second party [A] and the third party [C] may sign a transaction by using the private keys SK_A and SK_C and multi-party computation techniques.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The accompanying drawings, where like reference numerals refer to identical or functionally similar elements throughout the separate views, together with the detailed description below, are incorporated in and form part of the specification, and serve to further illustrate embodiments of concepts that include the claimed disclosure, and explain various principles and advantages of those embodiments.

[0008] The methods and systems disclosed herein have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent to understanding the embodiments of the present disclosure so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein.

[0009] FIG. 1 illustrates the various exemplary embodiments described herein that allow for a blockchain-agnostic safe multi-signature digital asset management.

[0010] FIG. 2 shows the Preliminary Phase.

[0011] FIG 3. shows the Enrollment Phase.

[0012] FIG 4. shows the Ordinary Signature Phase.

[0013] FIG 5. shows the Recovery Signature Phase where C is unable to sign.

[0014] FIG 6. shows the Recovery Signature Phase where A is unable to

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

[0015] While the present technology is susceptible of embodiment in many different forms, there is shown in the drawings and will herein be described in detail several specific embodiments with the understanding that the present disclosure is to be considered as an exemplification of the principles of the present technology and is not intended to limit the technology to the embodiments illustrated.

[0016] Digital assets (for example, cryptocurrencies such as Bitcoin, or tokens created with certain blockchains) are at their core defined by a single Public Key and Private Key pair. A digital asset transaction (for example, a digital asset transfer) is digitally signed with the original owner's Private Key, and any external observer can verify it by using the corresponding Public Key.

[0017] A Public Key can be communicated to the whole world, while the Private Key must be kept private by the owner. If the Private Key is lost, the owner can no longer access their digital asset. If the Private Key is given to or copied by someone else, that someone else can transact the digital asset, effectively stealing it from the owner.

[0018] In order to prevent this, a number of approaches have been suggested to safeguard the Private Key. For example, divide the Private Key in multiple parts, make multiple copies of each part, and store them in different secure places. Such approaches are manual, require a "ceremony" with the physical presence of several operators in the same place, and the loss of a part of the Private Key may still result in the total loss of the Private Key.

[0019] Other approaches rely on multiple Private Keys, preferably handled by different entities, where a minimum number of different Private Key signatures are needed to create a digital asset transaction. Such approaches are

specific to each different underlying blockchain technology (e.g., a multi-signature scheme on the Bitcoin blockchain is different from a multi-signature scheme on the Ethereum blockchain). In addition, some blockchains may not even allow a multi-signature scheme, and are simply limited to a single-signature scheme.

[0020] FIG. 1 illustrates the various exemplary embodiments described herein that allow for blockchain-agnostic safe multi-signature digital asset management.

[0021] Shown in FIG. 1 is a virtual layer and an underlying blockchain. Included in the virtual layer is Party A, for example, a server including one or more hardware processors executing instructions stored in a non-transitory computer readable medium. Party A has secret and public information. Also shown is Party B, for example, a backup server including one or more hardware processors executing instructions stored in a non-transitory computer readable medium. Party B has secret and public information. Party C, for example, a user, is shown. Party C has secret and public information. Party C may also have a server including one or more hardware processors executing instructions stored in a non-transitory computer readable medium, or a smartphone or other personal computing device. A single signature is generated by the appropriate combination of the information of any two of the three parties.

[0022] The exemplary embodiments herein do not need the underlying blockchain to support multi-signature schemes. They effectively create a virtual layer, where parties deal with a multi-signature scheme and the underlying blockchain deals with a single-signature scheme. As a bonus result, since the digital asset transactions are effectively single-signature on the blockchain, their size and cost are smaller than the approaches mentioned earlier.

[0023] According to various exemplary embodiments, they do not even need anyone to know what the Private Key related to the single-signature is (such a Private Key may not even be created at all), and it still allows transactions of the digital asset. Nor do all of the parties need to be online at the same time. One of the parties may even be disconnected from any network, and it still allows transactions of the digital asset.

[0024] In many exemplary embodiments, by applying the correct recovery methods, they effectively prevent the loss or theft of digital assets and also allow solving special real-life situations like transfer of a digital asset to an heir.

[0025] The various exemplary embodiments described herein are still able to enhance privacy by preventing the so-called address reusing: on the virtual layer, they properly derive the parties Private Keys and, on the underlying single-signature blockchain, for each derivation, a different Public Key (address) is generated.

[0026] According to various exemplary embodiments, there are three parties and four phases.

[0027] Parties:

[0028] A: a server, always online. In certain embodiments, it is offered by a service provider.

[0029] B: a backup server, online only in the preliminary phase and the recovery phase. In certain embodiments, it is offered by a provider different from A (for example, B may be a financial institution). In other embodiments, it may be handled by the user C itself if the user does not want to rely on other providers.

[0030] C: the user, online starting from the enrollment phase. In certain embodiments, it is a person who wants digital assets, and may not even be known in the preliminary phase.

[0031] Phases:

[0032] Preliminary.

[0033] Enrollment.

[0034] Ordinary Signature.

[0035] Recovery Signature.

[0036] Communications between parties A, B and C may take place on insecure channels. So standard encryption mechanisms (e.g. HTTPS) are to be used.

[0037] The various exemplary embodiments described herein effectively create a virtual layer, where 3 Private Keys exist. They require at least any two Private Keys out of the three ("2-of-3") to create a signature, using proper threshold signature mechanisms. The blockchain underneath the virtual layer sees such a signature as if being signed by a single Private Key, and can verify it with its corresponding Public Key.

[0038] The various exemplary embodiments are structured so that all three parties' Private Keys are different from each other. It is also structured so that all three parties need not to be online at the same time. Additionally, one party may even cease to exist or not be available at all, and the digital asset can still be transacted or recovered.

[0039] FIG. 2 shows the Preliminary Phase.

[0040] Shown in FIG. 2 are Party B and Party A. Party B generates Party B's secret and public information. Party B sends Party B's public information to Party A. Party A receives Party B's public information.

[0041] As shown in FIG. 2, the process starts with a Preliminary Phase. This phase occurs only once, at the very beginning. The parties involved in this phase are A and B:

[0042] B generates a non-ephemeral private/public information pair (sk_B; pk_B).

[0043] B sends the public information pk_B to A.

[0044] B keeps the private information sk_B secret and never reveals it to the other parties.

[0045] FIG 3. shows the Enrollment Phase.

[0046] Shown in FIG. 3 are Party A and Party C. Party A sends Party B's public information to Party C. Party A also generates Party A's secret information, and combined Party A,C and A,B information. Party A sends the combined Party A,C and A,B information to Party C. Party A receives combined Party C,A and C,B information from Party C and generates private key SK_A and public key PK_ABC.

[0047] Party C receives Party B's public information from Party A. Party C generates Party C's secret information and combined Party C,A and C,B information. Party C receives combined Party A,C and A,B information from Party A. Party C sends combined Party C,A and C,B information to Party A. Party C also generates private key SK_C and public key PK_ABC.

[0048] The enrollment phase occurs whenever C, a new user, wants to deal with digital assets, and so it initiates its communication with A. The parties involved in this phase are A and C:

[0049] A sends pk_B to C.

[0050] Secrets generation:

[0051] A generates a secret s_A and two shards σ_AB and σ_AC.

[0052] C generates a secret s_C and two shards σ_CA and σ_CB.

[0053] A generates a shard σ_BA.

[0054] C generates a shard σ_BC.

[0055] A encrypts σ_AB and σ_BA with the public information pk_B, getting recovery secret "rec"_AB.

[0056] C encrypts σ_CB and σ_BC with the public information pk_B, getting rec_CB.

[0057] A shard is a piece of data meant to be combined with other shards or secret information to create some data in a multi-party computation protocol.

[0058] Shards communication:

[0059] A sends (σ_AC; rec_AB) to C.

[0060] C sends (σ_CA; rec_CB) to A.

[0061] A and C Private Keys generation:

[0062] A computes the Private Key SK_A, generated using s_A, σ_BA and σ_CA.

[0063] C computes the Private Key SK_C, generated using s_C, σ_BC and σ_AC.

[0064] The combined signature of these two Private Keys (SK_A, SK_C) allows to transact the digital asset ("2-of-3" signature scheme).

[0065] Public Key generation: A and C compute the public key PK_ABC. Such Public Key (PK_ABC) is communicated to the world. The blockchain underneath the virtual layer knows it, and may use it to verify that the signature (created on the virtual layer by multiple Private Keys) is valid. As a result, the underlying blockchain sees only a Public Key and a single signature: it is not aware that this is the result of multiple Private Keys on the virtual layer.

[0066] Common secret generation: A and C compute a common secret d, based on the shards σ_BA and σ_BC, that can be used to derive other keys without performing another enrollment.

[0067] It is worth noting that both A and C have the pair of encrypted recovery secrets (rec_AB; rec_CB), but none of them has the corresponding plaintext content in full: the only party who is able to fully decrypt (rec_AB; rec_CB) is B.

[0068] It is also worth noting that Private Key SK_ABC is not created and may never be created at all in any phase.

[0069] FIG 4. shows the Ordinary Signature Phase.

[0070] Shown in FIG. 4 are Party C and Party A. Party C signs a digital asset transaction with private key SK_C and multi-party computation techniques. Secure multi-party computation (also known as secure computation, multi-party computation (MPC), or privacy-preserving computation) is a subfield of cryptography with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private. Unlike traditional cryptographic tasks, where cryptography assures security and integrity of communication or storage and the adversary is outside the system of participants (an eavesdropper on the sender and receiver), the cryptography in this model protects participants' privacy from each other.

[0071] Also shown in FIG. 4, Party A signs a digital asset transaction with private key SK_A and multi-party computation techniques. The resulting signature of this "2-of-3" scheme is verifiable by anyone with the public key PK_ABC. This also supports key derivation. In such a case, Party A and Party C sign with private key Ski_A and Ski_C and multi-party computation techniques. The resulting signature is verifiable by anyone with the public key PKi_ABC.

[0072] As shown in FIG. 4, the Ordinary Signature Phase occurs whenever C, an existing user, wants to sign a digital asset transaction. The parties involved in this phase are A and C:

[0073] A and C sign the transaction by using the Private Keys SK_A and SK_C and multi-party computation techniques. The signature is verifiable by anyone with the public key PK_ABC.

[0074] In this phase, exemplary embodiments are also able to support "Key Derivation." That is, the Private Keys SK_A and SK_C obtained in the Enrollment Phase can be utilized directly to sign messages and transactions, or they can be used to derive deterministically other key pairs. For example, in Bitcoin it is good practice to always use new addresses that correspond to different keys (as seen in BIP32).

[0075] Various exemplary embodiments use their own way to derive keys: it is sufficient that A and C agree on a (public) derivation index i; then, using the common secret d computed during the Enrollment phase, they can independently derive the keys SKi_A and SKi_C, and use them in the Signature phase in place of SK_A and SK_C, respectively. Note that the derived Private Keys correspond to a new Public Key PKi_ABC. The derivation can also be compounded: that is, more keys can be derived from a derived key.

[0076] FIG 5. shows the Recovery Signature Phase where C is unable to sign.

[0077] Shown in FIG. 5 are Party A and Party B. Party A sends combined Party A,B and C,B information to Party B. Party A also signs a digital asset transaction with private key SK_A and multi-party computation techniques. Party B receives the combined Party A,B and C,B information from Party A, generates private key SK_B and signs a digital asset transaction with private key SK_B and multi-party computation techniques. Signature verification

and eventual key derivation operations are analogous to the ones in the Ordinary Signature Phase.

[0078] As shown in FIG. 5, certain exemplary embodiments comprise a Recovery Signature phase. This phase occurs whenever A or C can no longer sign a transaction, e.g. because one of them has lost their secret key material. As a result, the solution is able to recover a digital asset even if one of the parties is no longer available. If C is unable to sign, then the actors involved in this phase are A and B:

[0079] Communication:

[0080] A contacts B, which comes back online to join the Recovery Signature phase.

[0081] A sends (rec_AB; rec_CB) to B.

[0082] B Private Key creation:

[0083] B decrypts rec_AB and rec_CB using the secret key sk_B, getting (σ_AB; σ_BA; σ_CB; σ_BC).

[0084] B generates the secret s_B by using σ_BA and σ_BC. B generates the Private Key SK_B by using s_B, σ_AB and σ_CB. This key is compatible with the "2-of-3" multi-signature scheme.

[0085] B computes the common secret d using σ_BA and σ_BC.

[0086] A and B sign the transaction using the Private Keys SK_A and SK_B respectively (or the derived keys SKi_A and SKi_B, computed using the common secret d and a derivation index i on which they agreed), using computation techniques analogous to the ones used in in the Ordinary Signature phase. This signature is verifiable by anyone with the public key PK_ABC (or the derived PKi_ABC).

[0087] The digital asset is transferred to a new digital wallet.

[0088] FIG 6. shows the Recovery Signature Phase where A is unable to sign.

[0089] Shown in FIG. 6 are Party C and Party B. Party C sends combined Party A,B and C,B information to Party B. Party C also signs a digital transaction with private key SK_C and multi-party computation techniques. Party B receives combined Party A,B and C,B information from Party C. Party B generates private key SK_B and signs a digital transaction with private key SK_B and multi-party computation techniques. Signature verification and eventual key derivation operations are analogous to the ones in the Ordinary Signature Phase.

[0090] As shown in FIG. 6, if A is unable to sign, then the actors involved in this phase are B and C:

[0091] Communication:

[0092] C contacts B, which comes back online to join the Recovery Signature phase.

[0093] C sends (rec_AB; rec_CB) to B.

[0094] B Private Key creation:

[0095] B decrypts rec_AB and rec_CB using the secret key sk_B, getting (σ_AB; σ_BA; σ_BC; σ_CB).

[0096] B generates the secret s_B by using σ_BA and σ_BC.

[0097] B generates the Private Key SK_B by using s_B, σ_AB and σ_CB. This key is compatible with the "2-of-3" multi-signature scheme.

[0098] B computes the common secret d using σ_BA and σ_BC.

[0099] C and B sign the transaction using the Private Keys SK_C and SK_B respectively (or the derived keys SKi_C and SKi_B, computed using the common secret d and a derivation index i on which they agreed), using computation techniques analogous to the ones used in in the Ordinary Signature

phase. This signature is verifiable by anyone with the public key PK_ABC (or the derived PKi_ABC).

[00100] The digital asset is transferred to a new digital wallet.

[00101] While specific embodiments of, and examples for, the system are described above for illustrative purposes, various equivalent modifications are possible within the scope of the system, as those skilled in the relevant art will recognize. For example, while processes or steps are presented in a given order, alternative embodiments may perform routines having steps in a different order, and some processes or steps may be deleted, moved, added, subdivided, combined, and/or modified to provide alternative or sub-combinations. Each of these processes or steps may be implemented in a variety of different ways. Also, while processes or steps are at times shown as being performed in series, these processes or steps may instead be performed in parallel, or may be performed at different times.

[00102] While various embodiments have been described above, it should be understood that they have been presented by way of example only, and not limitation. The descriptions are not intended to limit the scope of the present technology to the particular forms set forth herein. To the contrary, the present descriptions are intended to cover such alternatives, modifications, and equivalents as may be included within the spirit and scope of the present technology as appreciated by one of ordinary skill in the art. Thus, the breadth and scope of a preferred embodiment should not be limited by any of the above-described exemplary embodiments.

CLAIMS

What is claimed is:

1. A method for safe creation, custody, recovery and management of a digital asset, agnostic to an underlying blockchain technology, the method comprising:

establishing a virtual layer where three private keys are generated;

transacting the digital asset by using two of three of the private keys and multi-party computation techniques;

abstracting interactions between the three private keys from the underlying blockchain technology;

having a digital asset transaction considered as a single-signature by the underlying blockchain technology;

recovering the digital asset if any of the three private keys is no longer available.

2. The method of claim 1, wherein the digital asset is a cryptocurrency.

3. The method of claim 1, further comprising disconnecting a party from any network during the normal user operation phases.

4. The method of claim 1, further comprising the digital asset transaction considered as a single-signature, as seen by the underlying blockchain technology, is associated to a private key SK_ABC that is never created.

5. The method of claim 1, further comprising the digital asset transaction considered as a single-signature, as seen by the underlying blockchain technology, is associated to a public key PK_ABC that is created and that is used to verify the transaction.

6. The method of claim 1, further comprising transacting and recovering the digital asset through derived keys.

7. A method comprising:

a first party [B] generating a private and public information pair (sk_B; pk_B);

the first party [B] transmitting the public information (pk_B) to a second party [A].

8. The method of claim 7, further comprising:

the first party [B] keeping the private information sk_B secret and never revealing it.

9. The method of claim 8, further comprising:

a third party [C] initiating communication with the second party [A];

the second party [A] transmitting the public information pk_B to the third party [C];

the second party [A] generating a secret s_A and two shards σ_AB and σ_AC;

the third party [C] generating a secret s_C and two shards σ_CA and σ_CB;

the second party [A] generating a shard σ_BA; and

the third party [C] generating a shard σ_BC.

10. The method of claim 9, further comprising:

the second party [A] encrypting shard σ_AB and shard σ_BA with the public information pk_B, getting rec_AB;

the third party [C] encrypting shard σ_CB and shard σ_BC with the public information pk_B, getting rec_CB.

11. The method of claim 10, further comprising:

the second party [A] sending (σ_AC; rec_AB) to the third party [C]; and

the third party [C] sending (σ_CA; rec_CB) to the second party [A].

12. The method of claim 11, further comprising:

the second party [A] computing the private key SK_A, generated using s_A, σ_BA and σ_CA; and

the third party [C] computing the private key SK_C, generated using s_C, σ_BC and σ_AC.

13. The method of claim 12, further comprising:

combining a signature of private keys (SK_A, SK_C) to transact a digital asset.

14. The method of claim 13, further comprising the second party [A] and the third party [C] computing a public key PK_ABC.

15. The method of claim 14, further comprising communicating the public key PK_ABC to a blockchain underneath a virtual layer.

16. The method of claim 15, further comprising the blockchain underneath the virtual layer using the public key PK_ABC to verify that a signature is valid.

17. The method of claim 16, further comprising the signature being created on the virtual layer by multiple private keys.

18. The method of claim 17, further comprising the blockchain underneath the virtual layer having access only to the public key PK_ABC and the signature.

19. The method of claim 18, further comprising the blockchain underneath the virtual layer not having access to the multiple private keys on the virtual layer.

20. The method of claim 19, further comprising:

the second party [A] and the third party [C] signing a transaction by using the private keys SK_A and SK_C and multi-party computation techniques.

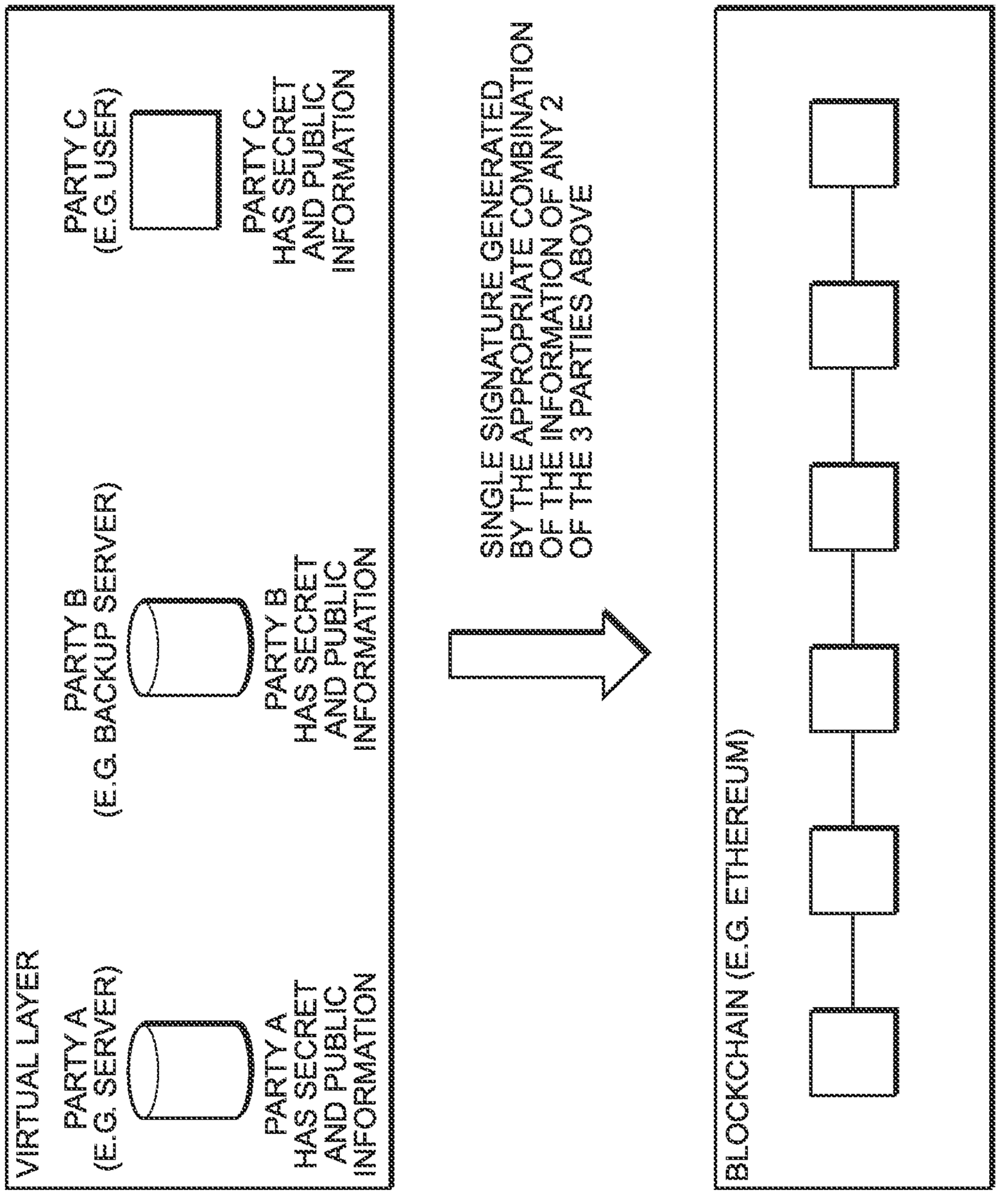
VIRTUAL LAYER
PARTY A
(E.G. SERVER)
PARTY A
HAS SECRET
AND PUBLIC
INFORMATION
PARTY B
(E.G. BACKUP SERVER)
PARTY B
HAS SECRET
AND PUBLIC
INFORMATION
PARTY C
(E.G. USER)
PARTY C
HAS SECRET
AND PUBLIC
INFORMATION
SINGLE SIGNATURE GENERATED
BY THE APPROPRIATE COMBINATION
OF THE INFORMATION OF ANY 2
OF THE 3 PARTIES ABOVE
BLOCKCHAIN (E.G. ETHEREUM)

FIG. 1

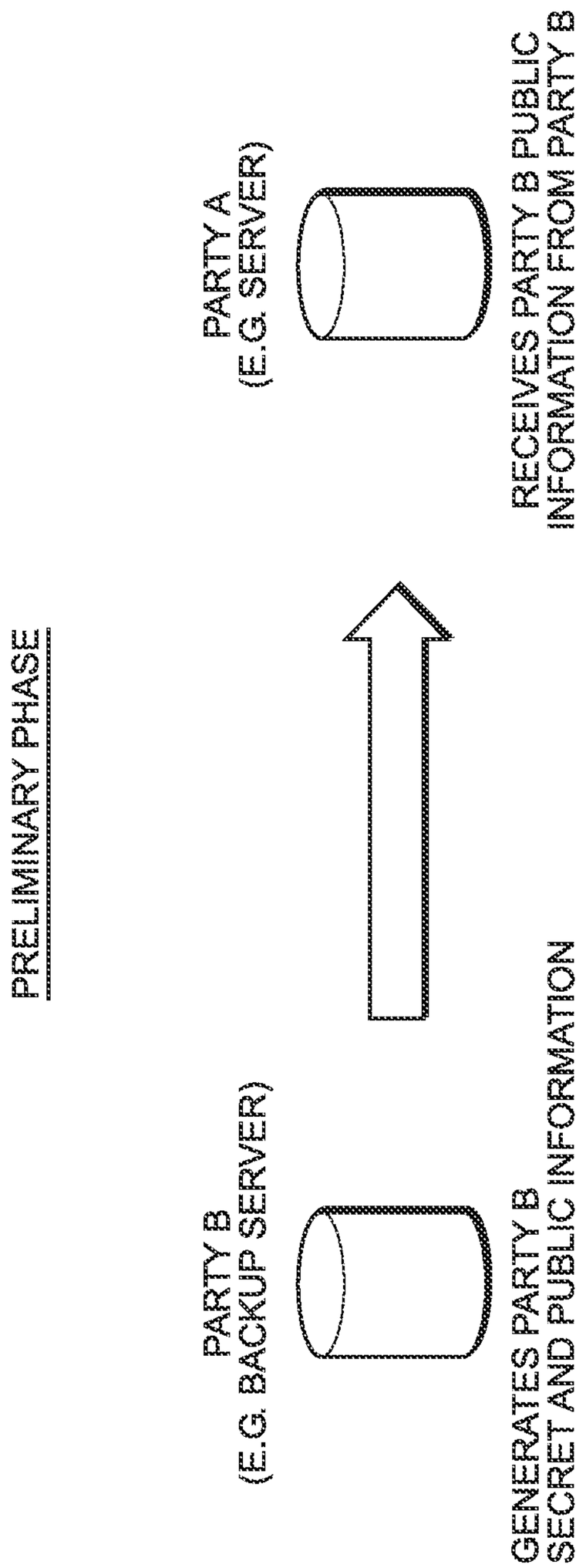
PRELIMINARY PHASE
PARTY B
(E.G. BACKUP SERVER)
GENERATES PARTY B
SECRET AND PUBLIC INFORMATION
SENDS PARTY B PUBLIC INFORMATION
TO PARTY A
PARTY A
(E.G. SERVER)
RECEIVES PARTY B PUBLIC
INFORMATION FROM PARTY B

FIG. 2

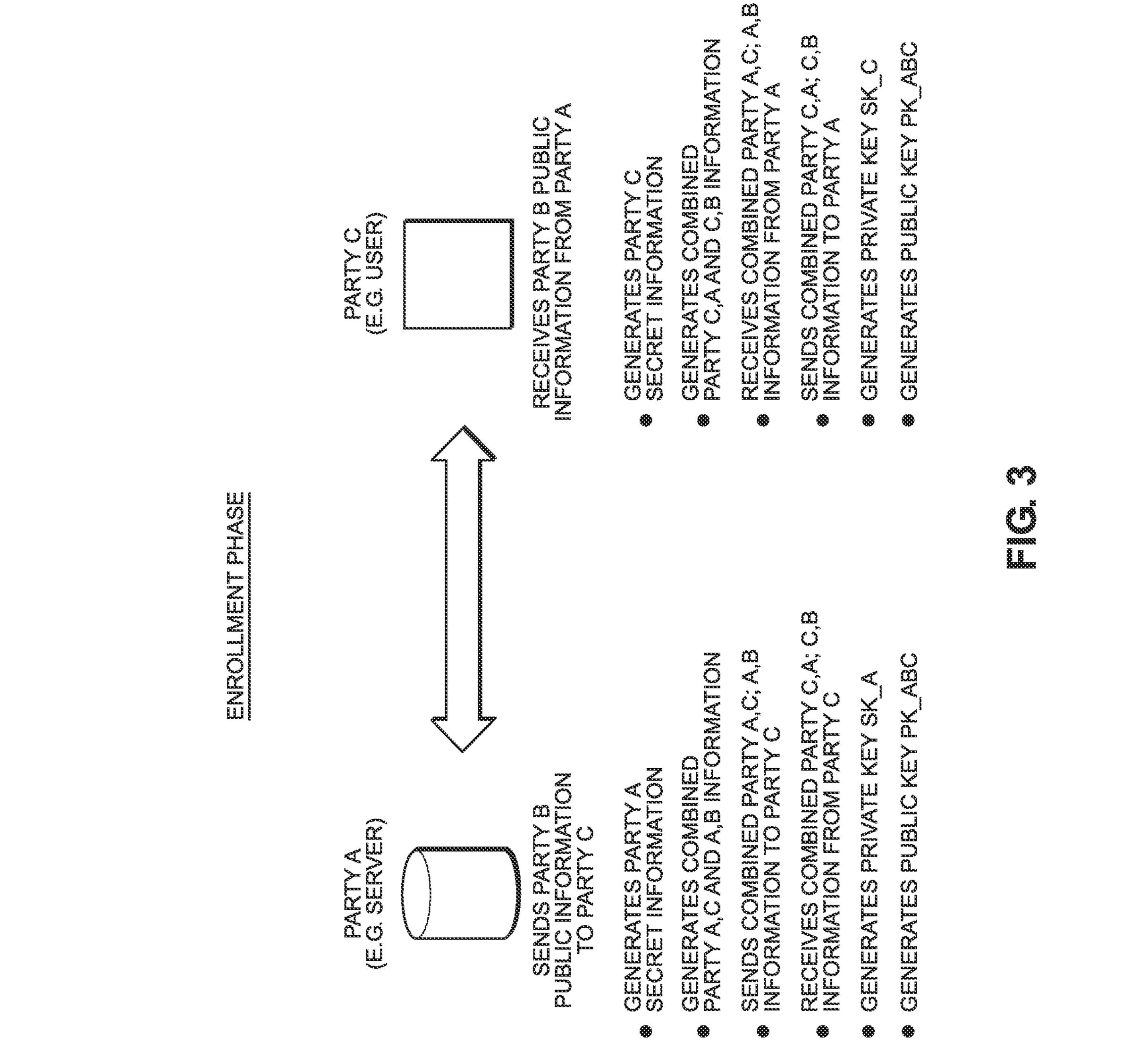
ENROLLMENT PHASE
PARTY A
(E.G. SERVER)
SENDS PARTY B
PUBLIC INFORMATION
TO PARTY C
GENERATES PARTY A
SECRET INFORMATION
GENERATES COMBINED
PARTY A,C AND A,B INFORMATION
SENDS COMBINED PARTY A,C; A,B
INFORMATION TO PARTY C
RECEIVES COMBINED PARTY C,A; C,B
INFORMATION FROM PARTY C
GENERATES PRIVATE KEY SK_A
GENERATES PUBLIC KEY PK_ABC
PARTY C
(E.G. USER)
RECEIVES PARTY B PUBLIC
INFORMATION FROM PARTY A
GENERATES PARTY C
SECRET INFORMATION
GENERATES COMBINED
PARTY C,A AND C,B INFORMATION
RECEIVES COMBINED PARTY A,C; A
INFORMATION FROM PARTY A
SENDS COMBINED PARTY C,A; C,B
INFORMATION TO PARTY A
GENERATES PRIVATE KEY SK_C
GENERATES PUBLIC KEY PK_ABC

FIG. 3

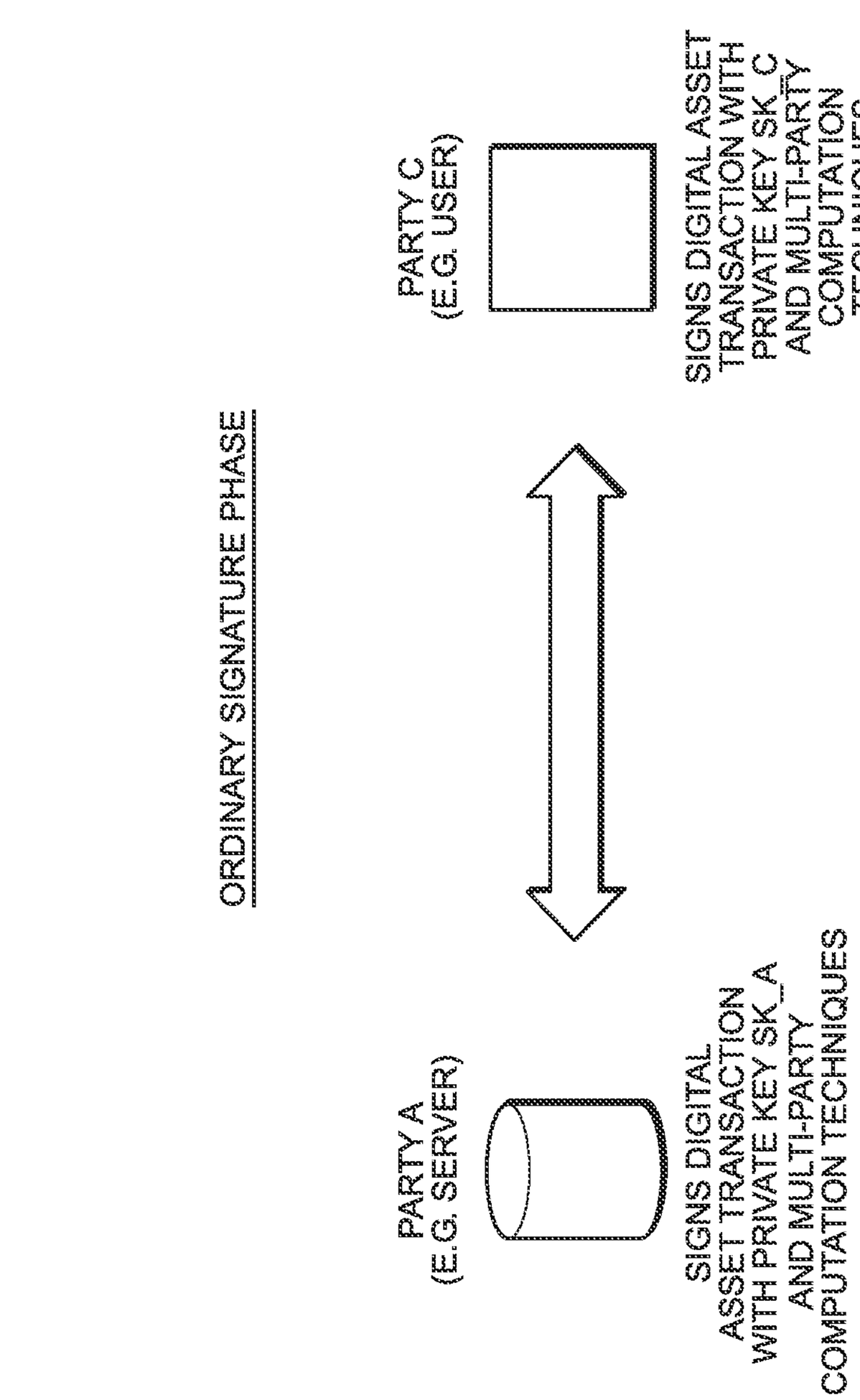
ORDINARY SIGNATURE PHASE
PARTY A
(E.G. SERVER)
SIGNS DIGITAL ASSET TRANSACTION WITH PRIVATE KEY SK_A AND MULTI-PARTY COMPUTATION TECHNIQUES
PARTY C
(E.G. USER)
SIGNS DIGITAL ASSET TRANSACTION WITH PRIVATE KEY SK_C AND MULTI-PARTY COMPUTATION TECHNIQUES
THE RESULTING SIGNATURE OF THIS "2-OF-3" SCHEME IS VERIFIABLE BY ANYONE WITH THE PUBLIC KEY PK_ABC
THE INVENTION ALSO SUPPORTS KEY DERIVATION. IN SUCH CASE, PARTY A AND PARTY C SIGN WITH PRIVATE KEY SK_A AND SK_C AND MULTI-PARTY COMPUTATION TECHNIQUES.
THE RESULTING SIGNATURE IS VERIFIABLE BY ANYONE WITH THE PUBLIC KEY PK_ABC

FIG. 4

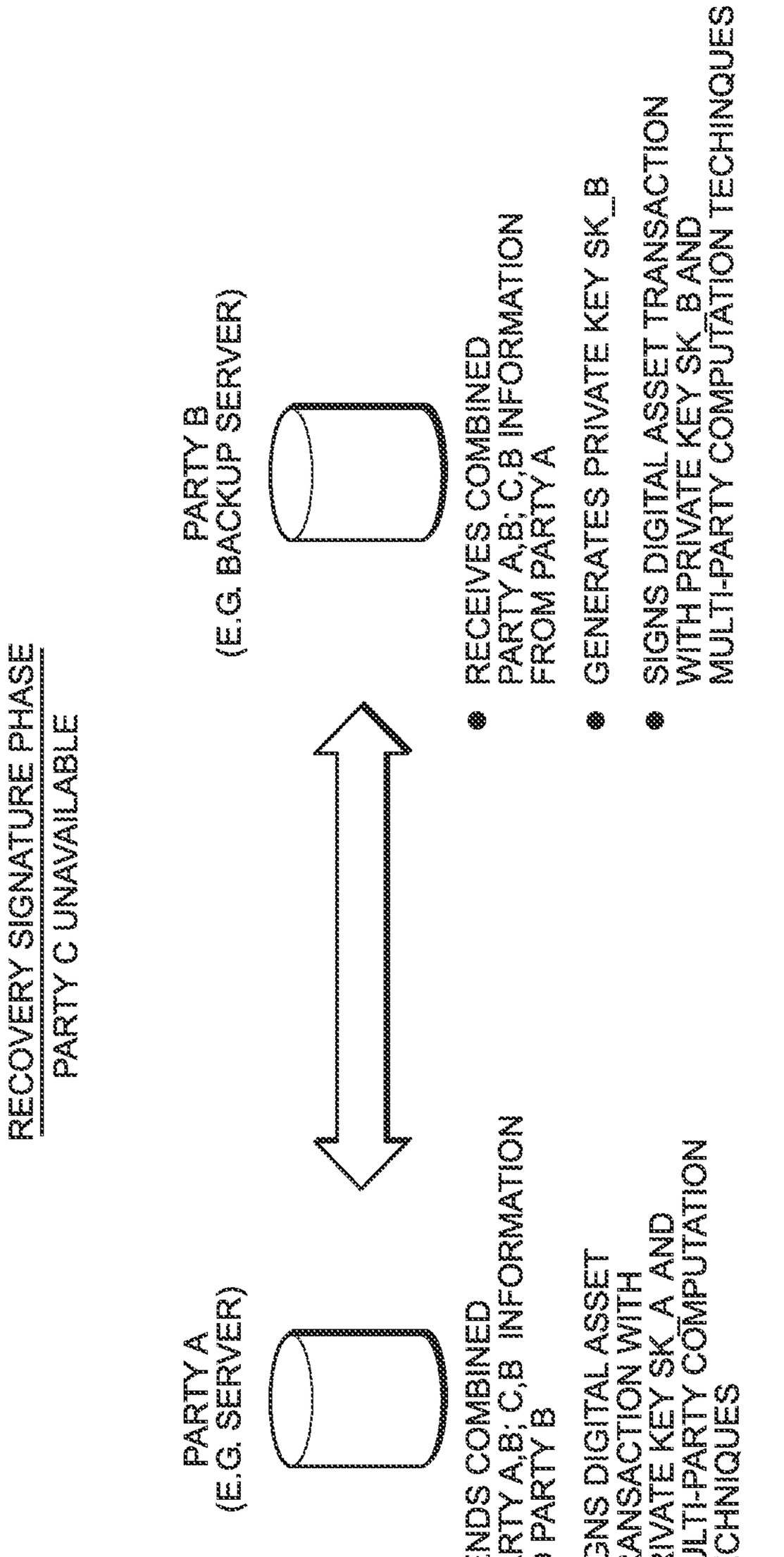
RECOVERY SIGNATURE PHASE
PARTY C UNAVAILABLE
PARTY A
(E.G. SERVER)
PARTY B
(E.G. BACKUP SERVER)
SIGNATURE VERIFICATION AND EVENTUAL KEY DERIVATION OPERATIONS ARE ANALOGOUS TO THE ONES IN THE ORDINARY SIGNATURE PHASE
SENDS COMBINED PARTY A,B; C,B INFORMATION TO PARTY B
SIGNS DIGITAL ASSET TRANSACTION WITH PRIVATE KEY SK_A AND MULTI-PARTY COMPUTATION TECHNIQUES
RECEIVES COMBINED PARTY A,B; C,B INFORMATION FROM PARTY A
GENERATES PRIVATE KEY SK_B
SIGNS DIGITAL ASSET TRANSACTION WITH PRIVATE KEY SK_B AND MULTI-PARTY COMPUTATION TECHNIQUES

FIG. 5

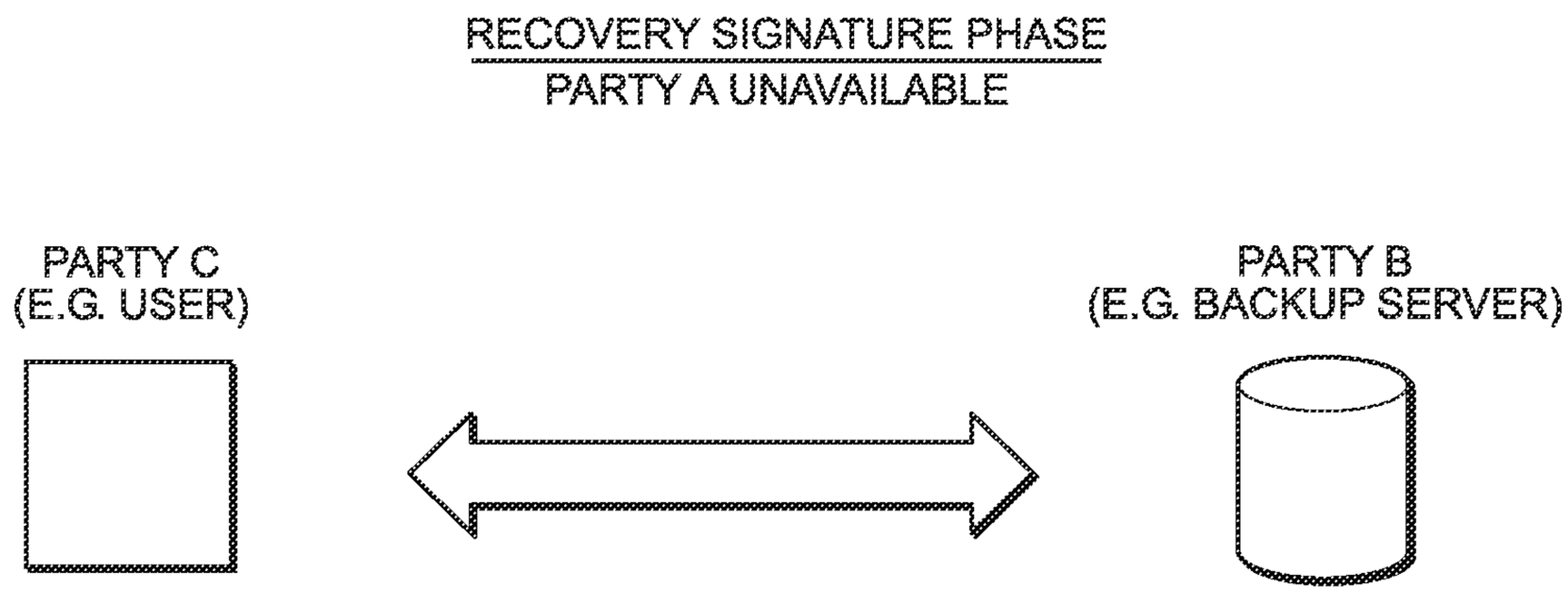
RECOVERY SIGNATURE PHASE
PARTY A UNAVAILABLE
PARTY C
(E.G. USER)
PARTY B
(E.G. BACKUP SERVER)
SENDS COMBINED PARTY A,B; C,B INFORMATION TO PARTY B
SIGNS DIGITAL ASSET TRANSACTION WITH PRIVATE KEY SK_C AND MULTI-PARTY COMPUTATION TECHNIQUES
RECEIVES COMBINED PARTY A,B; C,B INFORMATION FROM PARTY C
GENERATES PRIVATE KEY SK_B
SIGNS DIGITAL ASSET TRANSACTION WITH PRIVATE KEY SK_B AND MULTI-PARTY COMPUTATION TECHNIQUES
SIGNATURE VERIFICATION AND EVENTUAL KEY DERIVATION OPERATIONS ARE ANALOGOUS TO THE ONES IN THE ORDINARY SIGNATURE PHASE

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 20/61111

A. CLASSIFICATION OF SUBJECT MATTER

IPC - G06Q 20/38 (2021.01)

CPC - H04L 9/3218, G06Q 20/3829, G06Q 20/3825, H04L 9/0897, H04L 9/0861

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)
See Search History document

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2018/229608 A1 (NCHAIN HOLDINGS LIMITED) 20 December 2018 (20.12.2018) entire document (especially pg. 4, ln 9-22; pg. 5, ln 4-14; pg. 12, ln 14-17 ; pg. 16, ln 14-16)	1-6
Y	US 2018/0069697 A1 (Conio Inc.) 08 March 2018 (08.03.2018) entire document (especially para [0033]-[0045])	1-6
A	US 10,373,129 B1 (Winklevoss IP , LLC) 06 August 2019 (06.08.2019) entire document	1-6

☐ 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
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which 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	Date of mailing of the international search report
08 March 2021 (08.03.2021)	MAR 23 2021
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Lee Young Telephone No. PCT Helpdesk: 571-272-4300

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 20/61111

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

-see extra sheet-

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-6

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 20/61111

Continuation of Box III: Lack of Unity

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be searched, the appropriate additional search fees must be paid.

Group I: Claims 1-6 are directed to using a single-signature on blockchain and three generated private keys to recover digital assets, if any of the three private keys are unavailable during transaction then the asset is recovered.

Group II: Claims 7-20 are directed to generating private and public information pair by the first party and transmitting the public information to the second party.

The inventions listed as Groups I and II do not relate to a single general inventive concept under PCT Rule 13.1 because under PCT Rule 13.2 they lack the same or corresponding technical features for the following reasons:

Special Technical Features:
The special technical feature of Group I is using blockchain technology and three generated private keys to recover digital assets, if any of the three private keys are unavailable during transaction then the assetis recovered, not present in any other group.

The special technical feature of Group II is generating private and public information pair by the first party and transmitting the public information to the second party, not present in any other group.

Common Technical Feature:
Groups I and II share the technical feature of generating private keys/private information. However, this shared technical feature does not represent a contribution over US 10,373,129 B1 (Winklevoss IP , LLC) (hereinafter Winklevoss) 06 August 2019 (06.08.2019).

Winklevoss teaches generating private keys/private information (e.g. one or more private keys payments be stored off - line in...In such embodiments, keys may be generated, stored, and managed onboard hardware security modules (HSMs), col. 18, In 66 to col. 19, In 3; the ring confidential transactions protocol may hide the transferred amount as well, col. 16, In 19-20; e.g. third instructions using the third designated private key to generate third digitally signed instructions, col. 9, In 10-12).

Thus, unity of invention is lacking under PCT Rule 13.1 because Groups I and II do not share a same or corresponding special technical feature that would provide a unifying contribution over the prior art. None of these special technical features are common to the other groups.