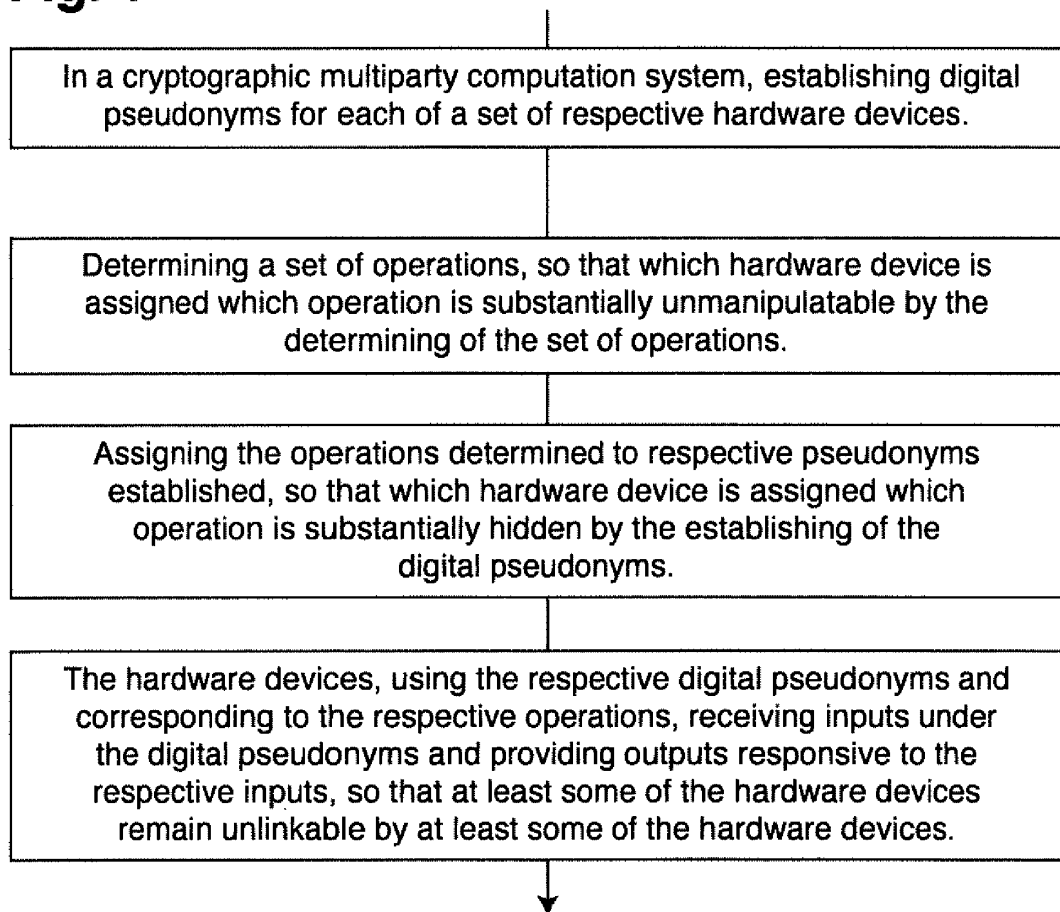
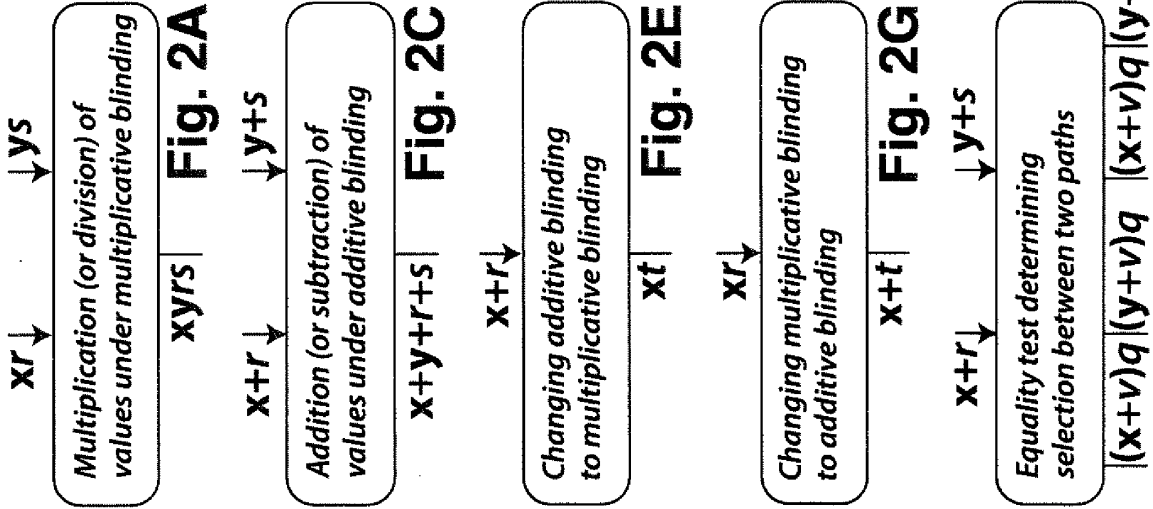
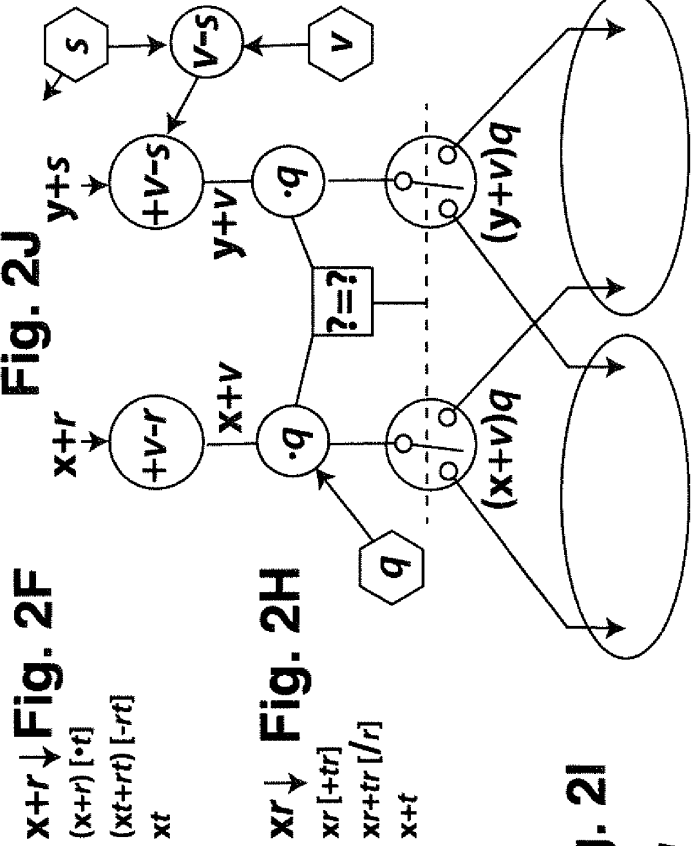
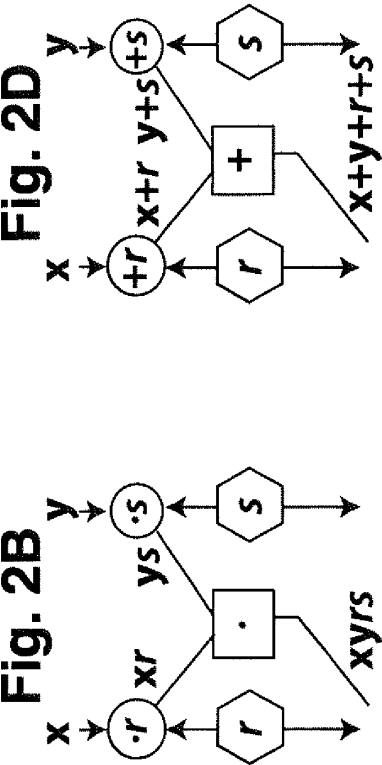
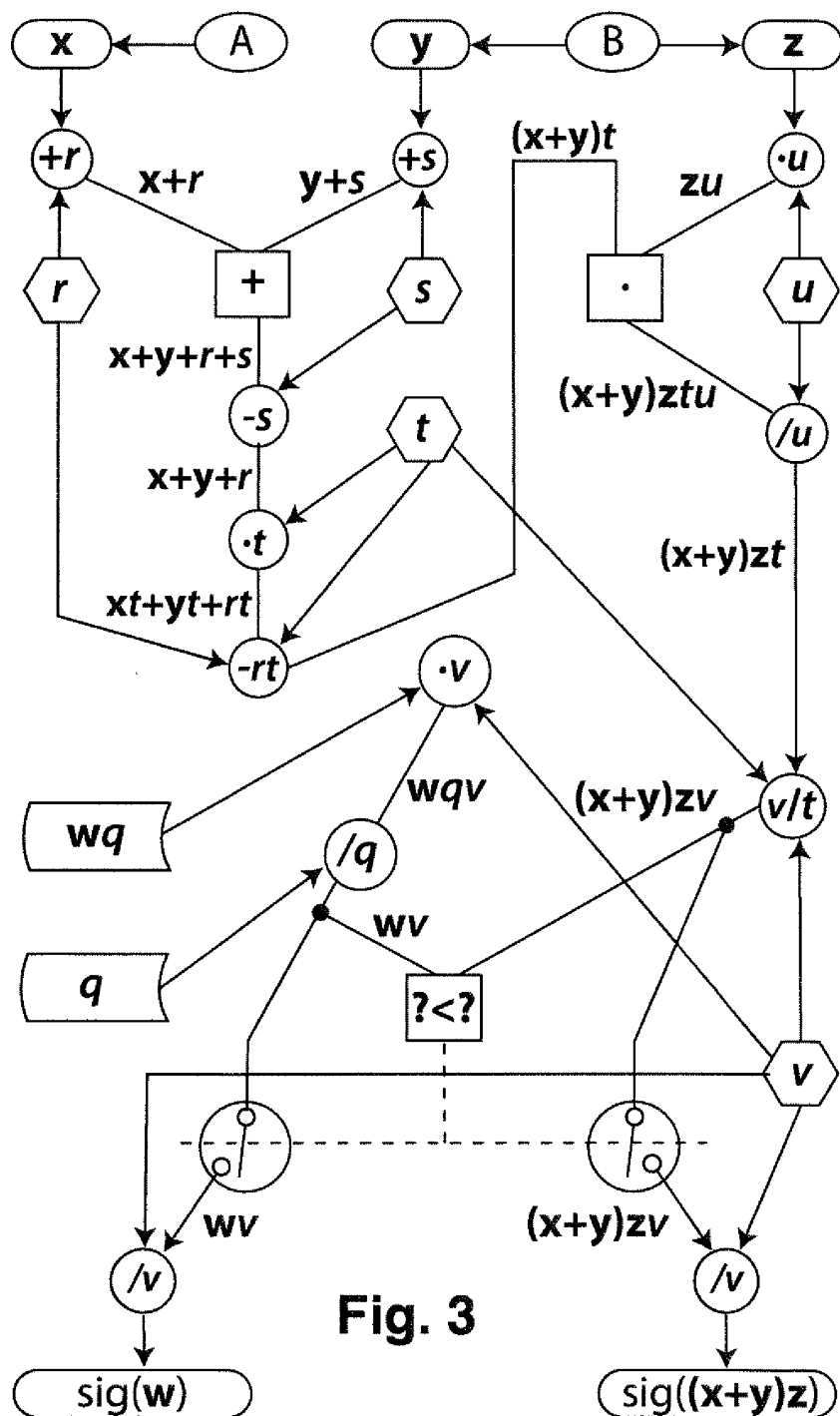


Fig. 1





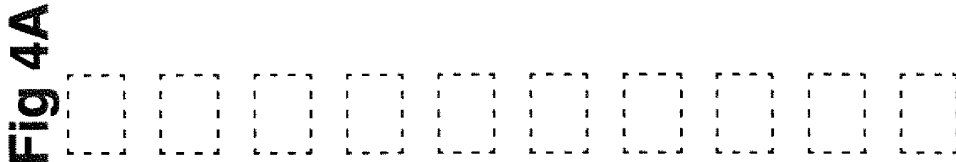
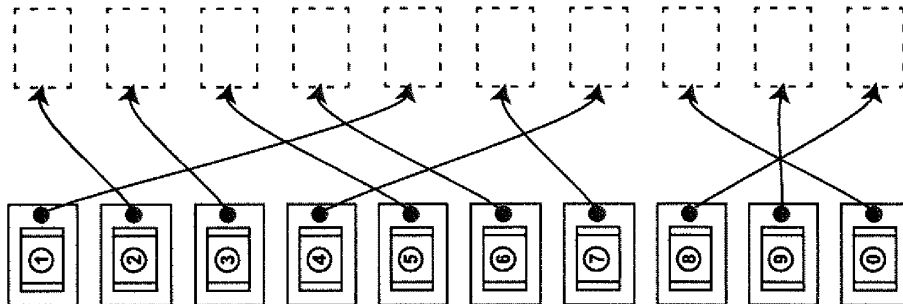
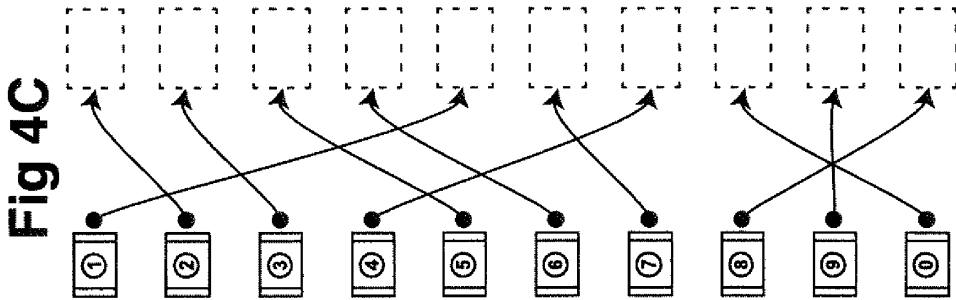
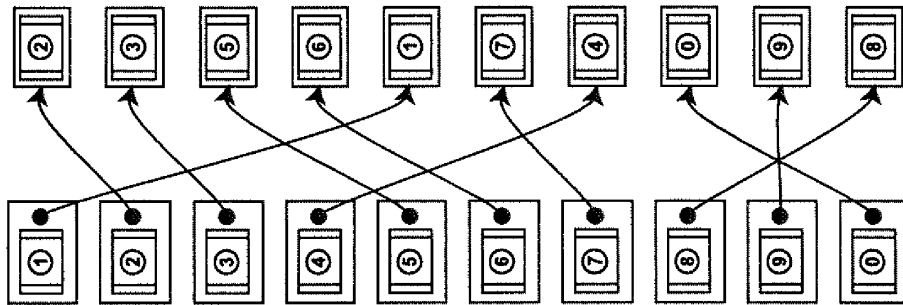
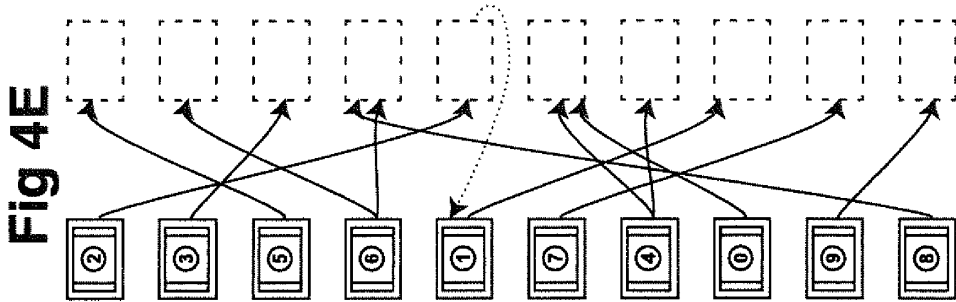


Fig 4D

Fig 4B

Fig 5A

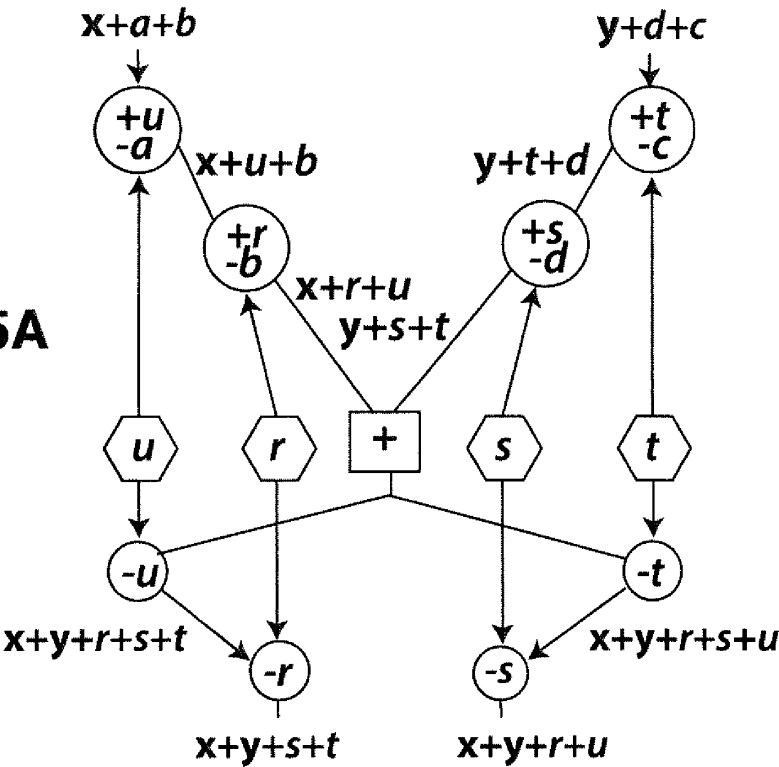
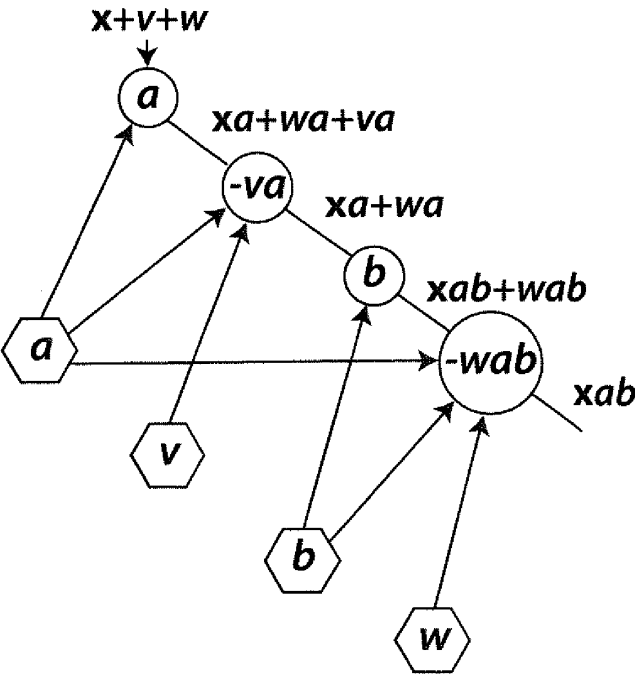
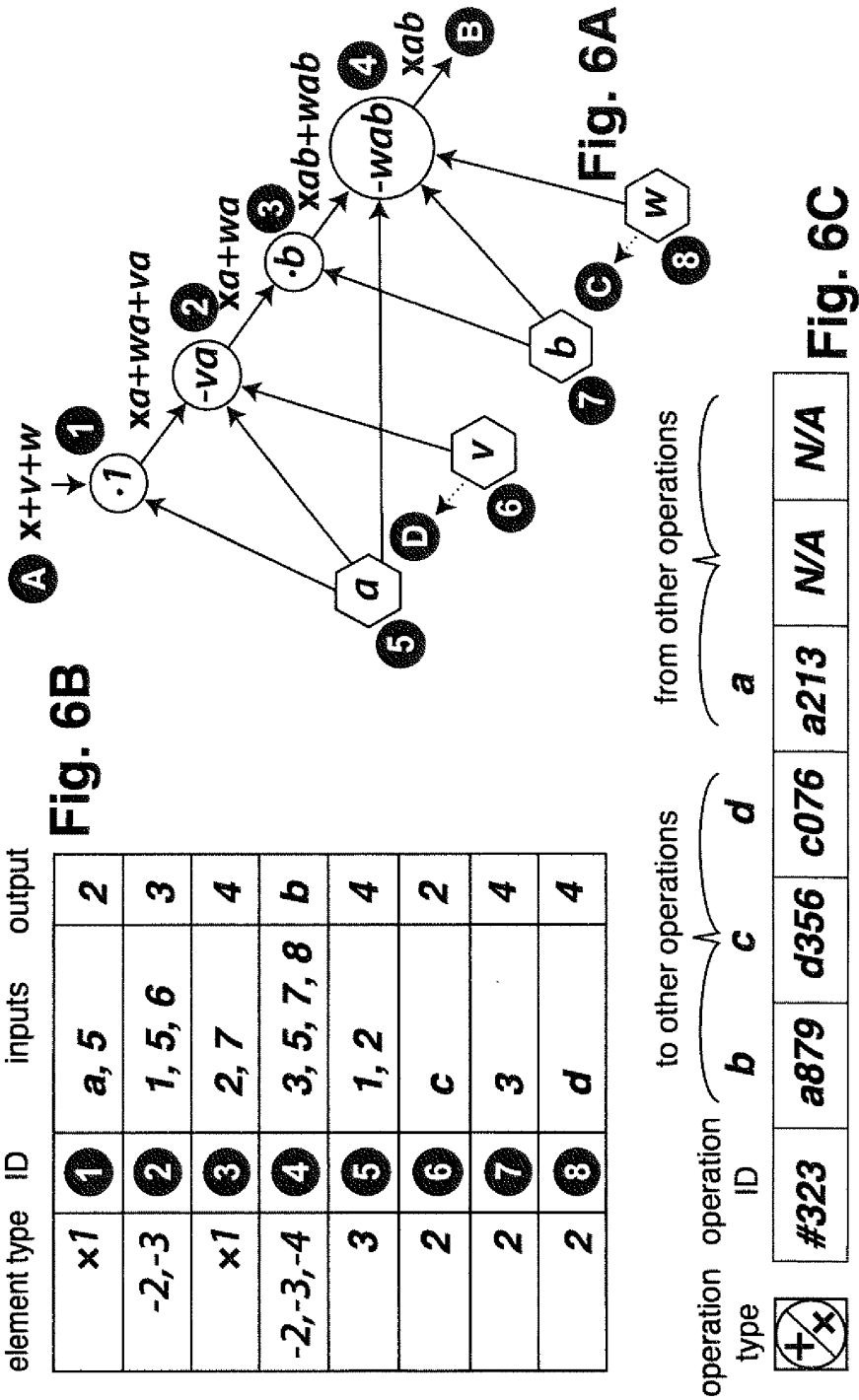


Fig 5B





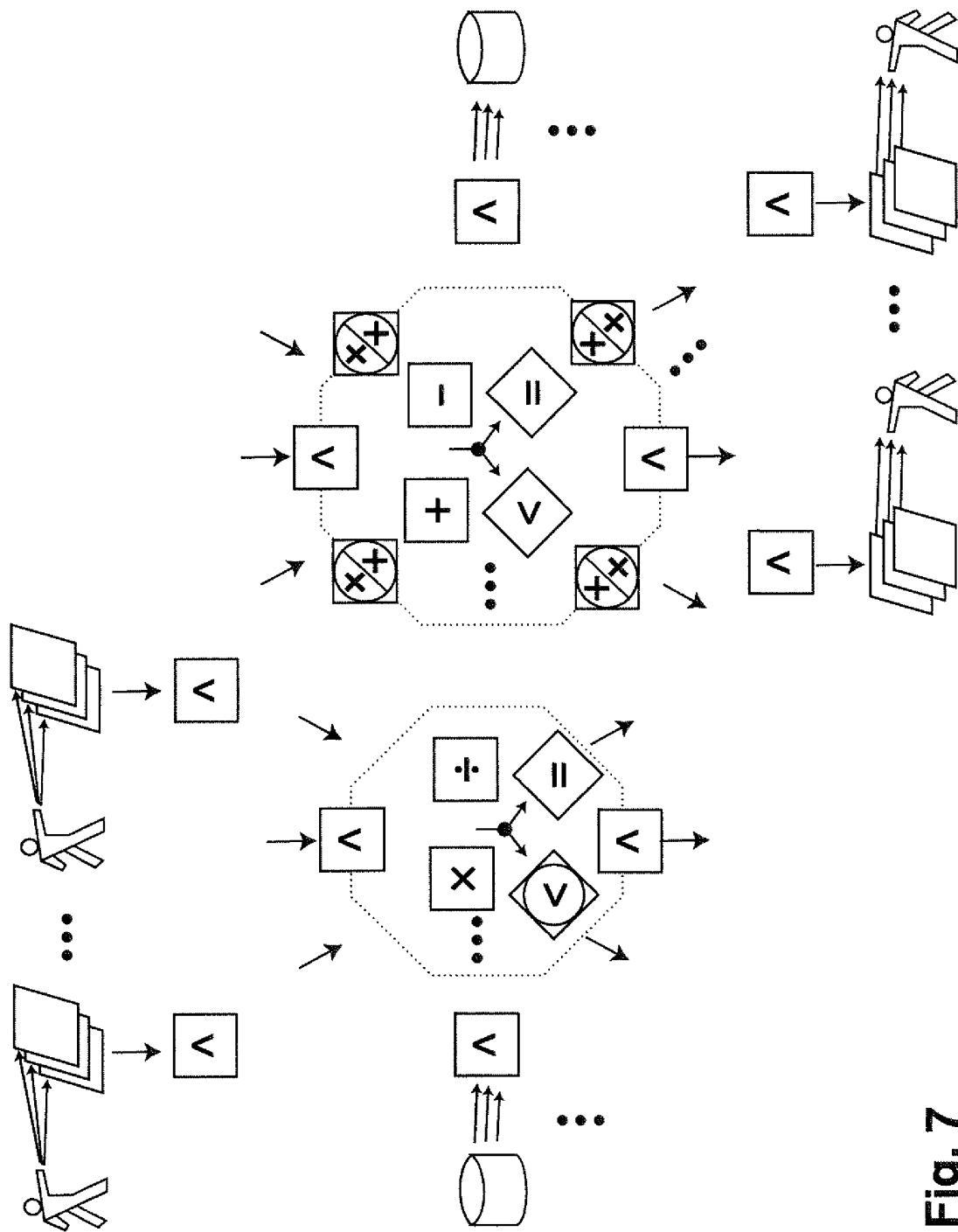
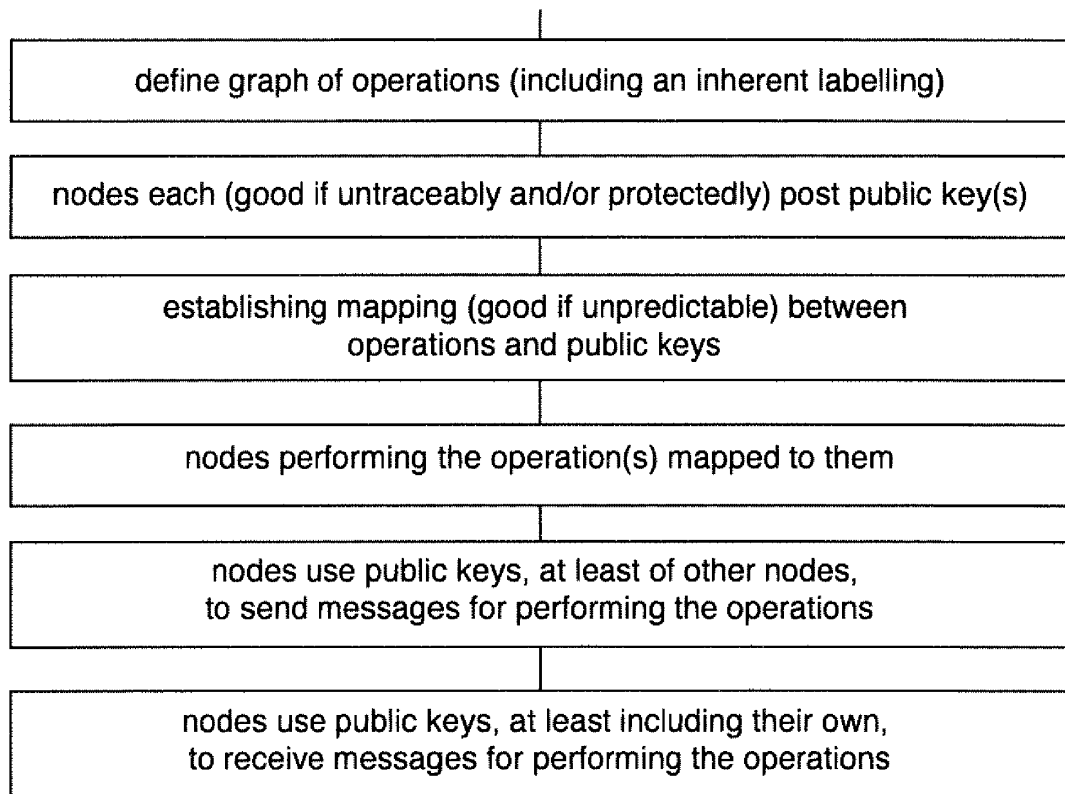
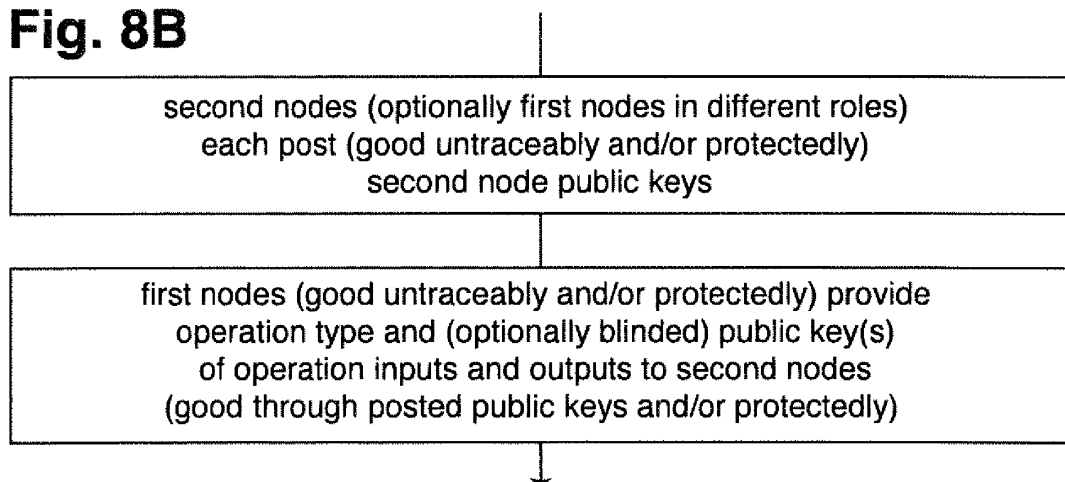
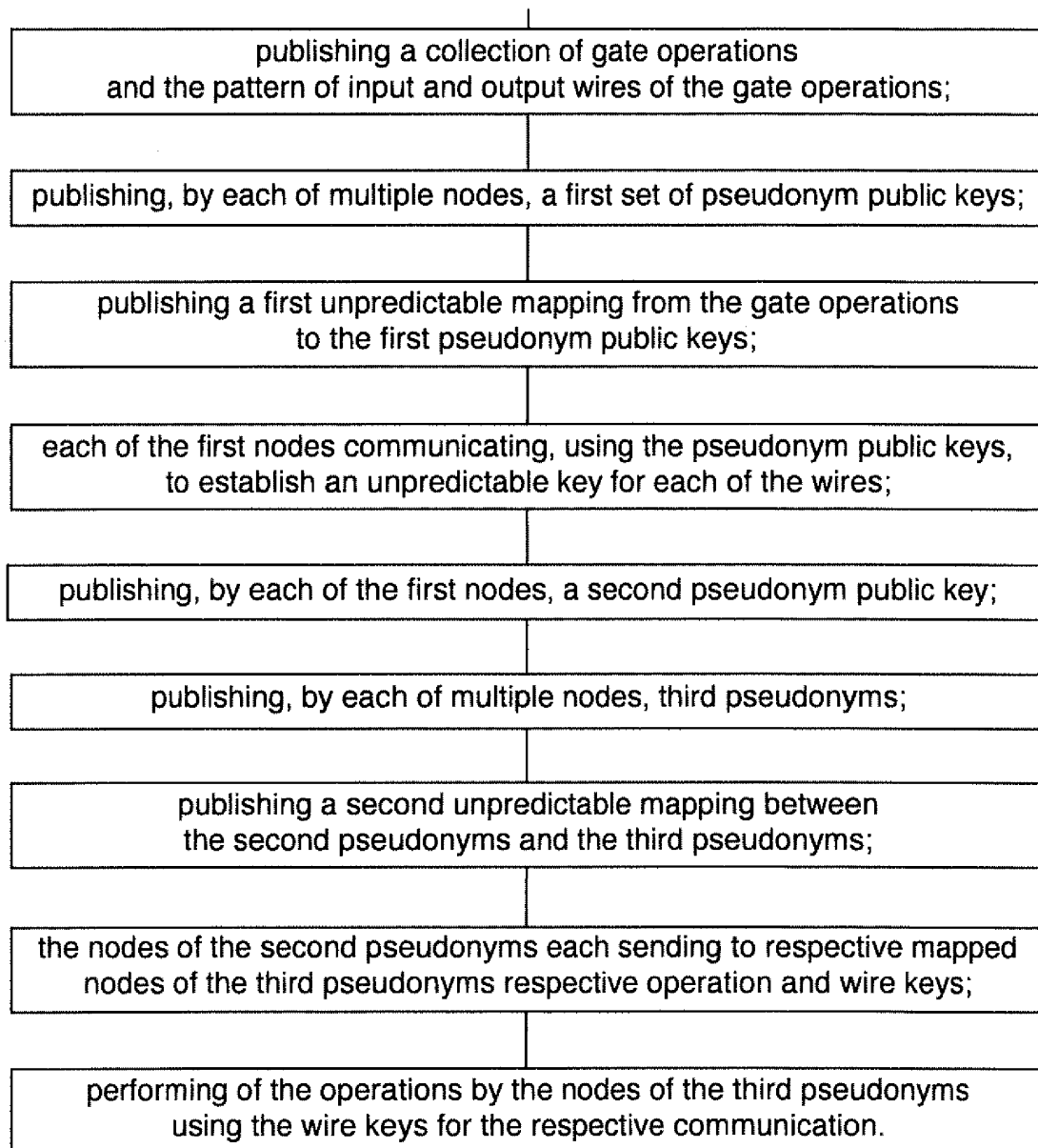


Fig. 7

**Fig. 8A****Fig. 8B**

**Fig. 9**

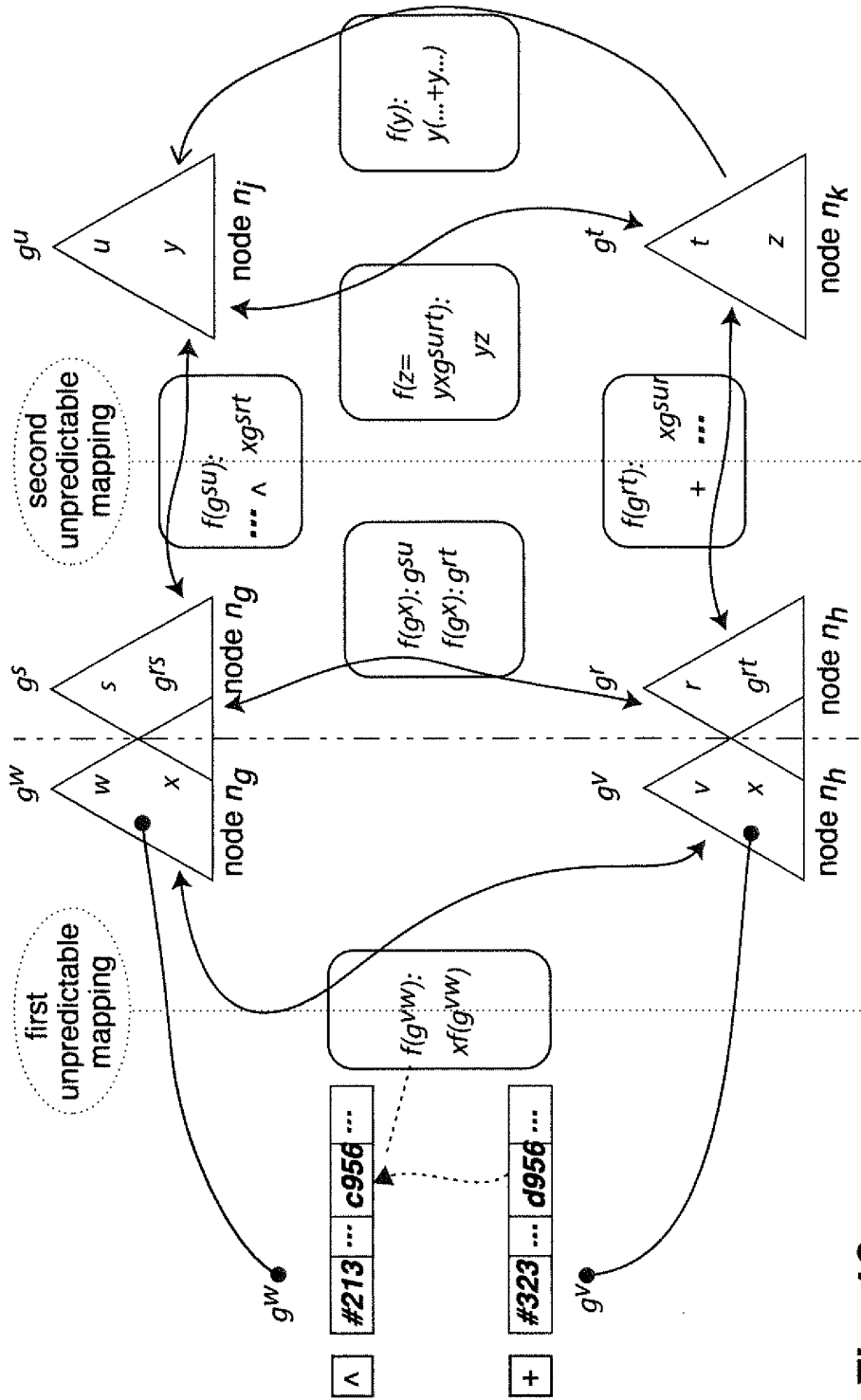


Fig. 10

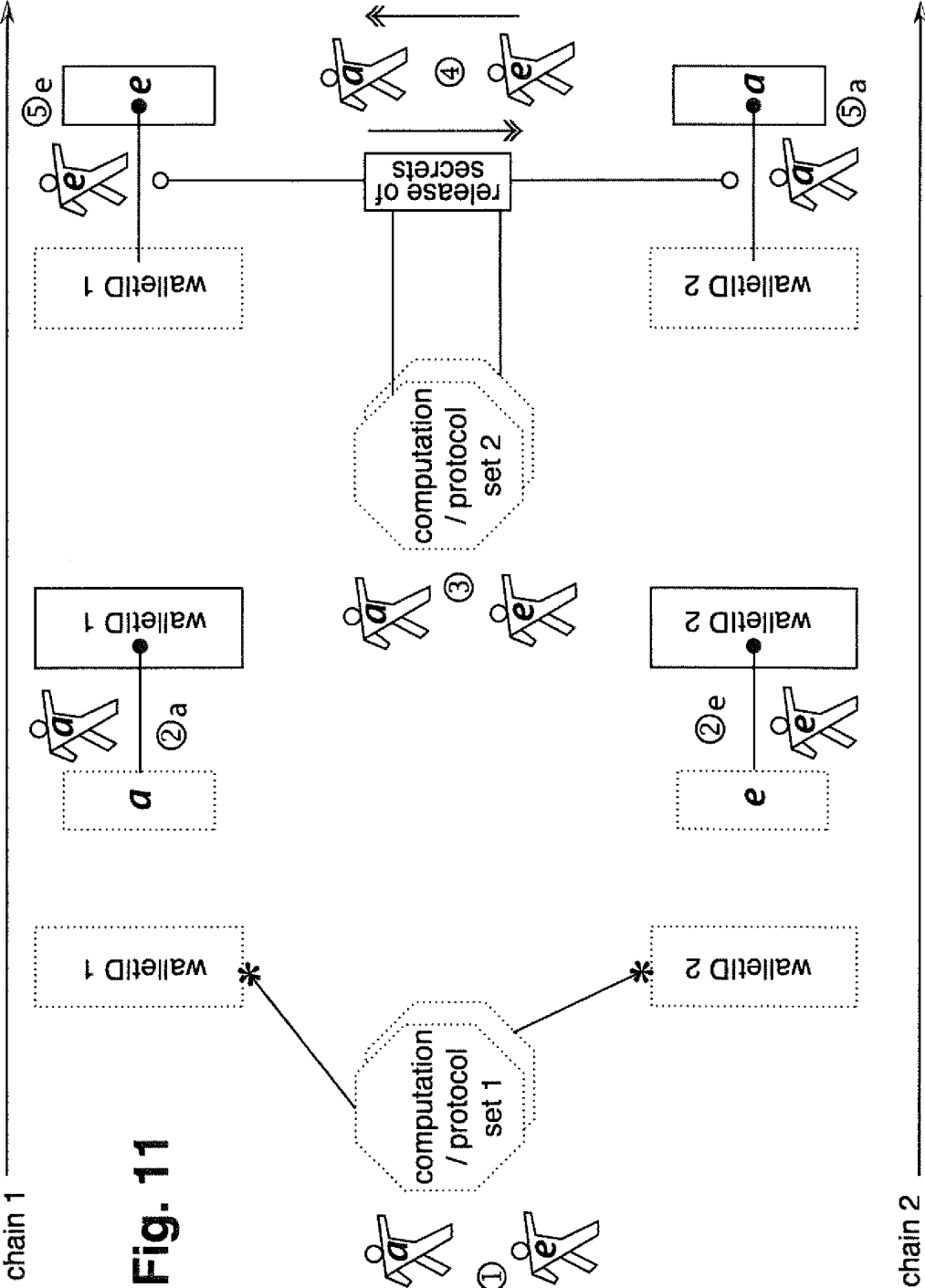
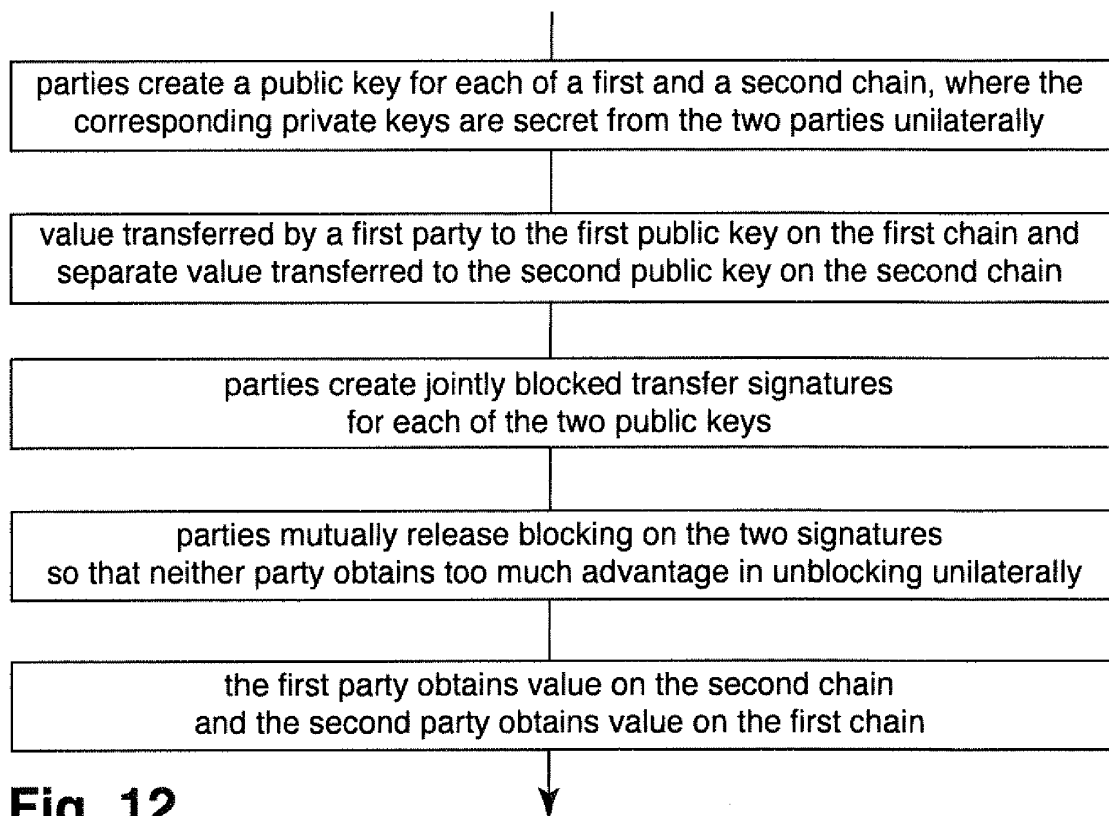
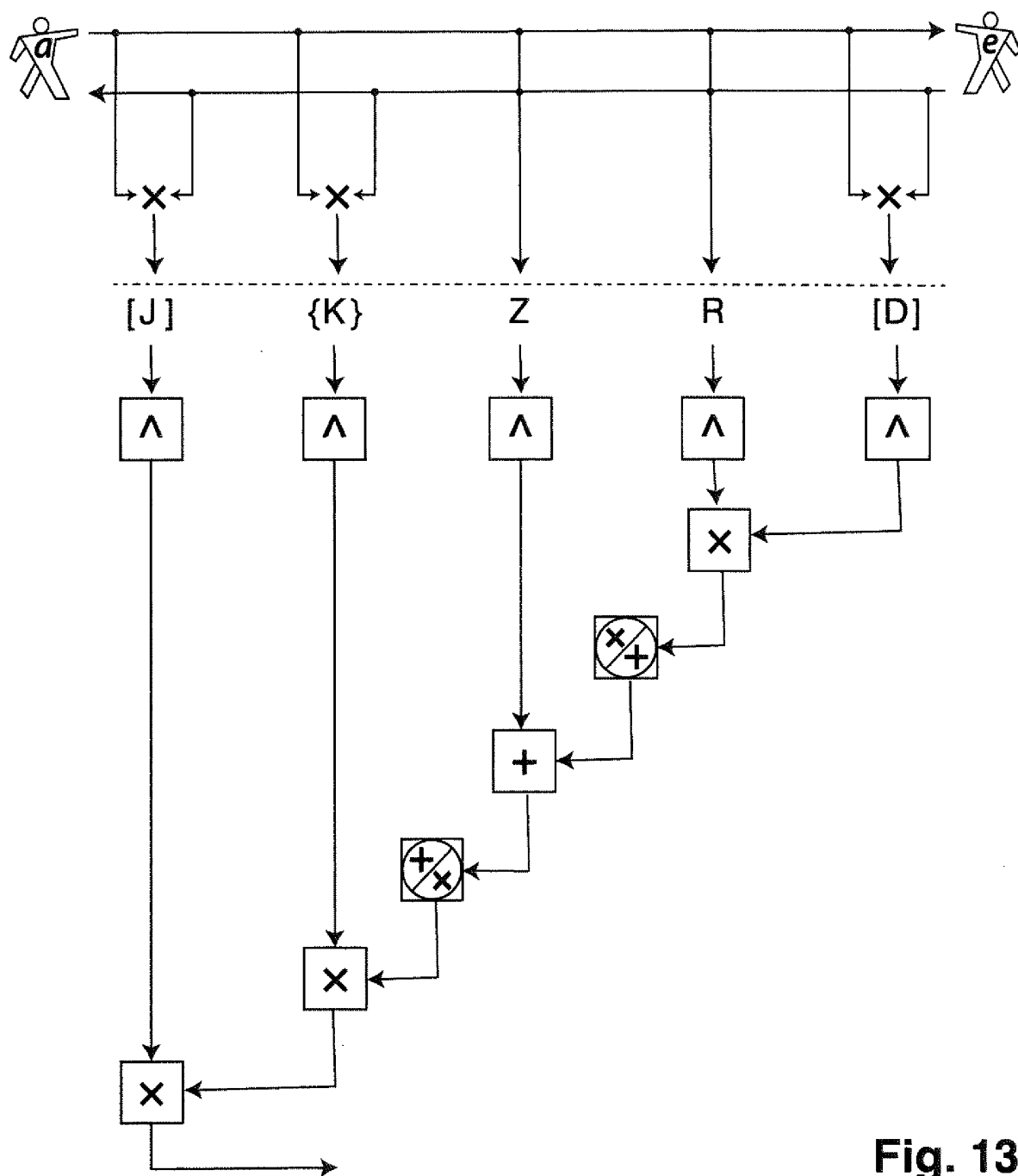
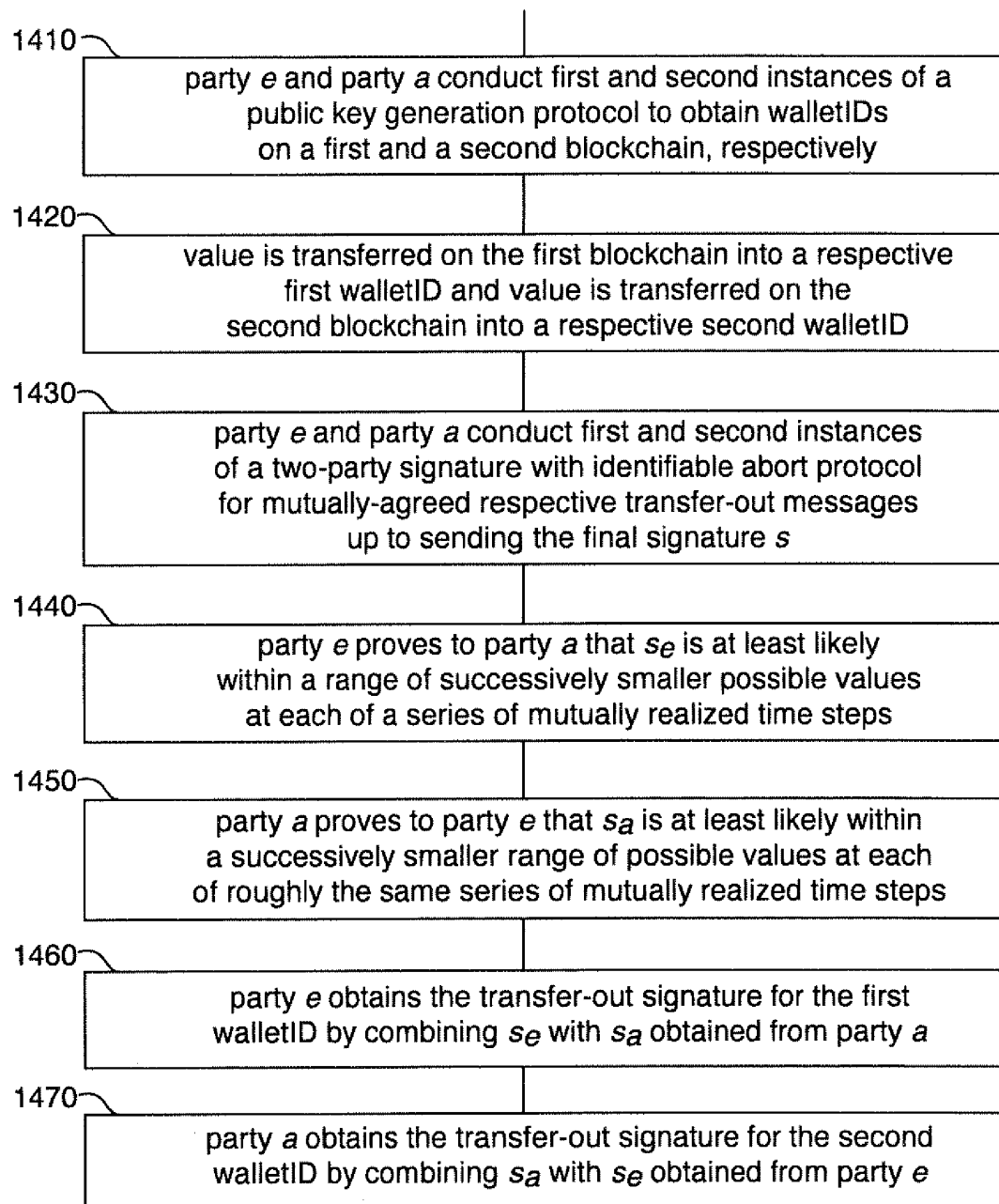
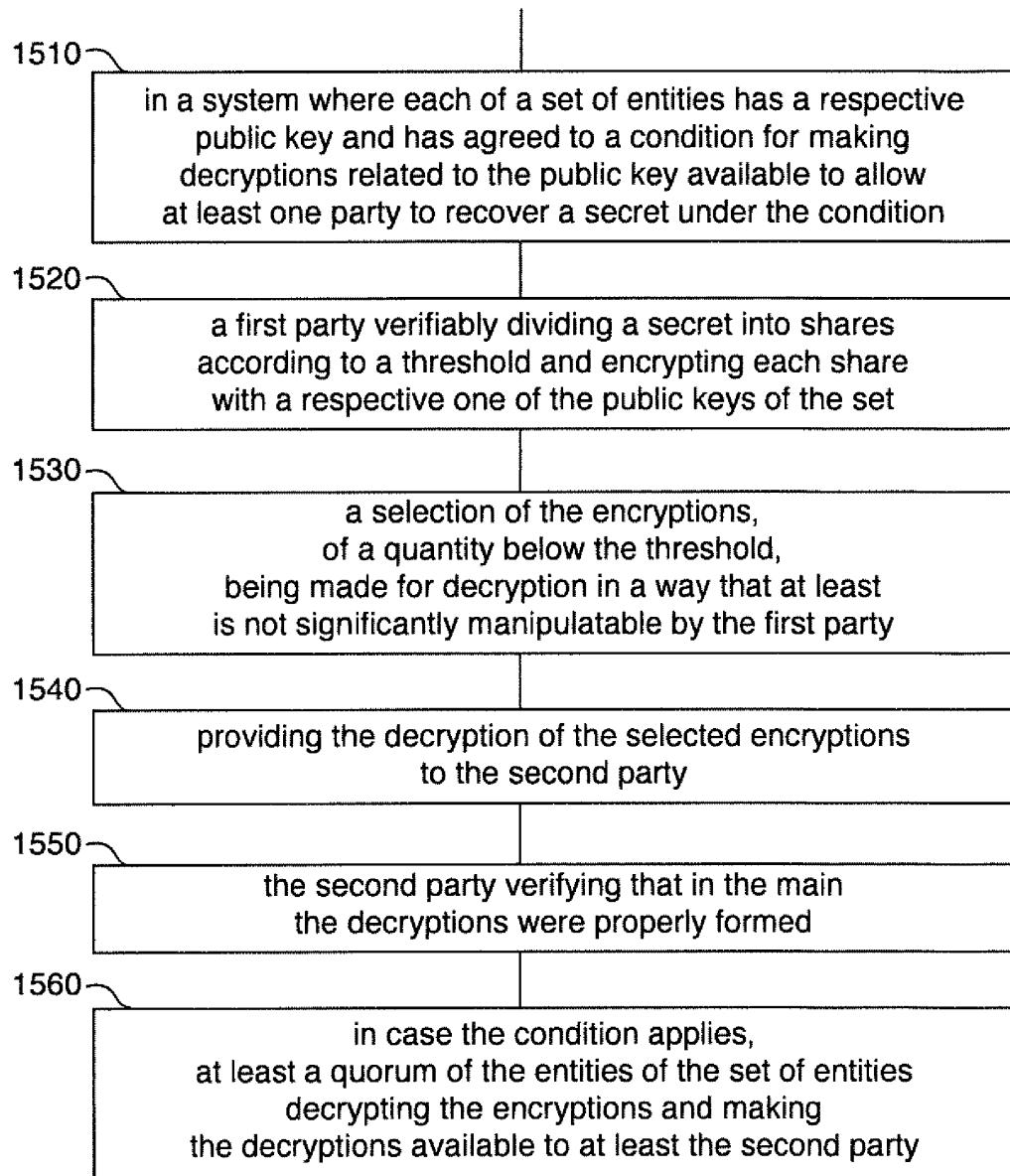


Fig. 11

**Fig. 12**

**Fig. 13**

**Fig. 14**

**Fig. 15**

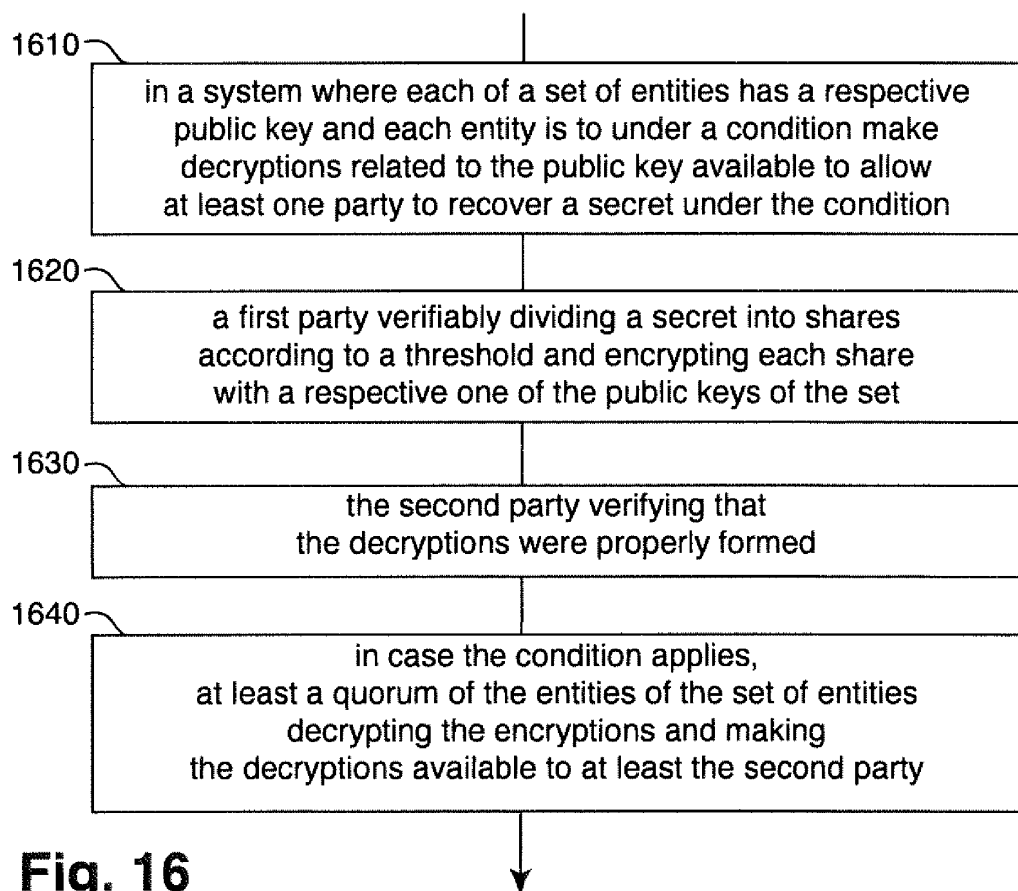
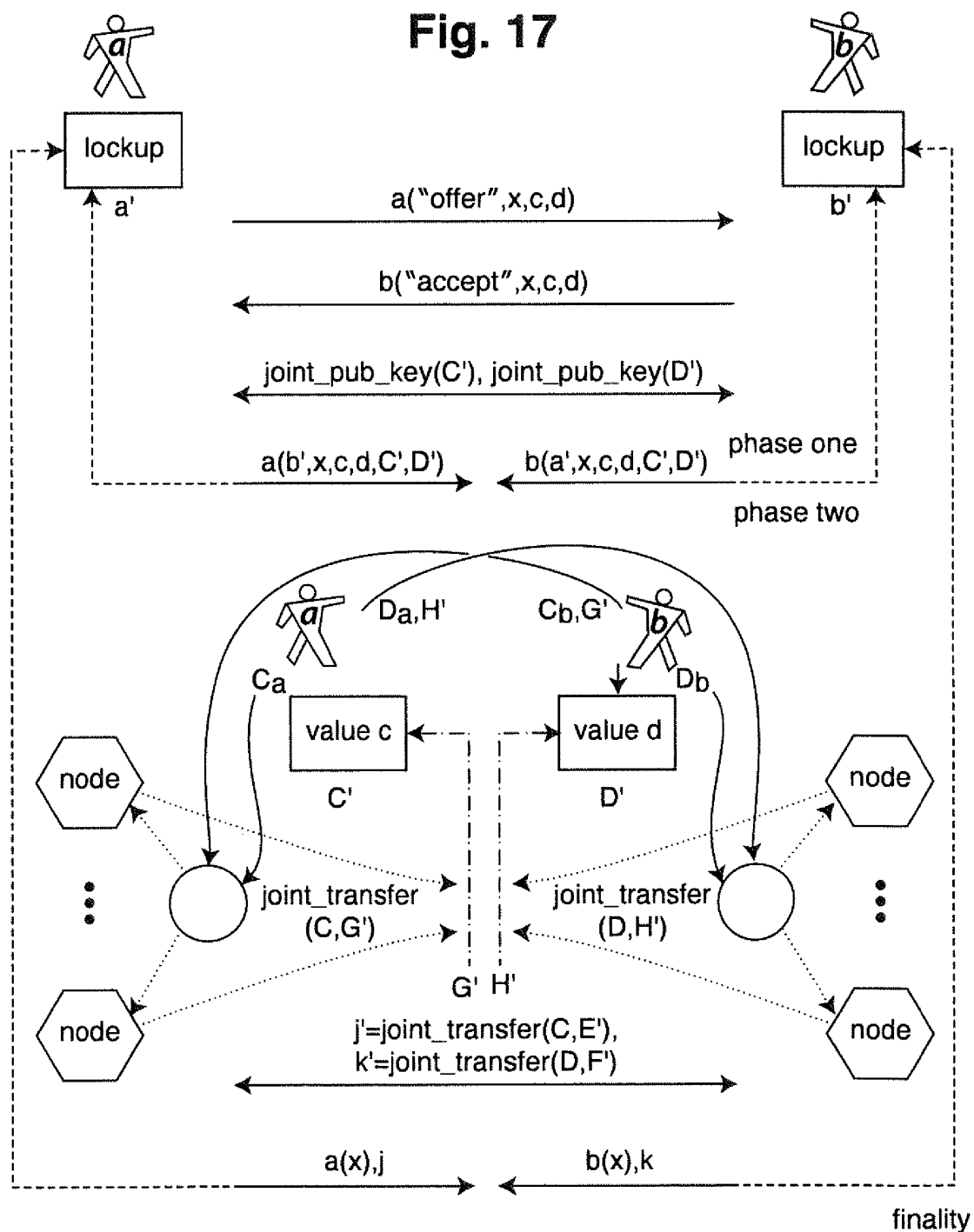
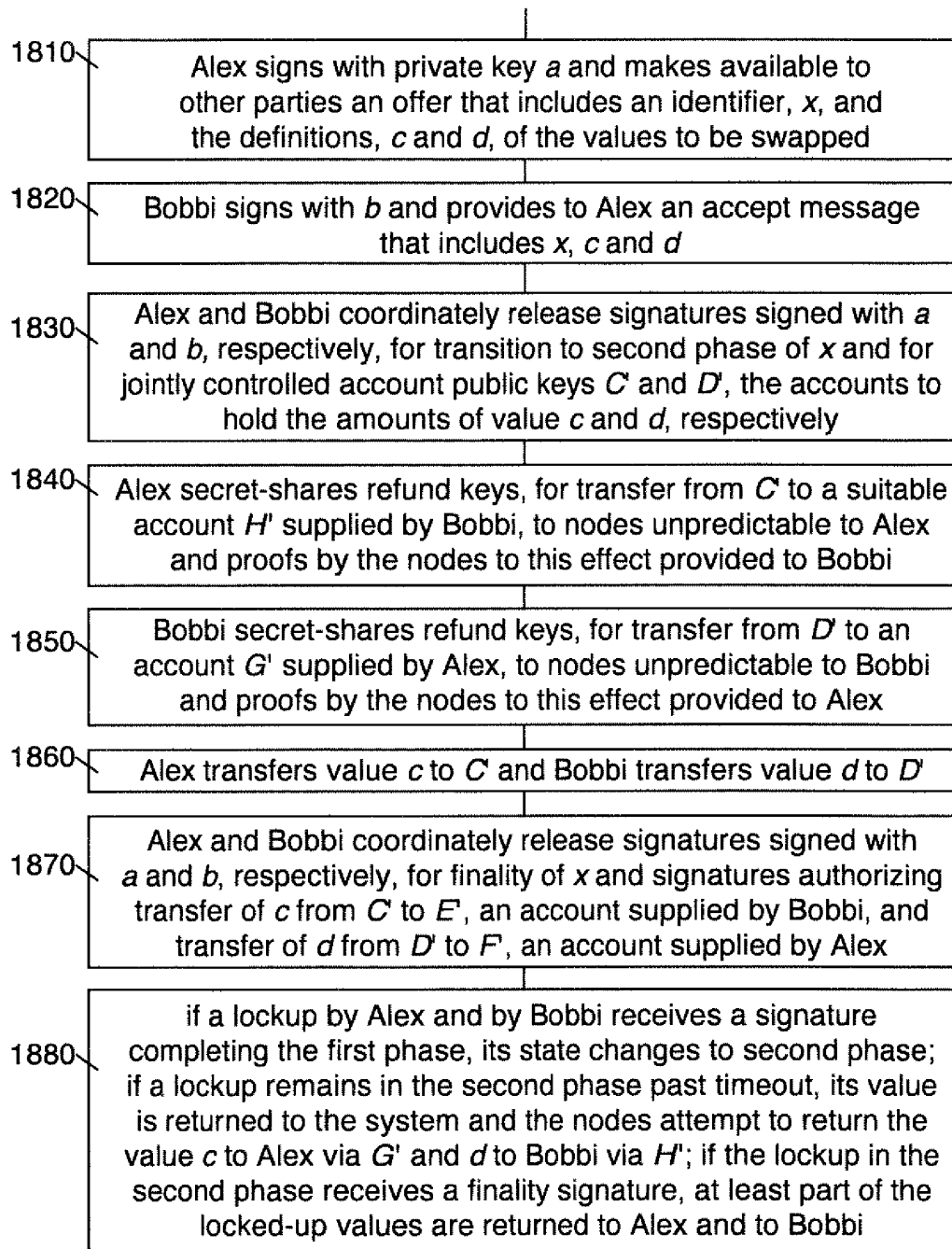


Fig. 17

**Fig. 18**

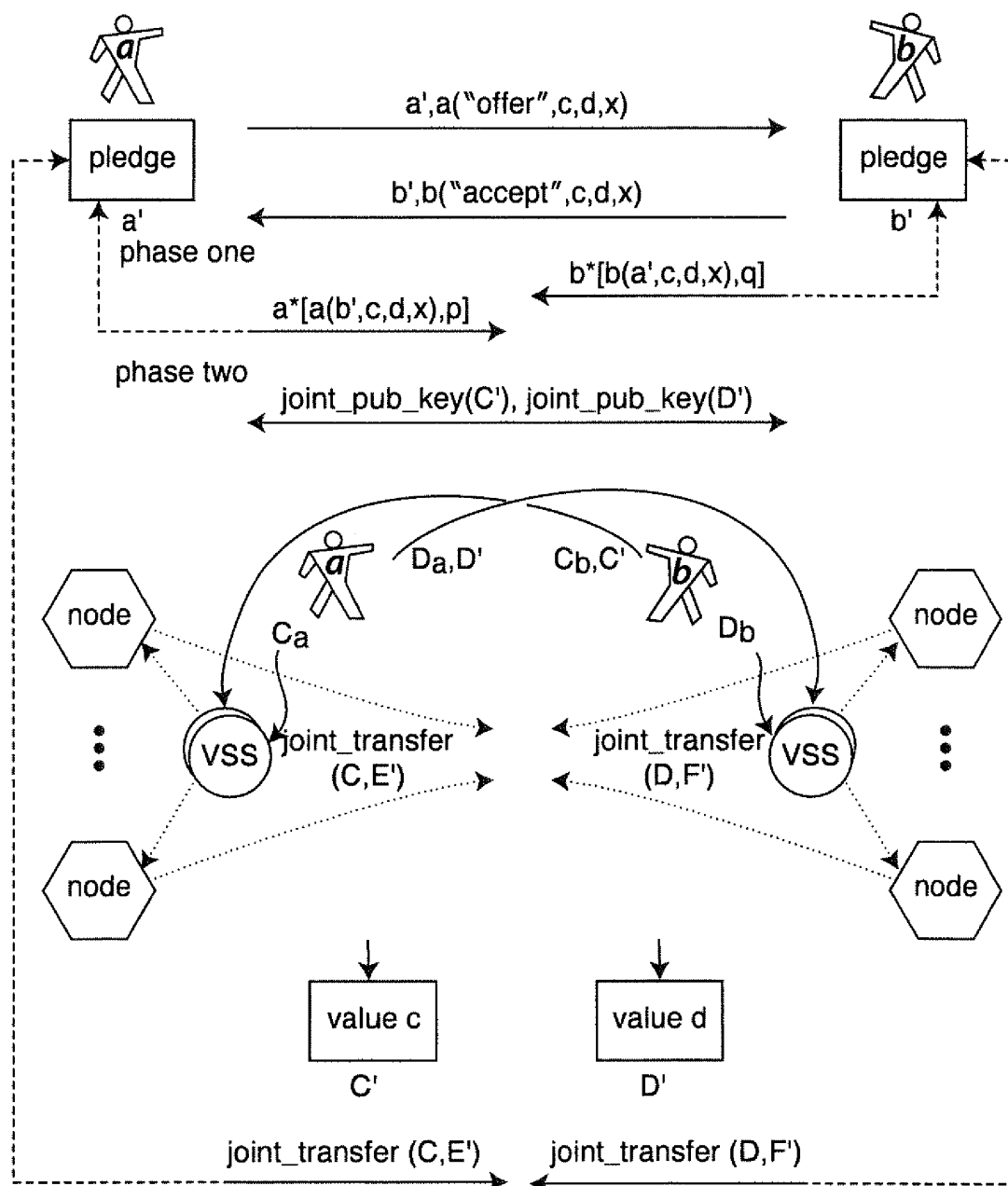
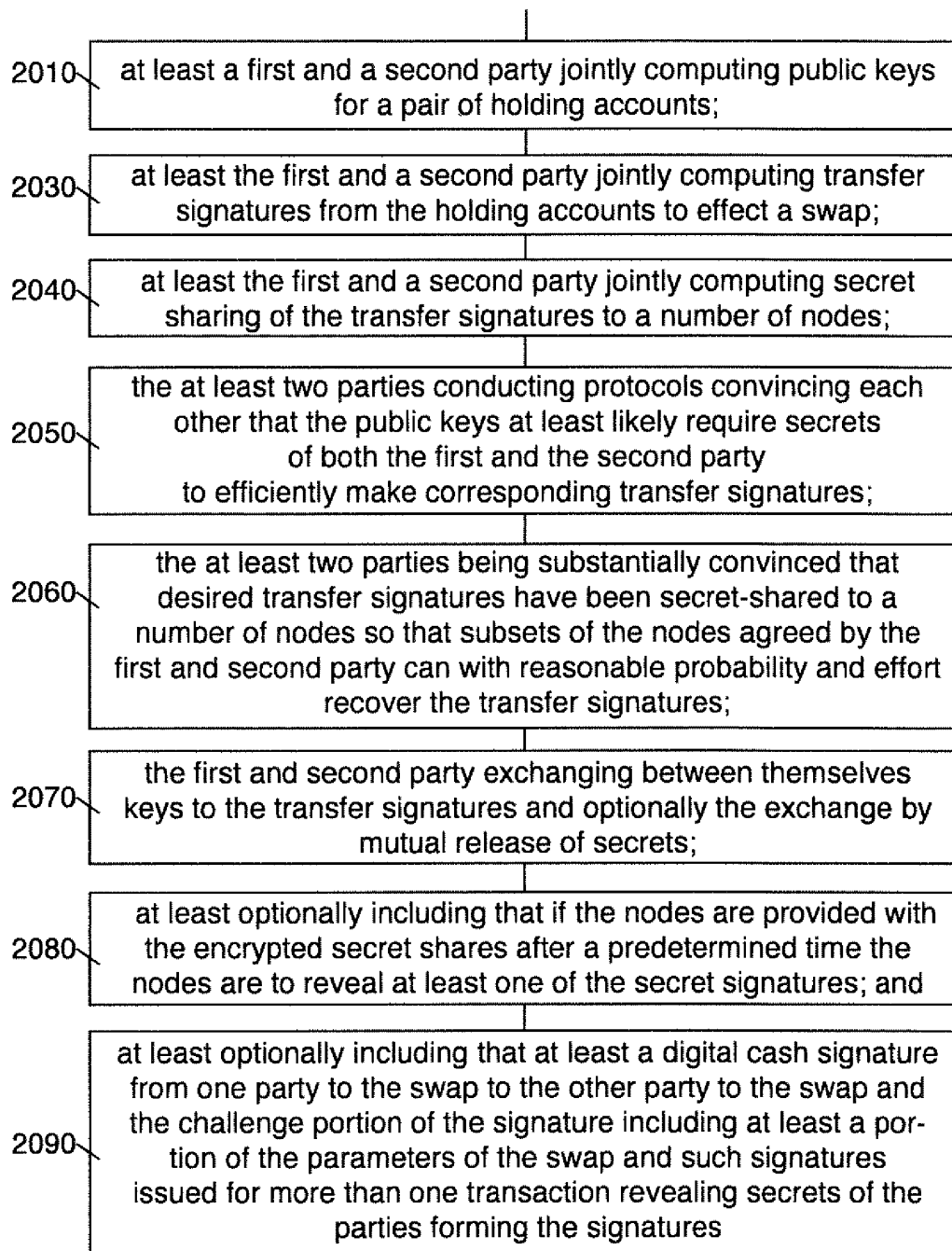


Fig. 19

**Fig. 20**

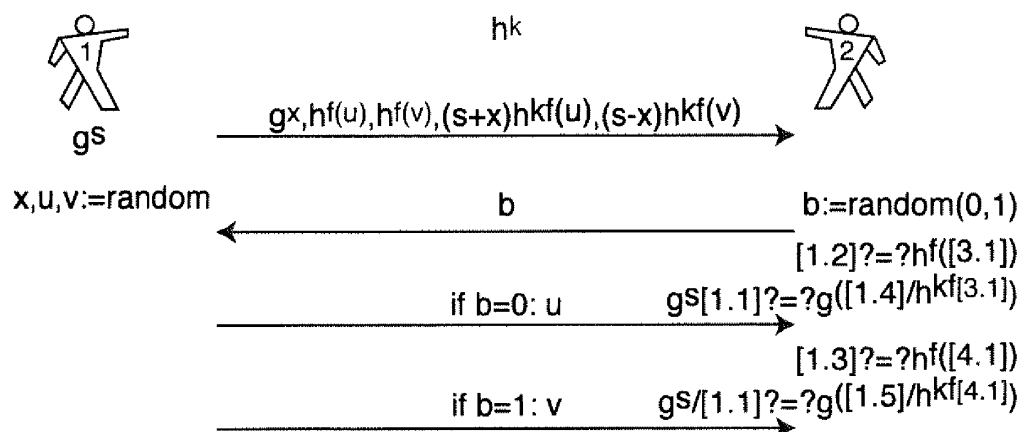


Fig. 21A

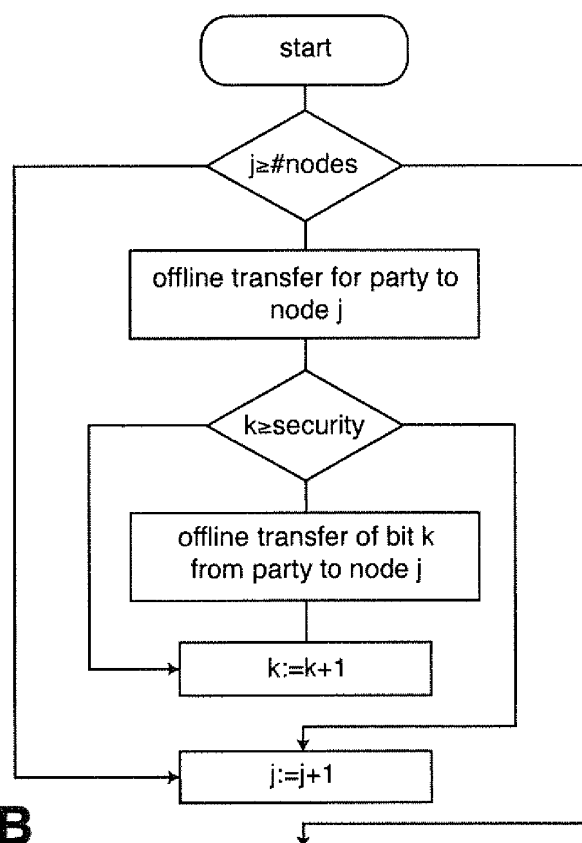


Fig. 21B

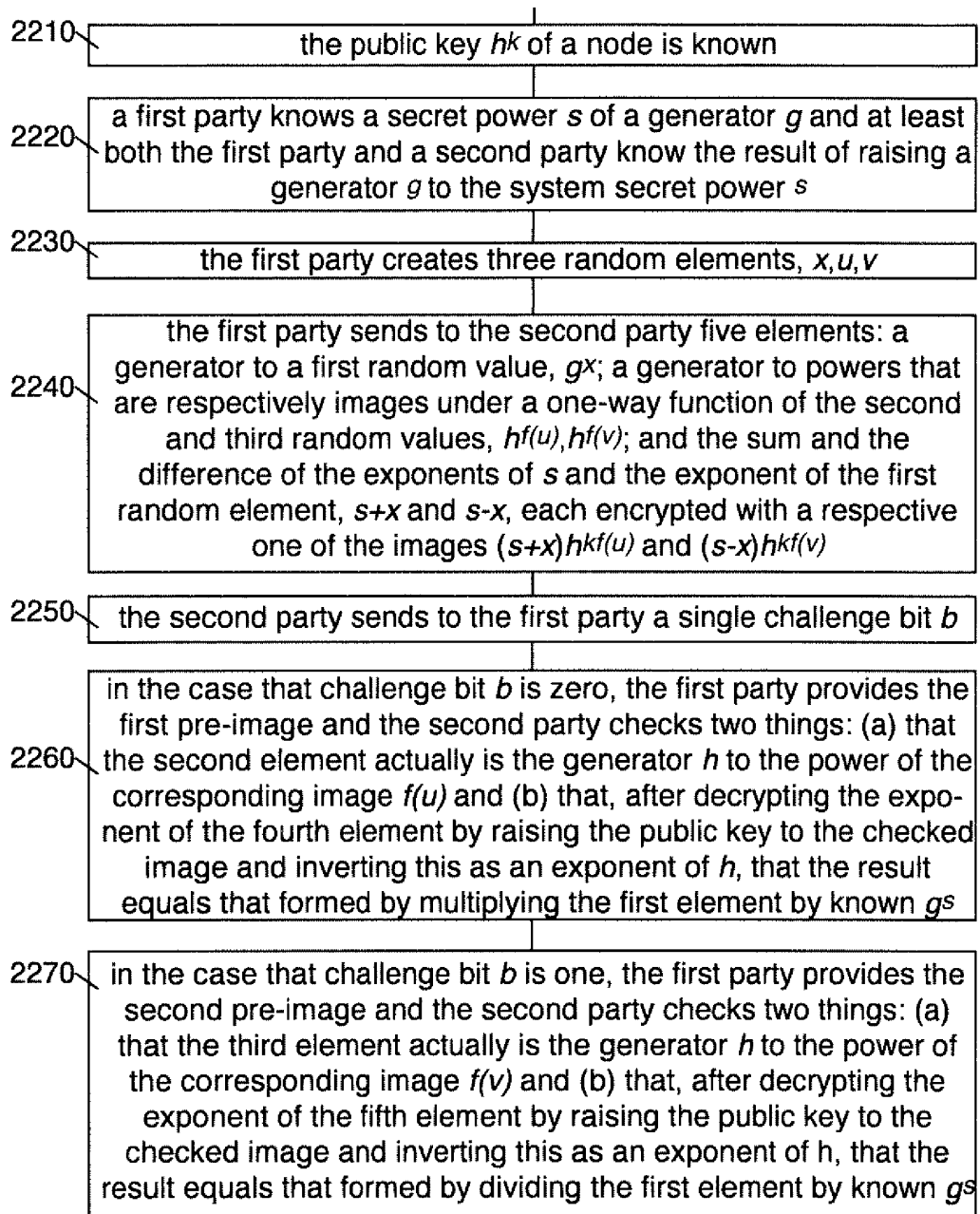
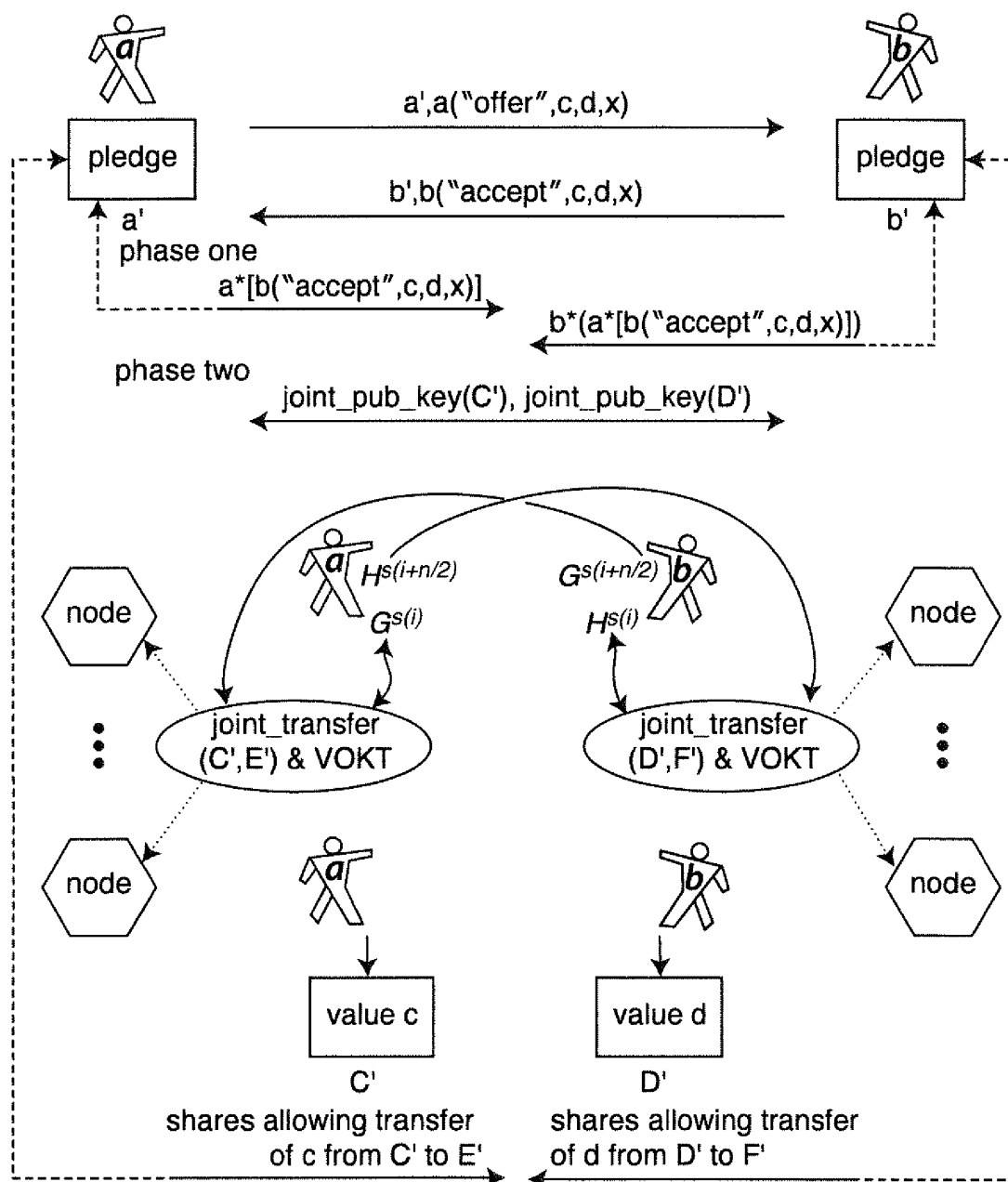
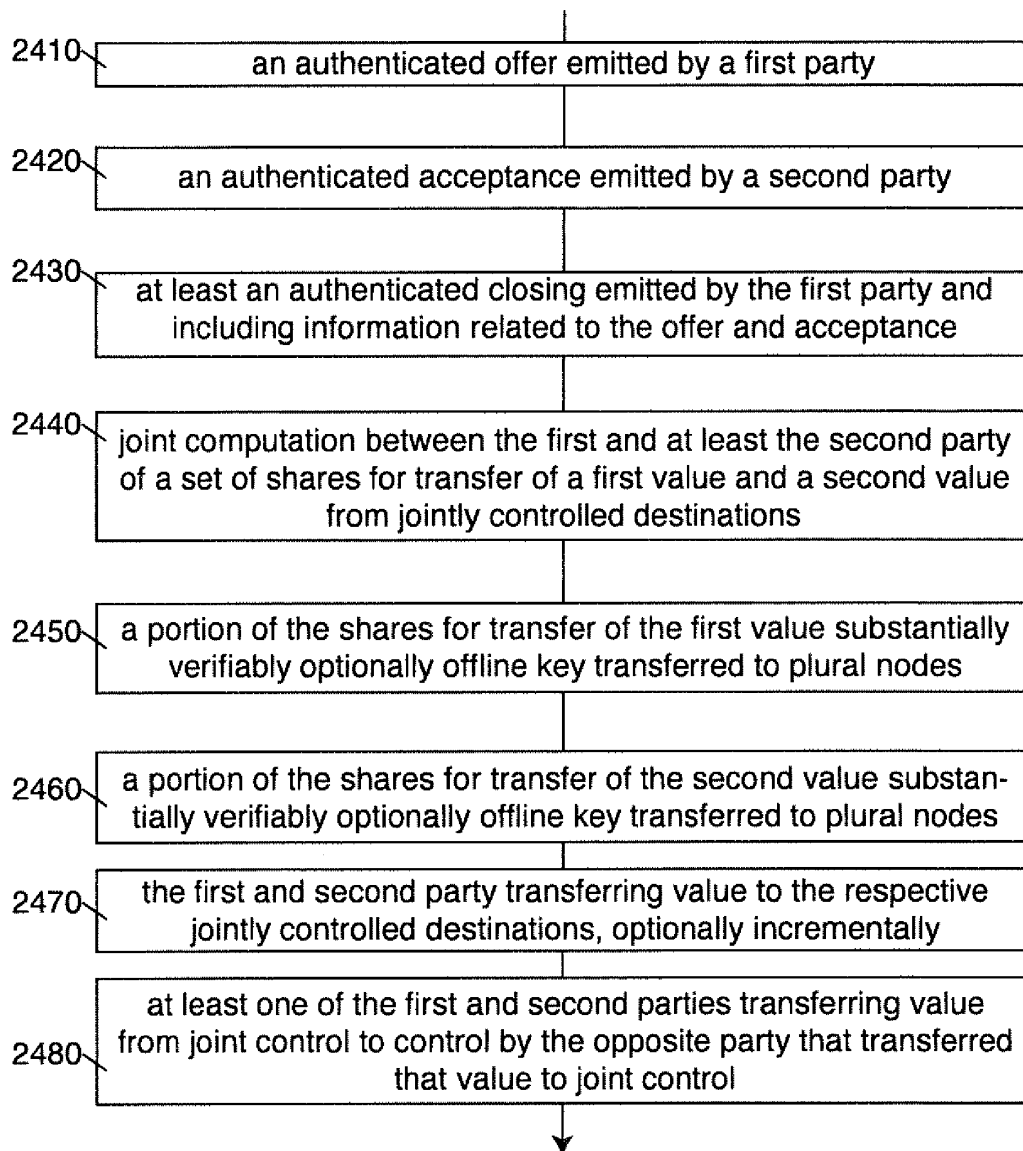
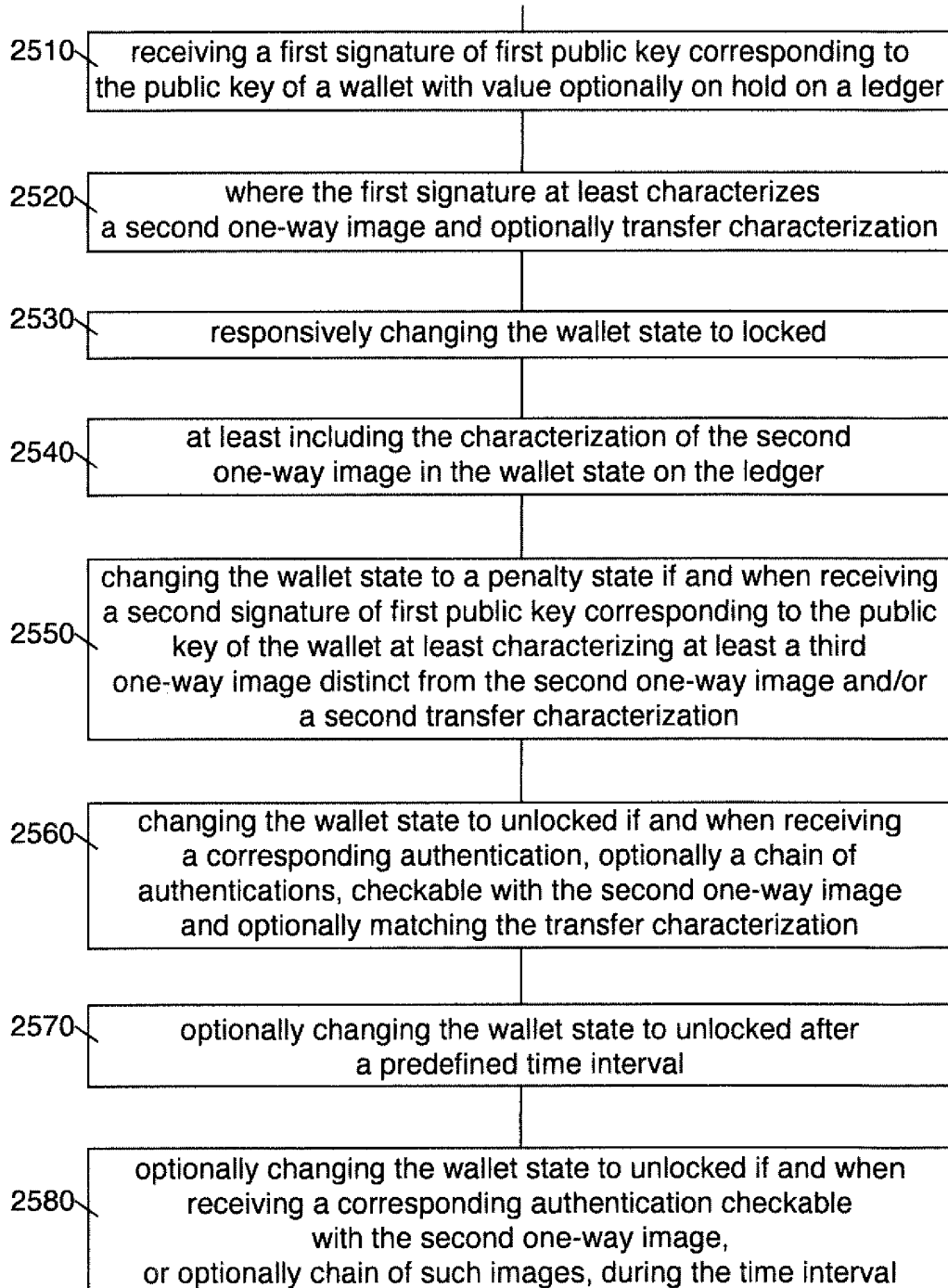
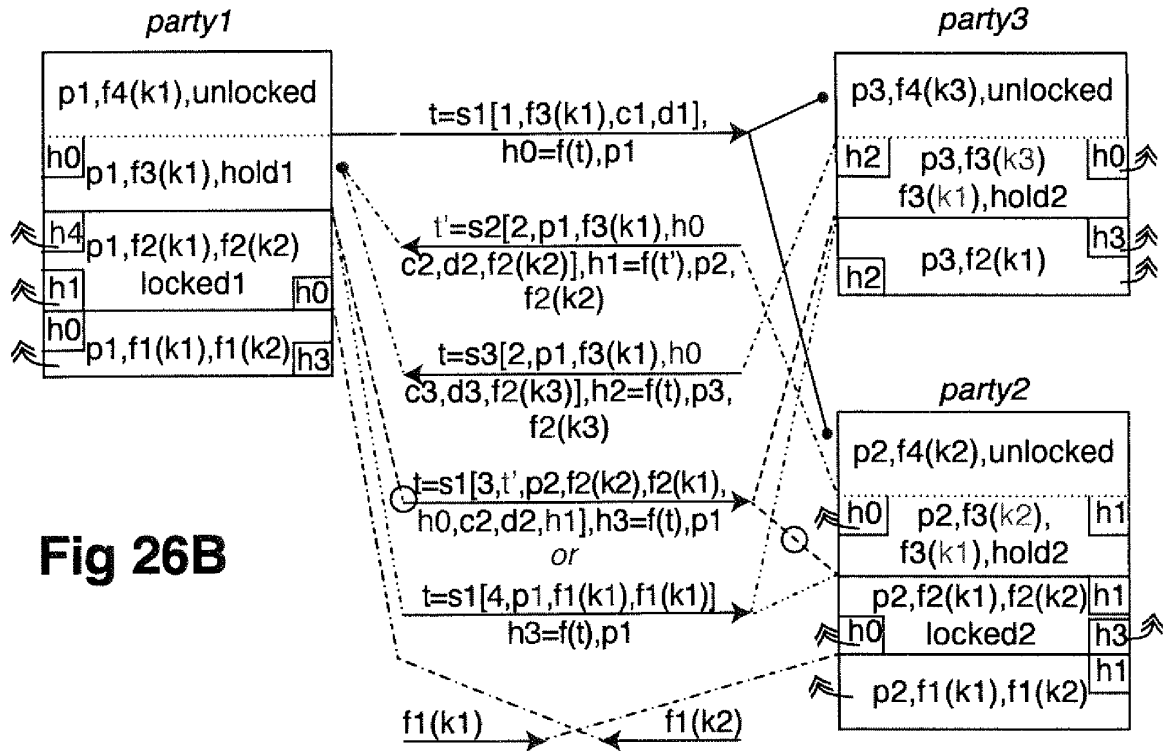
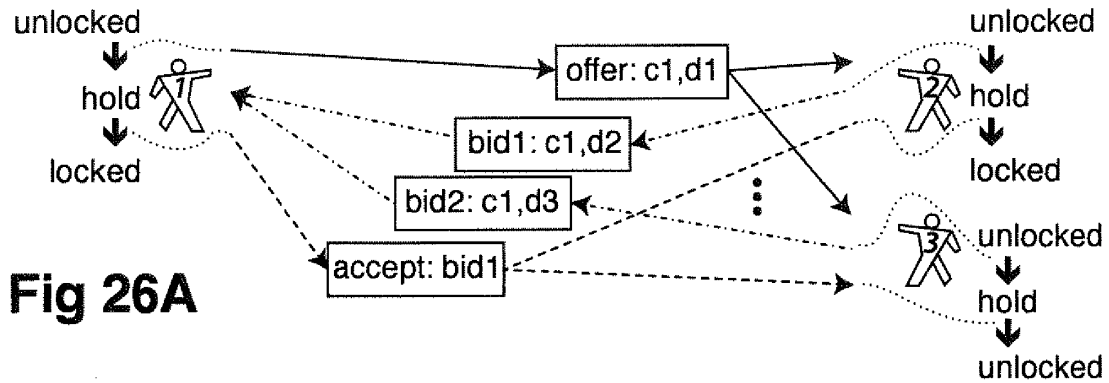


Fig. 22

**Fig. 23**

**Fig. 24**

**Fig. 25**

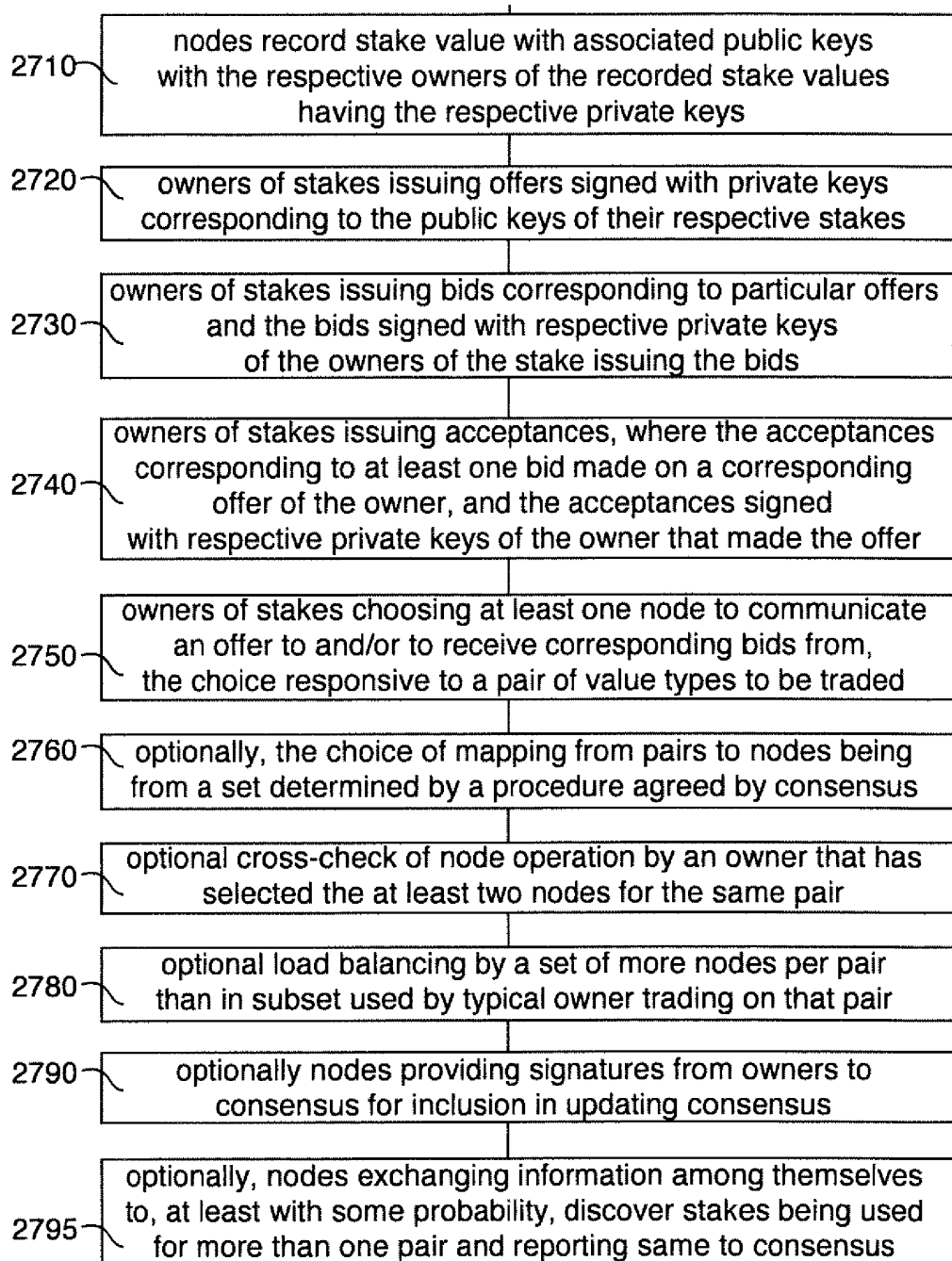


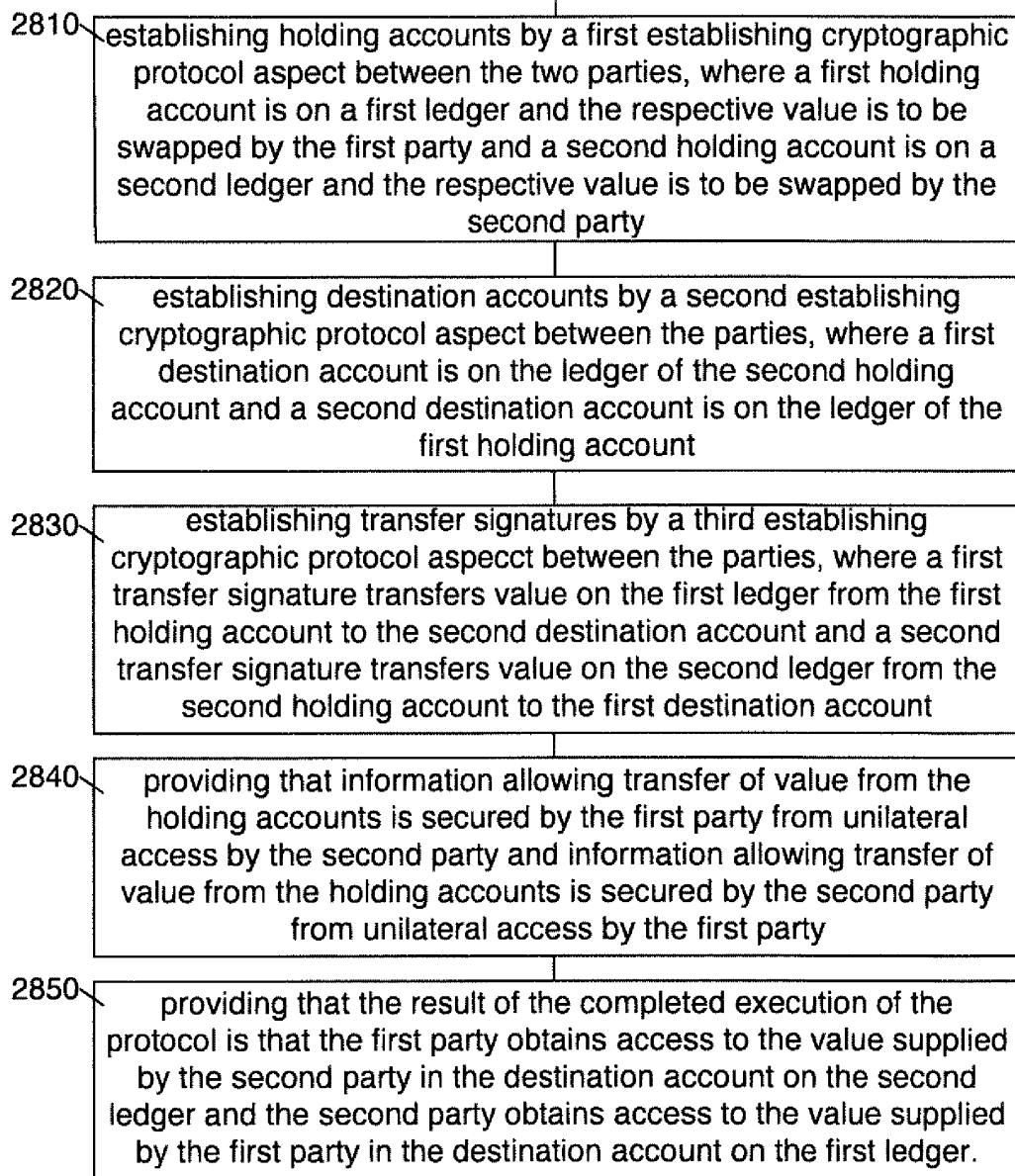
timestamps implicit for release from hold to fresh initial state

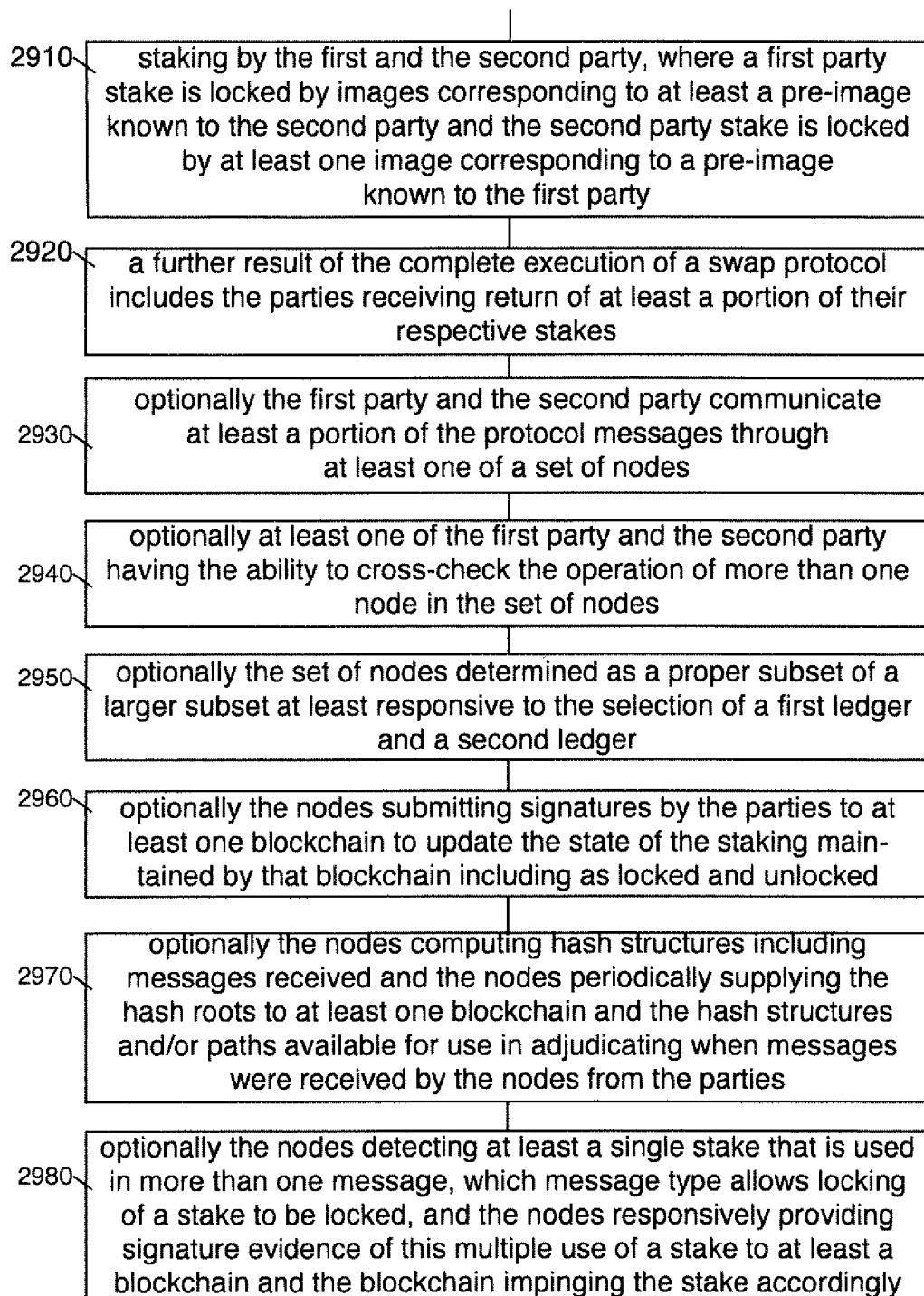
p_i = pubic key of party i s_i = signature by i k_i = secret random key of i

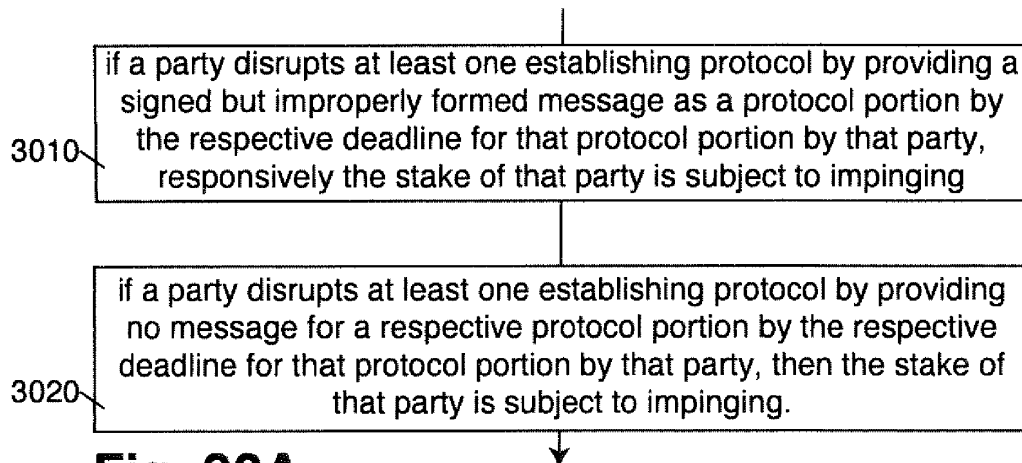
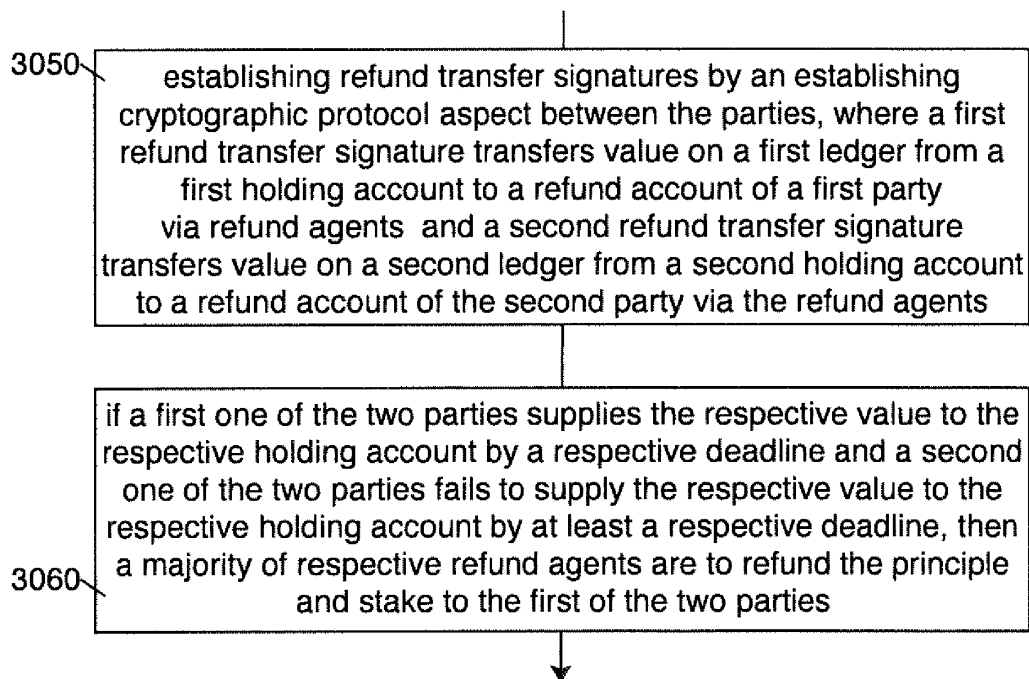
f_j = j th iteration of one-way f $\bigcirc$ = signature checking t = temporary variable

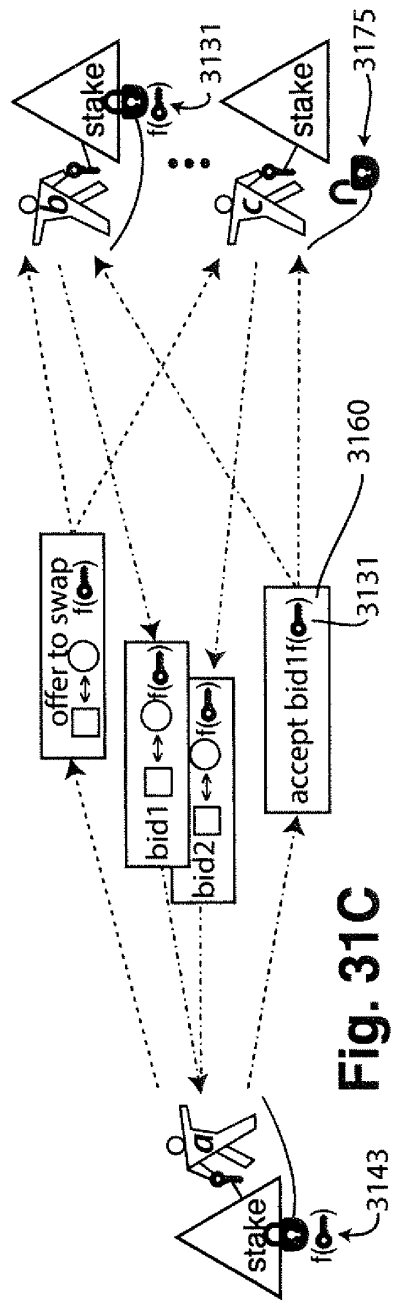
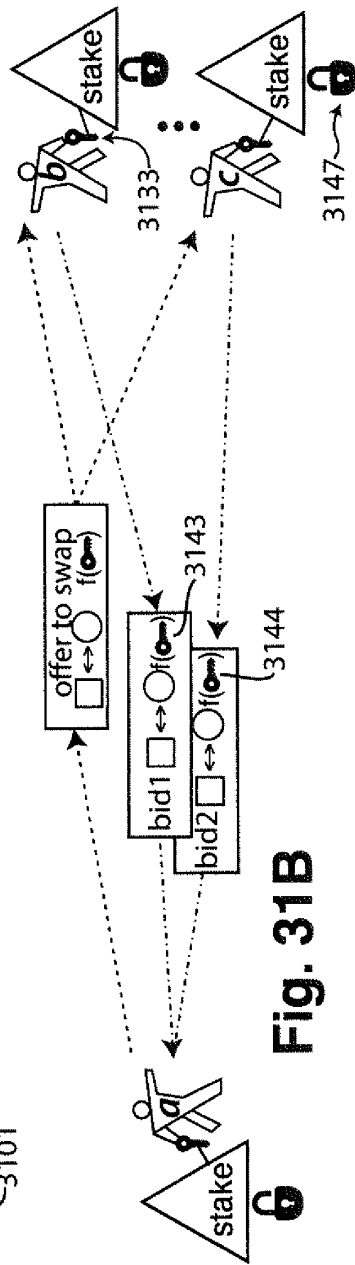
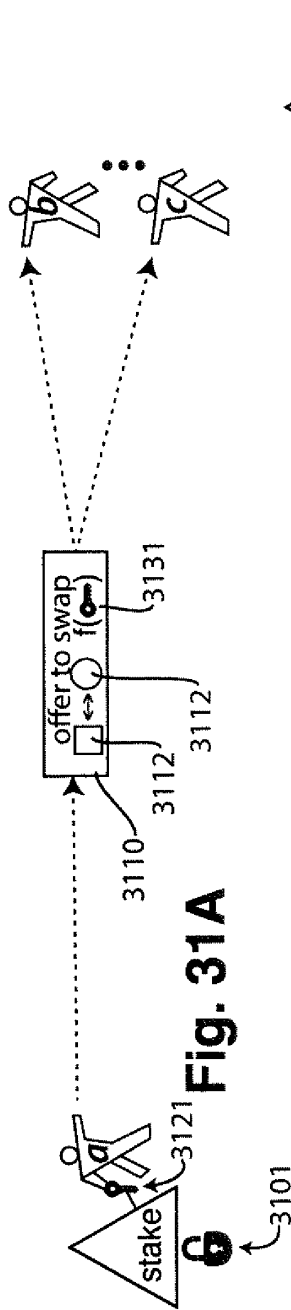
h_i = hash for double-signature checking $\rightsquigarrow$ = return to fresh initial state

**Fig. 27**

**Fig. 28**

**Fig. 29**

**Fig. 30A****Fig. 30B**



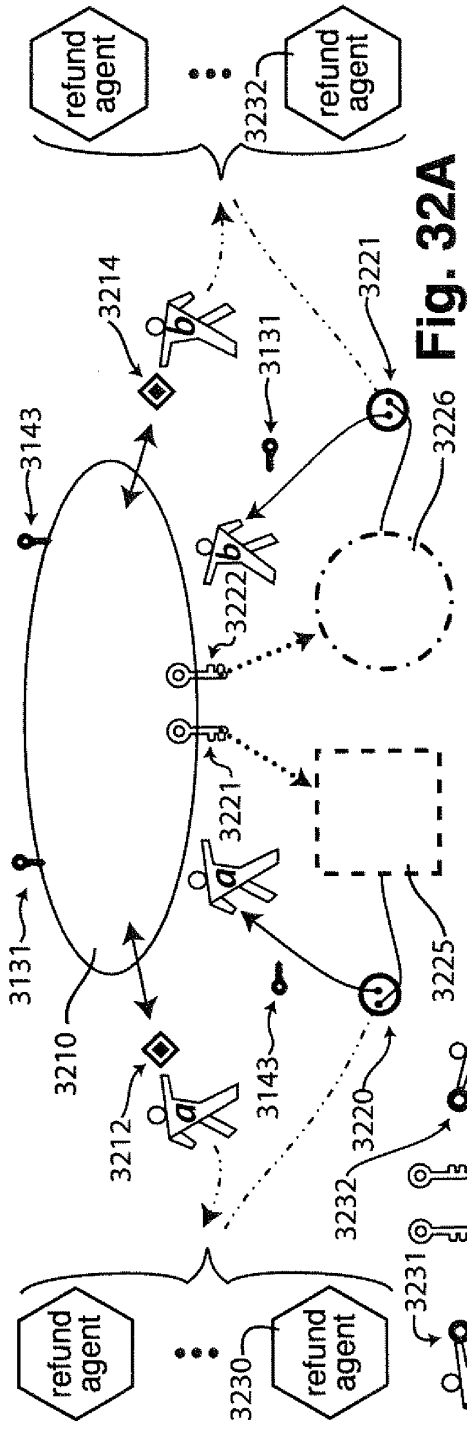


Fig. 32A

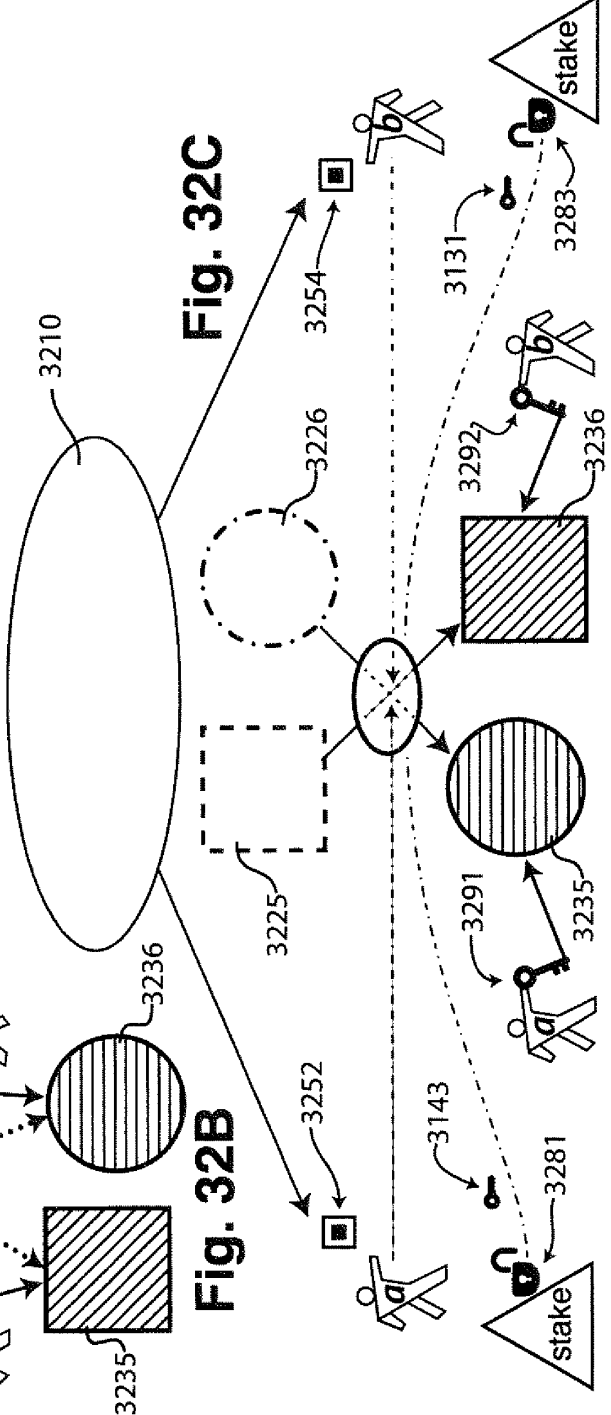
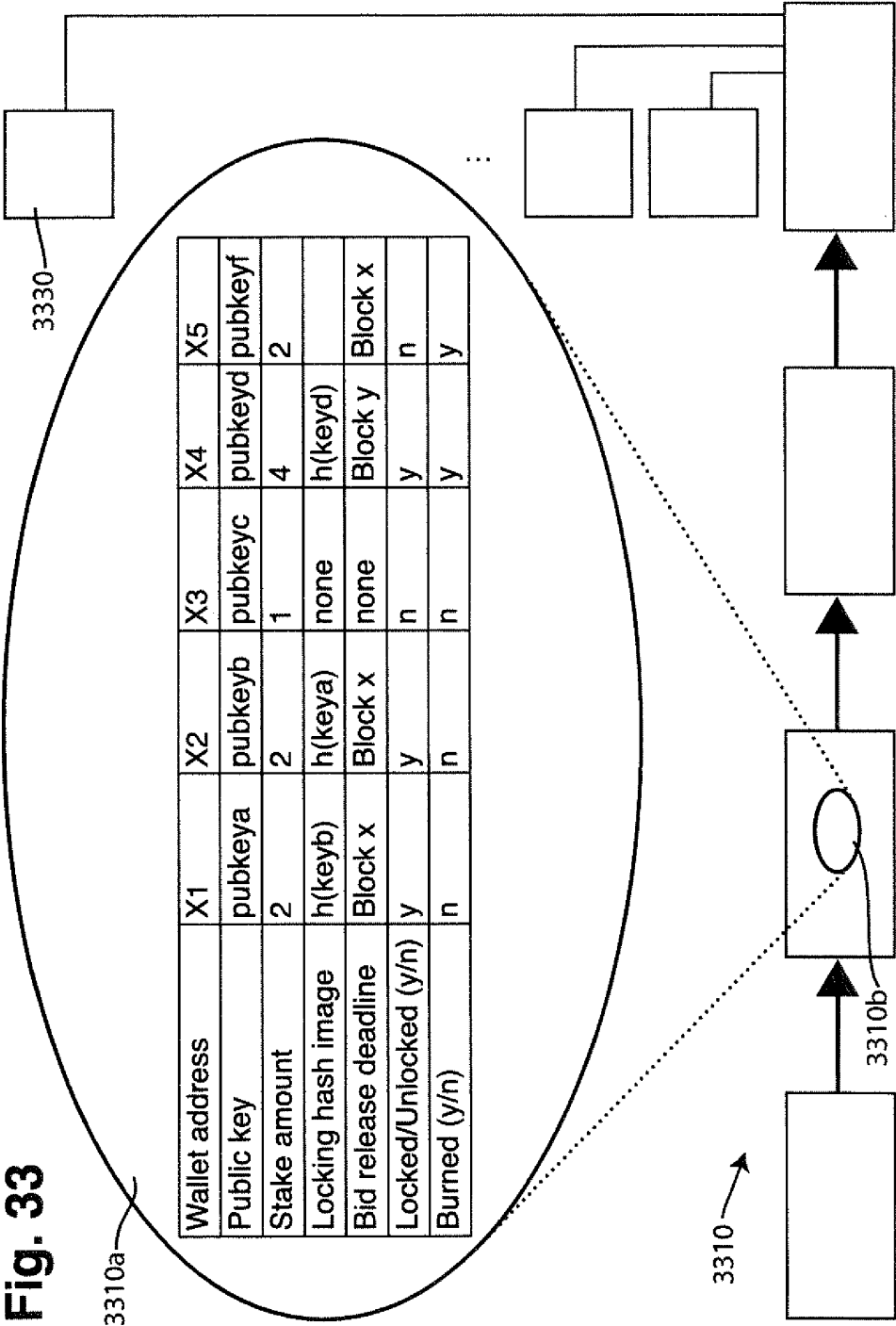


Fig. 32B

Fig. 32C



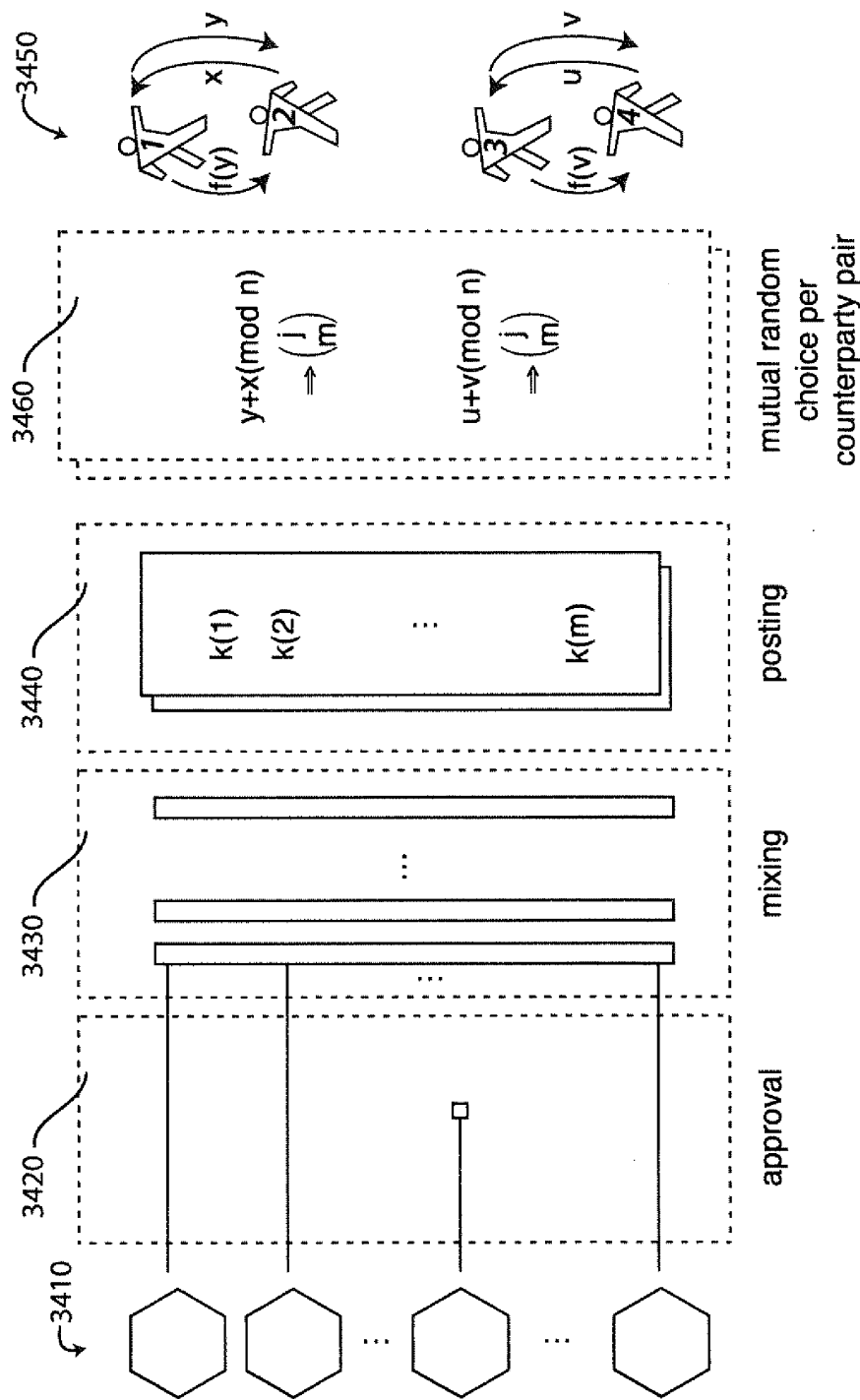


Fig. 34

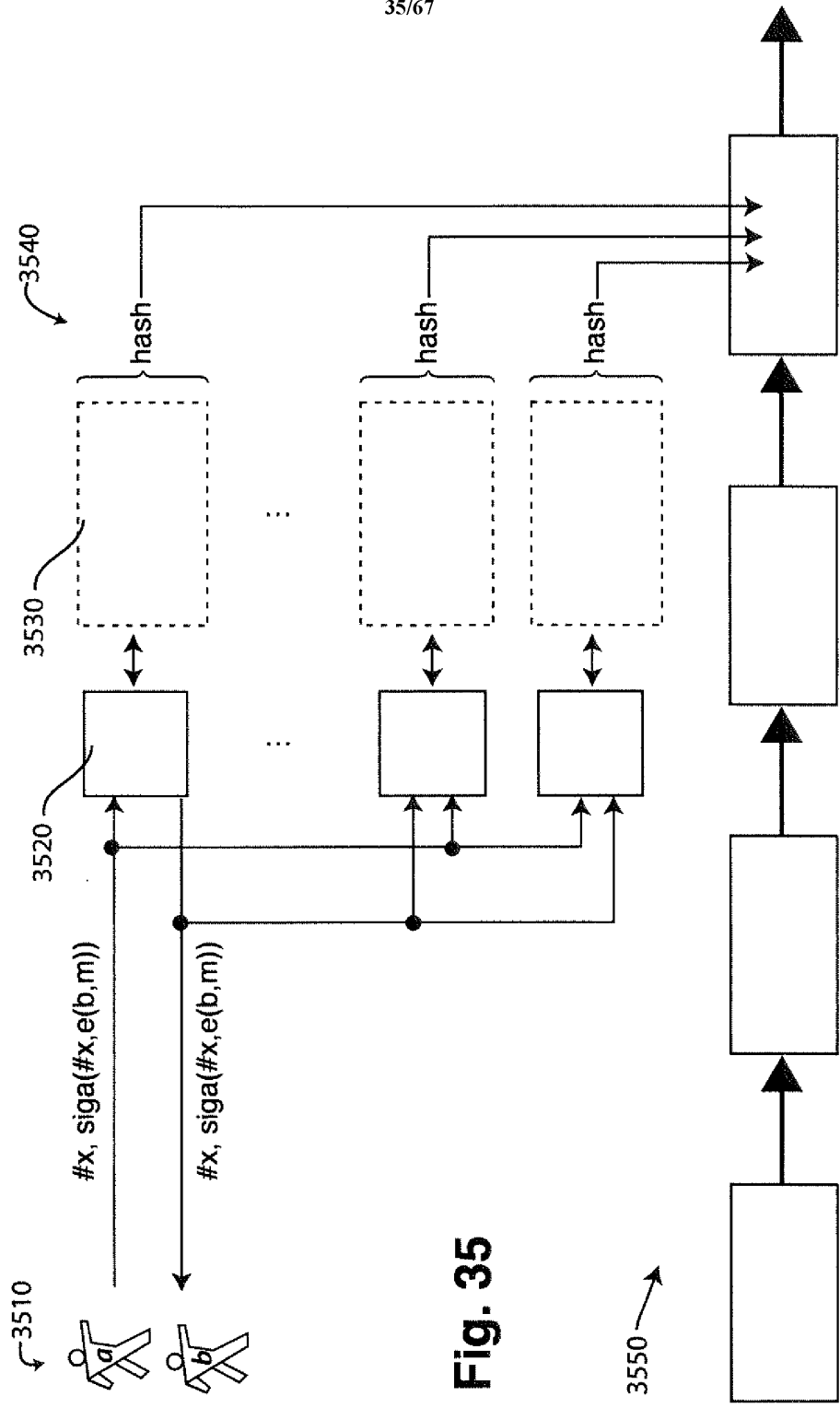


Fig. 35

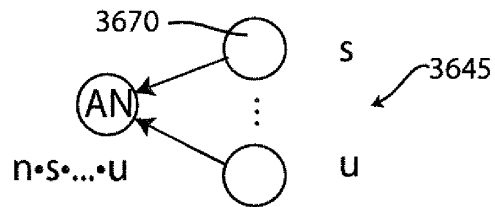


Fig. 36A

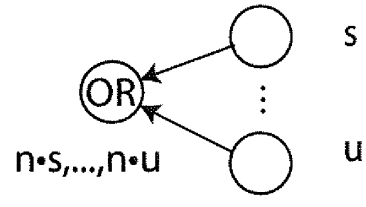


Fig. 36B

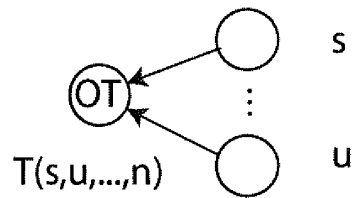


Fig. 36C

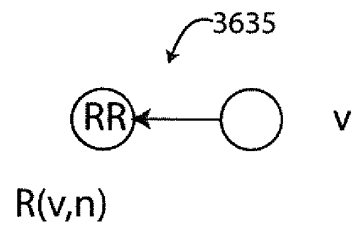


Fig. 36D

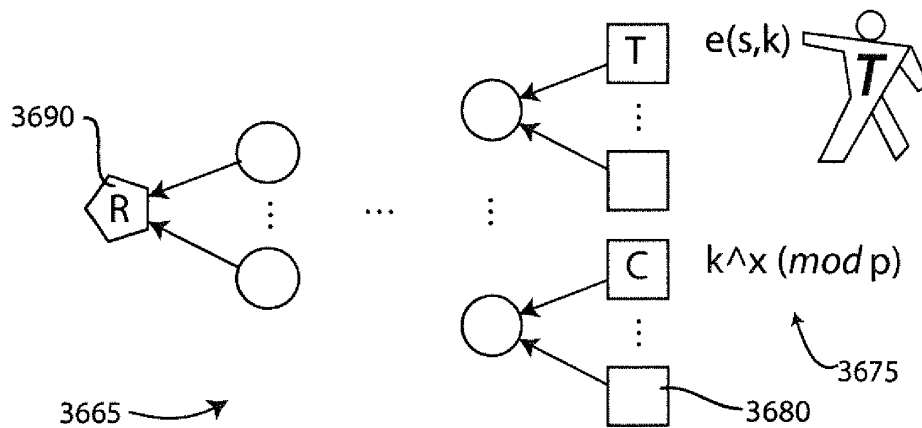
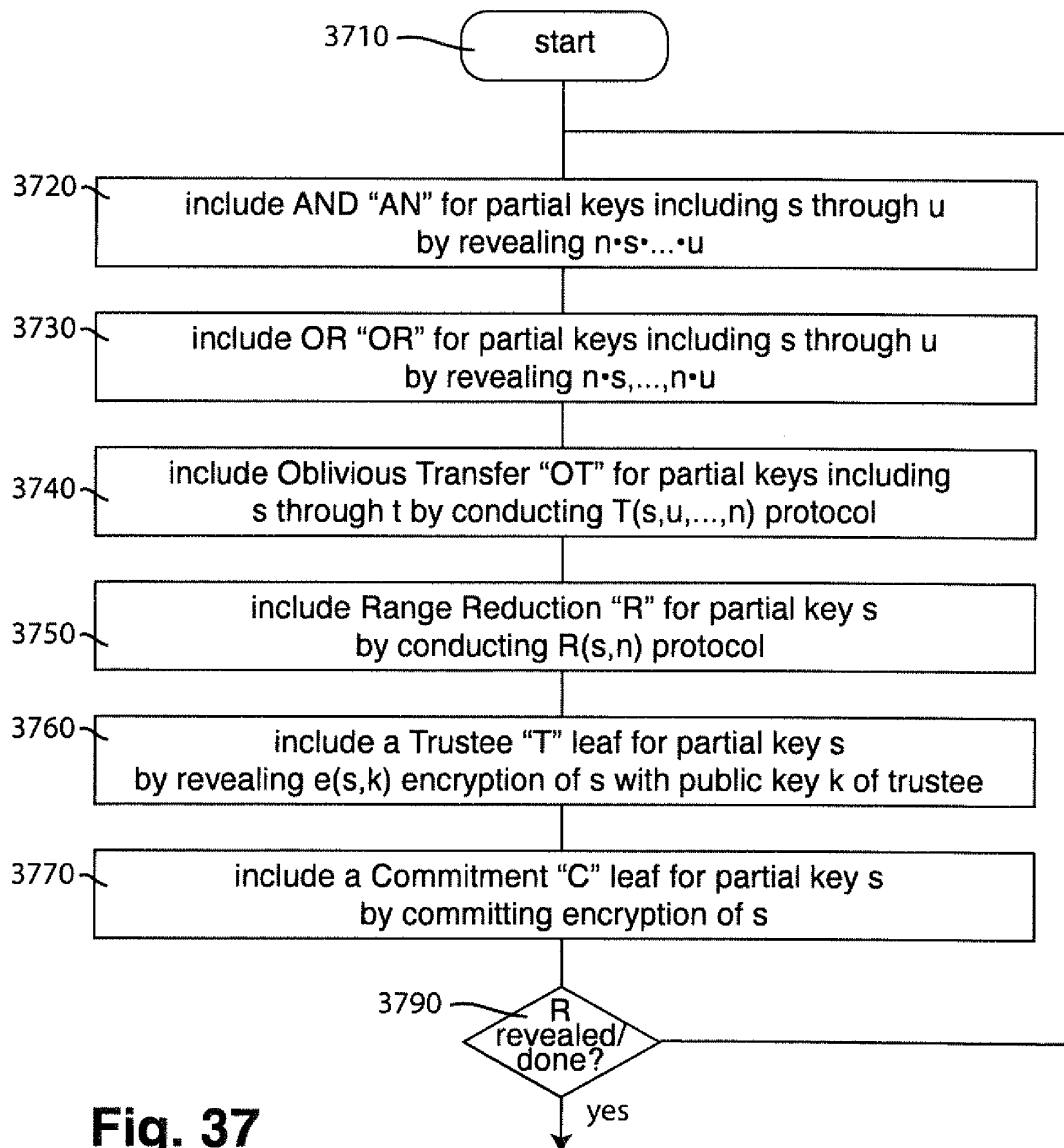
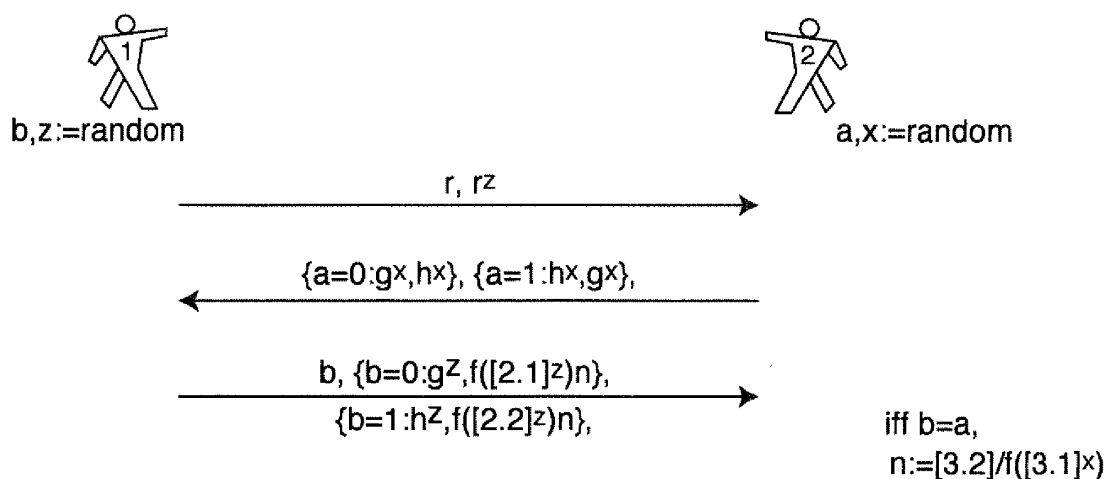
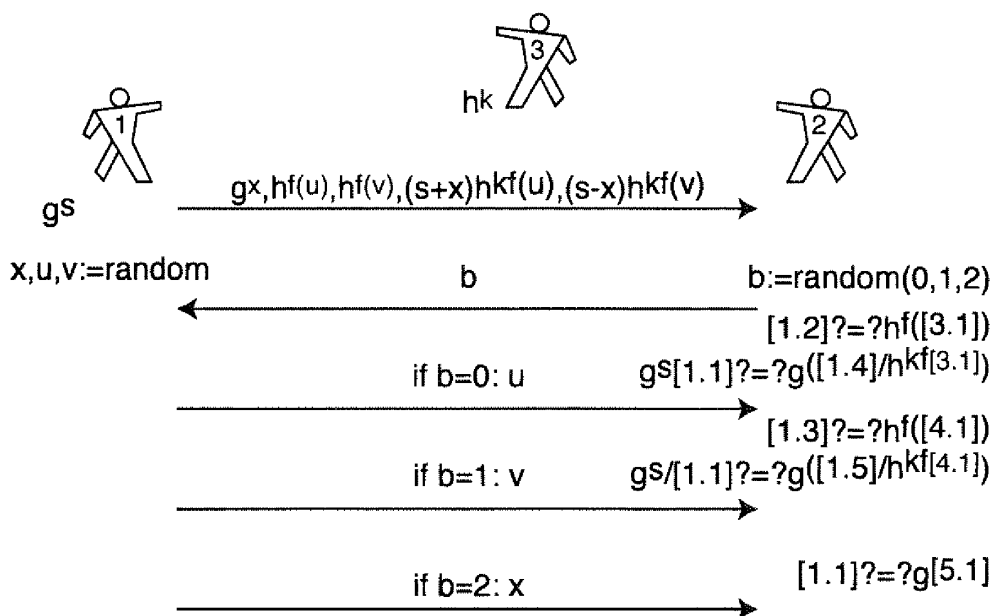
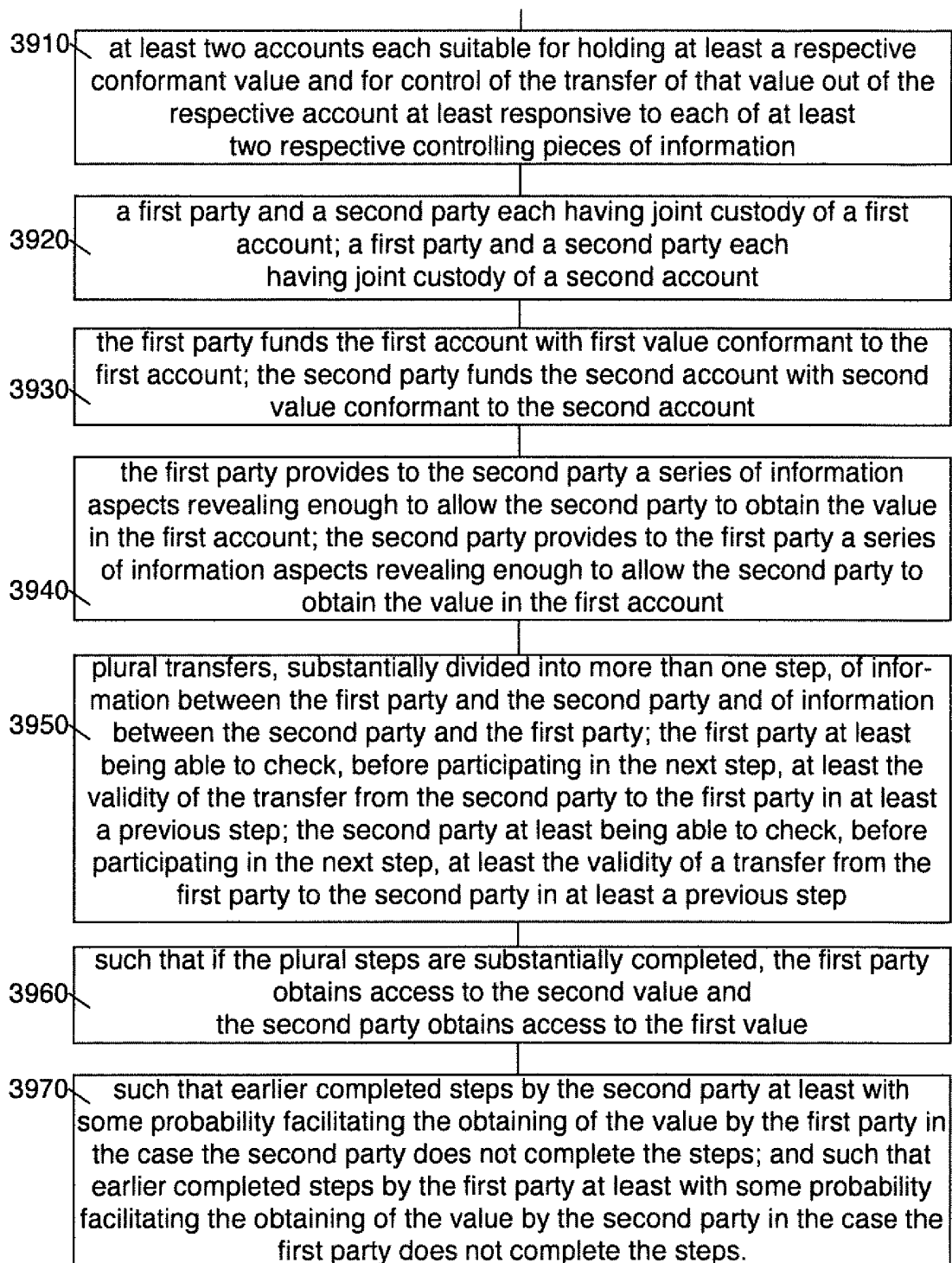
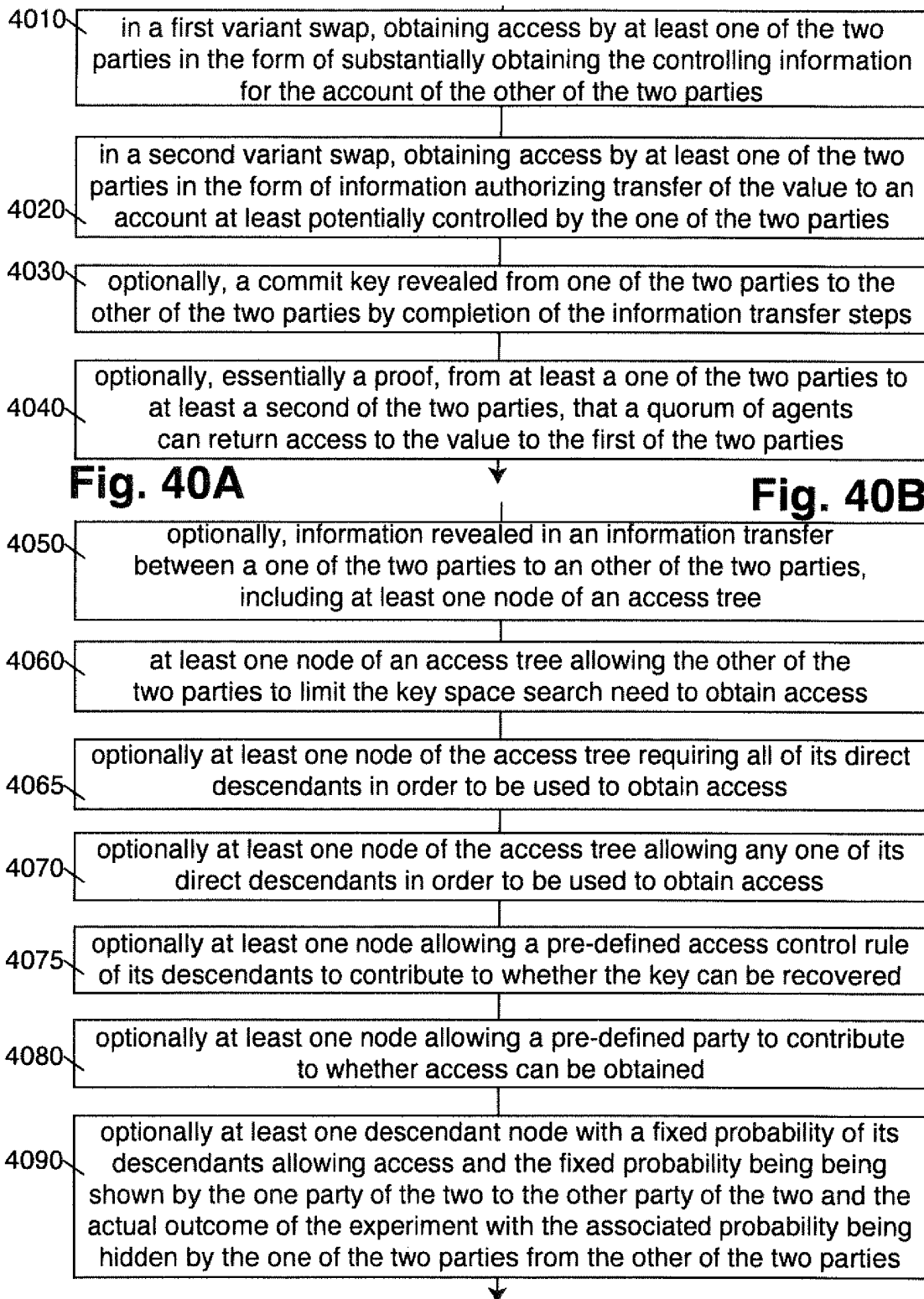


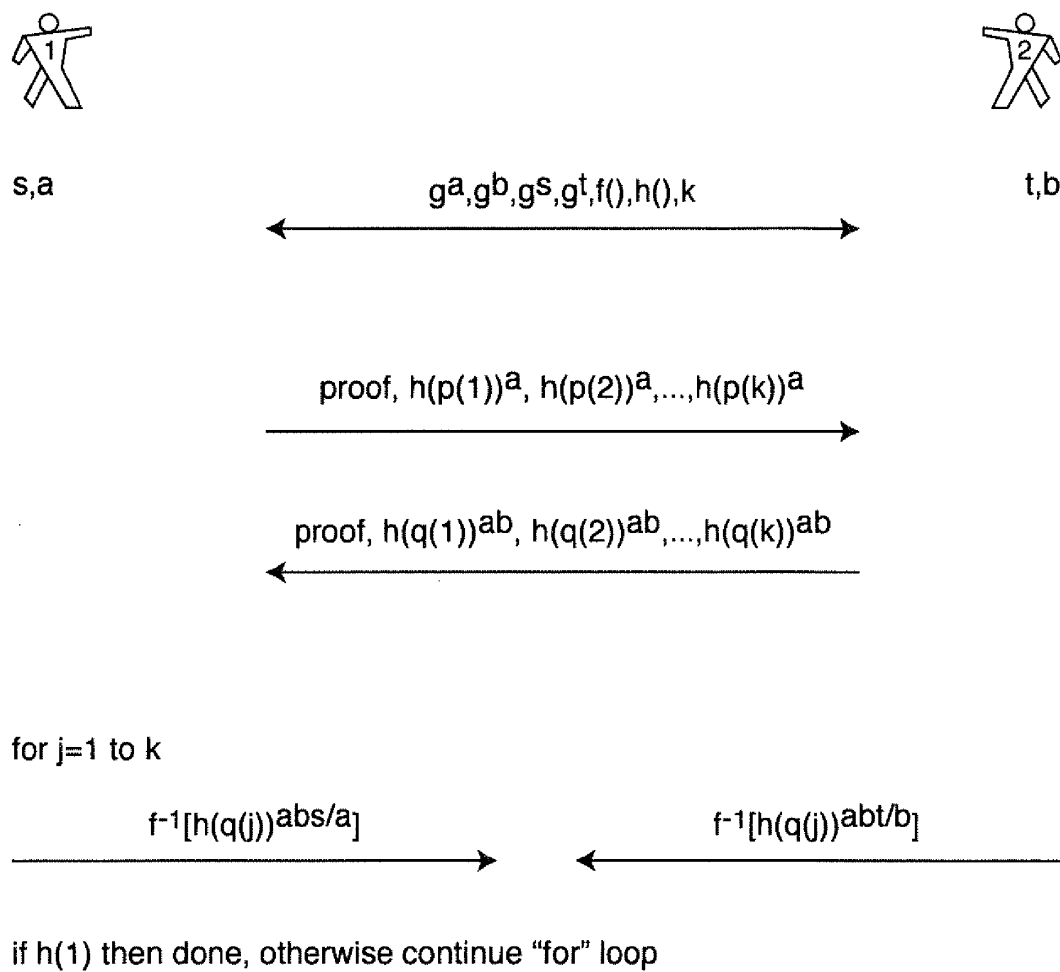
Fig. 36E

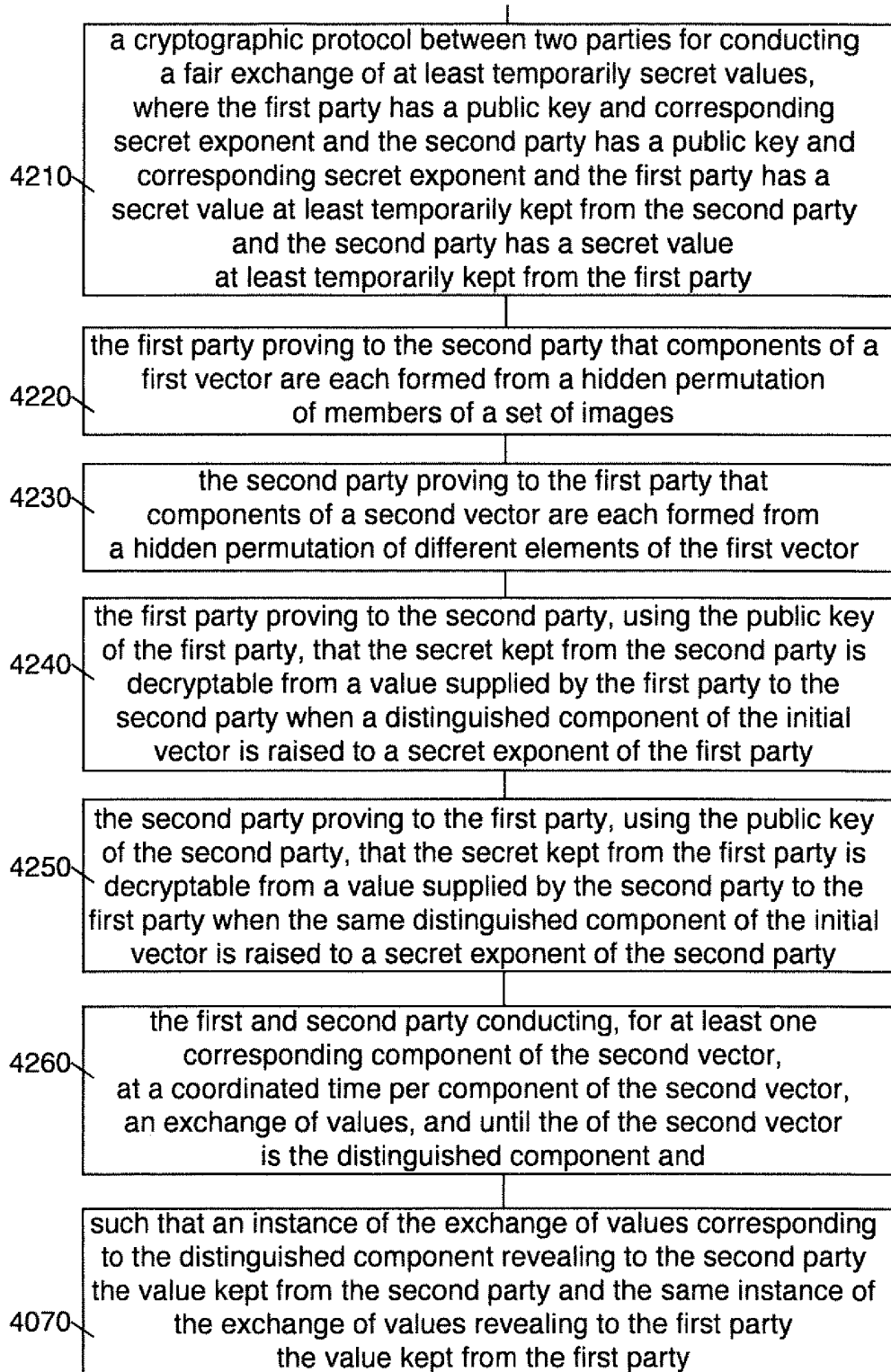
**Fig. 37**

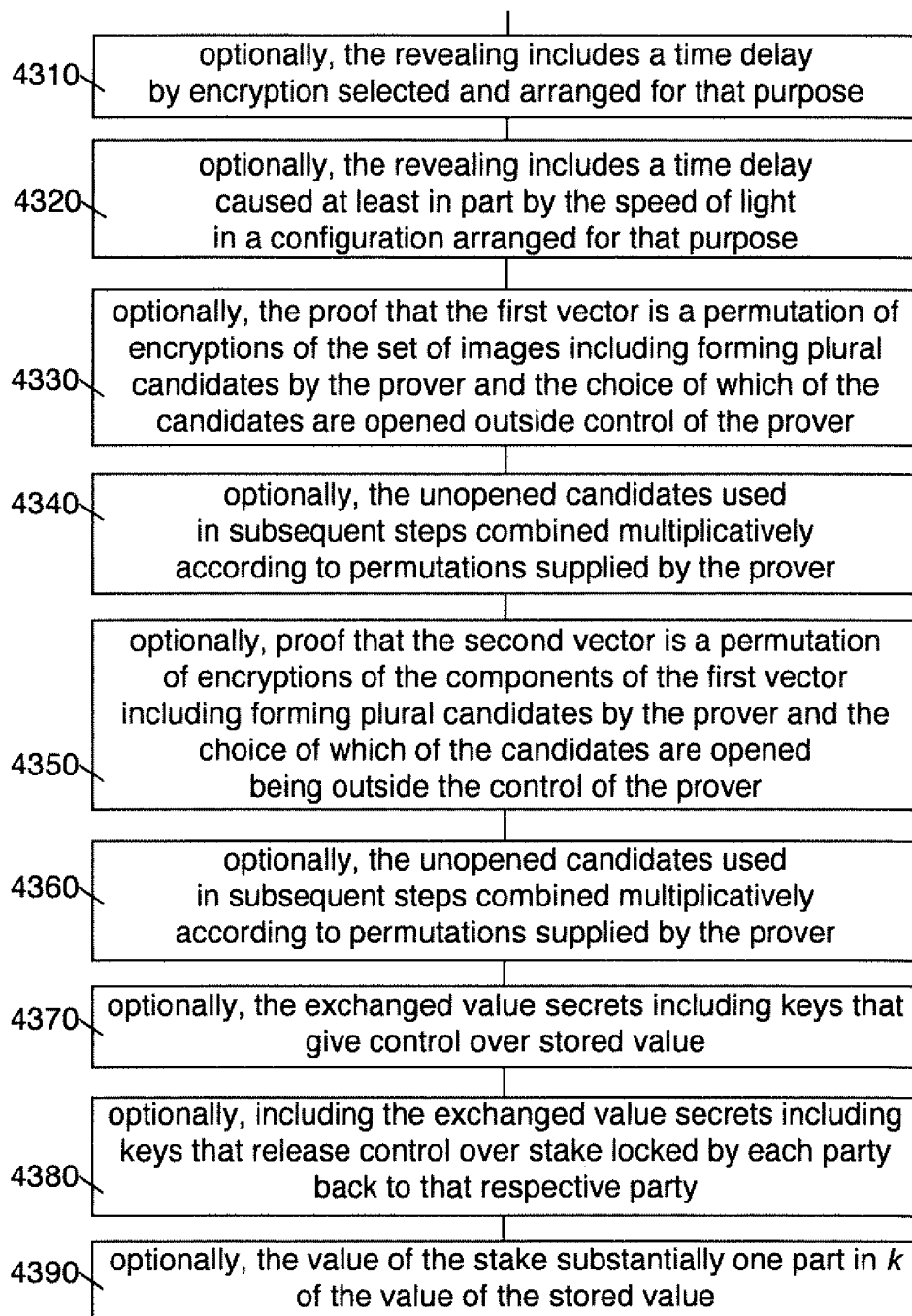
**Fig. 38A****Fig. 38B**

**Fig. 39**



**Fig. 41**

**Fig. 42**

**Fig. 43**

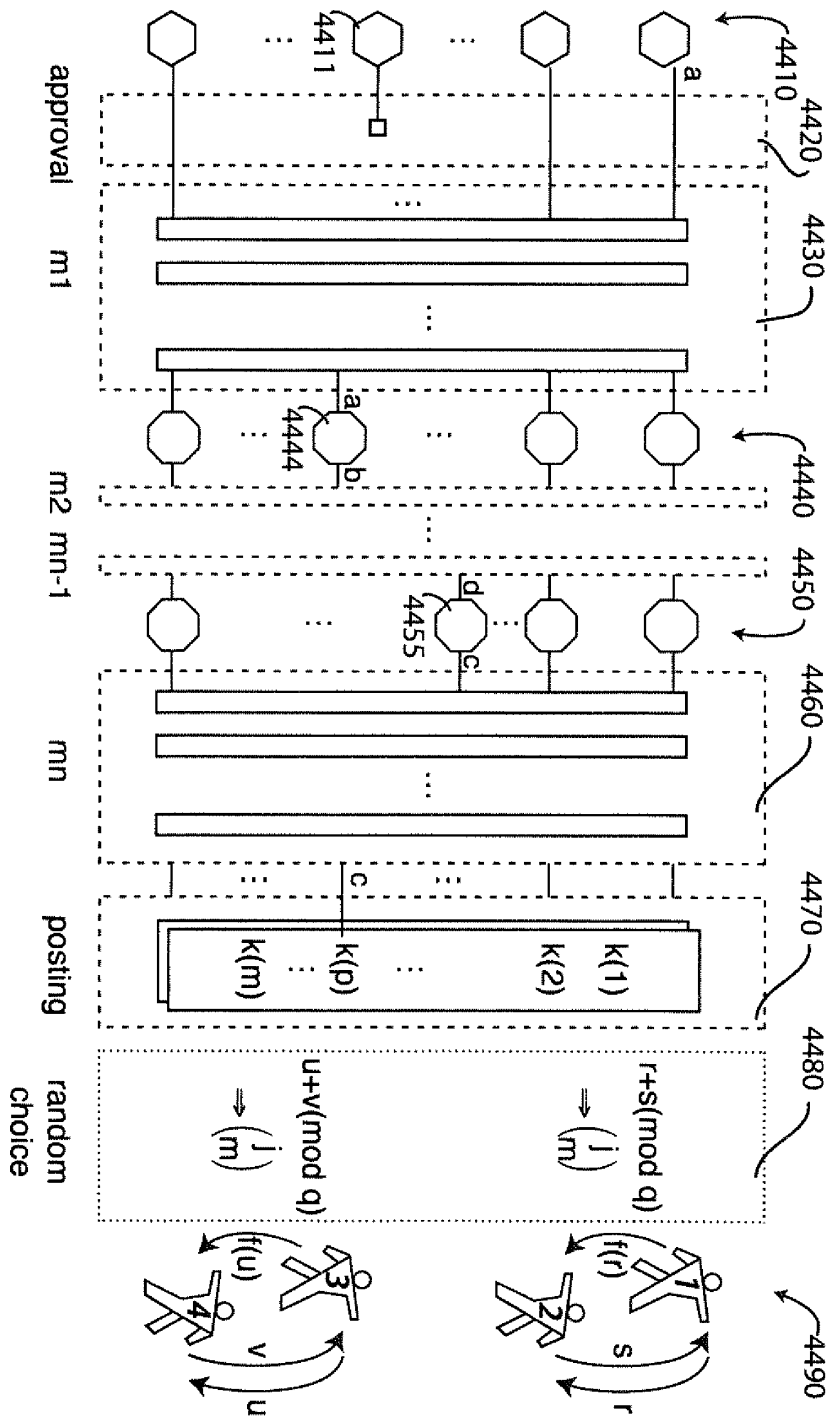
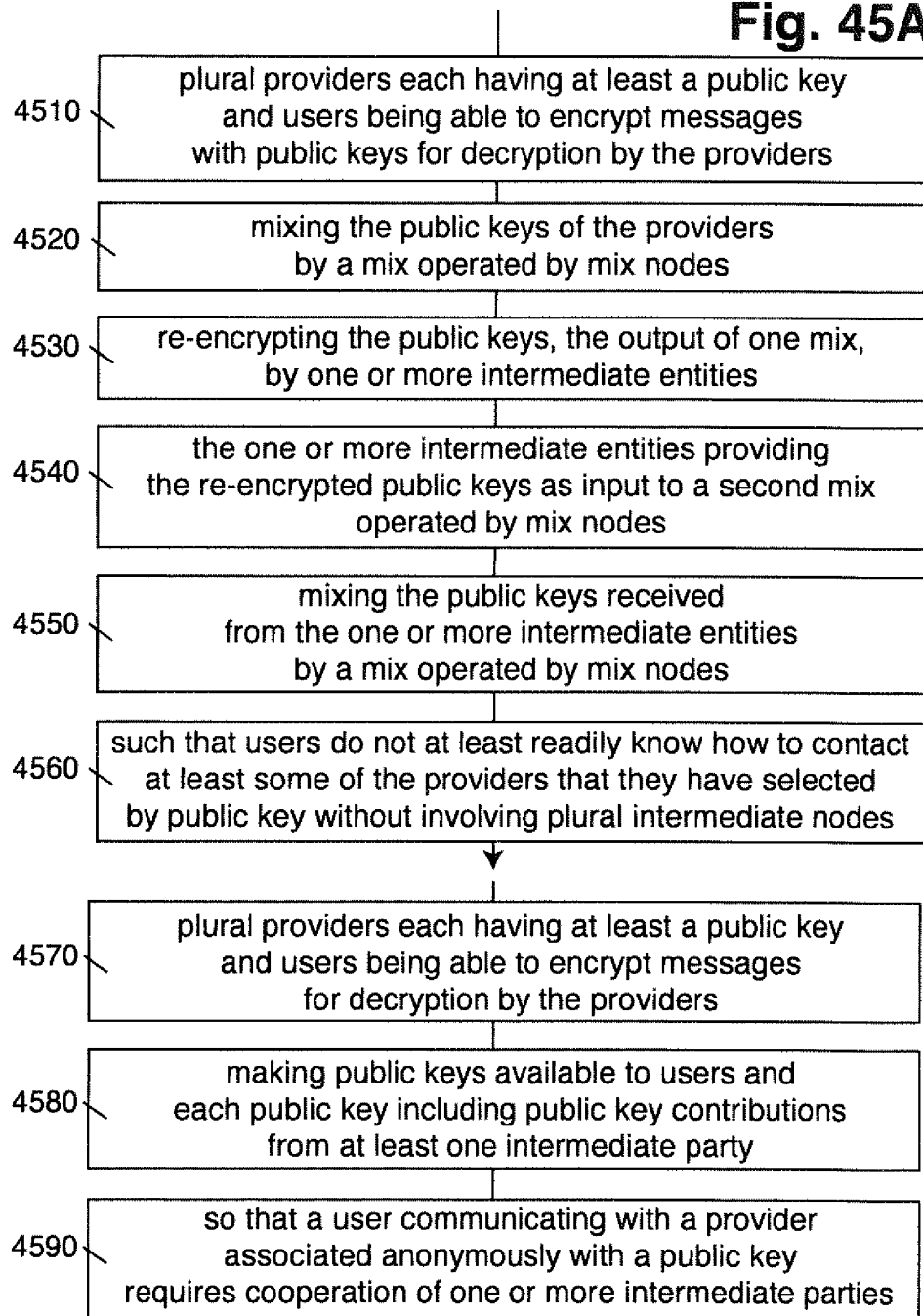


Fig. 44 $a = g^w$ $b = g^{wx}$ $d = g^{wx...y}$ $c = g^{wx...yz} = k(p)$

Fig. 45A**Fig. 45B**

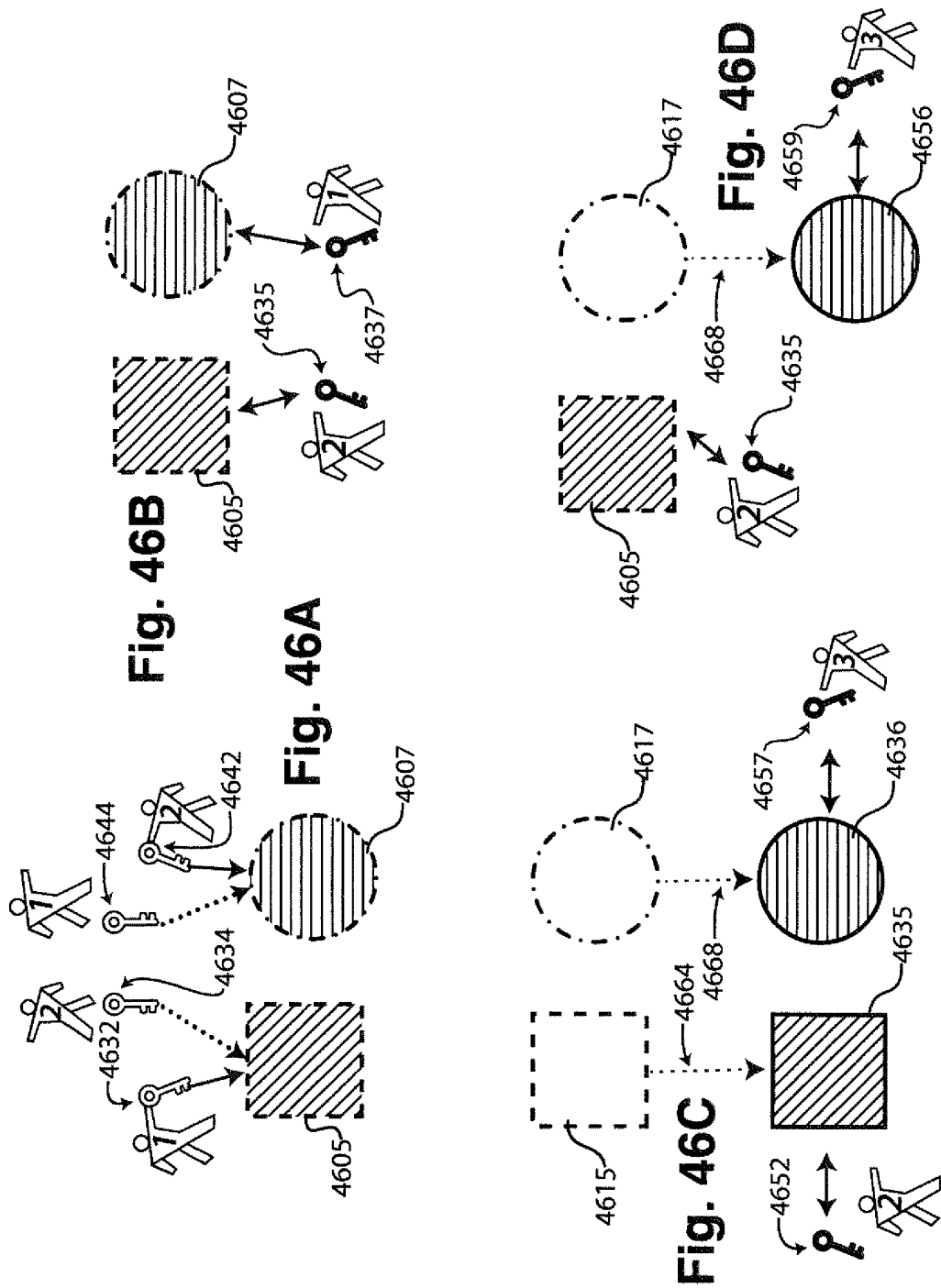
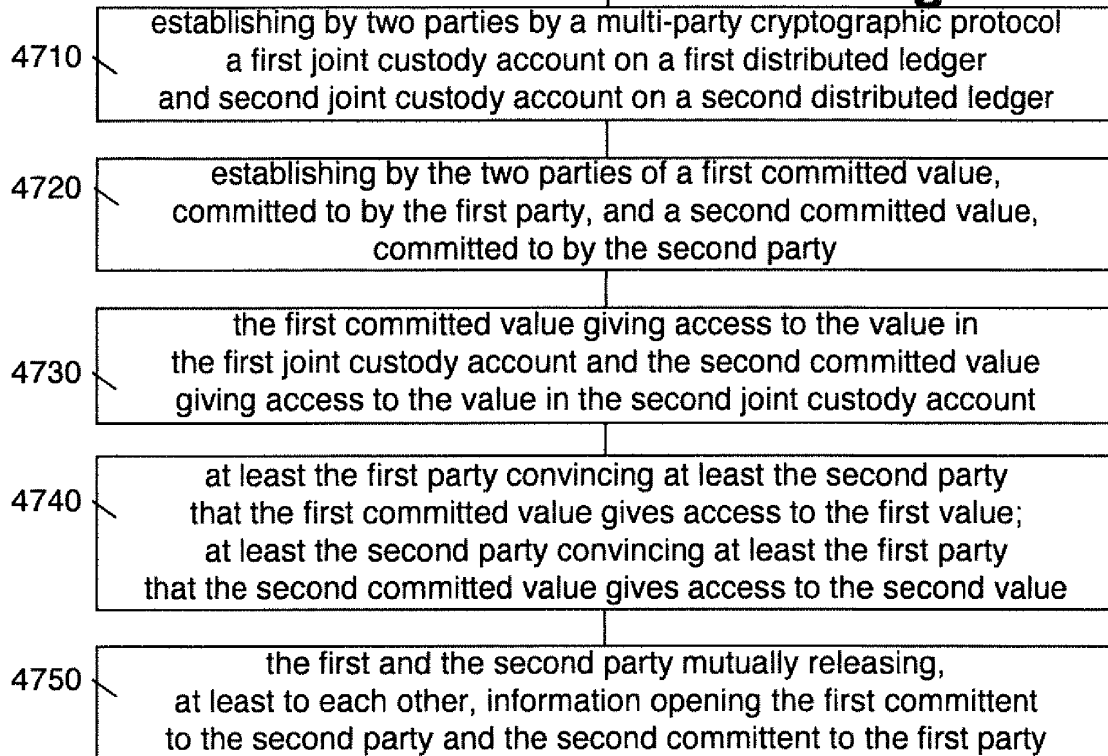
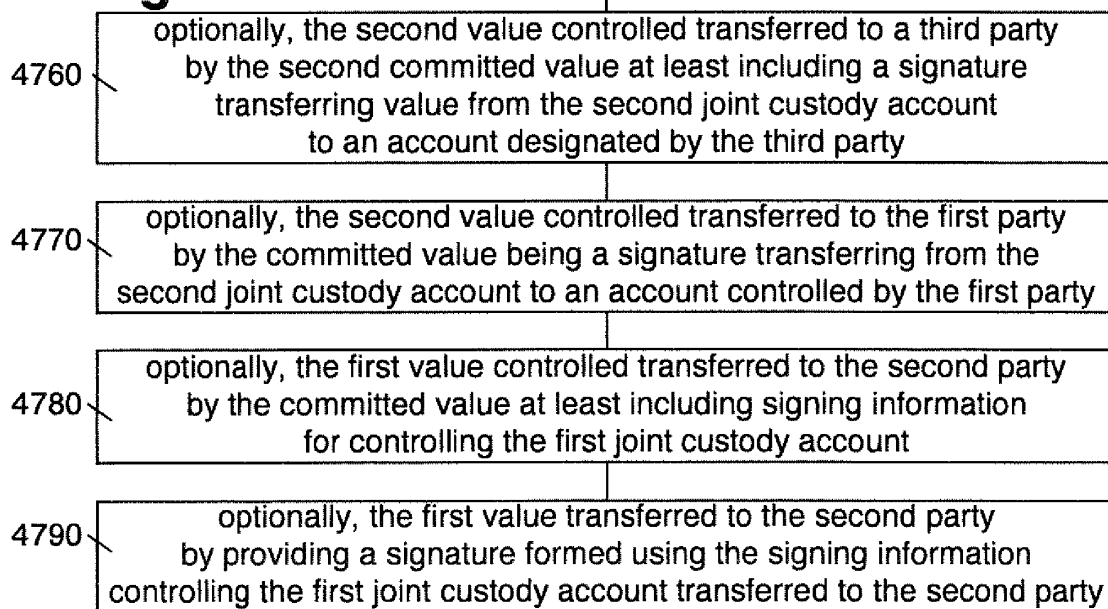


Fig. 47A**Fig. 47B**

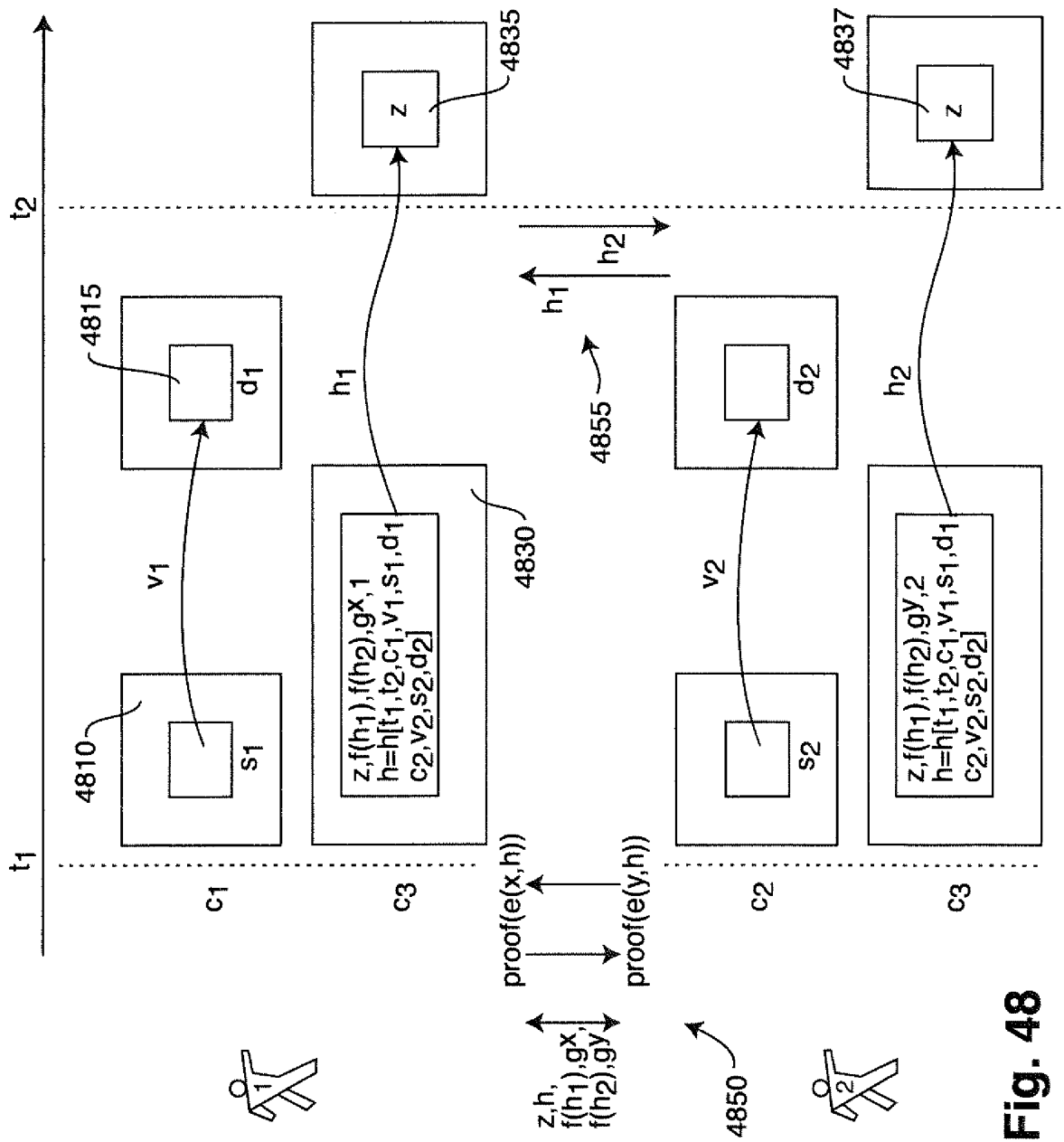
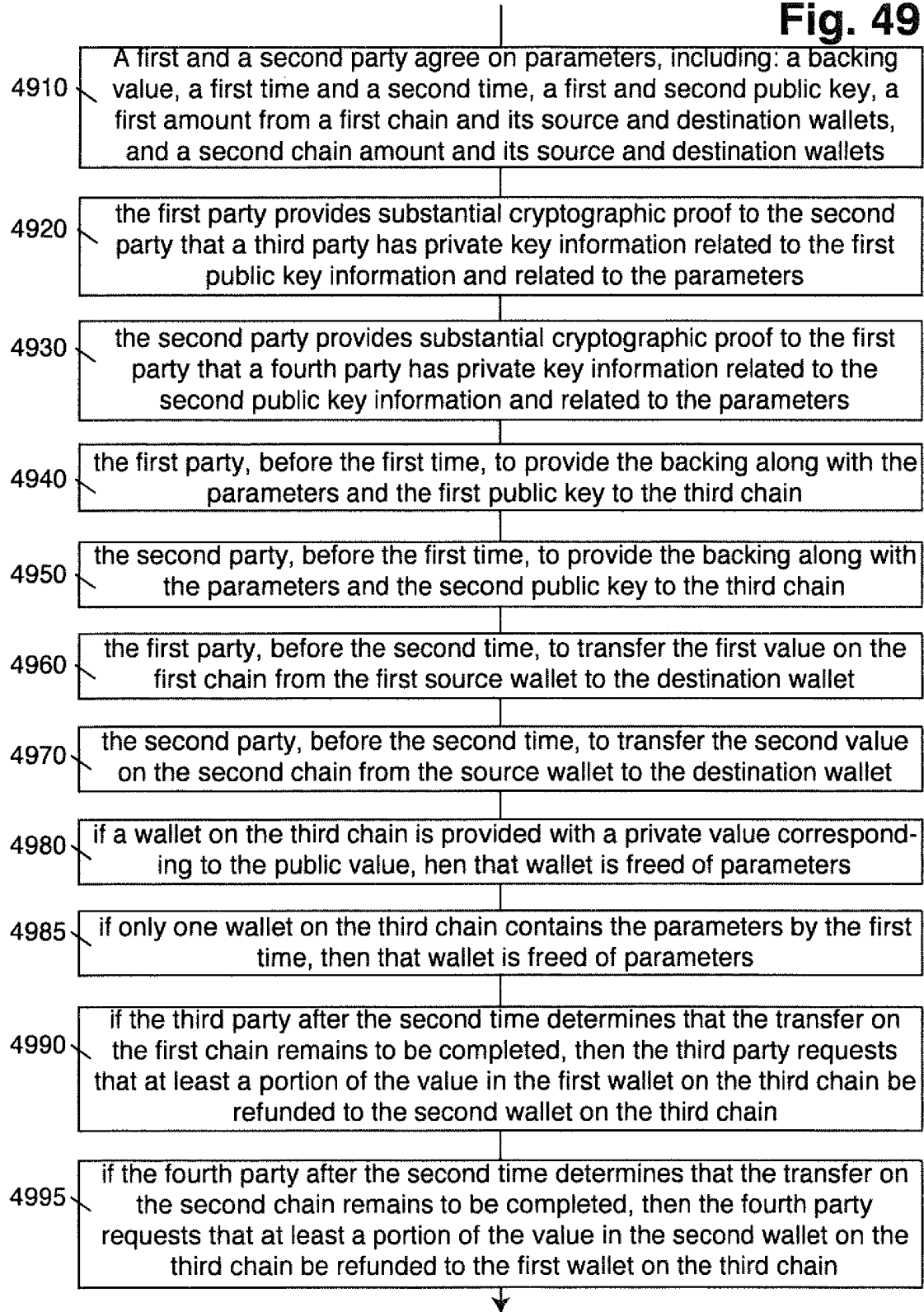


Fig. 48

Fig. 49

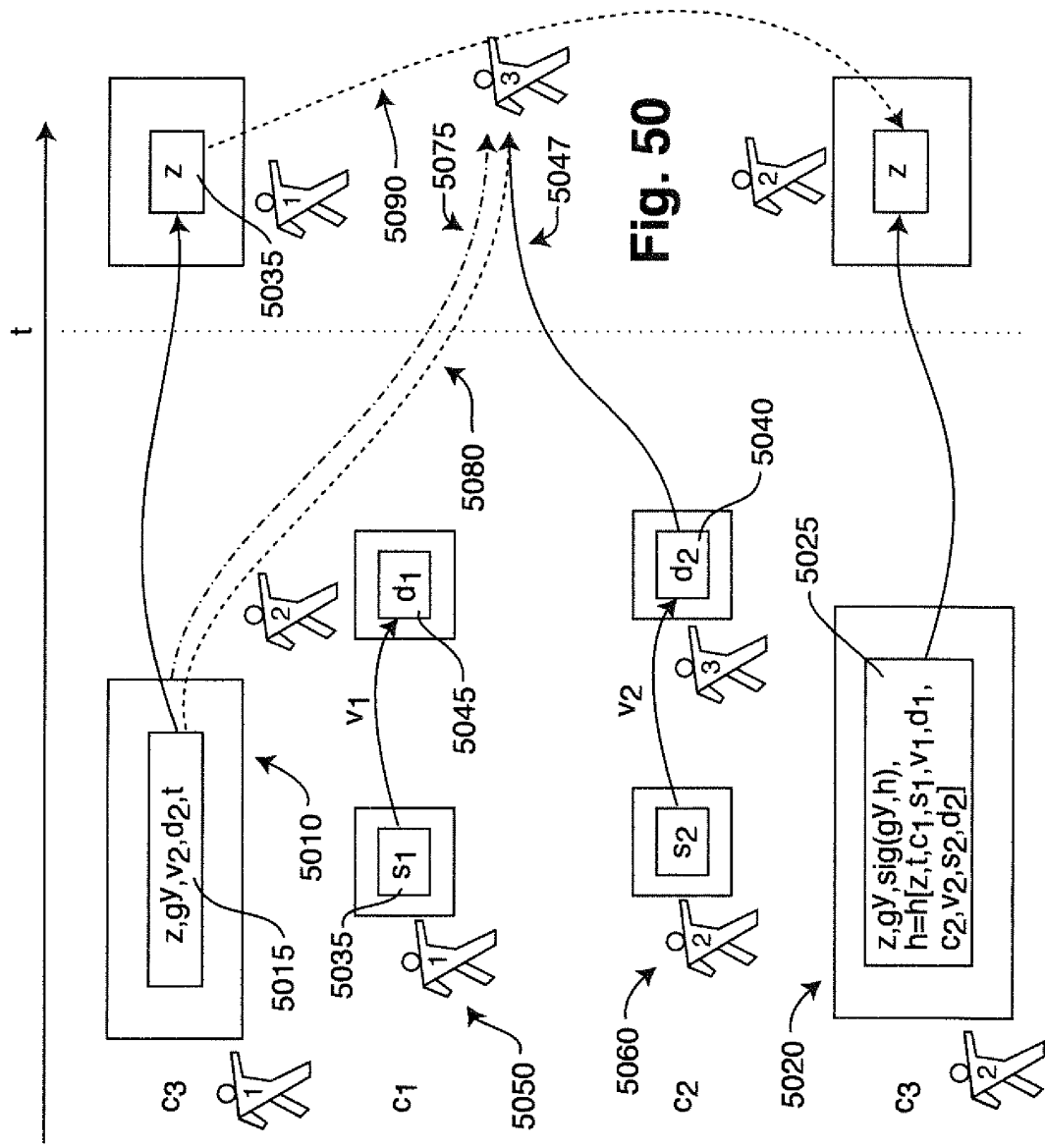
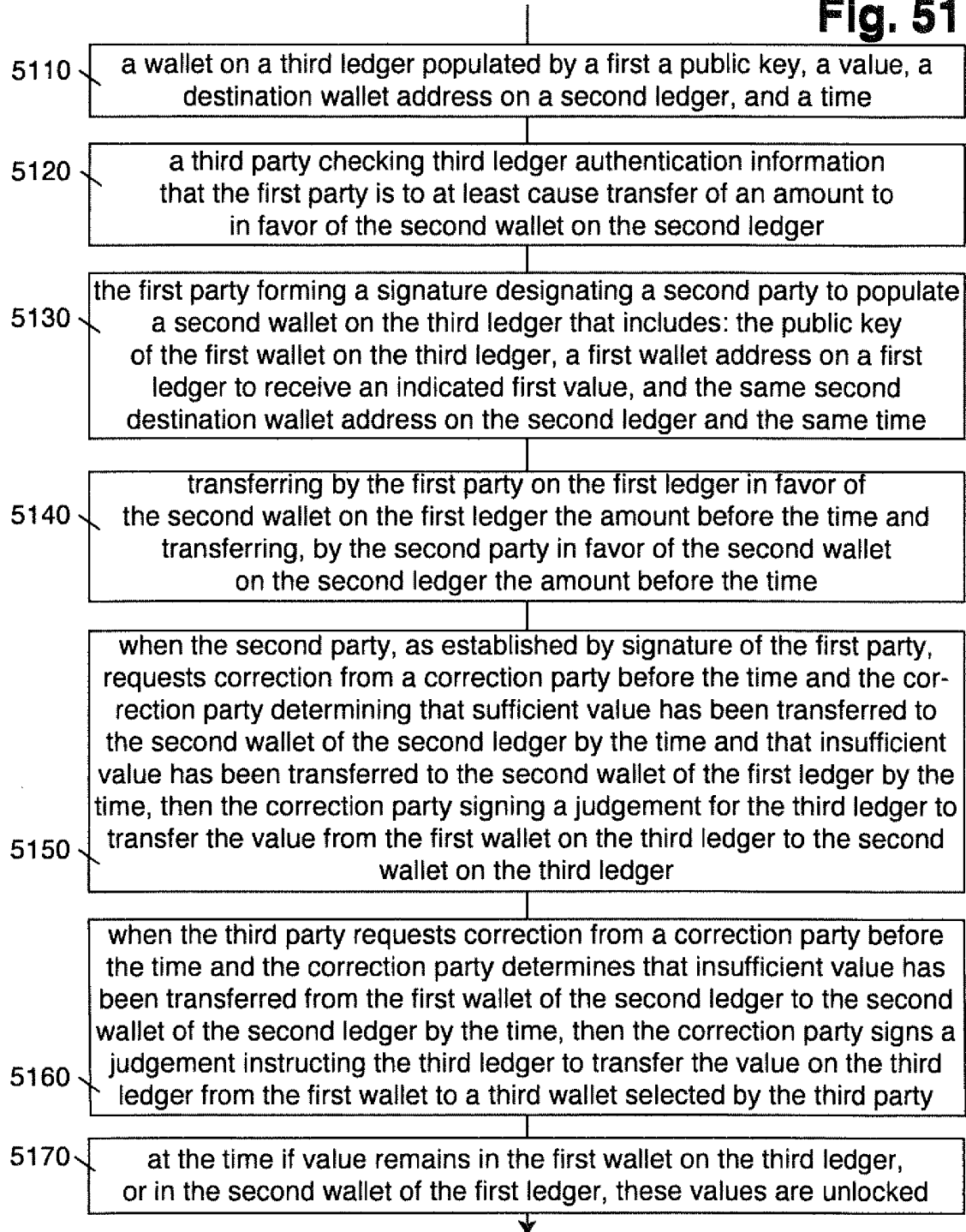
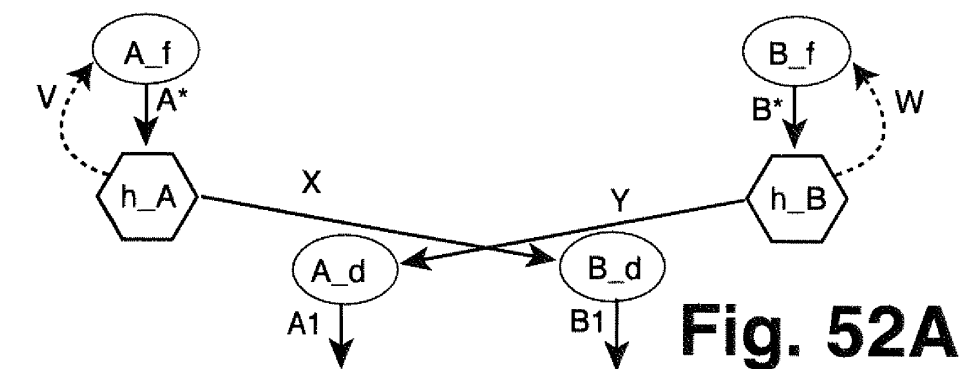


Fig. 50

Fig. 51



$$X=R(C_H1.1, C_H2.1,...C_Hn.1)$$
$$Y=R(C_H1.2, C_H2.2,...C_Hn.2)$$

$$W=R(C_H1.3, C_H2.3,...C_Hn.3)$$
$$W=R(C_H1.4, C_H2.4,...C_Hn.4)$$

Fig. 52B

- 5250 A cryptographic value exchange protocol between at least two parties establishing at least two joint custody accounts.
- 5260 The cryptographic protocol establishing at least one digital signature, the digital signature sufficient to move value from at least one of the joint custody accounts to an account selectable by one of the parties, and the digital signature encrypted so that it can be decrypted once at least one joint custody account meets a pre-defined condition.
- 5270 The pre-defined condition including at least that a first of the joint custody accounts has a pre-defined value present during at least one of a pre-defined set of block heights and the signature to transfer from the second account to an account selectable by the first party.
- 5280 The pre-defined value storage condition including substantially zero value present in the first joint custody account during at least a pre-defined set of block heights and the transfer substantially refunding the second party from the second joint custody account.

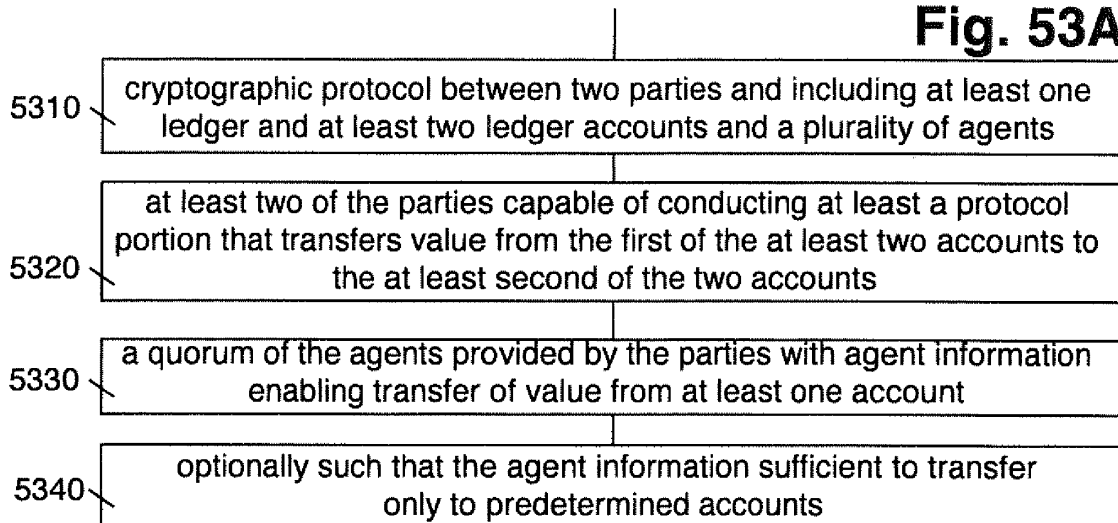
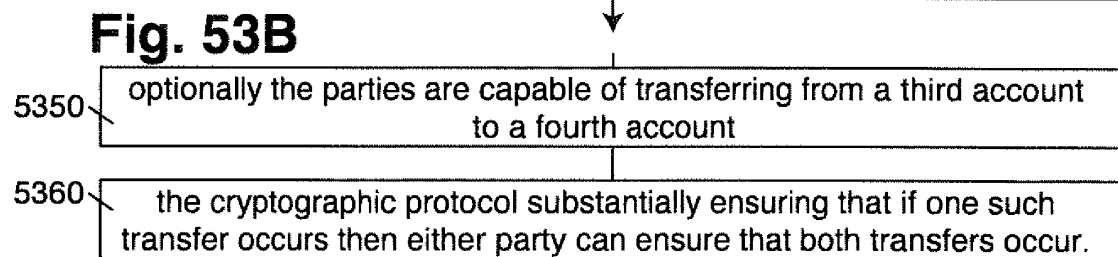
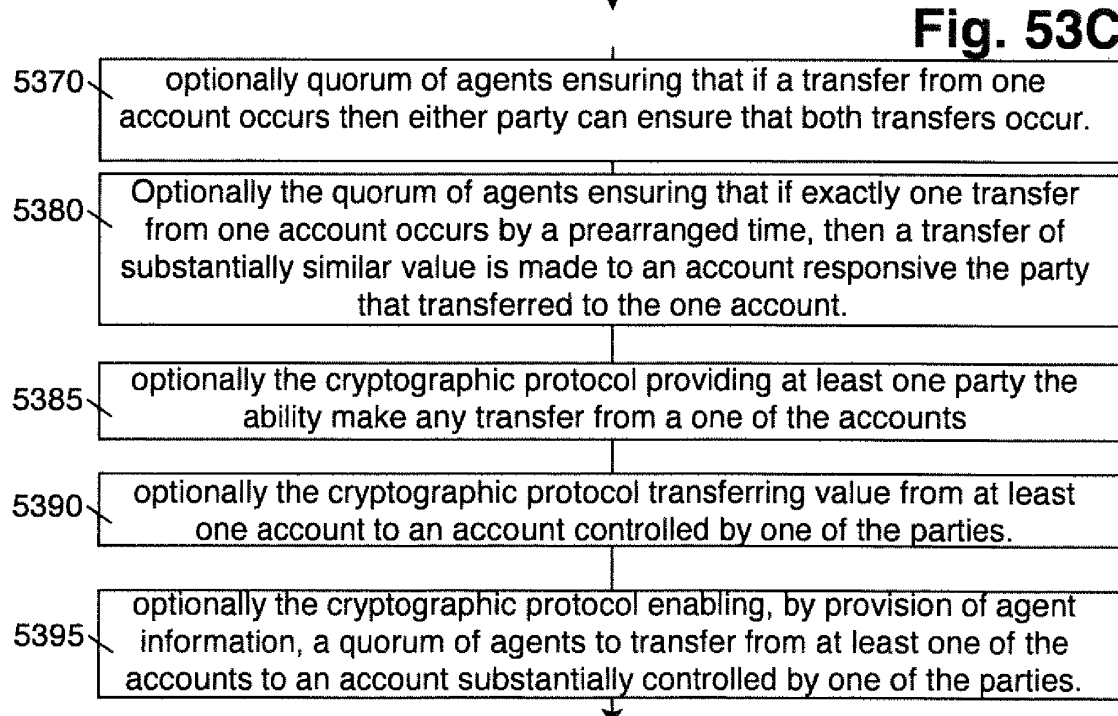
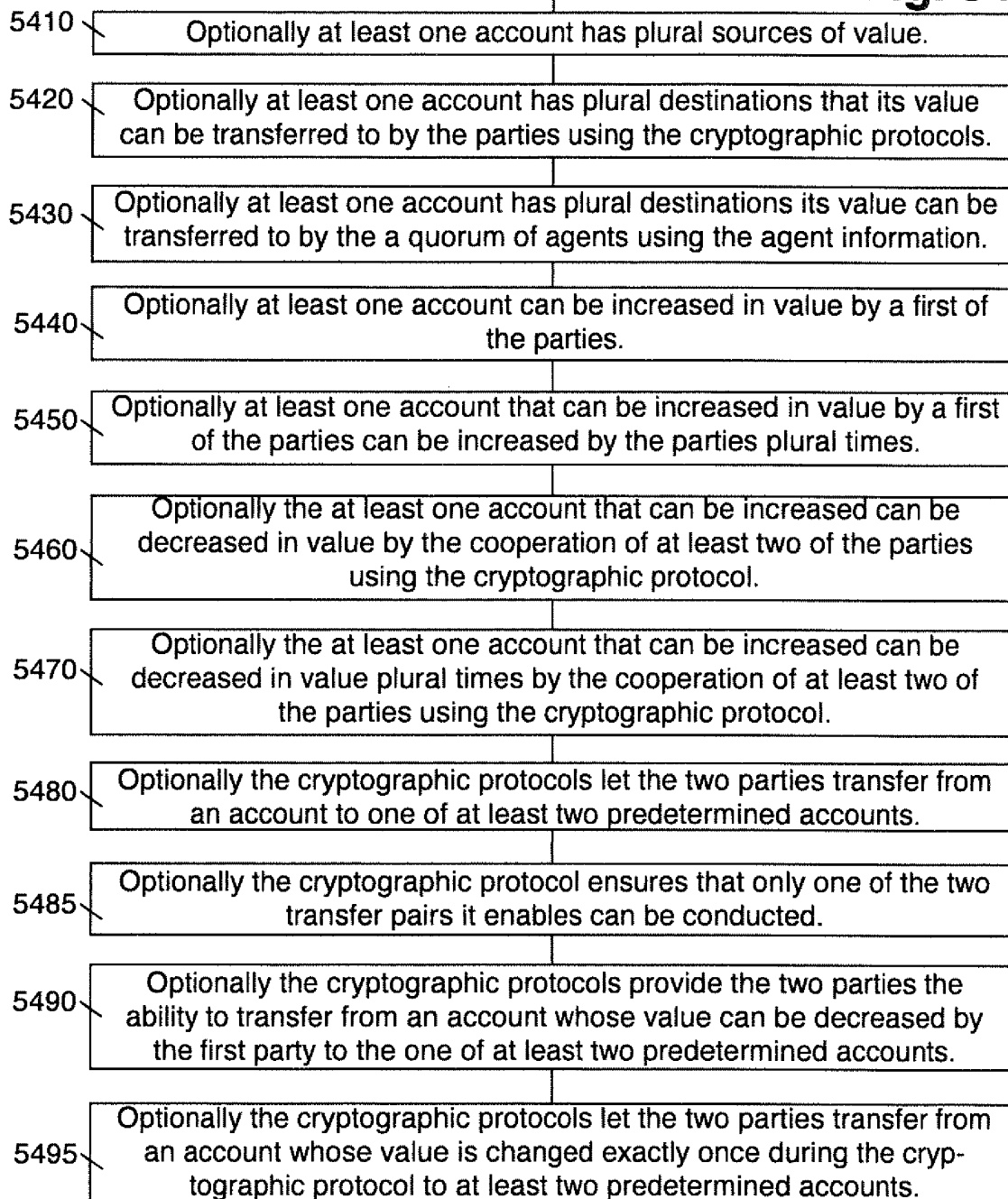
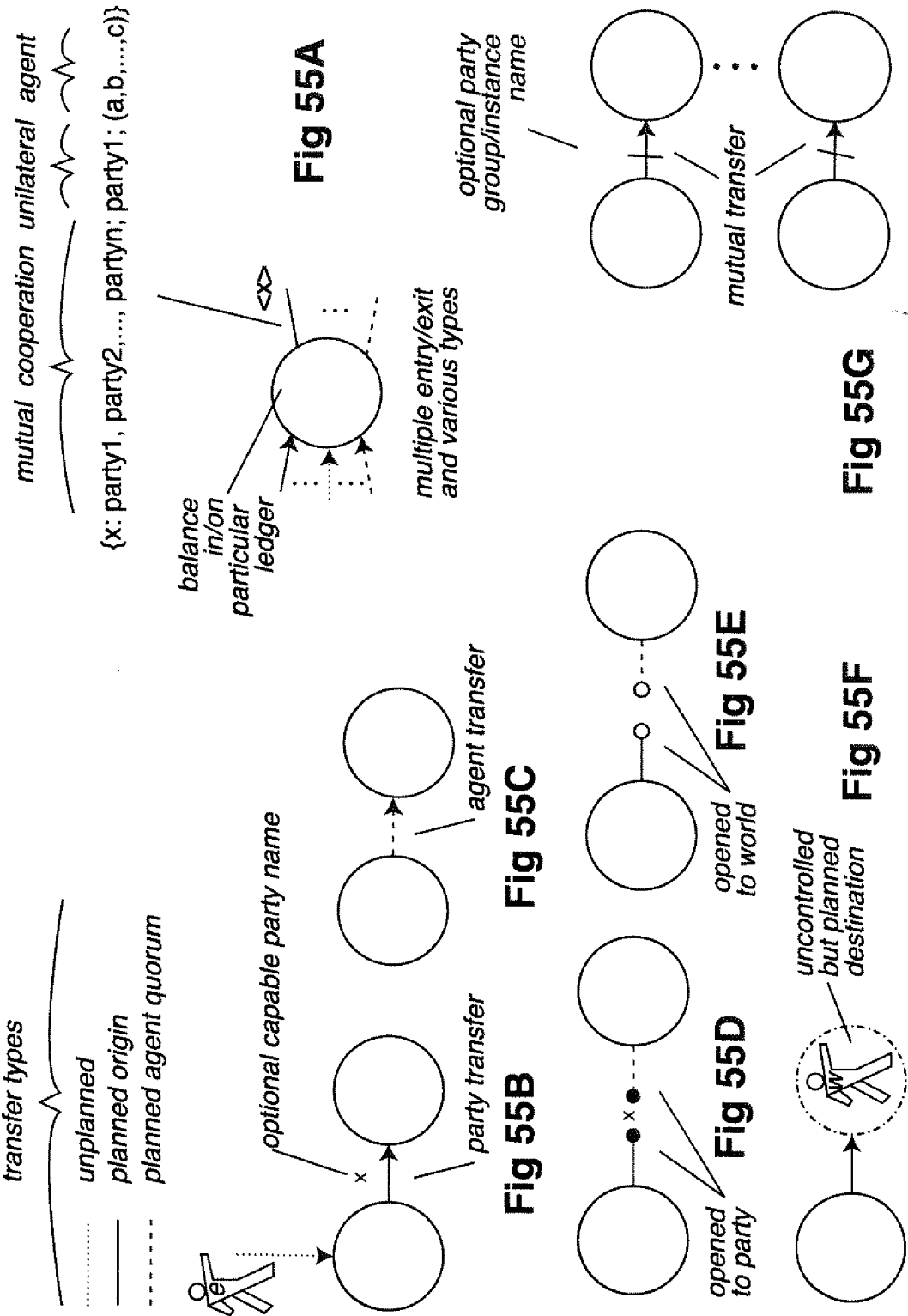
Fig. 53A**Fig. 53B****Fig. 53C**

Fig. 54



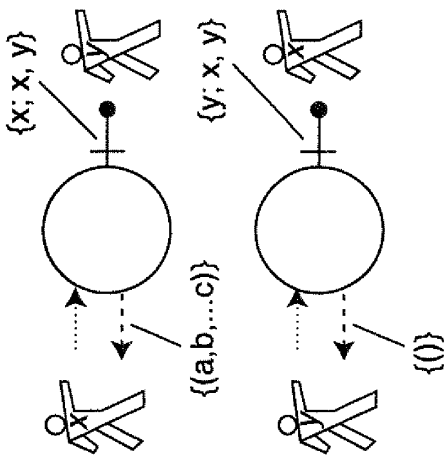


Fig 56A

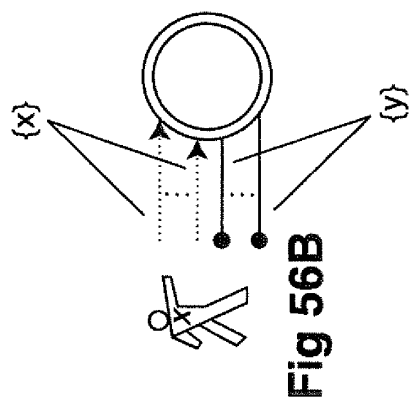


Fig 56B

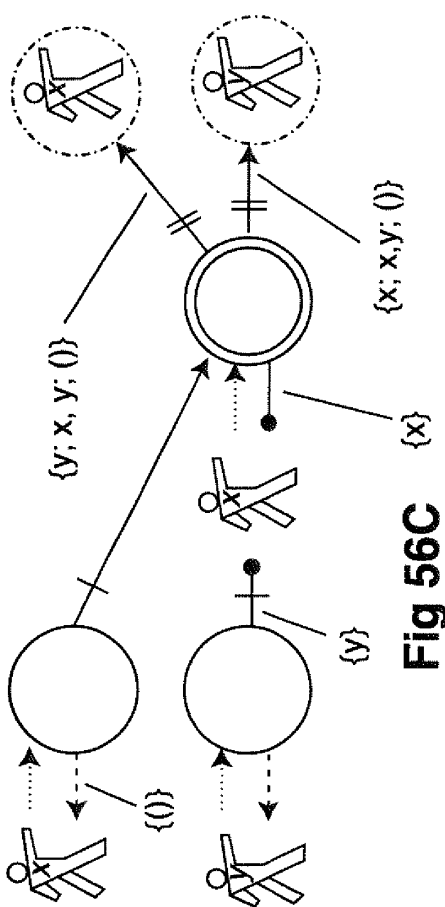


Fig 56C

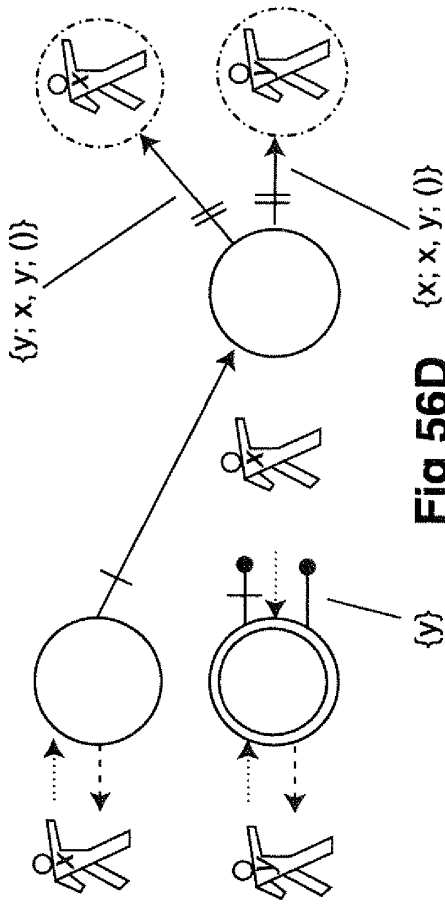


Fig 56D

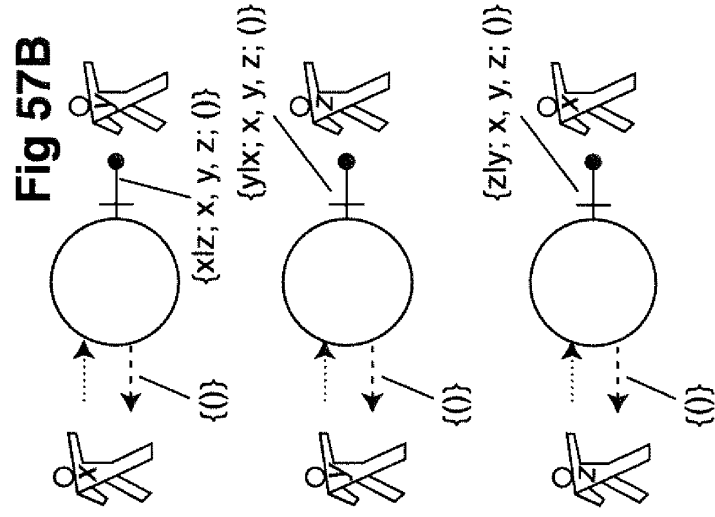
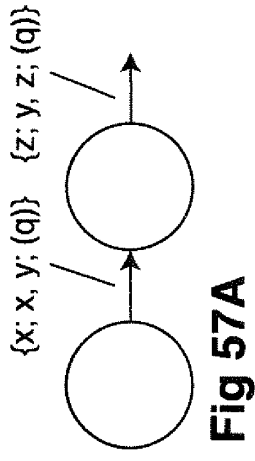
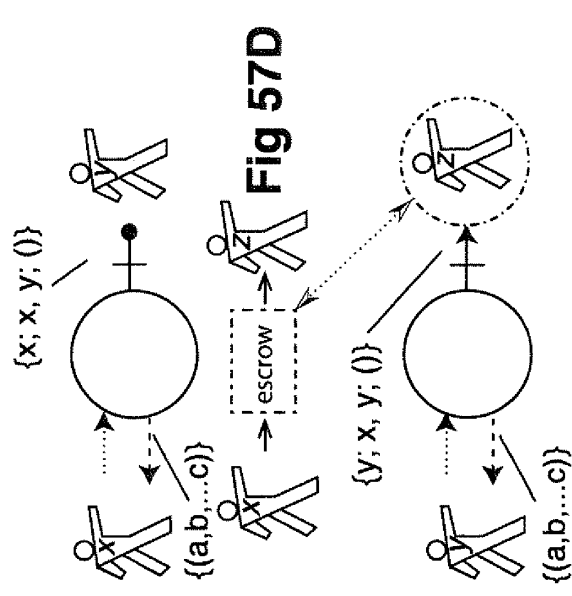
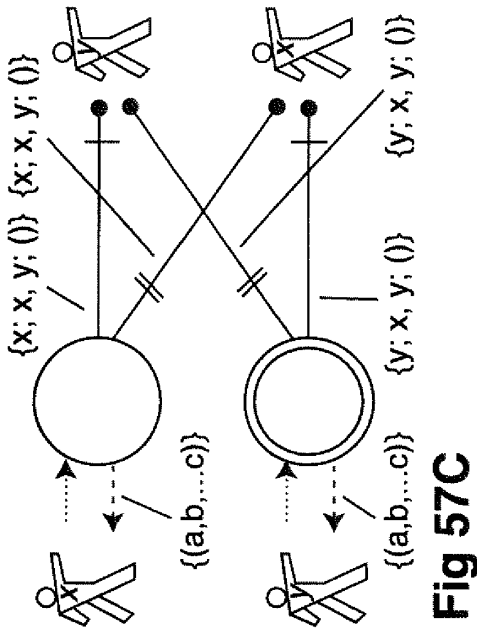


Fig. 58A

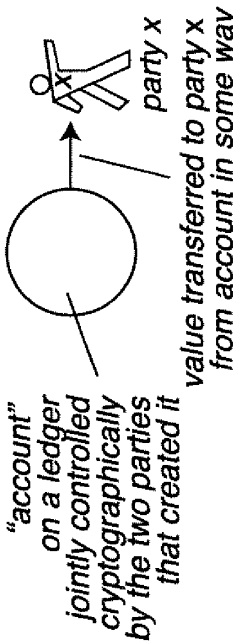


Fig. 58B

two parties jointly created both accounts on the same ledger

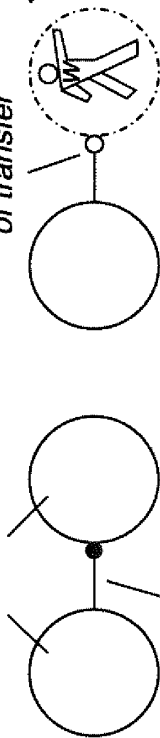


Fig. 58H

jointly-created signature to transfer between the two accounts

Fig. 58D

party x later given, by counterparty, control over jointly-created account

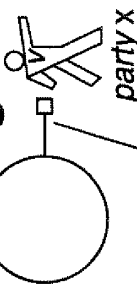


Fig. 58E

pre-arranged account created by whatever parties



Fig. 58F

joint account with multiple entry/exit

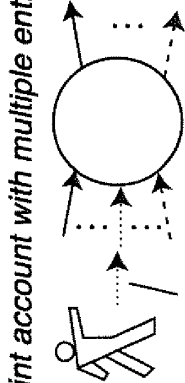


Fig. 58G

every quorum of agents overlaps

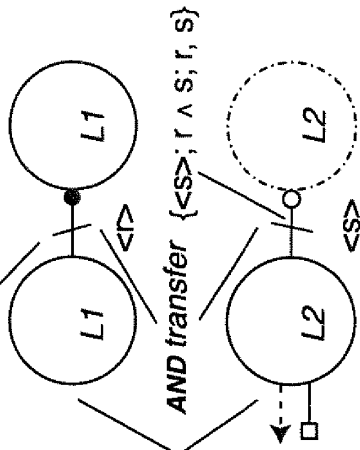


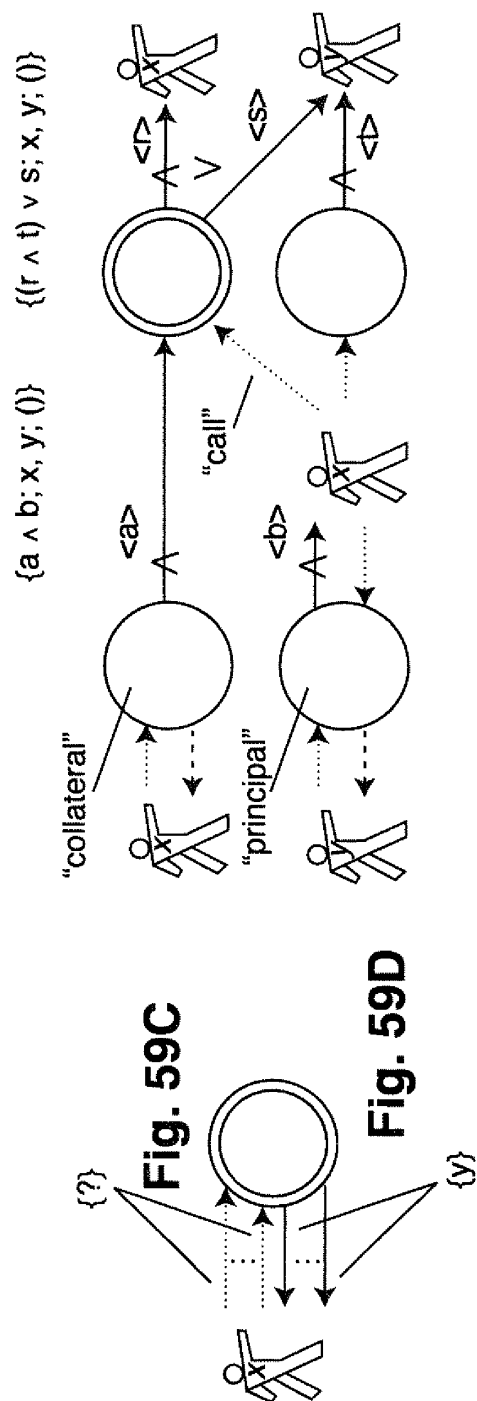
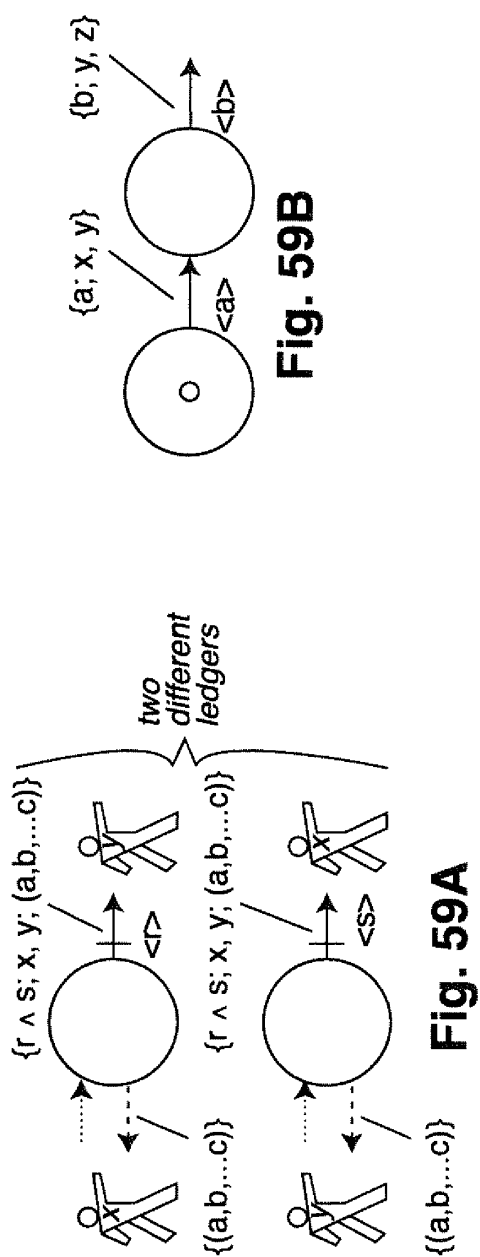
line rule mutual cooperation quorum transfer name formula of the parties listed of agents type

{<n>; line • line...; party1, party2,...; (a,b,...,c); >O●□◀}

Fig. 58I

accounts on two ledgers, L1 and L2





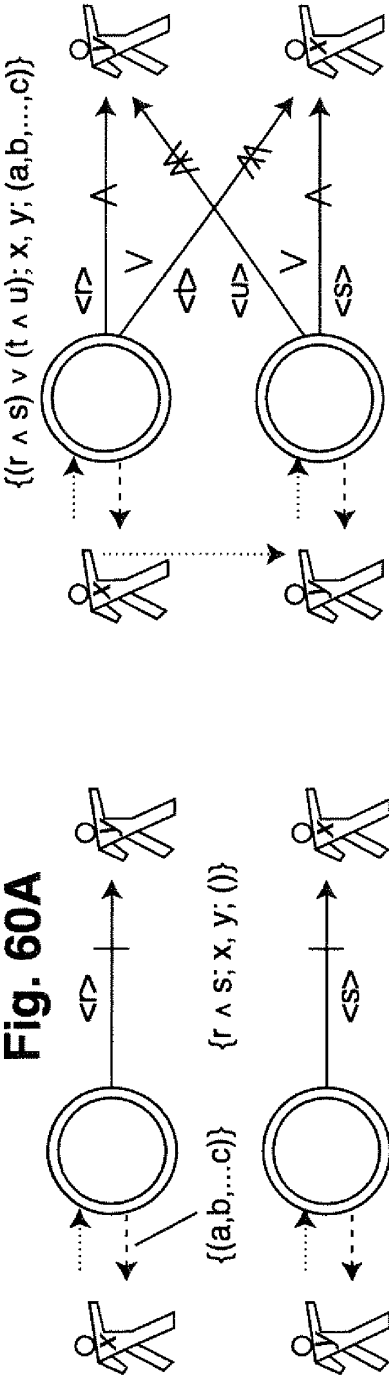


Fig. 60B

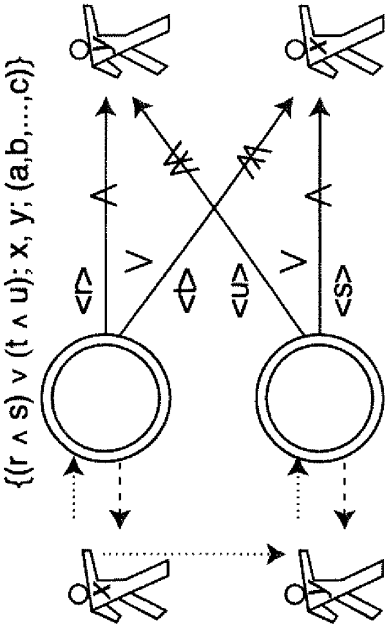


Fig. 60C

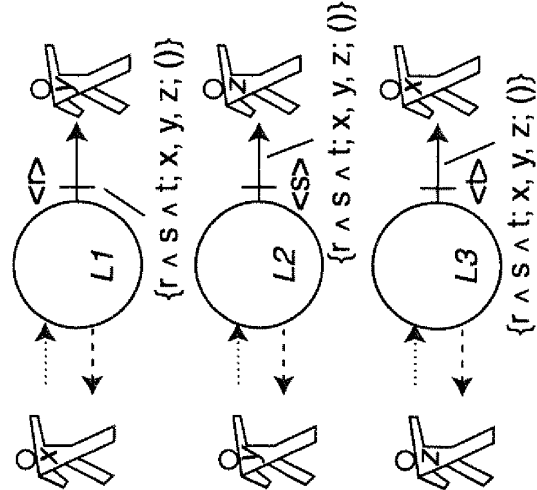


Fig. 60D

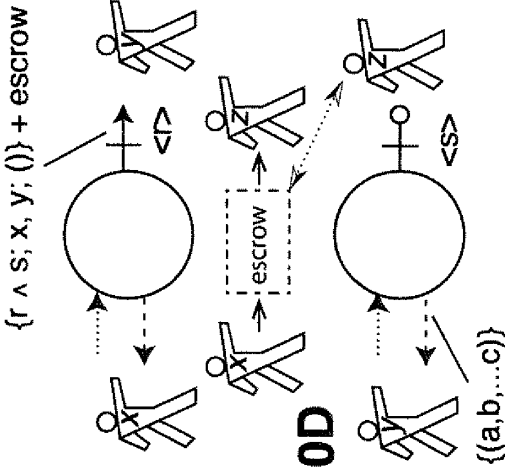


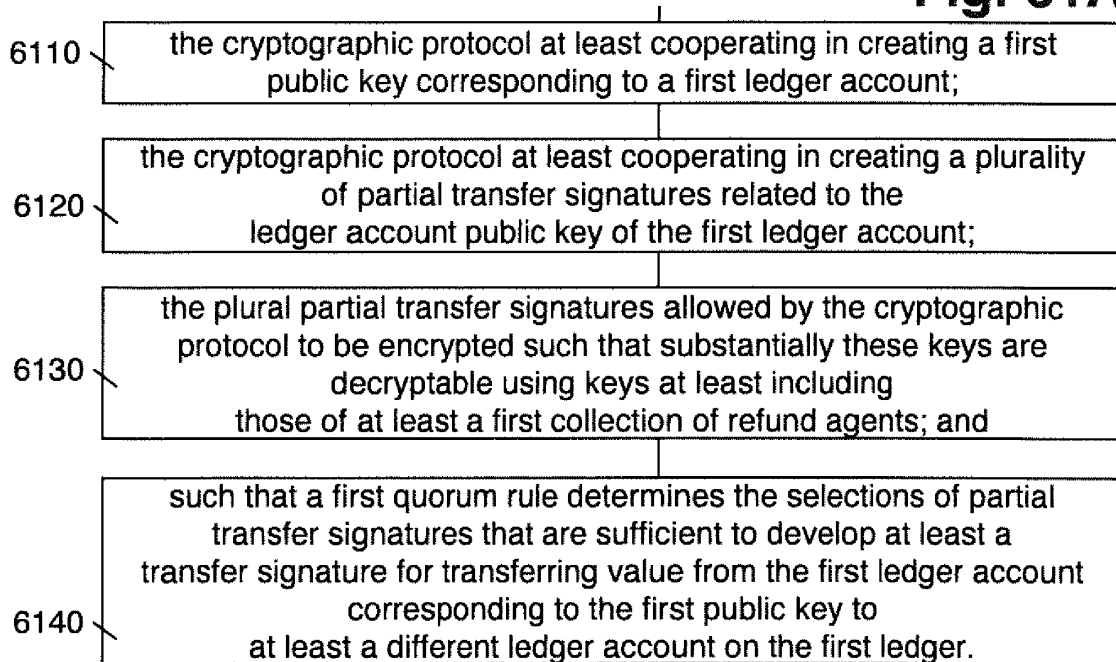
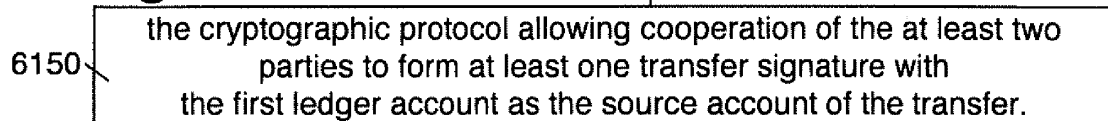
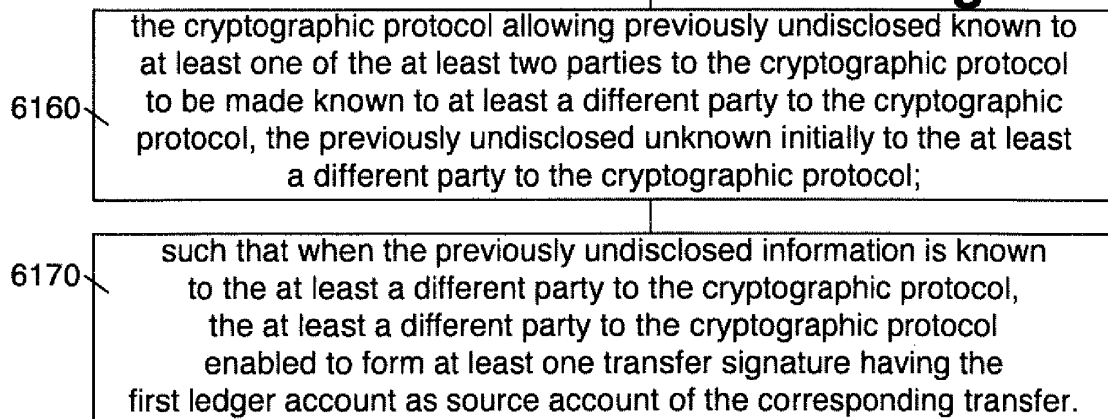
Fig. 61A**Fig. 61B****Fig. 61C**

Fig. 62A

6210 such that the first destination account of the first transfer signature at least in part selectable by at least one of the at least two parties.

Fig. 62B

6220 such that the first destination account of the first transfer signature selected at least in part by the cryptographic protocol and outside the control of either one of the at least two parties.

Fig. 62C

6230 the cryptographic protocol allowing at least two of the parties to cooperate in creating a public key corresponding to a second ledger account.

Fig. 62D

6240 the cryptographic protocol at least cooperating in creating a second plurality of partial transfer signatures related to at least a public key of the second ledger account;

6250 the second plural partial transfer signatures allowed by the cryptographic protocol to be encrypted such that substantially these keys can be decrypted at least in part by refund agents using keys at least including those of a second collection of refund agents; and

6260 such that a second quorum rule determines the selections of the second partial transfer signatures that are sufficient to develop at least a transfer signature for transfer from the second ledger account to at least a ledger account different from the first ledger account and different from the second ledger account.

Fig. 62E

6270 such that the combination of the first quorum rule and the second quorum rule ensuring a predetermined minimum number of refund agents in the intersection of substantially any quorum allowed simultaneously by the first quorum rule and any quorum allowed by the second quorum rule.

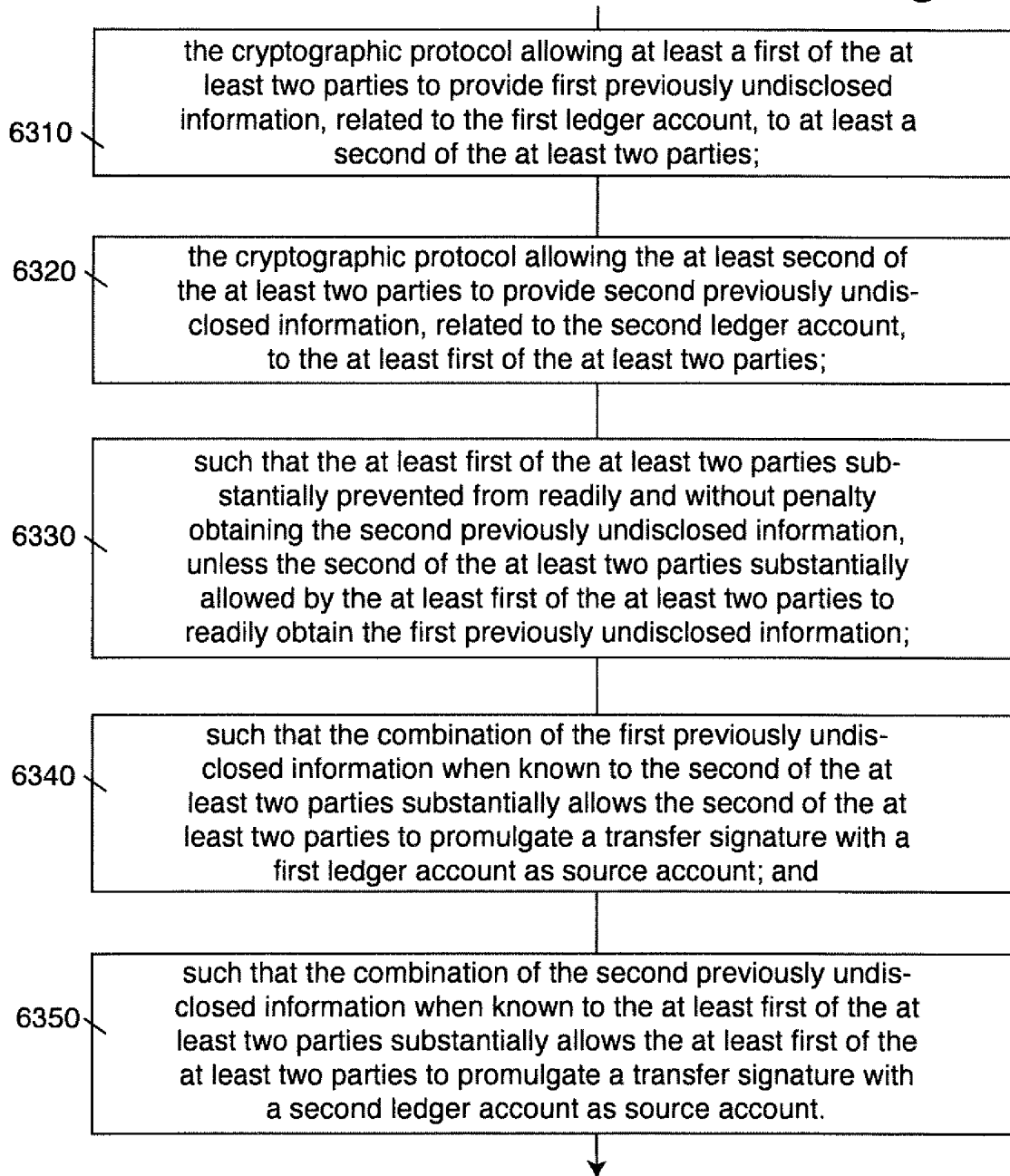
Fig. 63

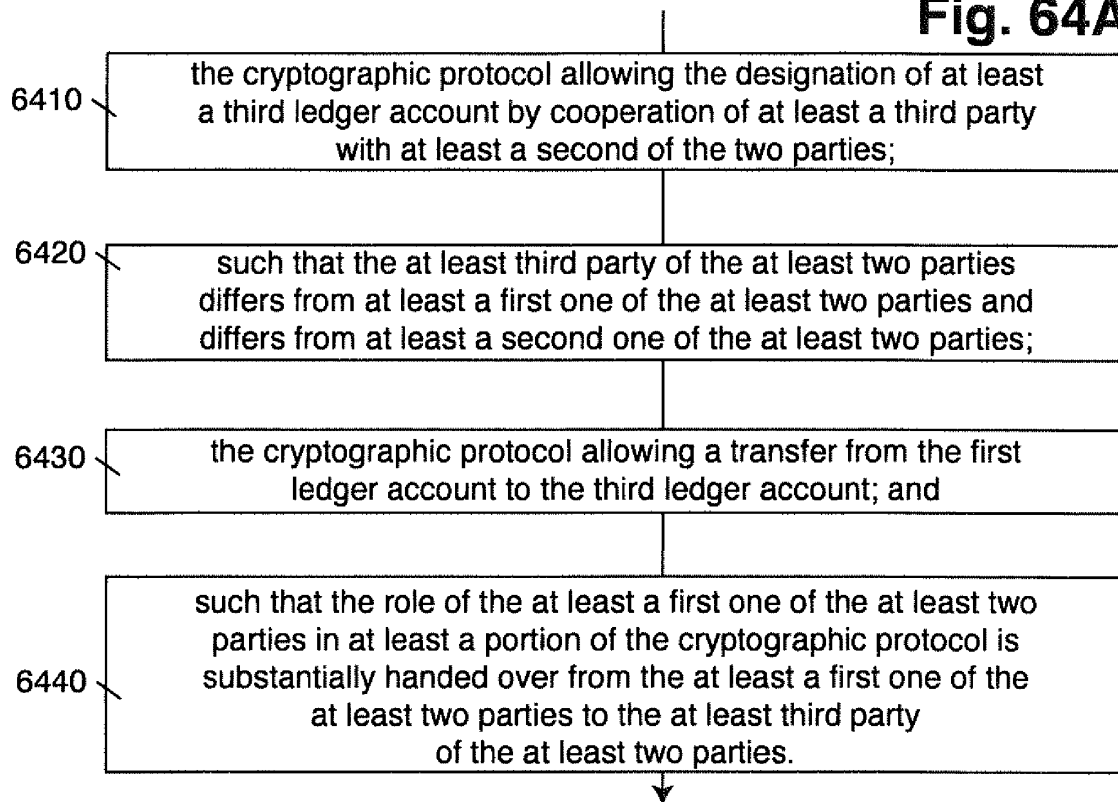
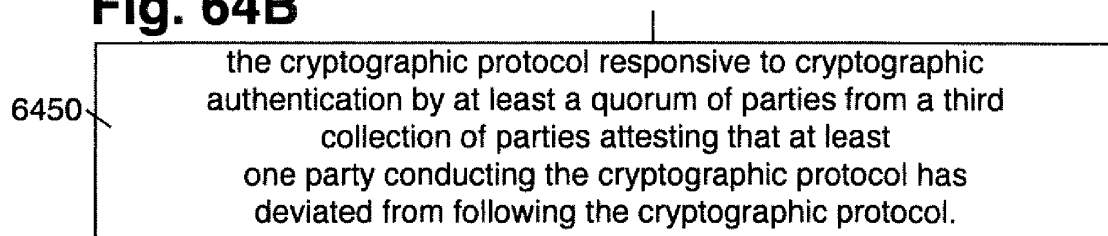
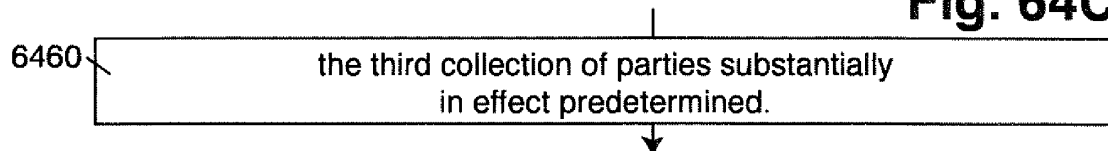
Fig. 64A**Fig. 64B****Fig. 64C**

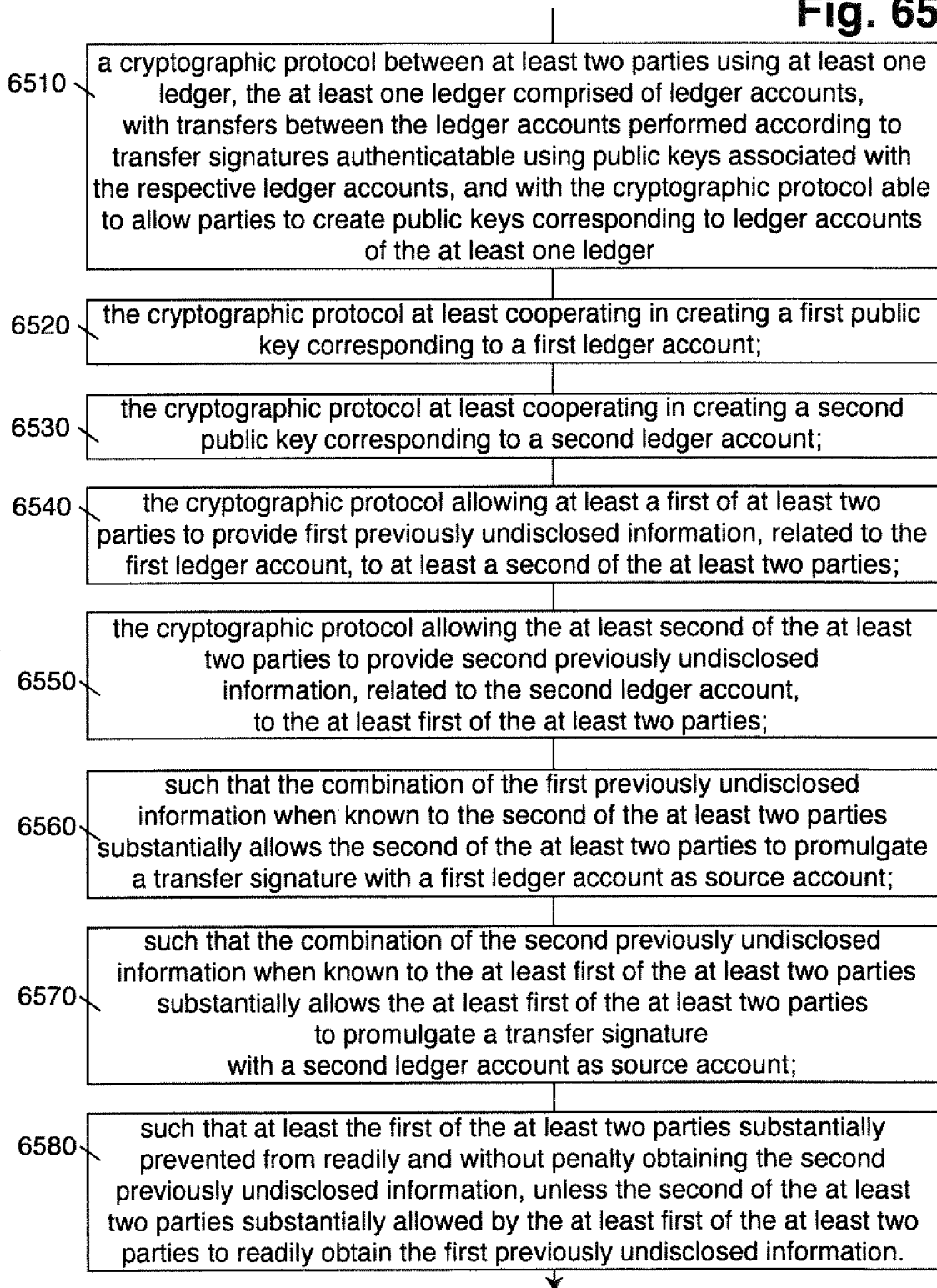
Fig. 65

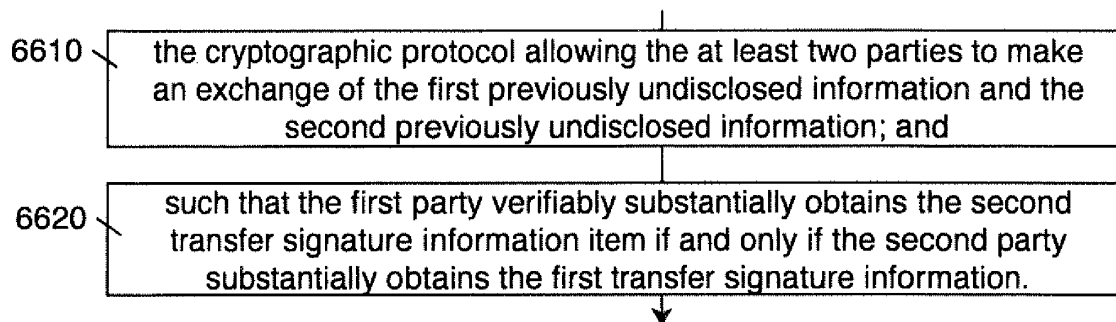
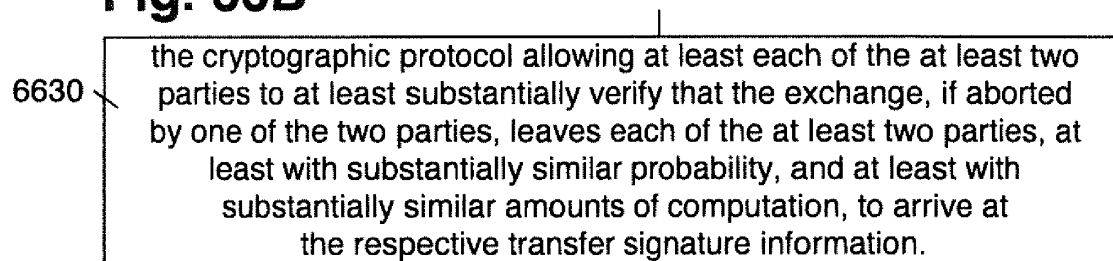
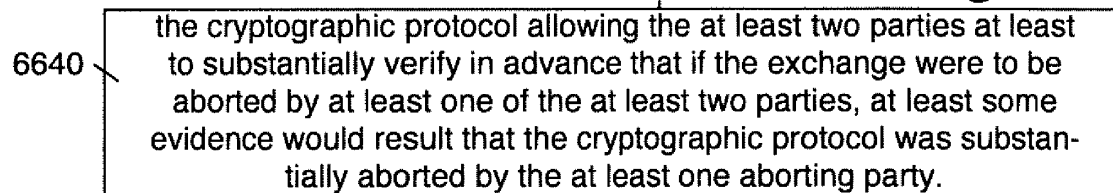
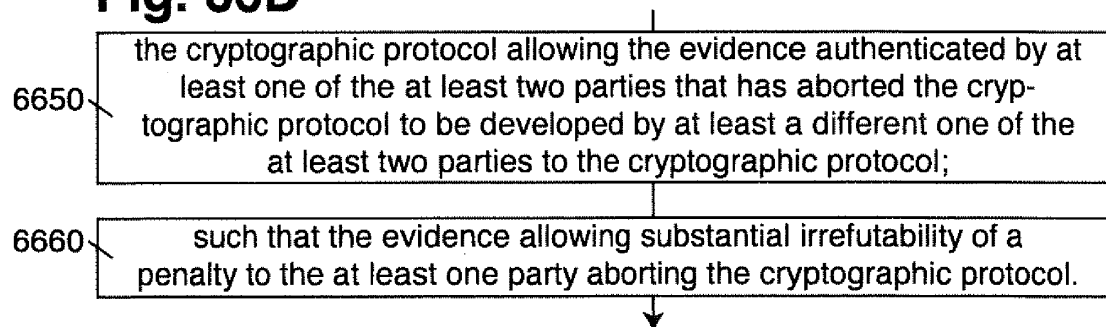
Fig. 66A**Fig. 66B****Fig. 66C****Fig. 66D**

Fig. 67