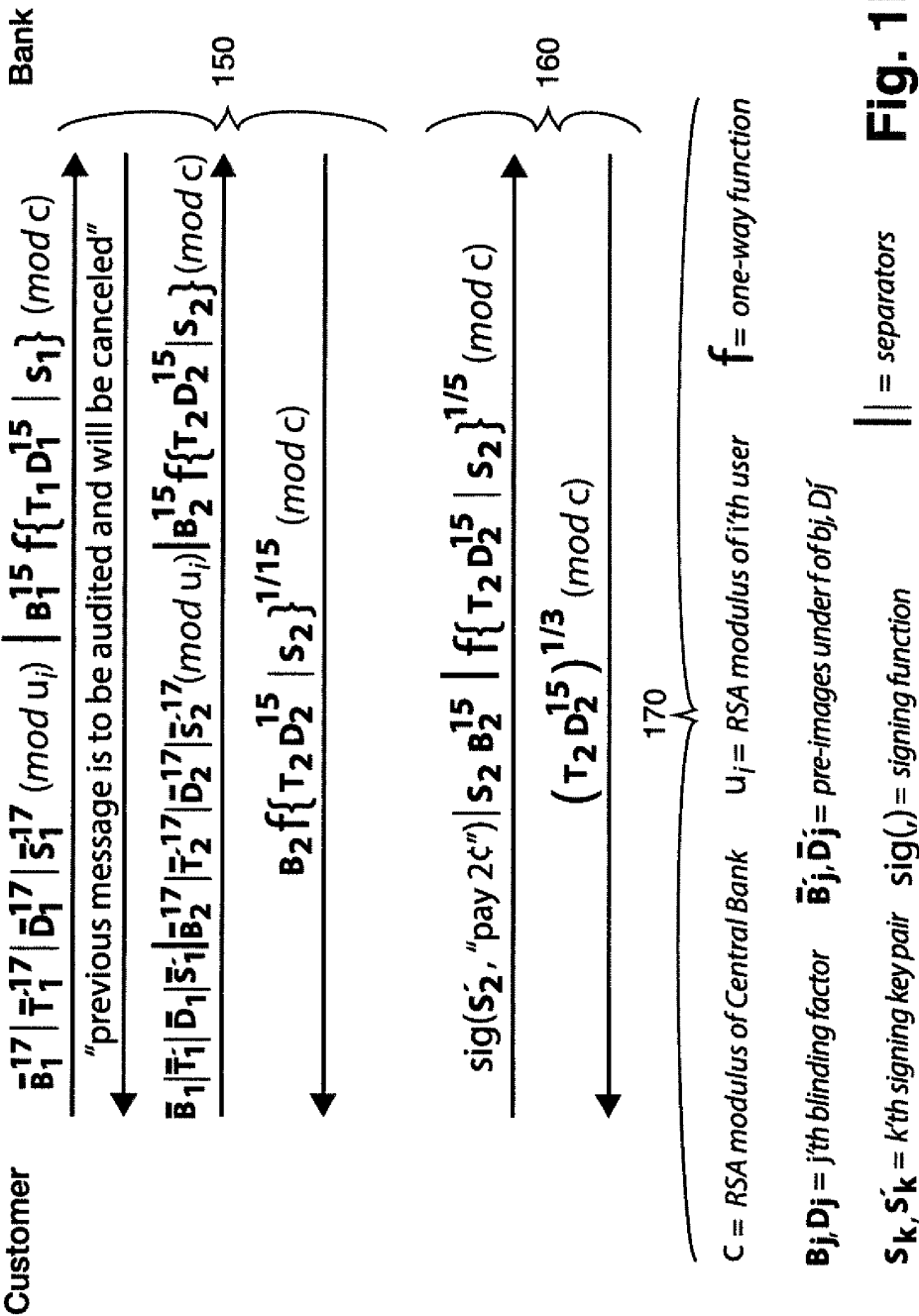




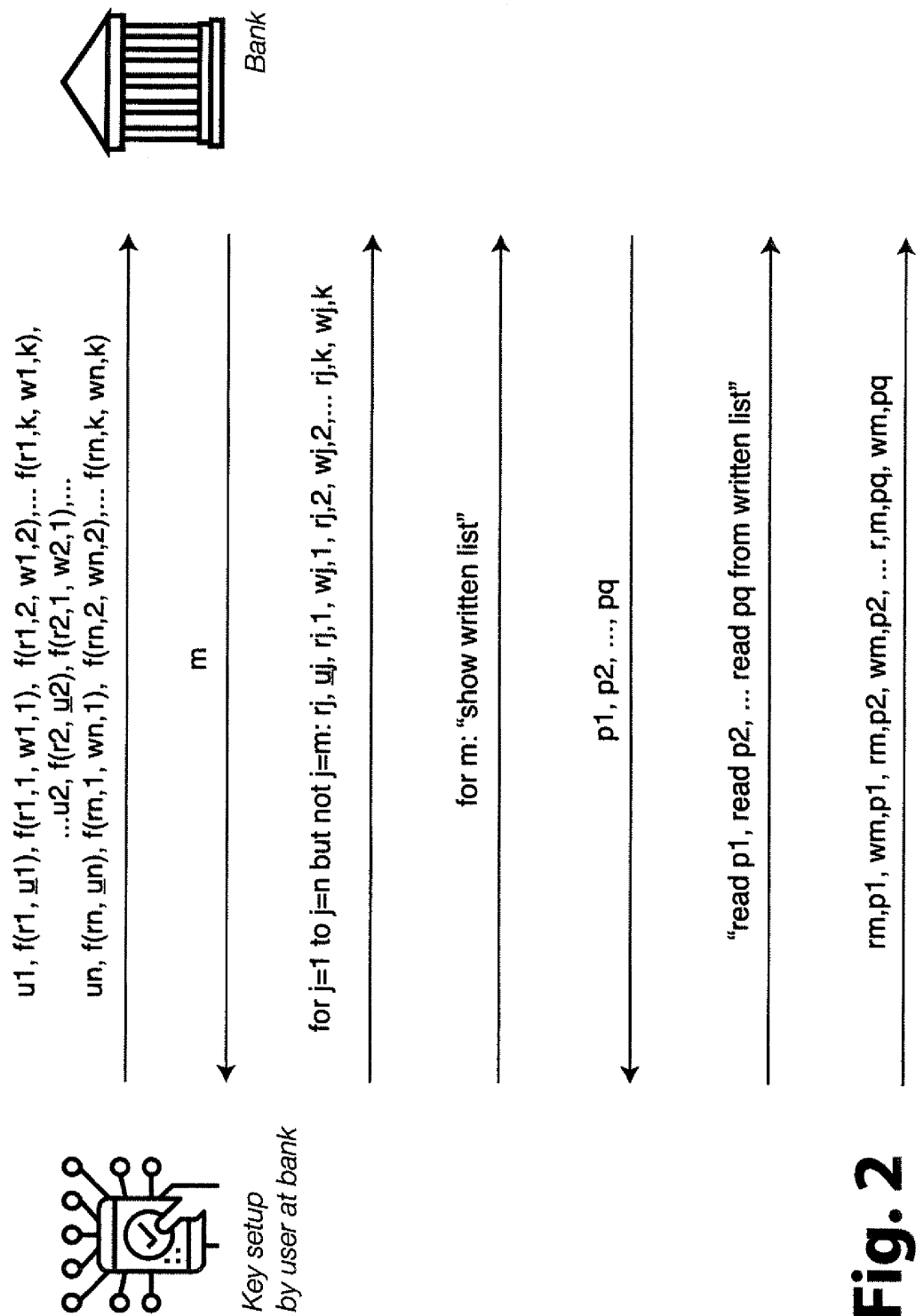
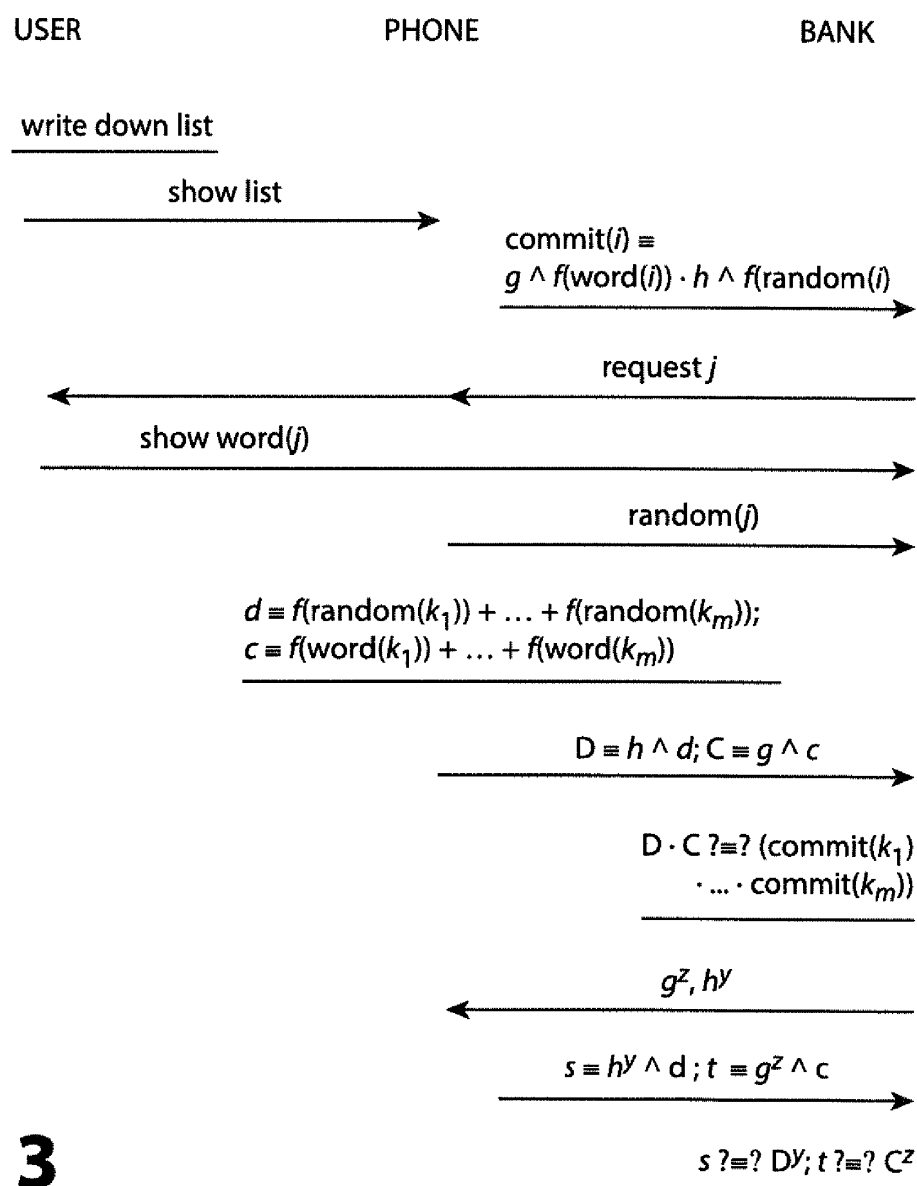


Fig. 2

**Fig 3**

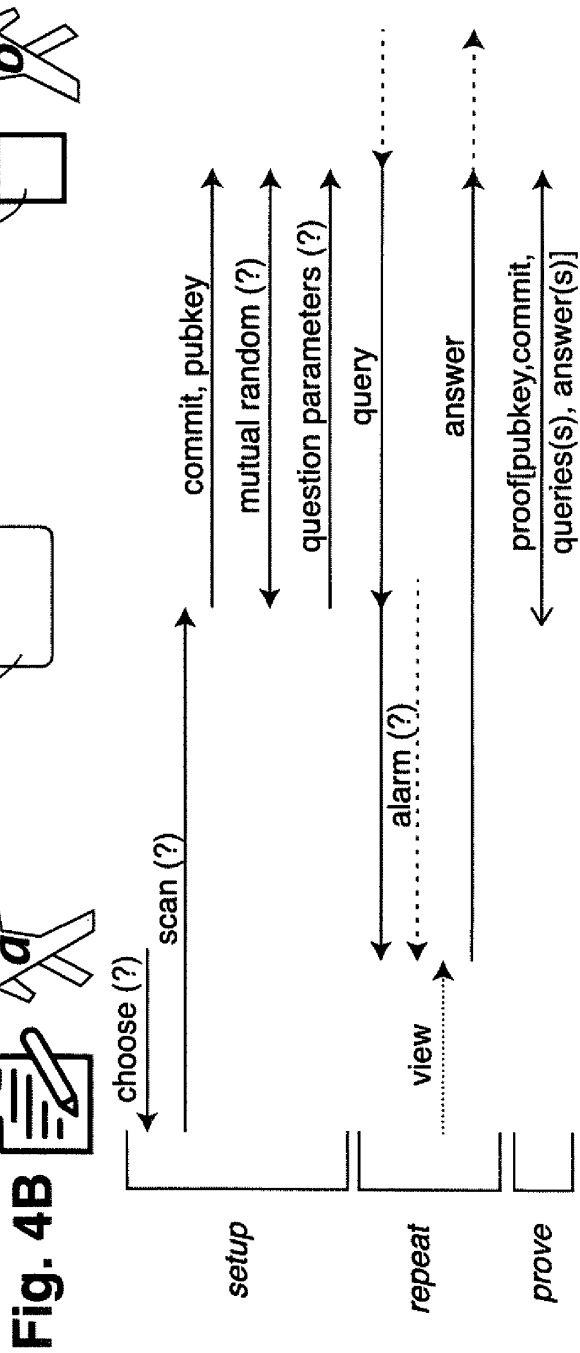
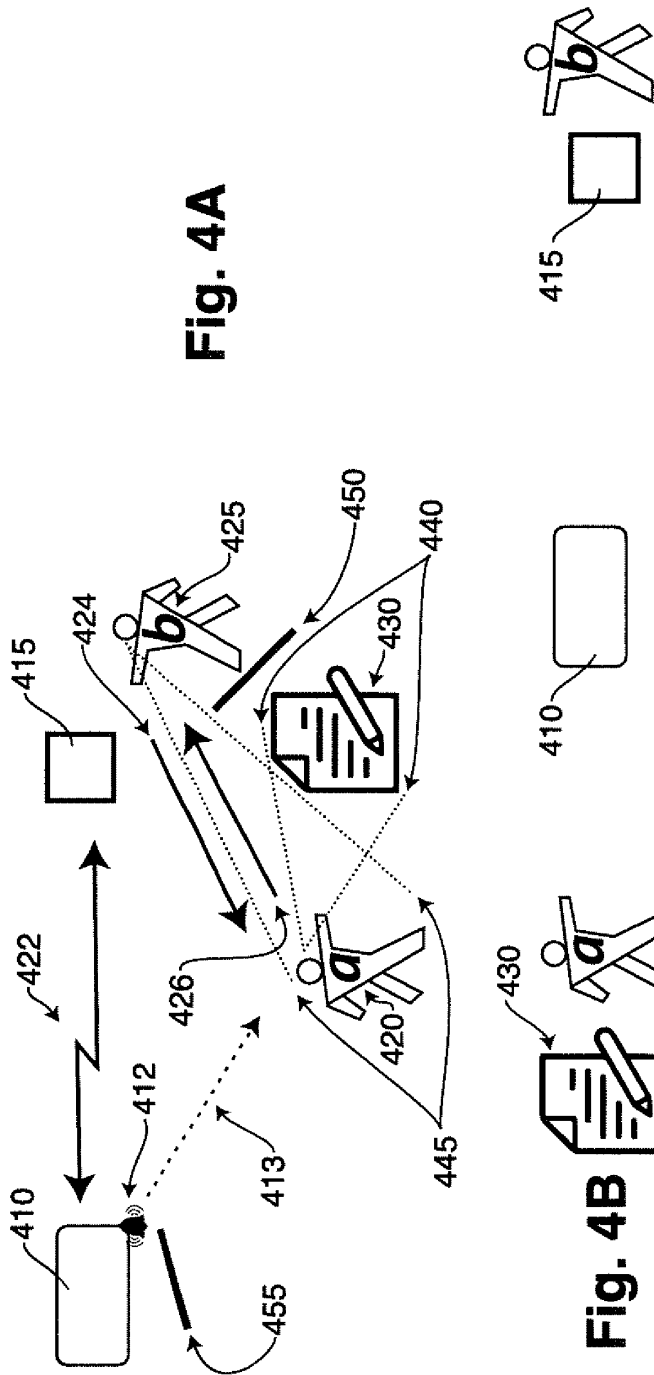


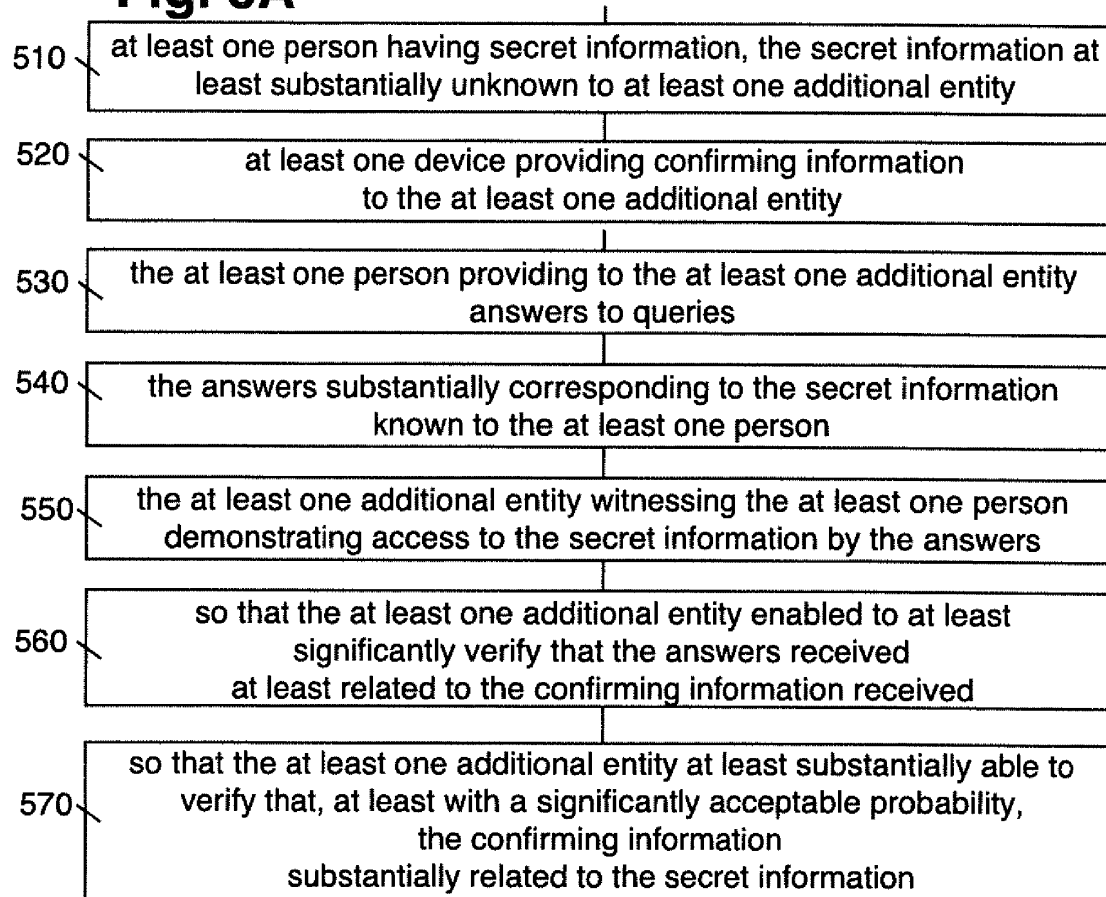
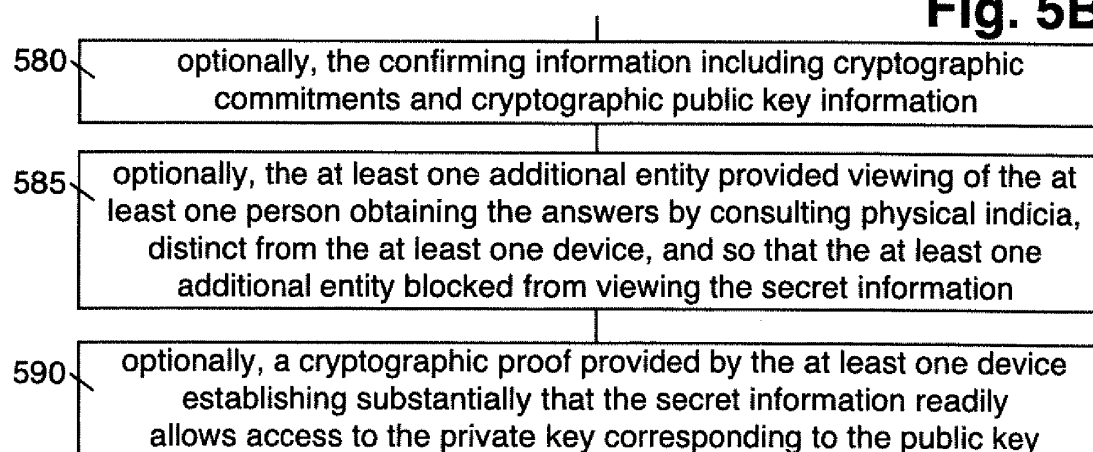
Fig. 5A**Fig. 5B**

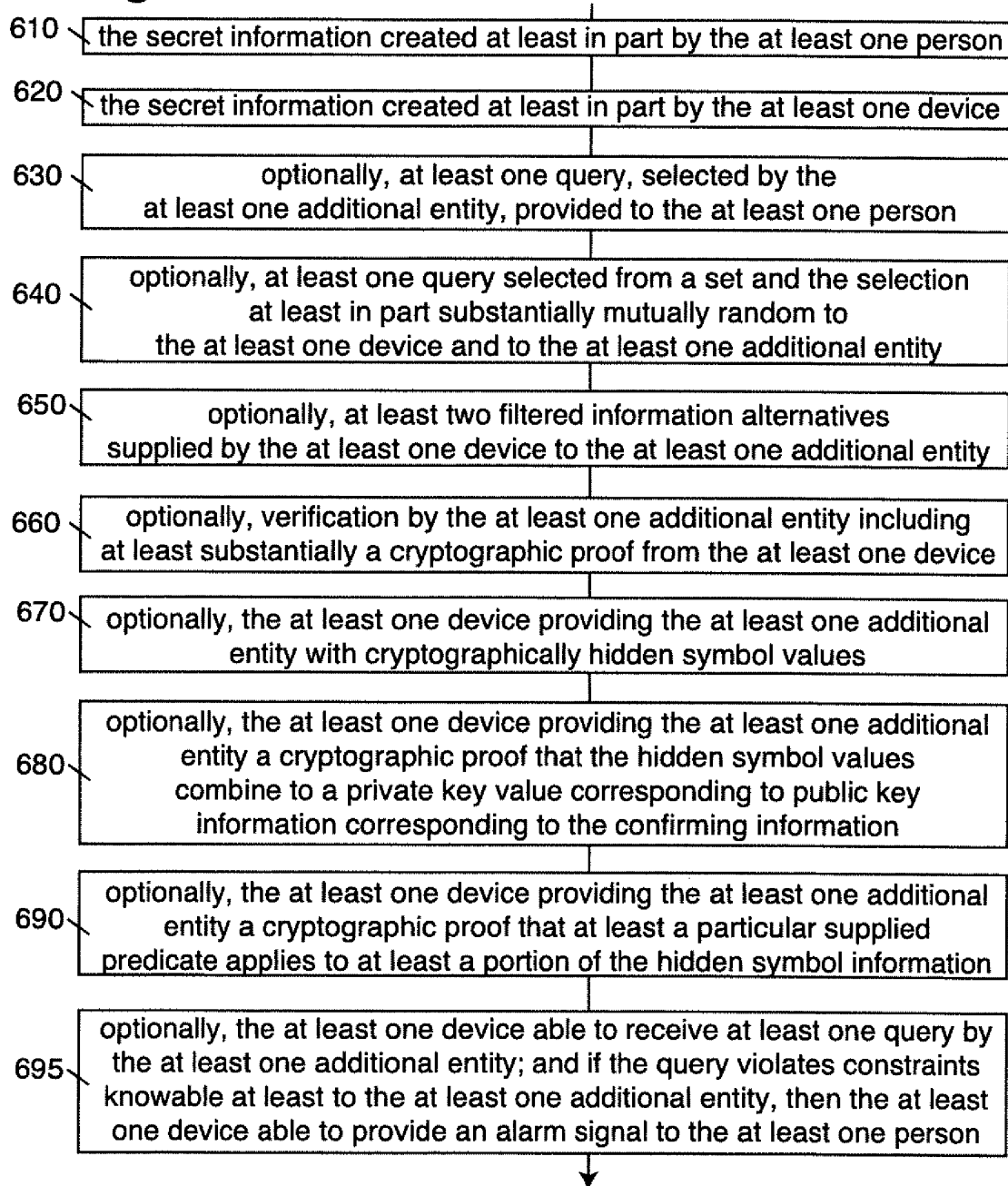
Fig. 6

Fig. 7

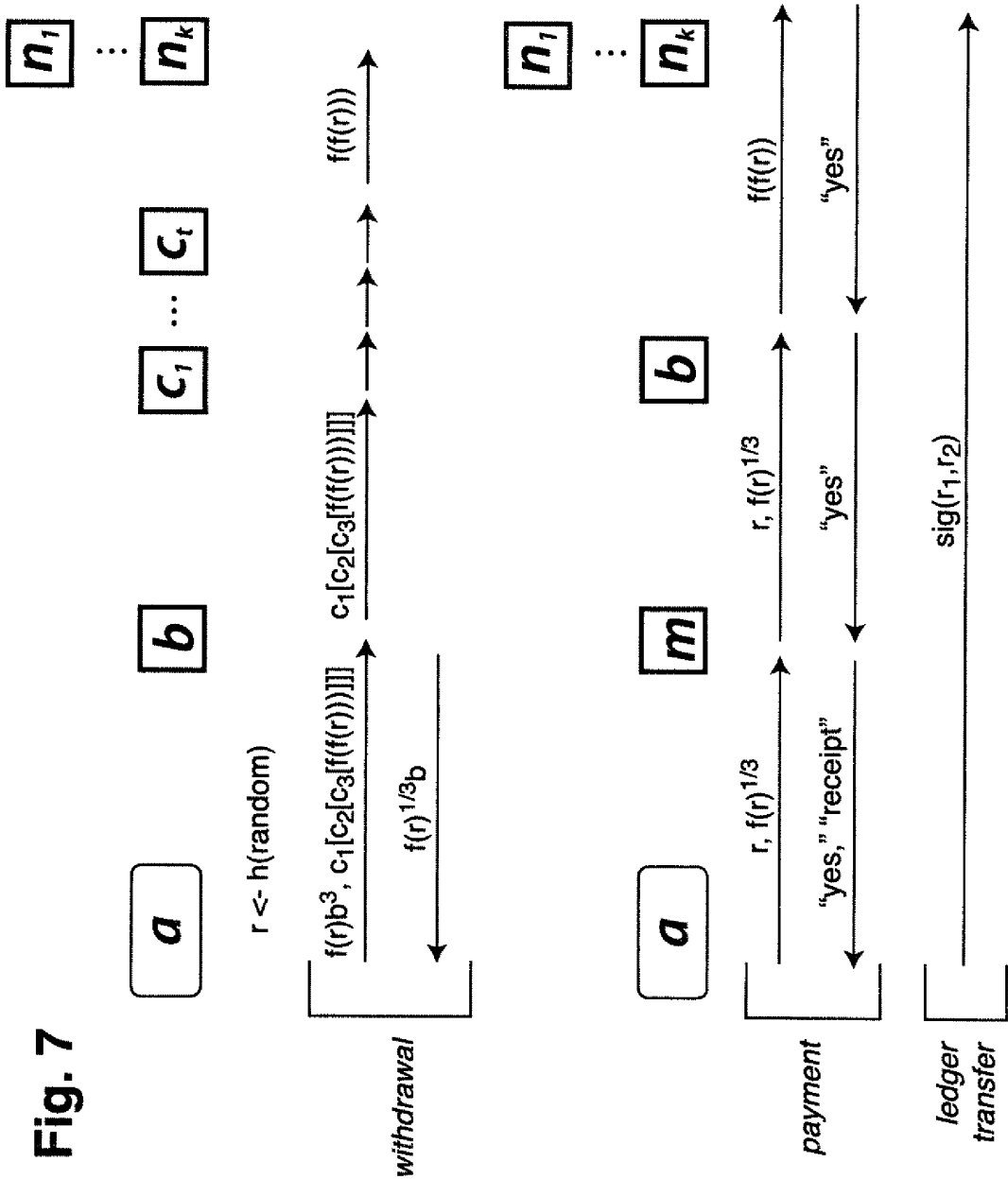
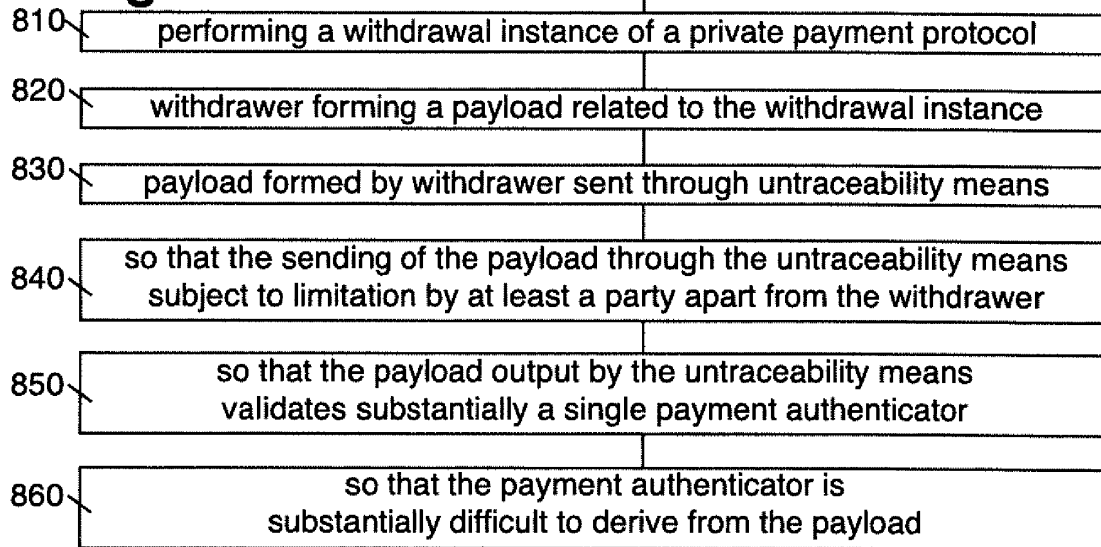
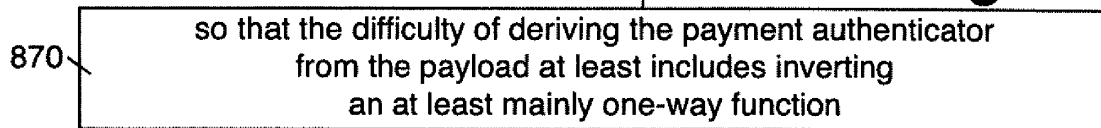
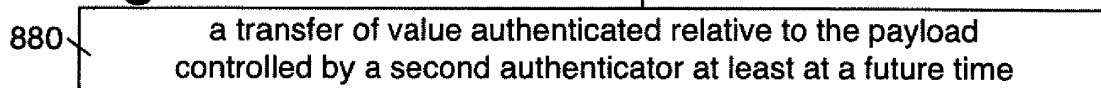
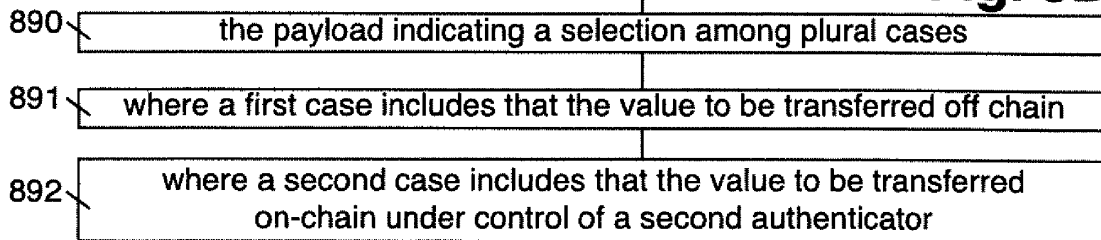
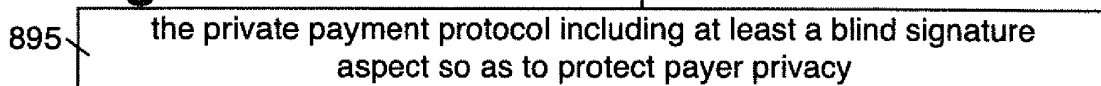
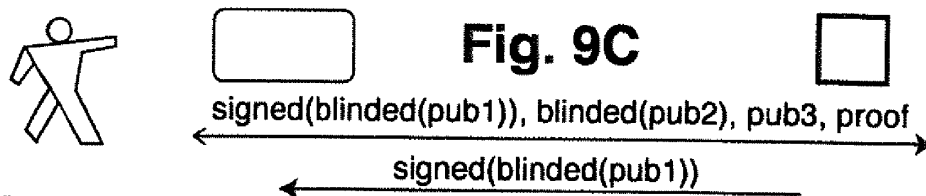
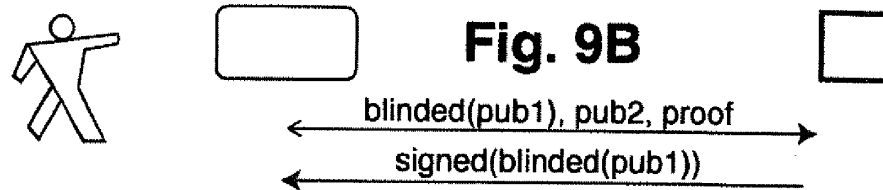
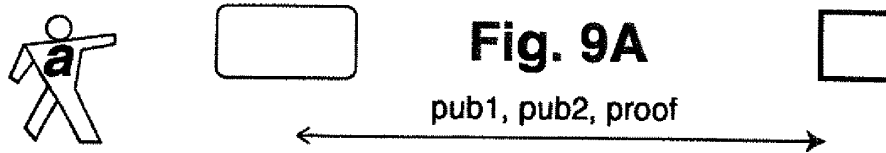
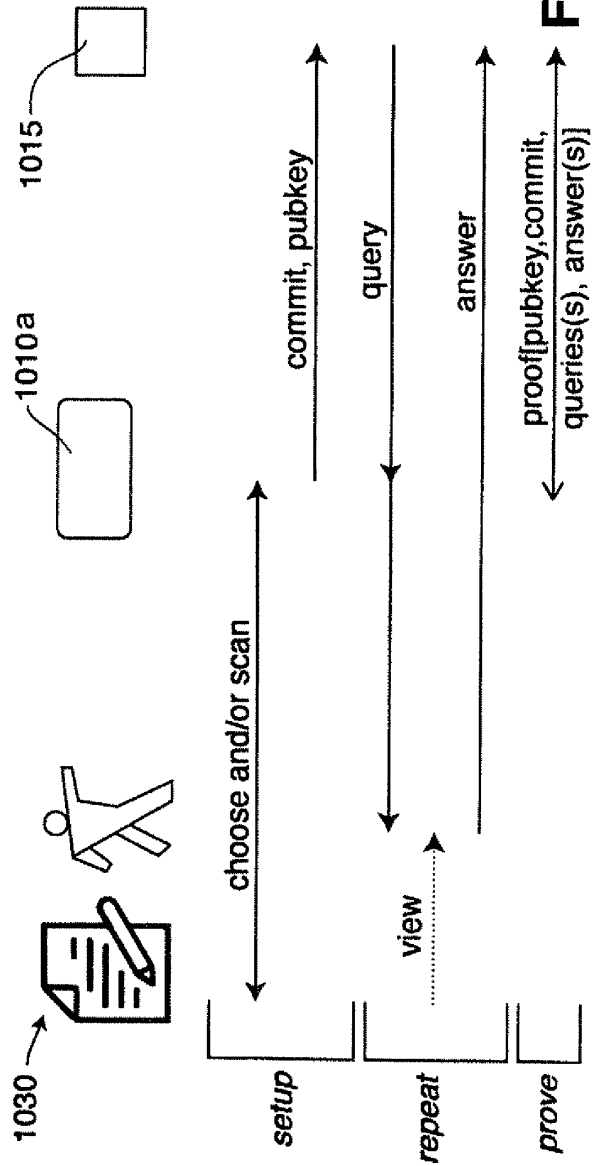
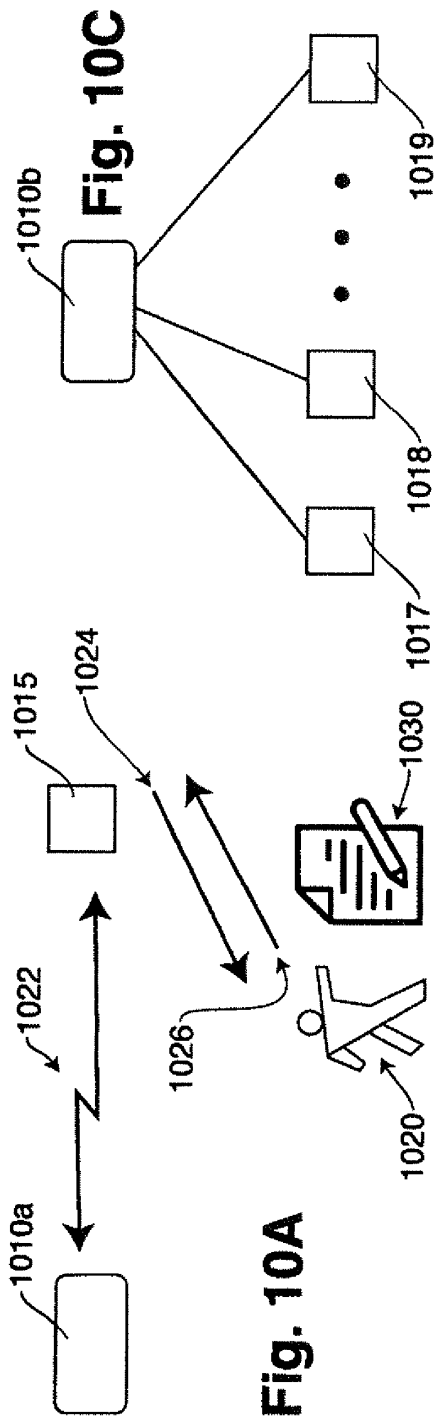


Fig. 8A**Fig. 8B****Fig. 8C****Fig. 8D****Fig. 8E**

**Fig. 9D**

- 950 a first party providing proof that a private key corresponding to a first provided public key is at least substantially readily computable from the private key corresponding to a second provided public key
- 960 a first party providing proof that a private key corresponding to a first provided blinded public key is at least substantially readily computable from the private key corresponding to a second provided public key
- 970 optionally returning by a second party to the first party a signature on the blinded first public key received by the second party
- 980 a first party providing proof that a private key corresponding to a first provided signed blinded public key is at least substantially readily computable from the private key corresponding to a second provided blinded public key and at least substantially readily computable from a third provided public key
- 990 optionally returning by a second party to the first party a signature on the blinded first public key received by the second part



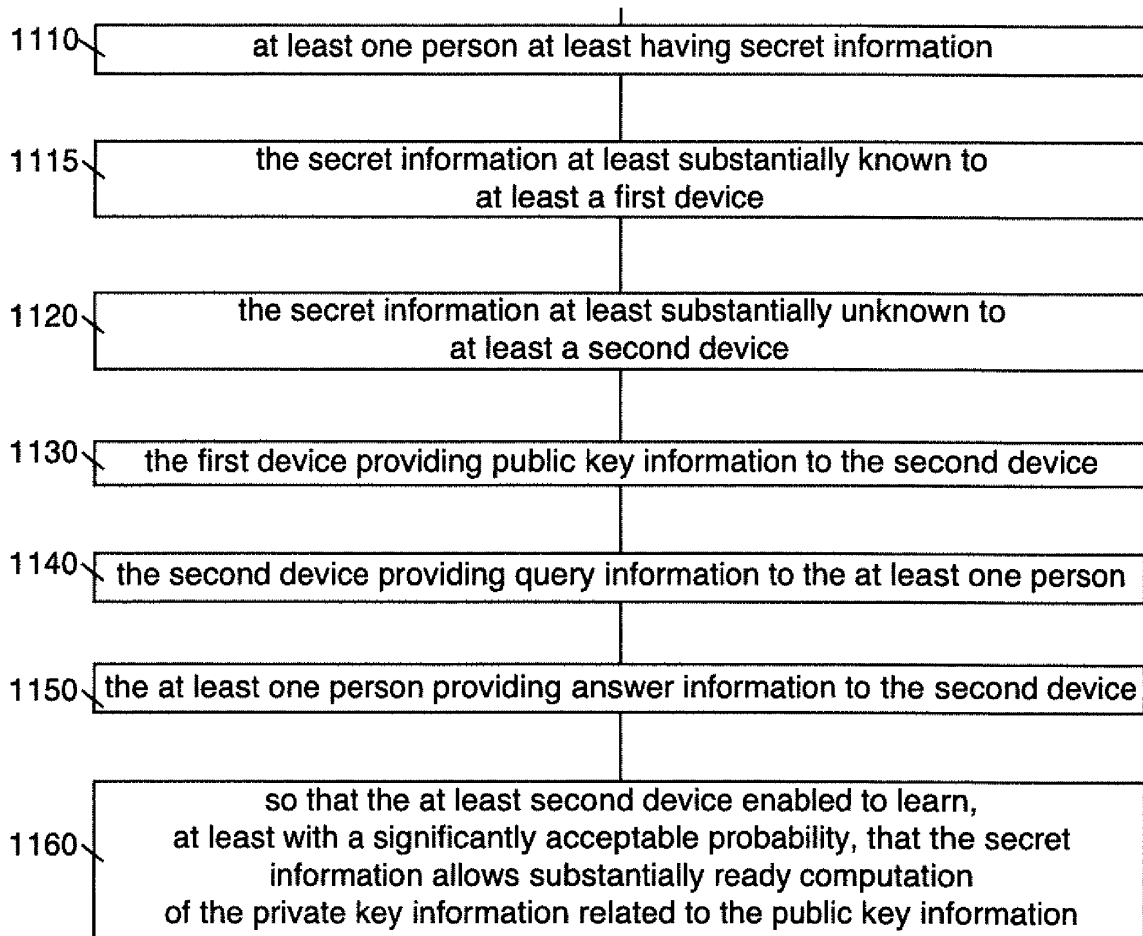
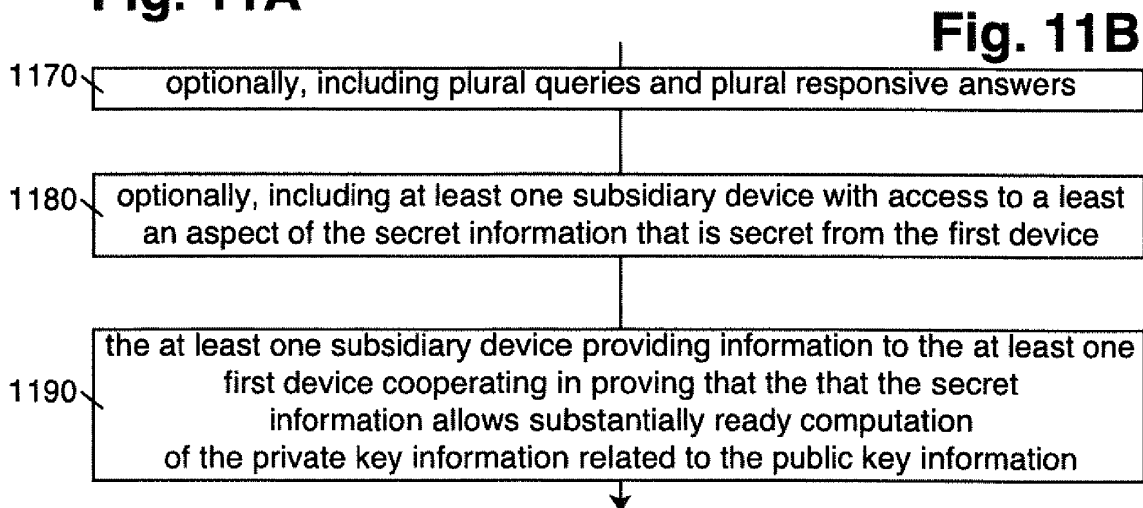
**Fig. 11A**

Fig. 12A *the s_i are well formed*

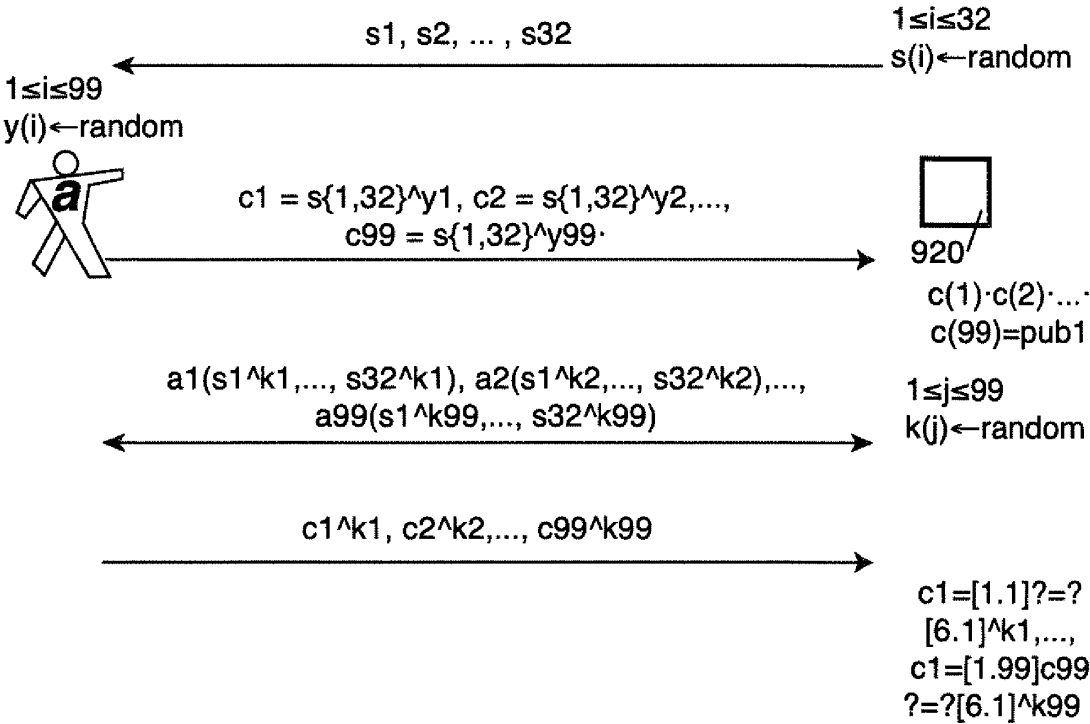
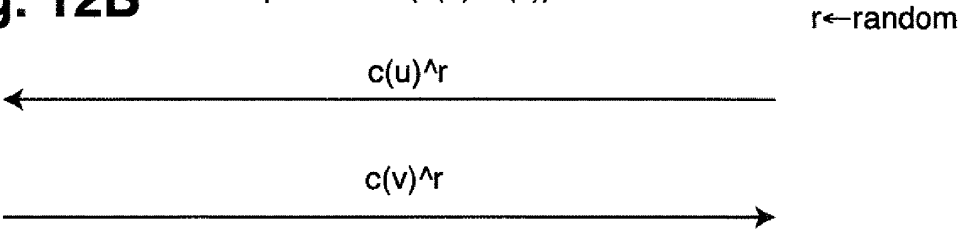


Fig. 12B *a proof that $(c(u)=c(v))$*



The passphrase is $s(1), \dots, s(100)$, each $s(j)$ from the same 32 fixed symbols. There are 32×100 distinct fixed public generators, $c(i,j), 1 \leq i \leq 32, 1 \leq j \leq 100$. Symbols map to integers $1, \dots, 32, s(j) \equiv x(j)$, and the public key is $\prod c(x(j), j)$. For each “cut and choose” instance, $\forall i, j, 1 \leq i \leq 32, 1 \leq j \leq 100$: each column of $p(i, j) \in \text{random permutation}, p(i, \cdot) = (\pi_i(1), \pi_i(2), \dots, \pi_i(32))$; $k(j)$ reveals for each j which row of $p(\cdot, j) = x(j)$; blinding exponents $r(i, j) \in \text{random exponent}$; g is a fixed public generator; and f is a fixed public one-way committent function.

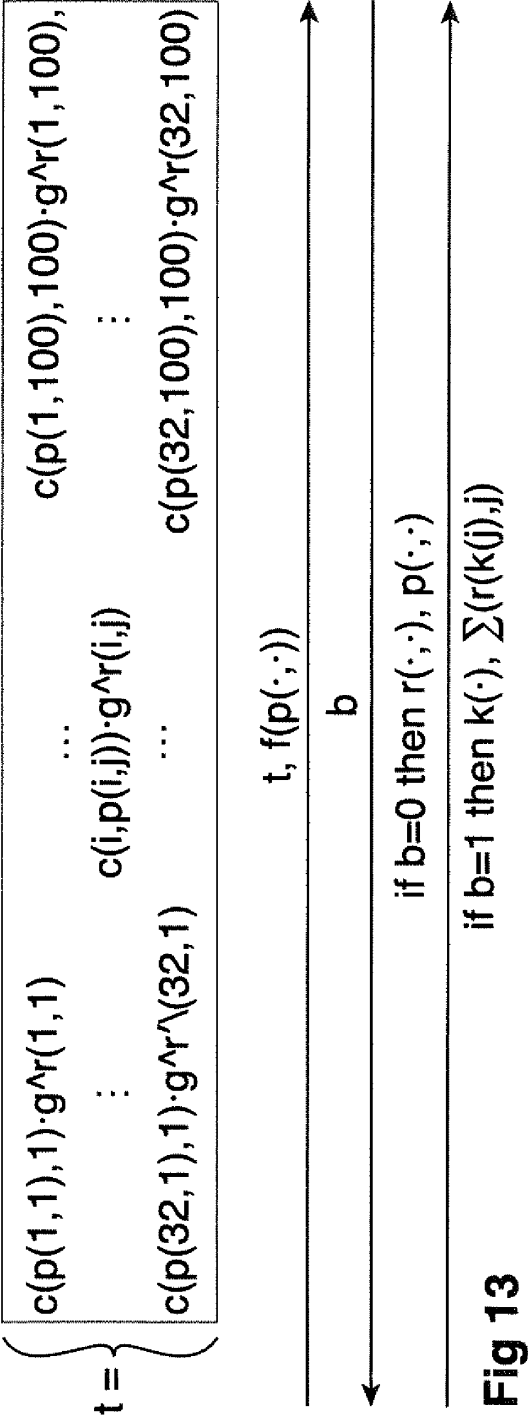


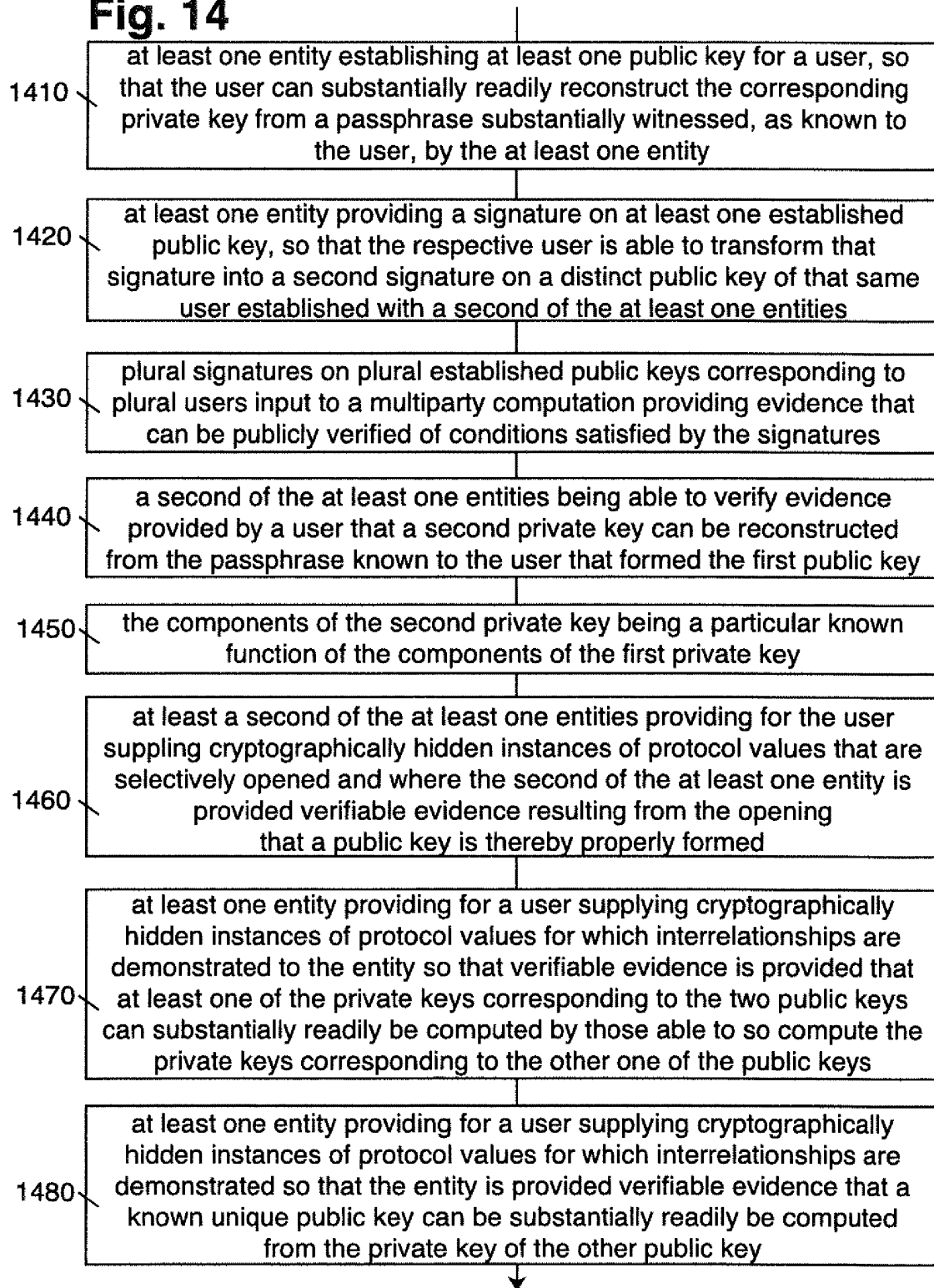
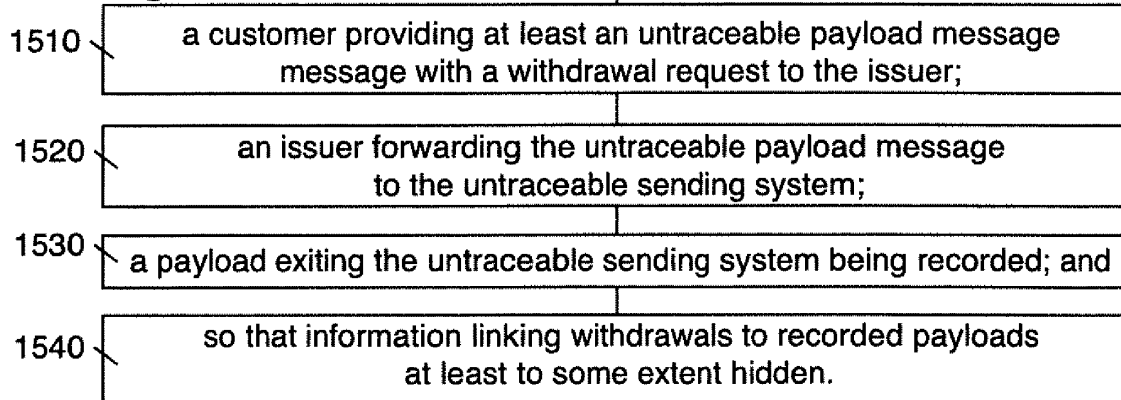
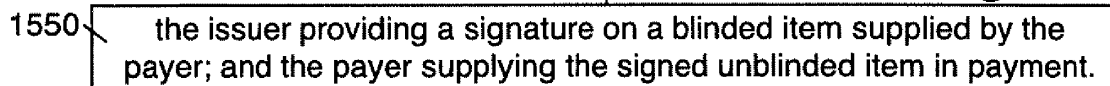
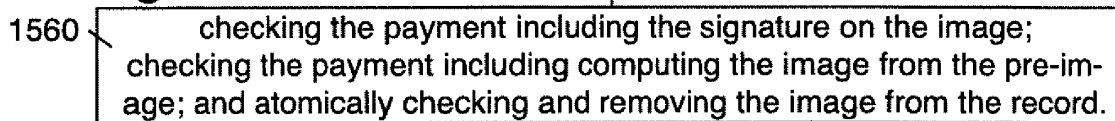
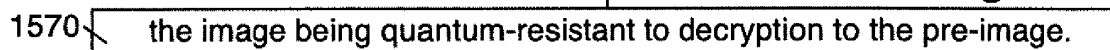
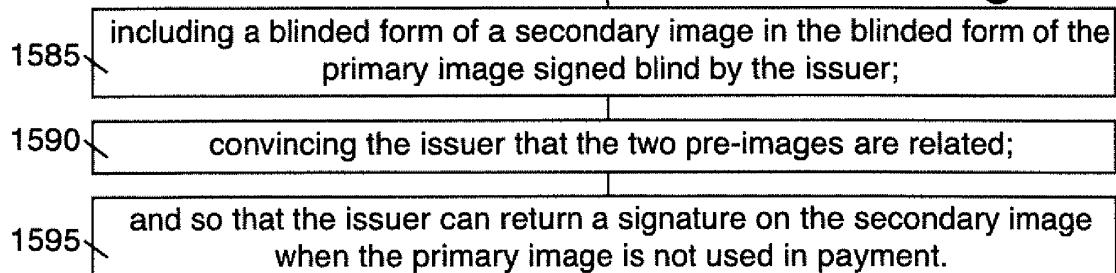
Fig. 14

Fig. 15A**Fig. 15B****Fig. 15C****Fig. 15D****Fig. 15E****Fig. 15F**

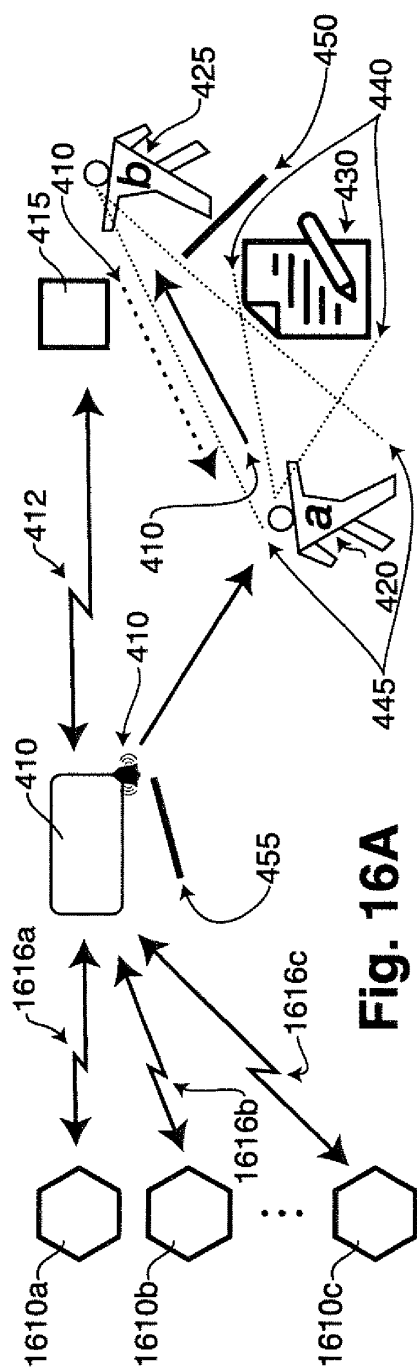


Fig. 16A

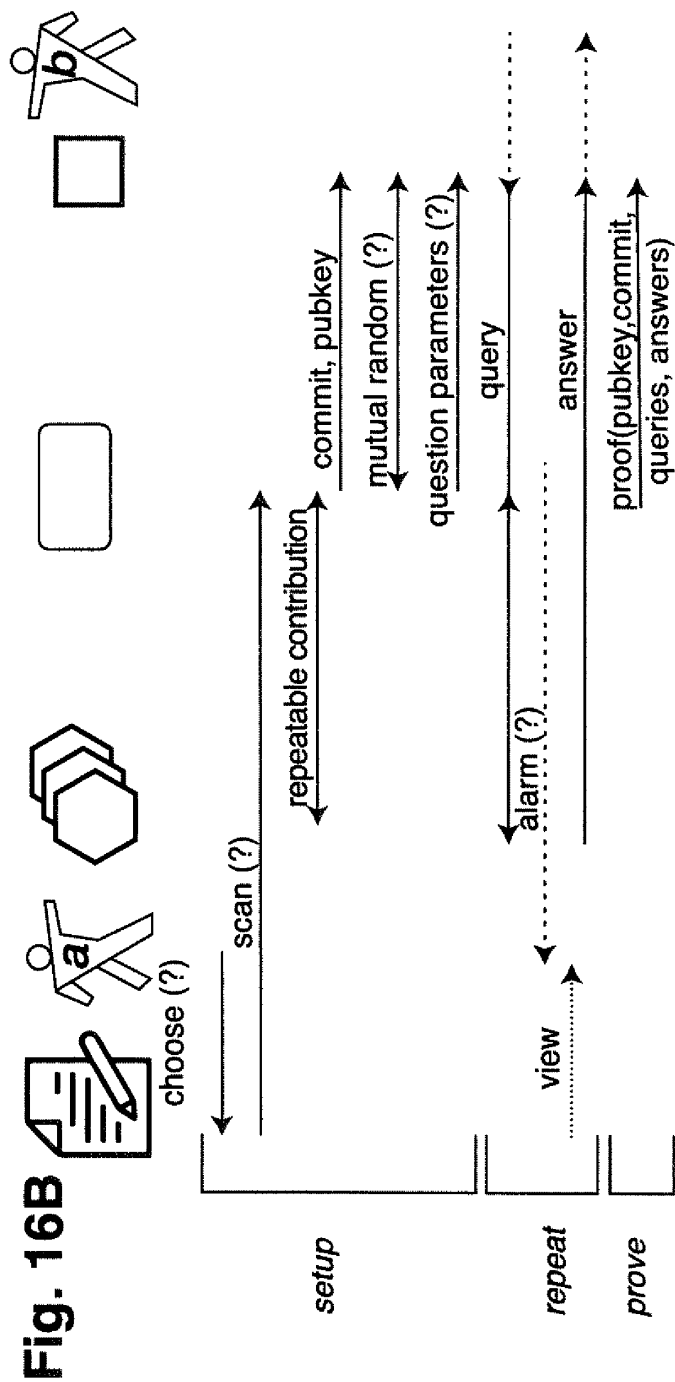


Fig. 16B

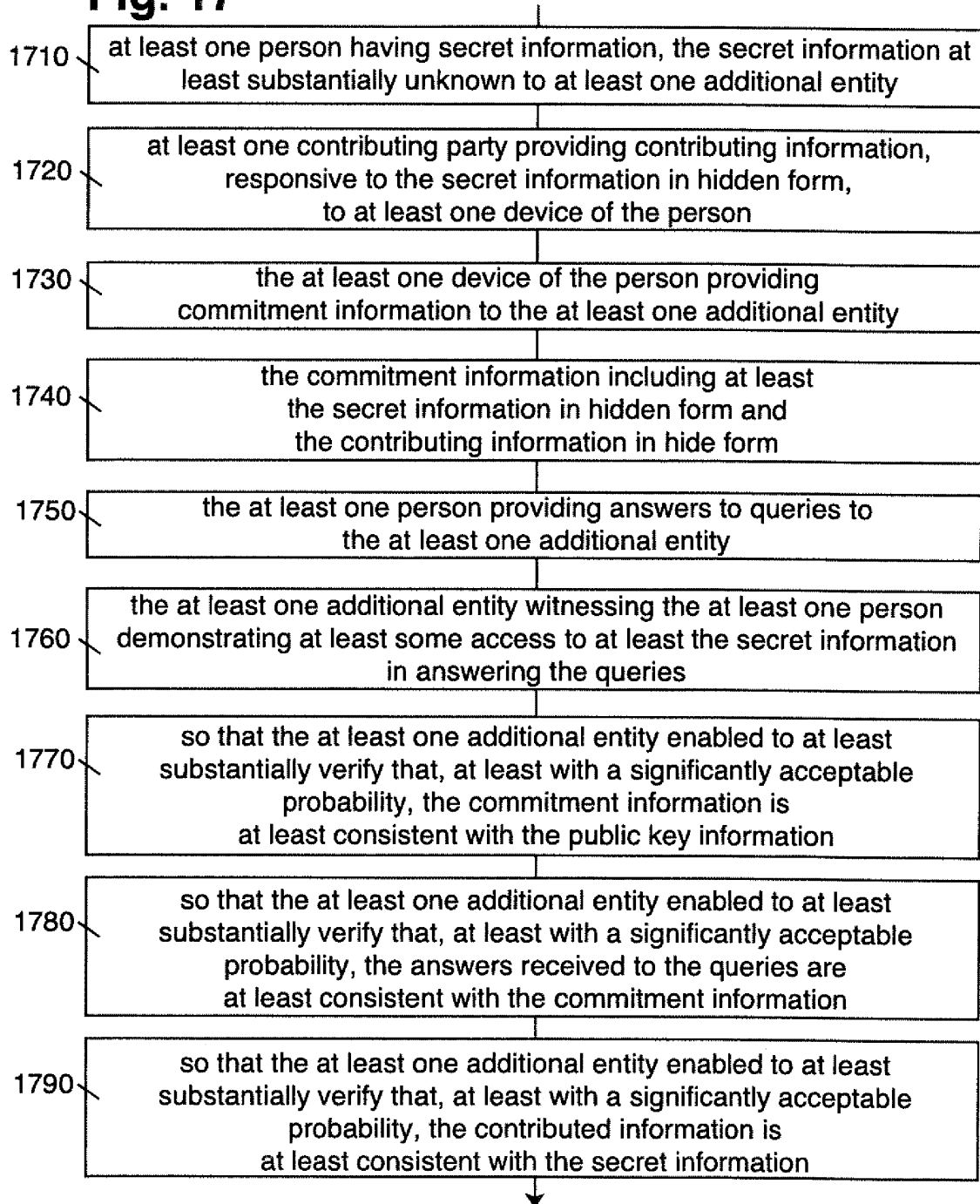
Fig. 17

FIG. 18

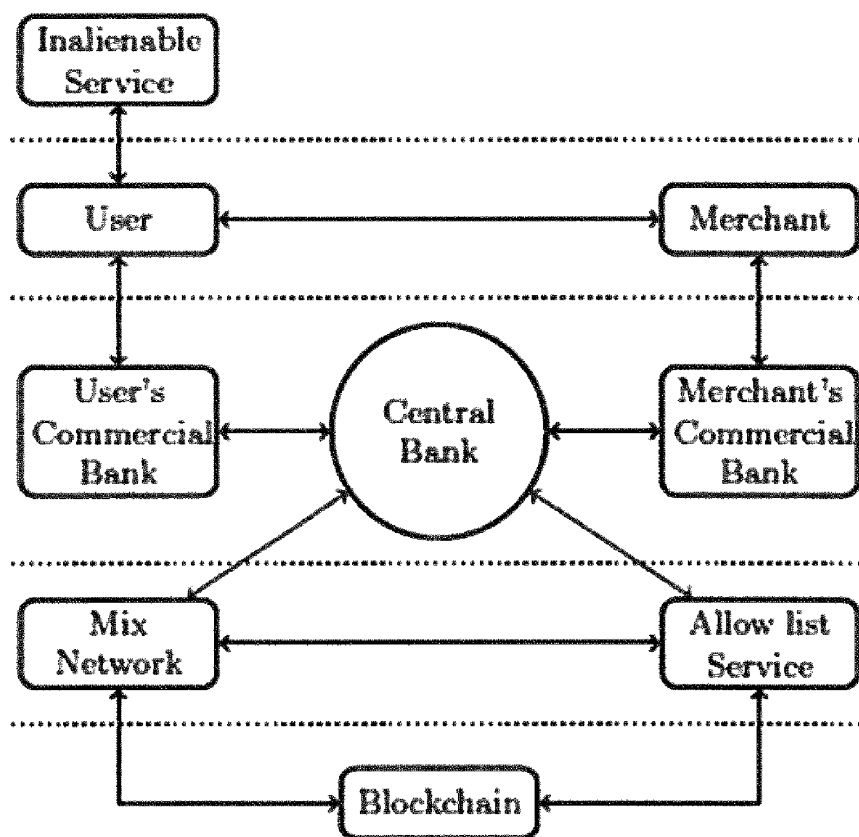


FIG. 19

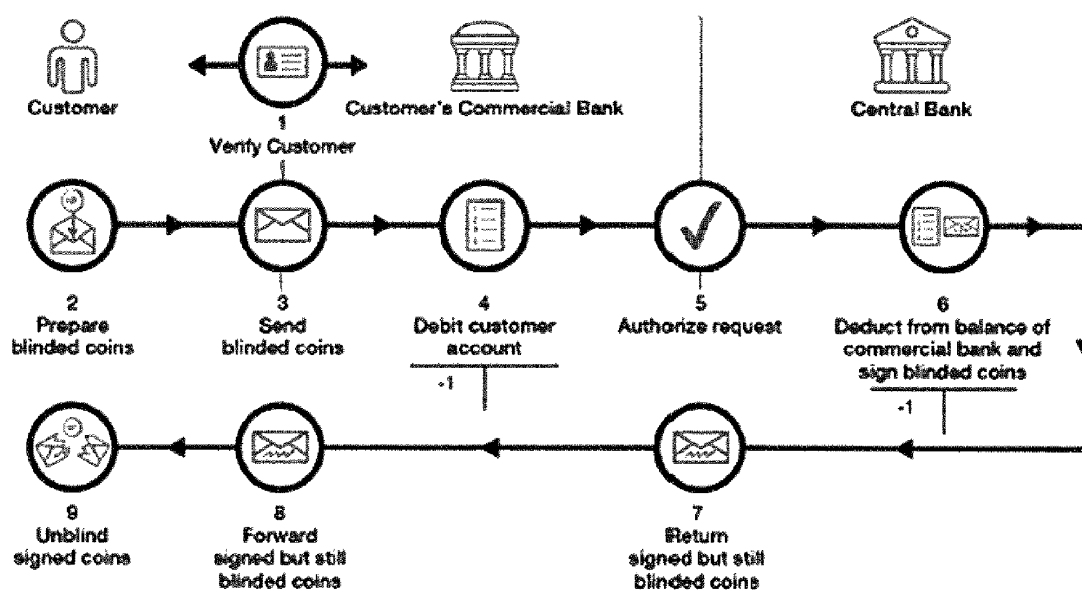


FIG. 20

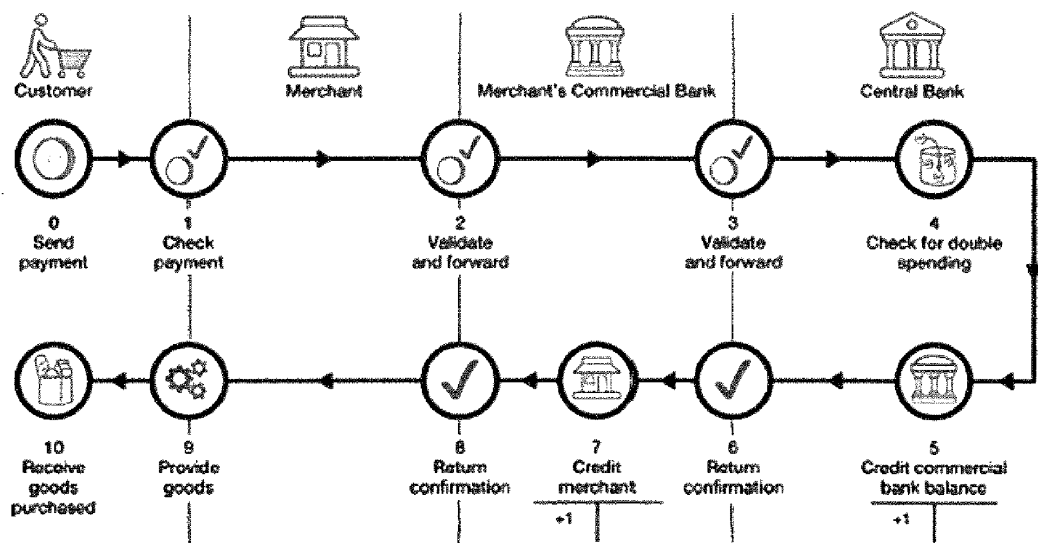


FIG. 21

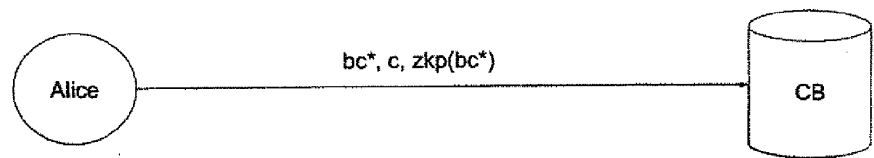


FIG. 22

