

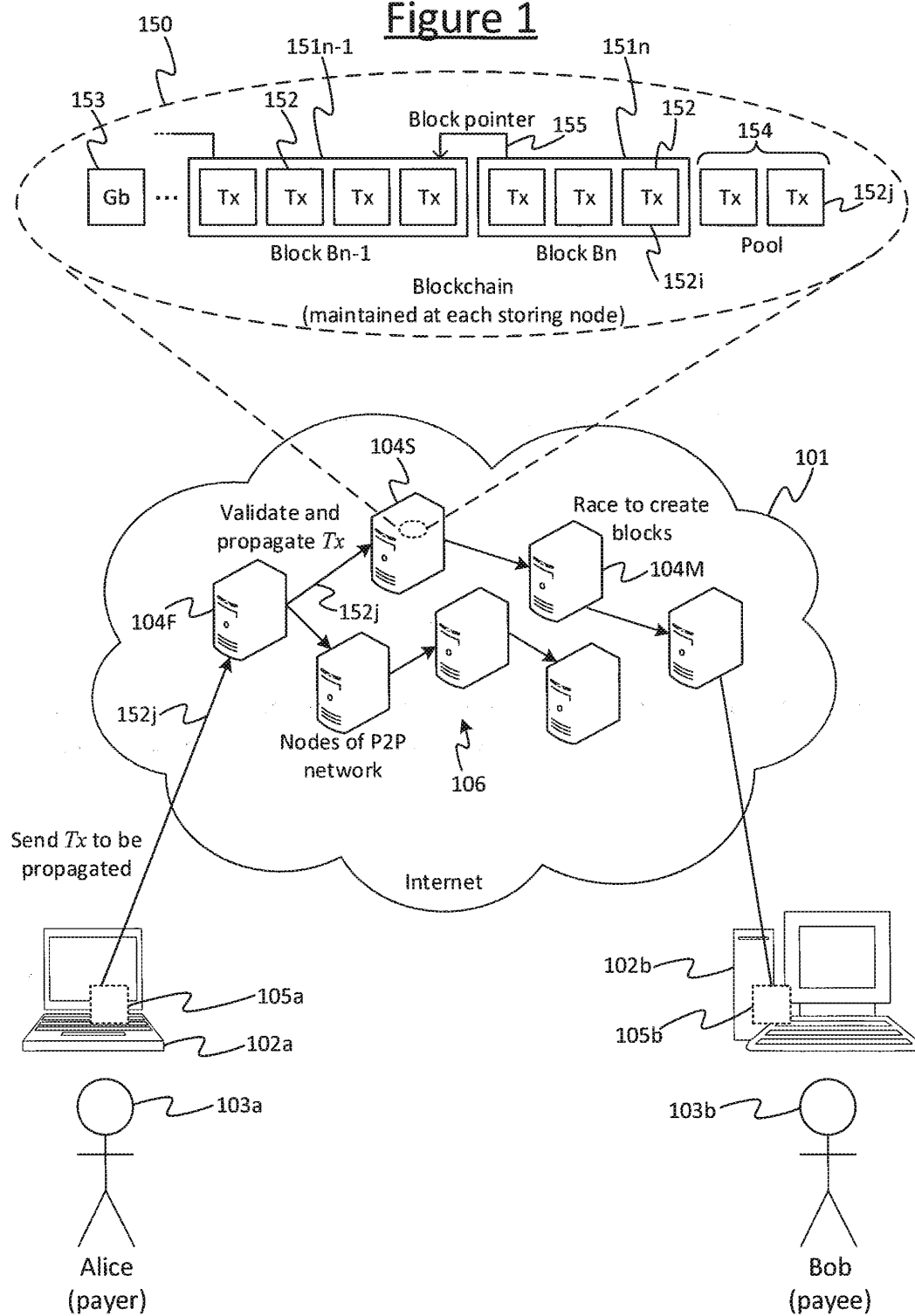
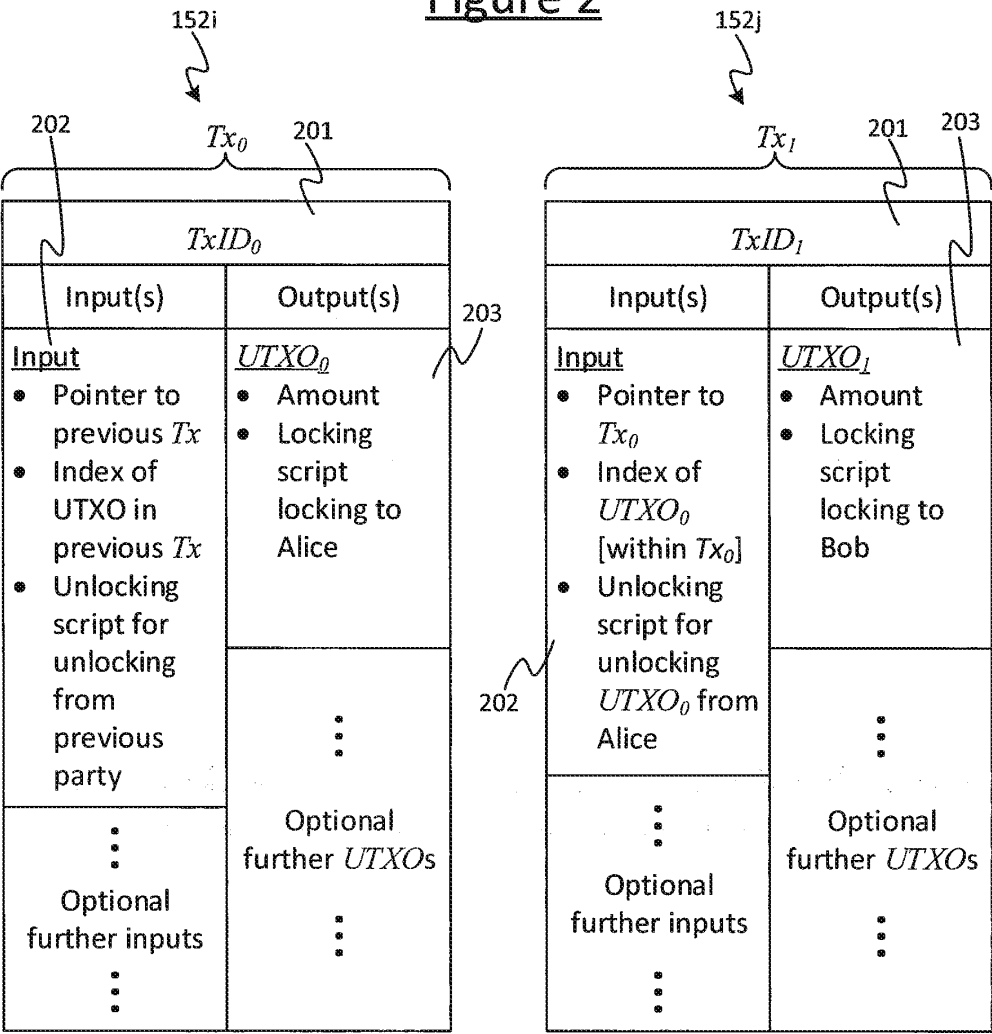
Figure 1

Figure 2



Transaction
from Alice to Bob

↓

Validated by running: Alice's locking script (from output of Tx_0), together with Alice's unlocking script (as input to Tx_1). This checks that Bob's unlocking script in Tx_1 meets the condition(s) defined in Alice's locking script in Tx_0 .

Figure 3

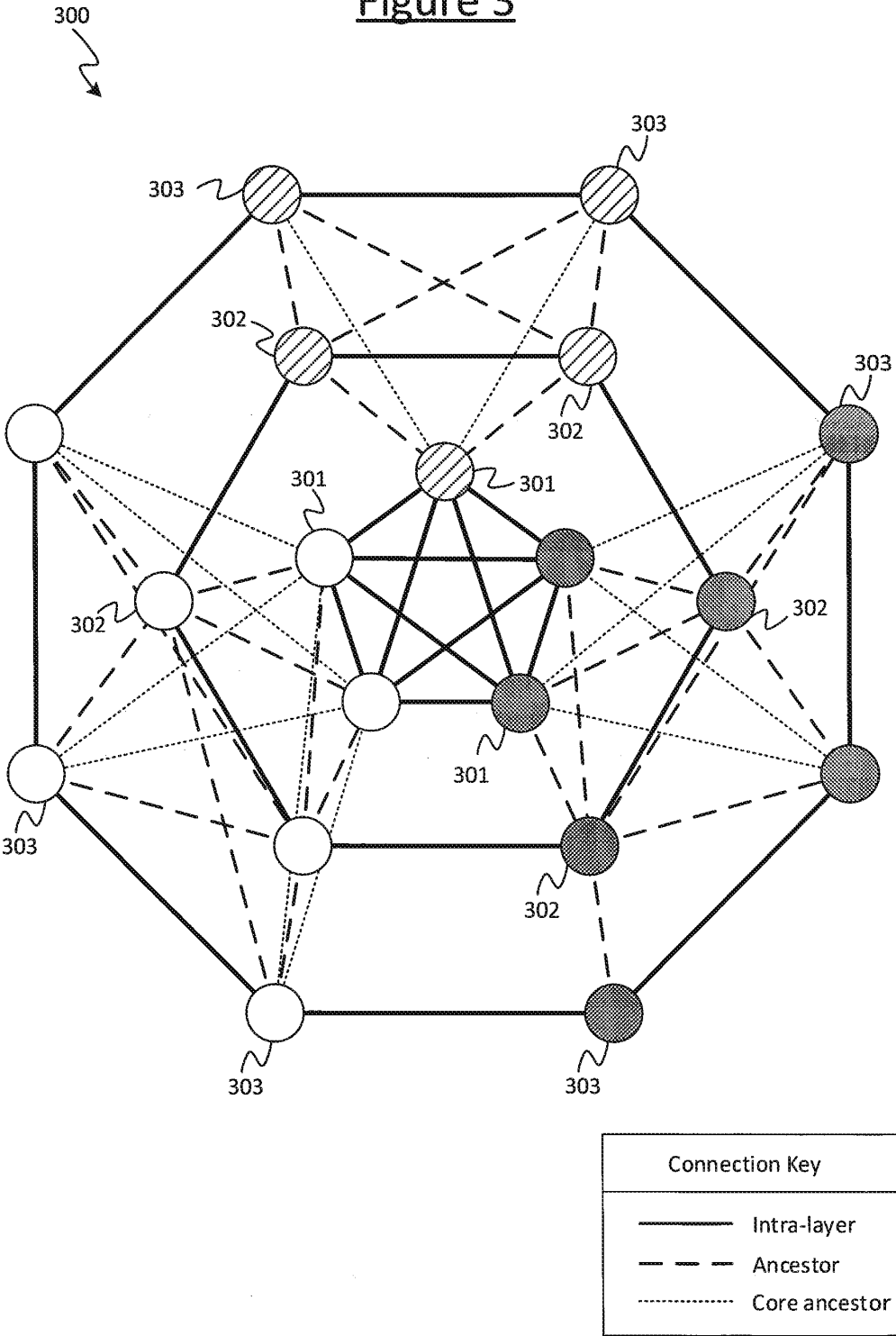


Figure 4

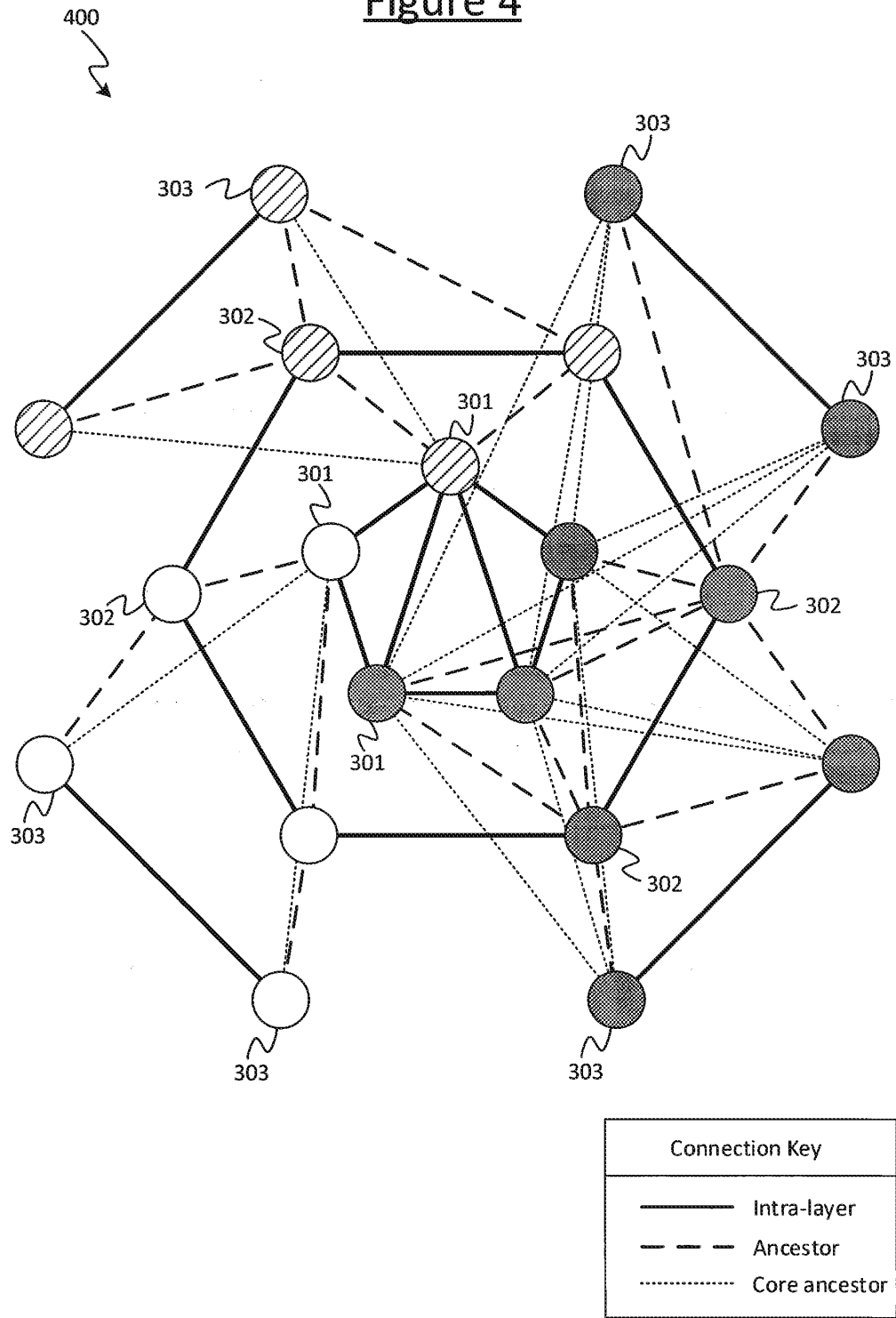


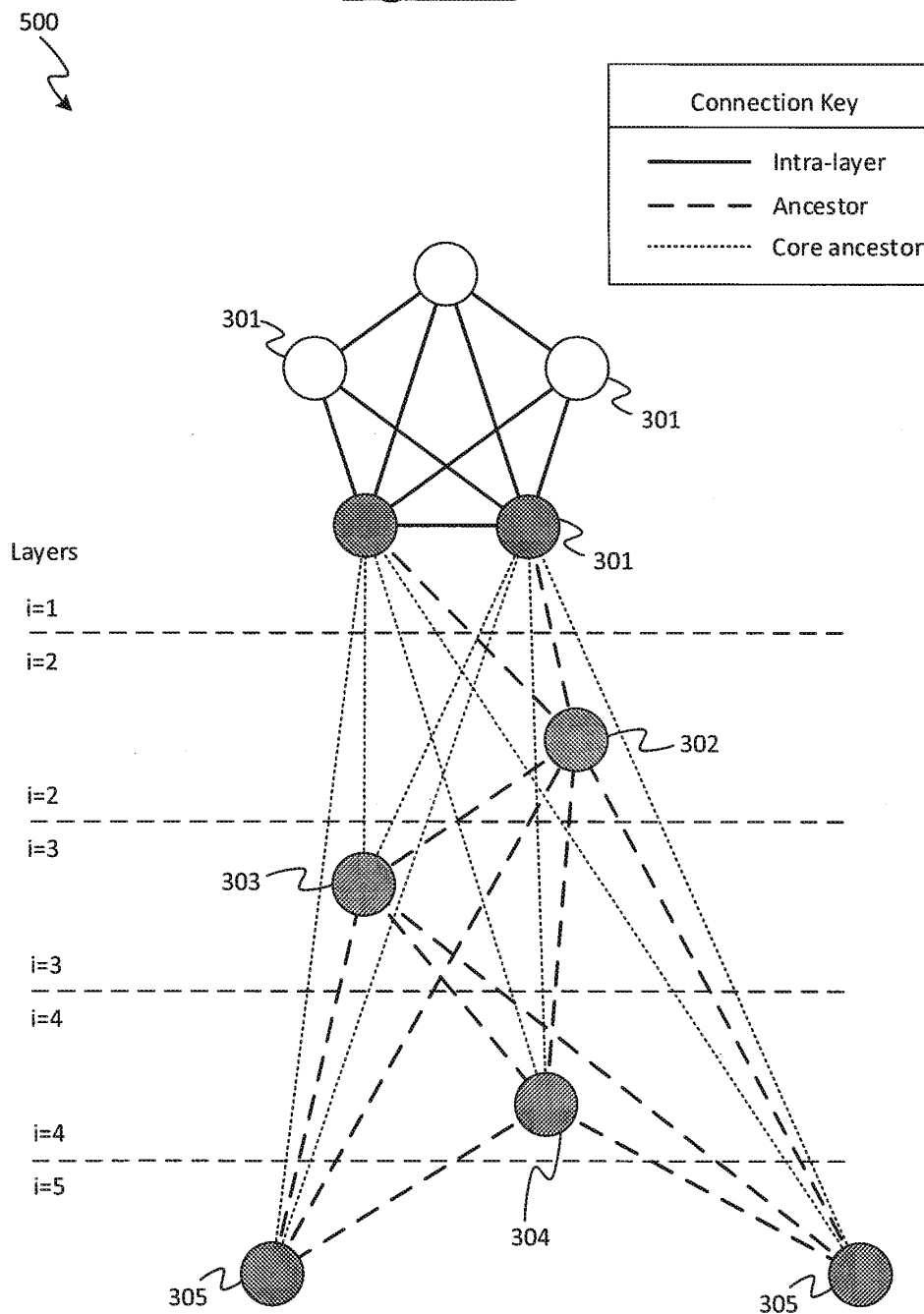
Figure 5

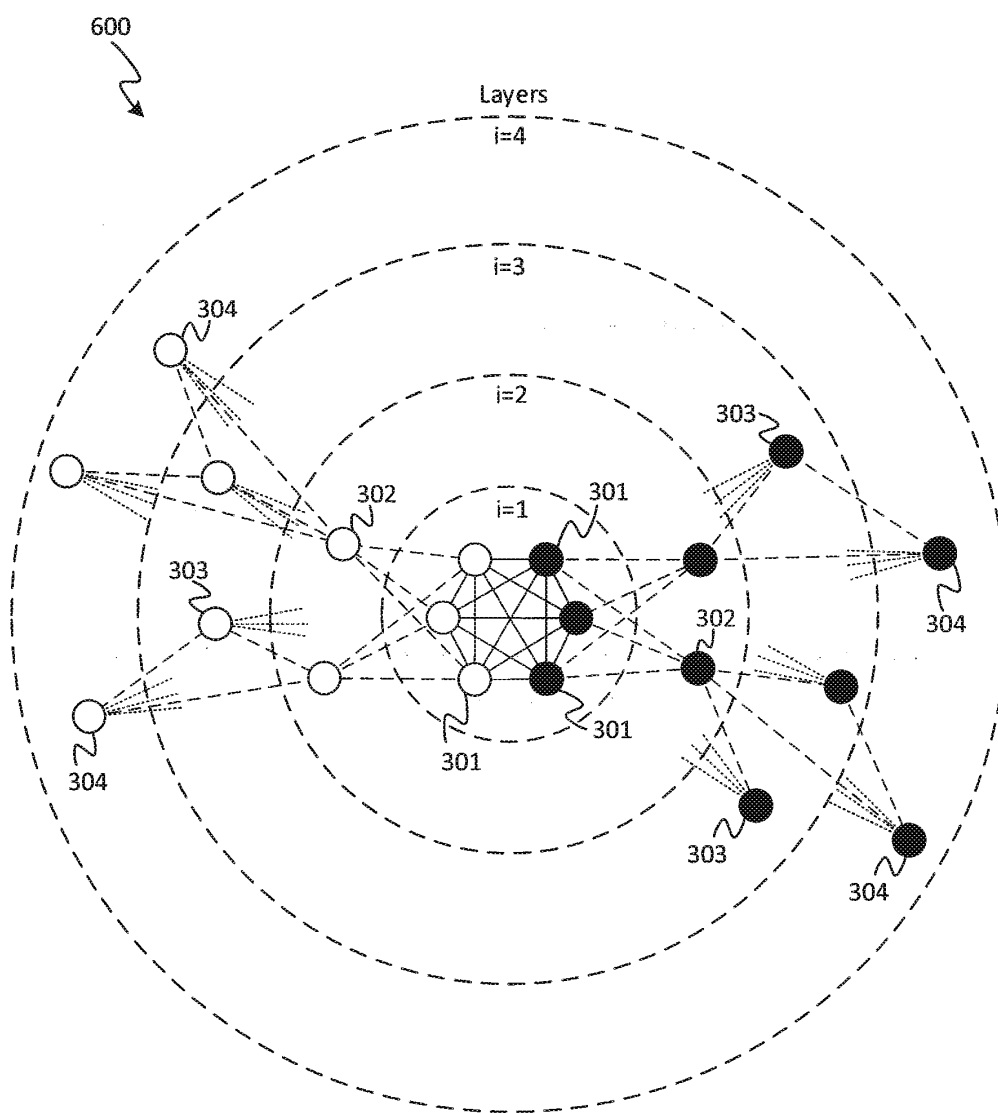
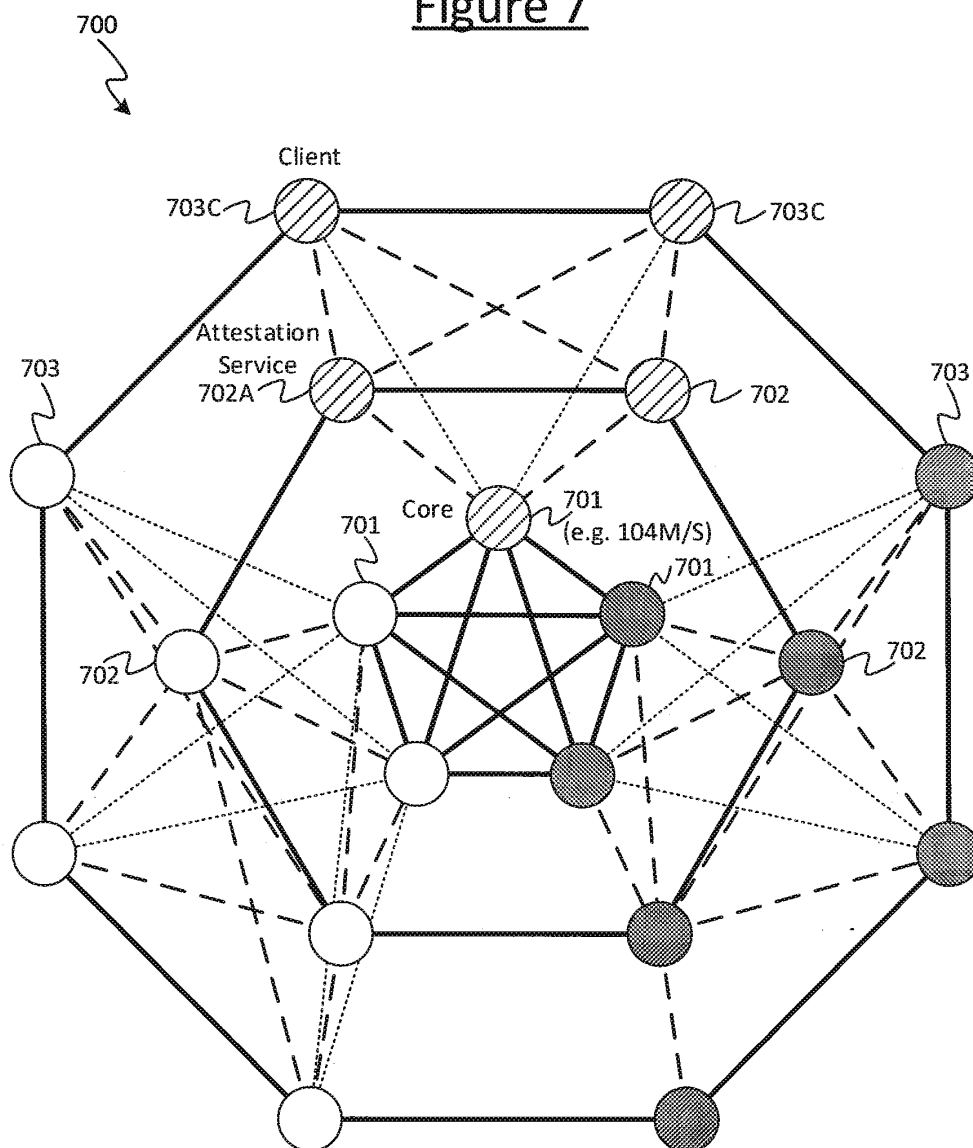
Figure 6

Figure 7

152 / Tx₁
↙

Figure 8

TxID ₁			
Version	1	Locktime	0
In-count	1	Out-count	2
Input list		Output list	
Outpoint	Unlocking script	Value	Locking script
TxID ₀ 0	< Sig ₁ > < P ₁ >	dust	[Checksigs P ₂]
		0	OP_FALSE OP_RETURN < data ₁ >
202		203	

Figure 9

Index	Data	Hash chain element
1	D ₁	H ₁ = H(D ₁)
2	D ₂	H ₂ = H(D ₂ H ₁)
3	D ₃	H ₃ = H(D ₃ H ₂)
		⋮
n ₁	D _{n₁}	H _{n₁} = H(D _{n₁} H _{n₁-1})

Figure 10

Index	Data	Public key	Signature
1	D_1	$P_{11} = P_1 + H(D_1) \cdot G$	$\text{Sig}(P_{11}, H(D_1))$
2	D_2	$P_{12} = P_1 + H(D_2 \parallel P_{11}) \cdot G$	$\text{Sig}(P_{12}, H(D_2))$
3	D_3	$P_{13} = P_1 + H(D_3 \parallel P_{12}) \cdot G$	$\text{Sig}(P_{13}, H(D_3))$
		$\vdots$	
n_1	D_{n_1}	$P_{1n_1} = P_1 + H(D_{n_1} \parallel P_{1(n_1-1)}) \cdot G$	$\text{Sig}(P_{1n_1}, H(D_{n_1}))$

Figure 11

Index	Data	Ephemeral key	Signature
1	D_1	$R_{11} = R_1 + H(D_1) \cdot G$	$\langle S_1, R_{11} \rangle(H(D_1))$
2	D_2	$R_{12} = R_1 + H(D_2 \parallel R_{11}) \cdot G$	$\langle S_1, R_{12} \rangle(H(D_2))$
3	D_3	$R_{13} = R_1 + H(D_3 \parallel R_{12}) \cdot G$	$\langle S_1, R_{13} \rangle(H(D_3))$
		$\vdots$	
n_1	D_{n_1}	$R_{1n_1} = R_1 + H(D_{n_1} \parallel R_{1(n_1-1)}) \cdot G$	$\langle S_1, R_{1n_1} \rangle(H(D_{n_1}))$

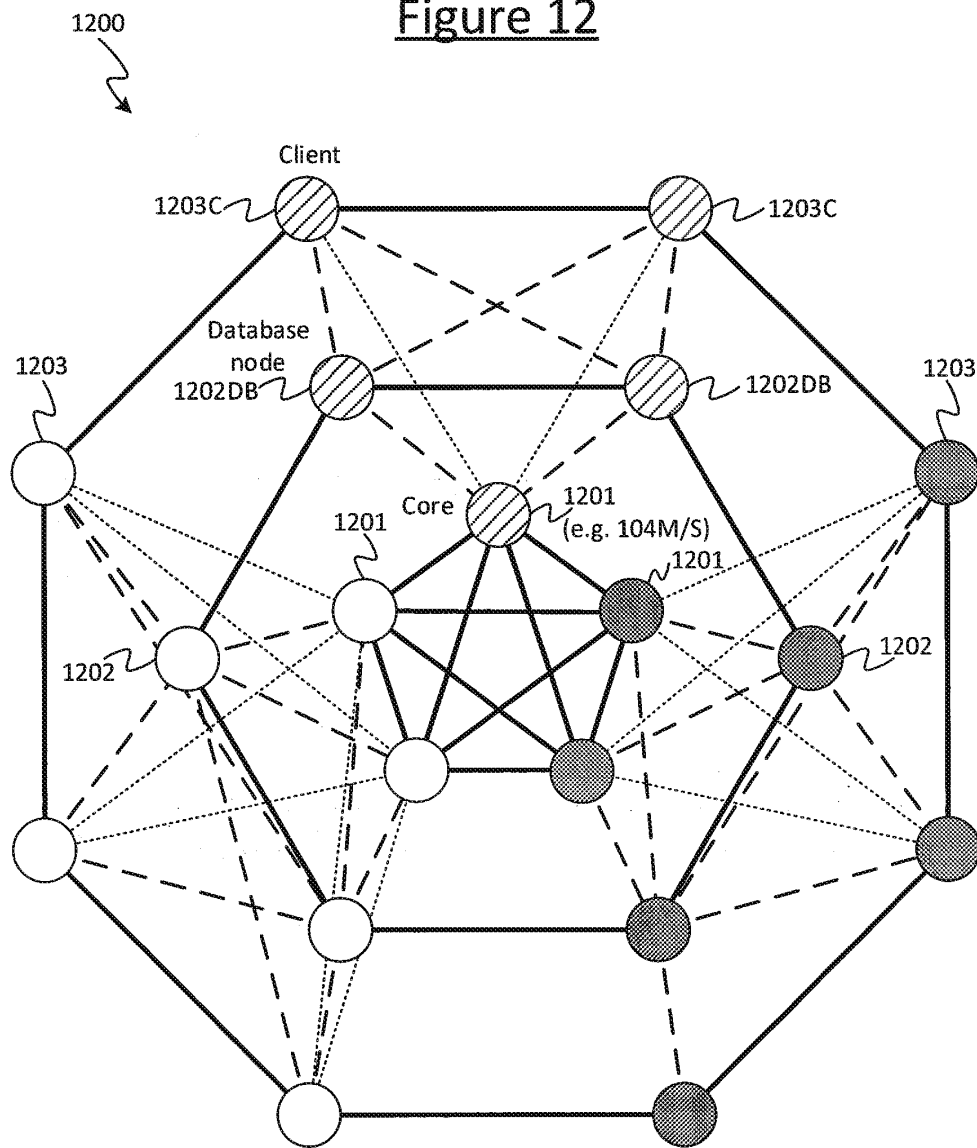
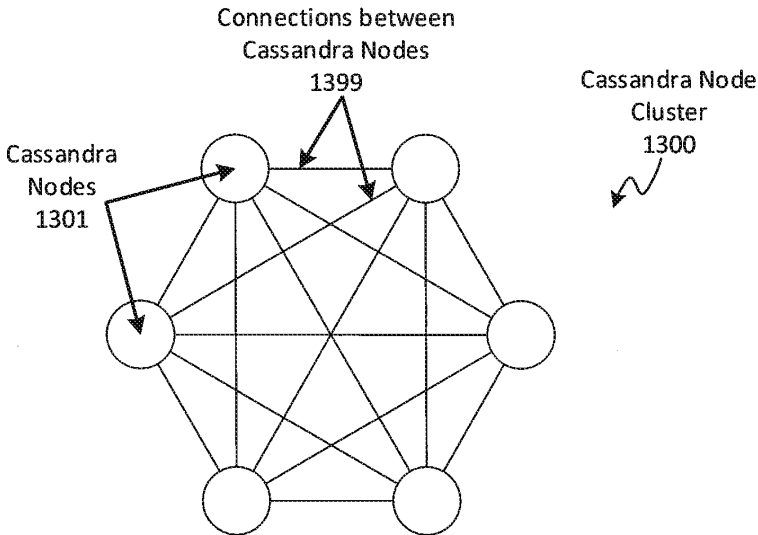
Figure 12

Figure 13

(a)



(b)

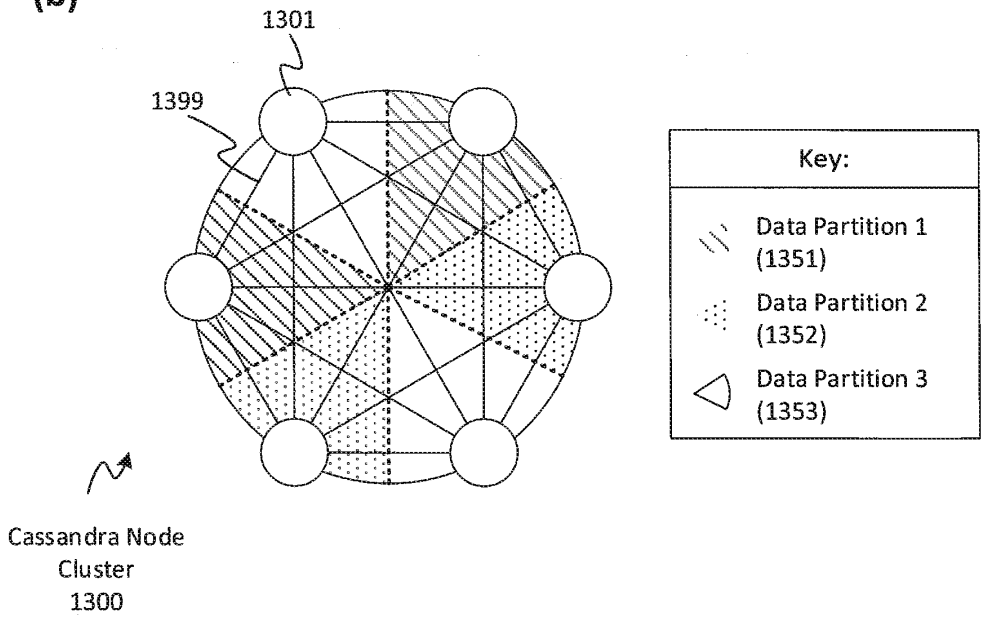


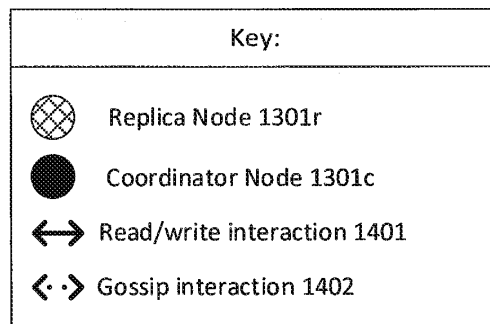
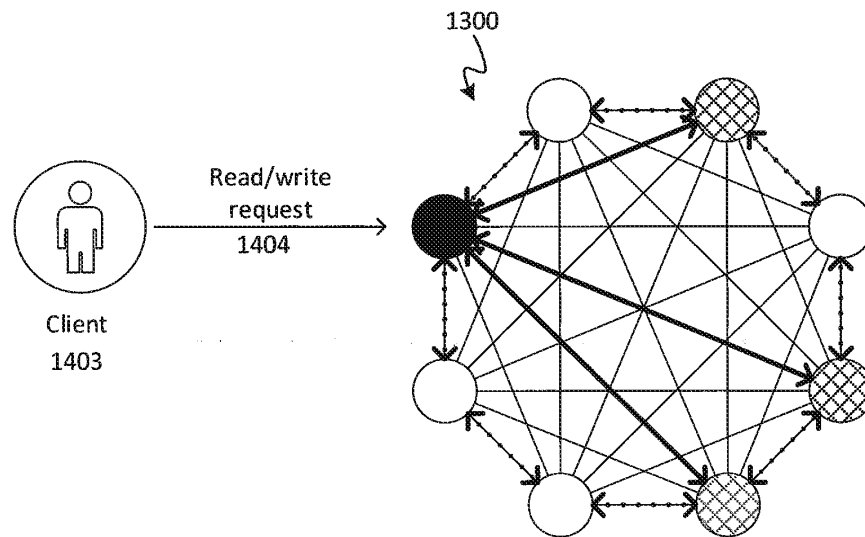
Figure 14

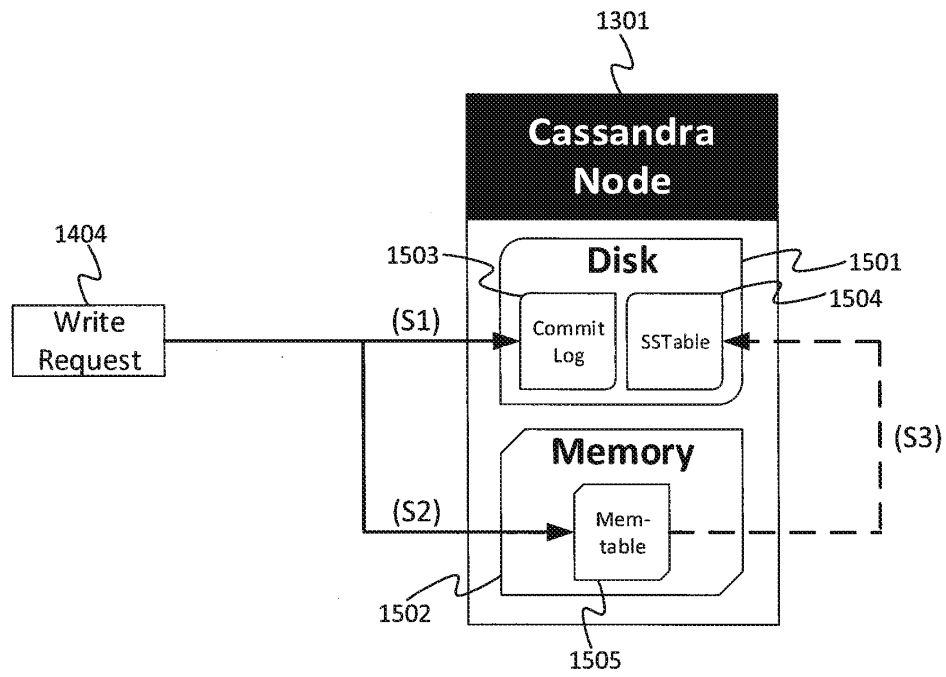
Figure 15

Figure 16

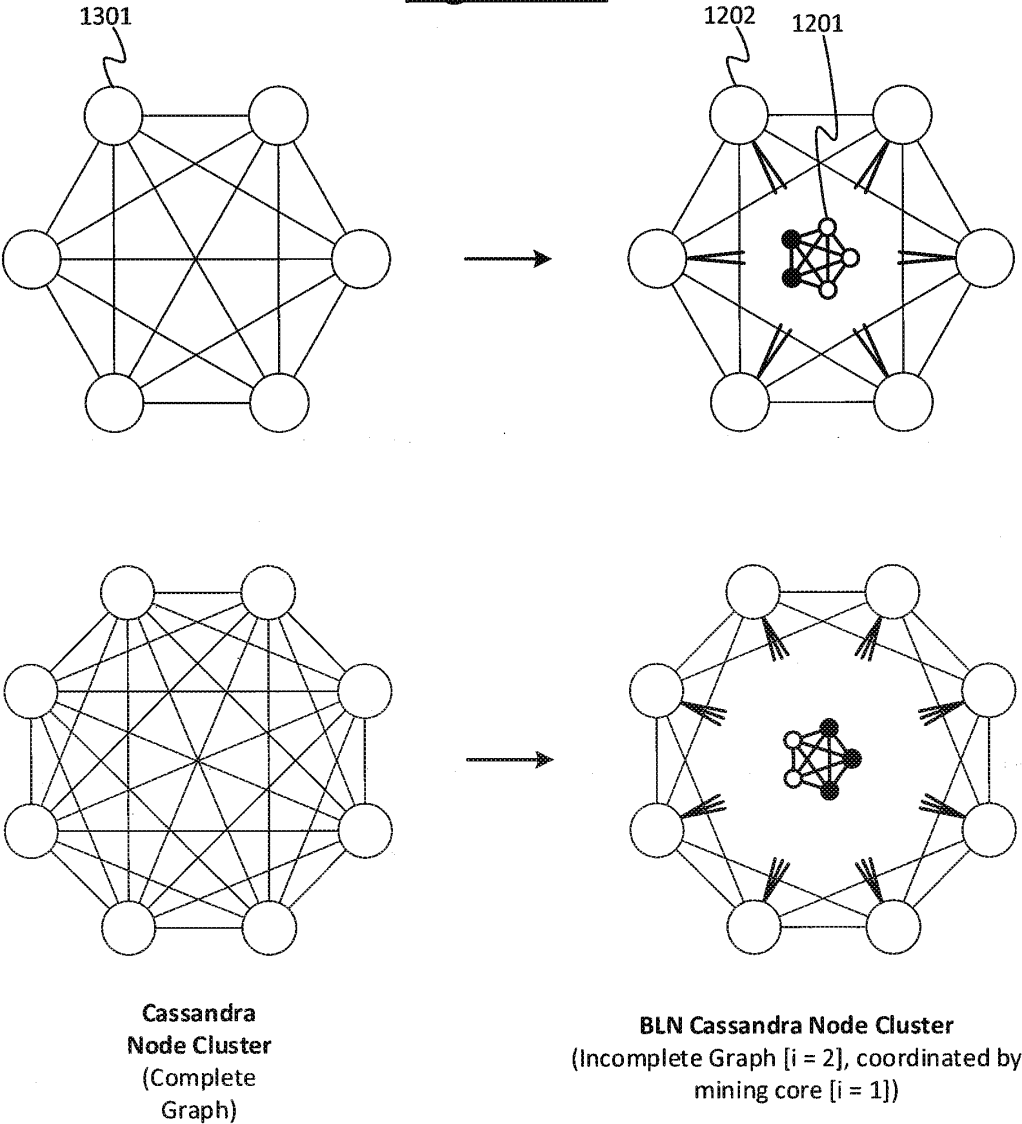


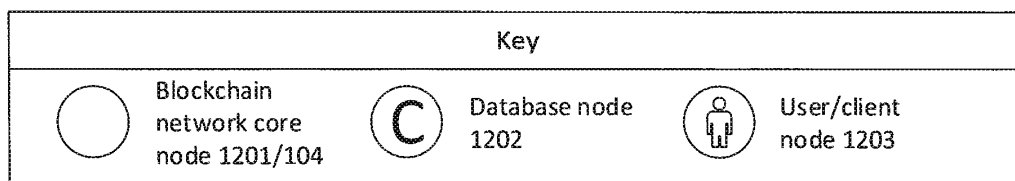
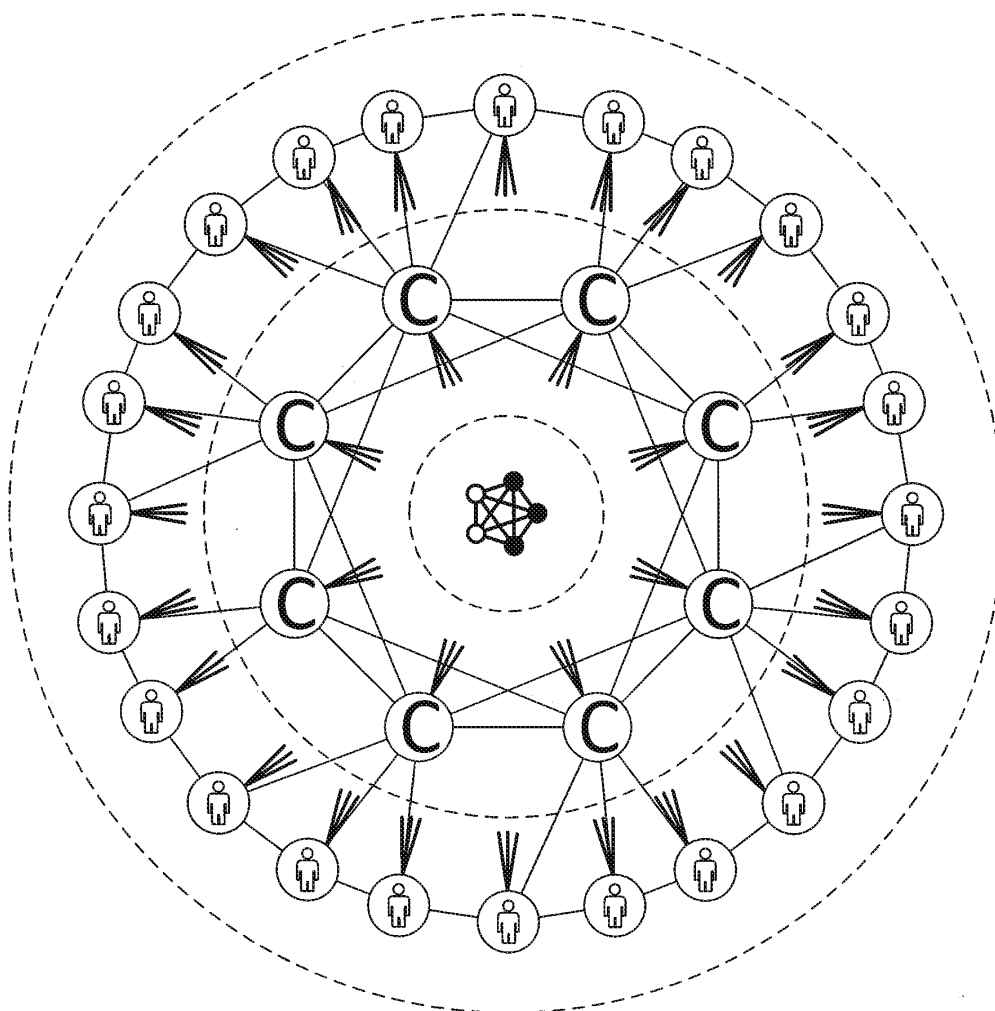
Figure 17

Figure 18

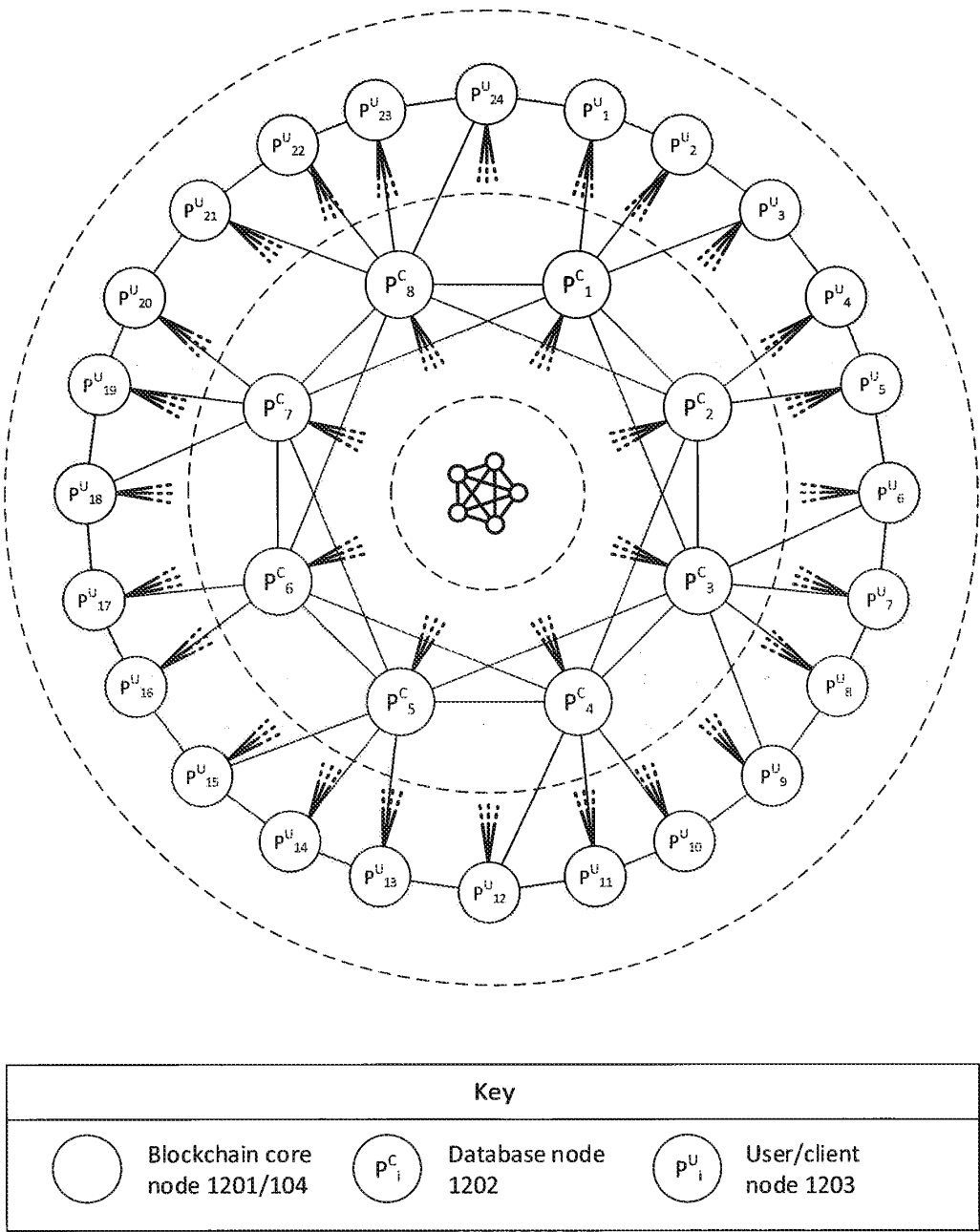


Figure 19

TxID _{R/W} Request			
Version	1	Locktime	0
In-count	1	Out-count	2
Input list		Output list	
Outpoint	Unlocking script	Value	Locking script
TxID ₀ 0	< Sig _{Coord.} > < P ^C _{Coord.} >	dust	[Checksig P ^C _{Coord.} .]
		0	OP_FALSE OP_RETURN < Request Data >

Figure 20

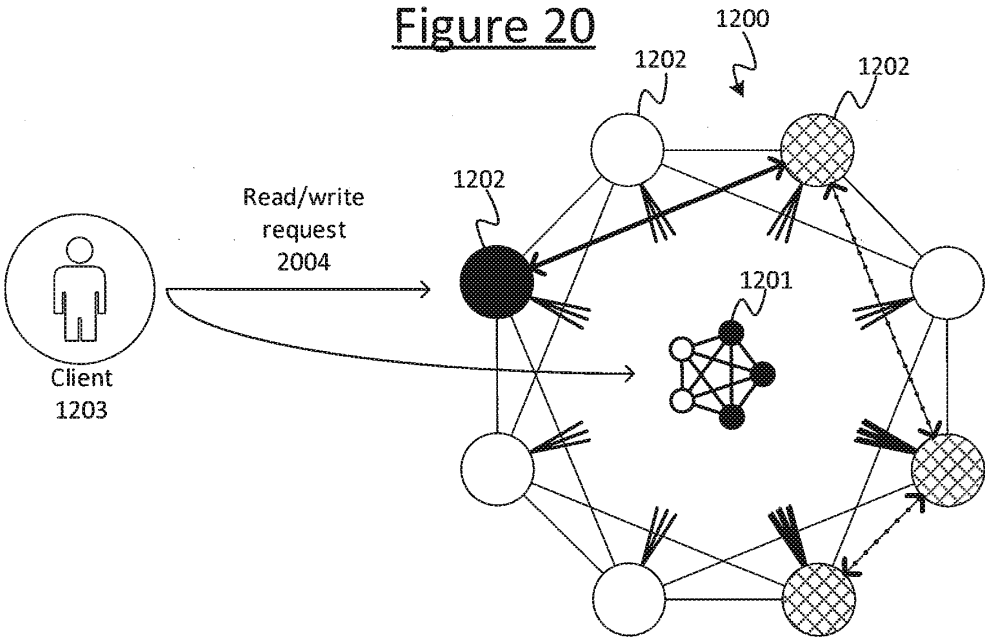


Figure 21

$TxID_{\text{Hinted Handoff}}$			
Version	1	Locktime	0
In-count	1	Out-count	2
Input list		Output list	
Outpoint	Unlocking script	Value	Locking script
$TxID_0 \parallel 0$	$\langle Sig_{Coord.} \rangle \langle P_{Coord.}^C \rangle$	dust	$[Checksig\ P_{Coord.}^C]$
		0	OP_FALSE OP_RETURN $\langle Hinted\ Handoff \rangle$