

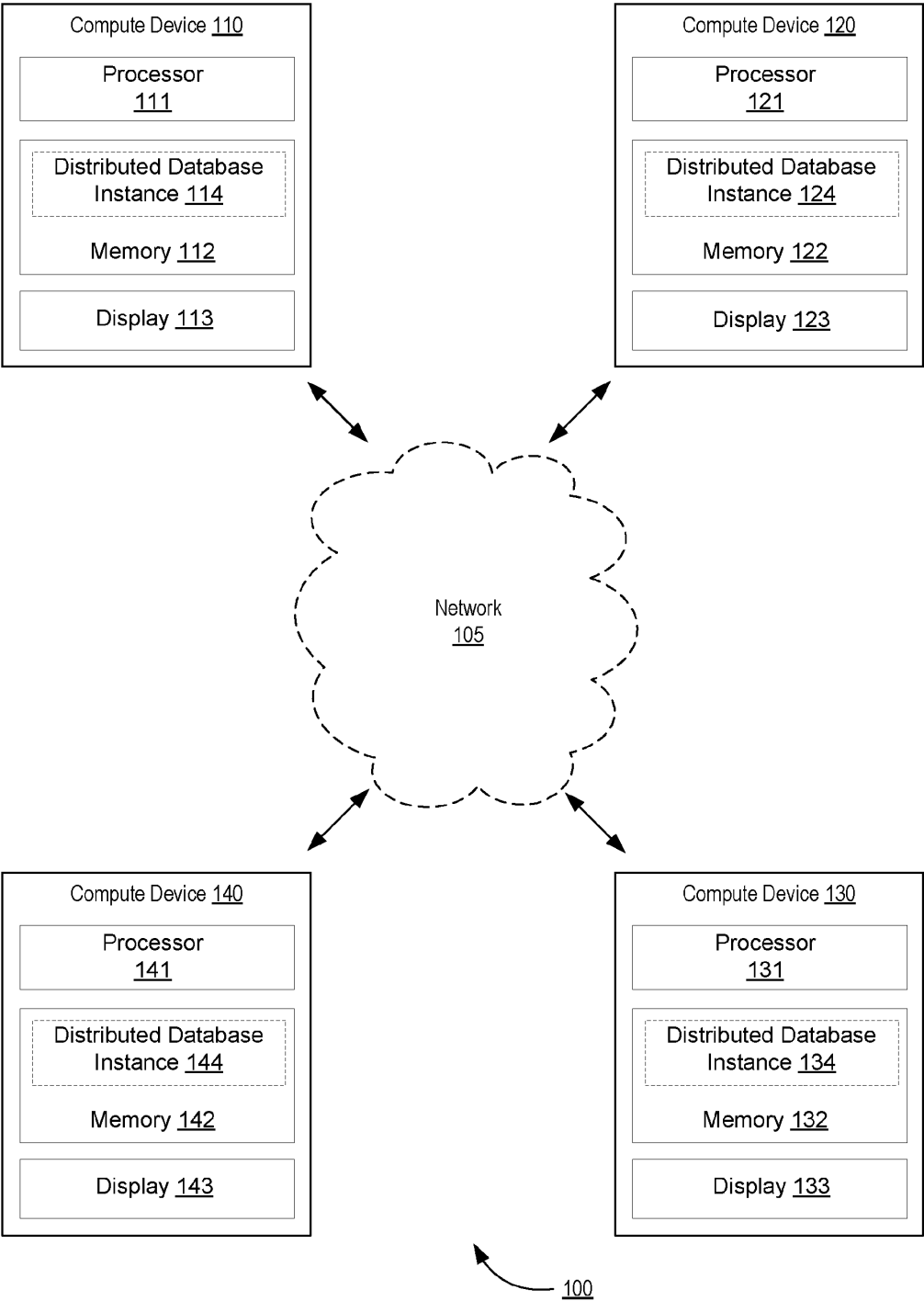


FIG. 1

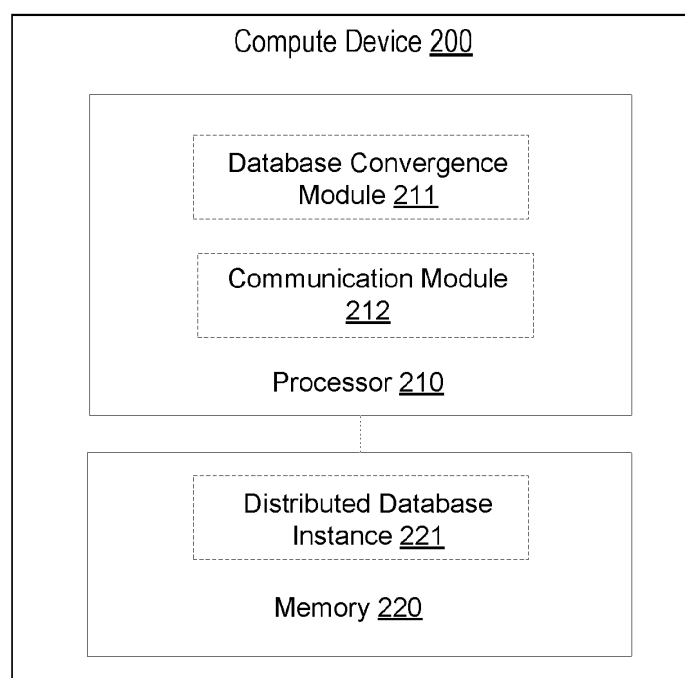


FIG. 2

600

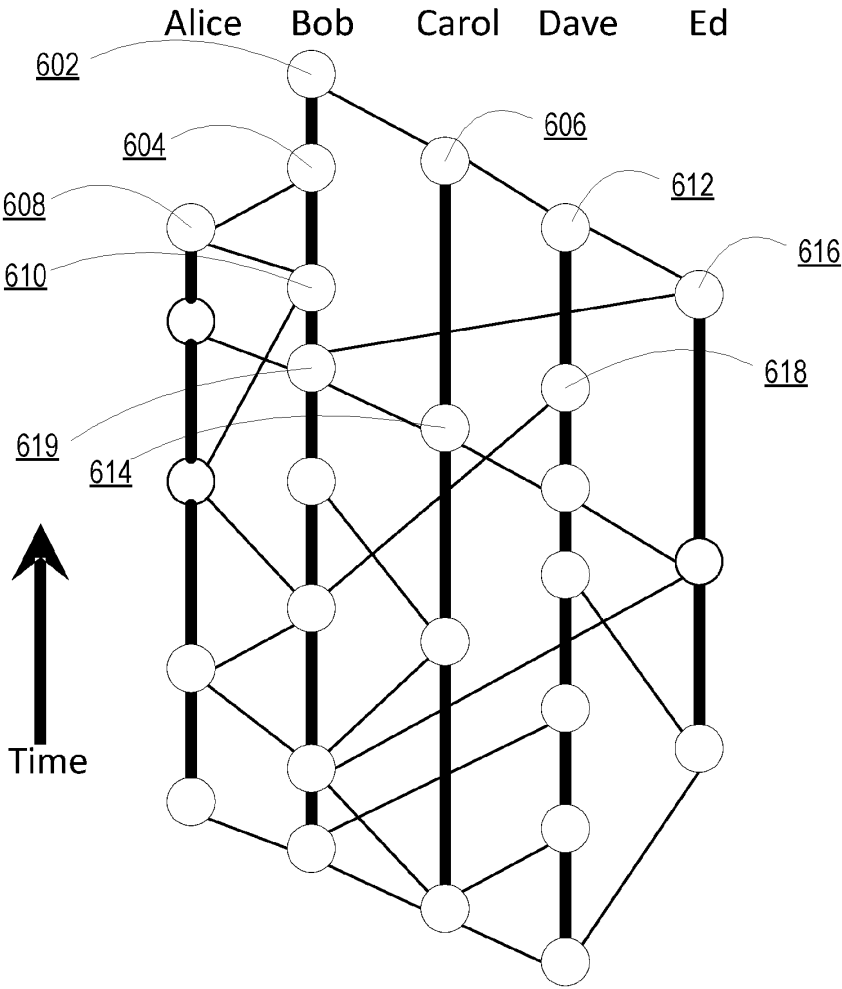


FIG. 3

620

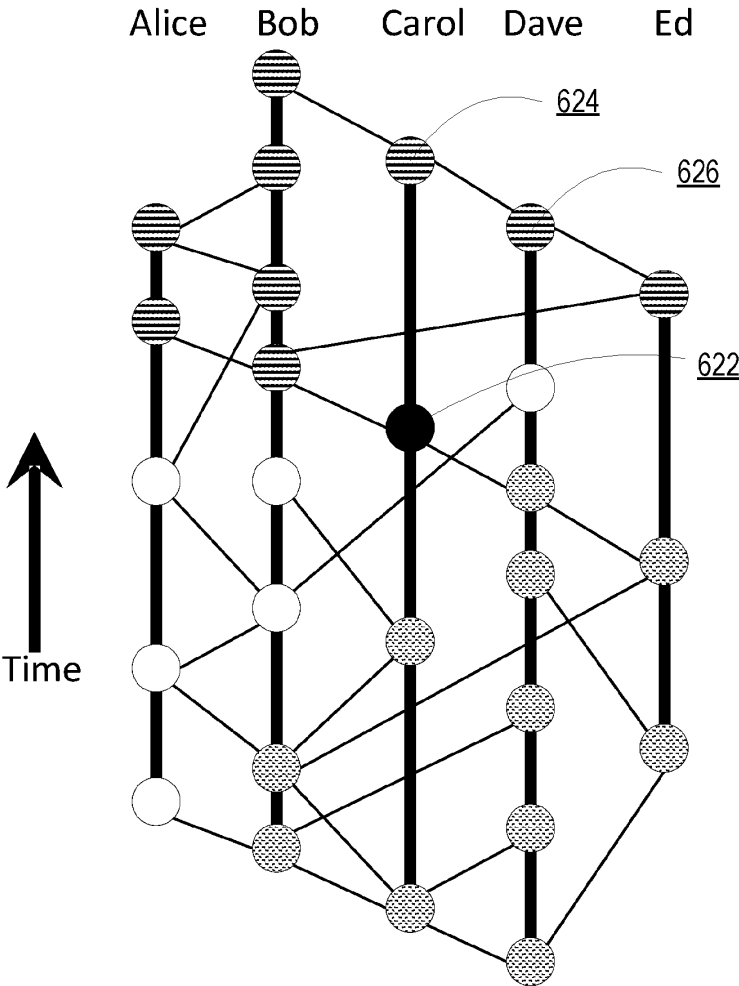


FIG. 4

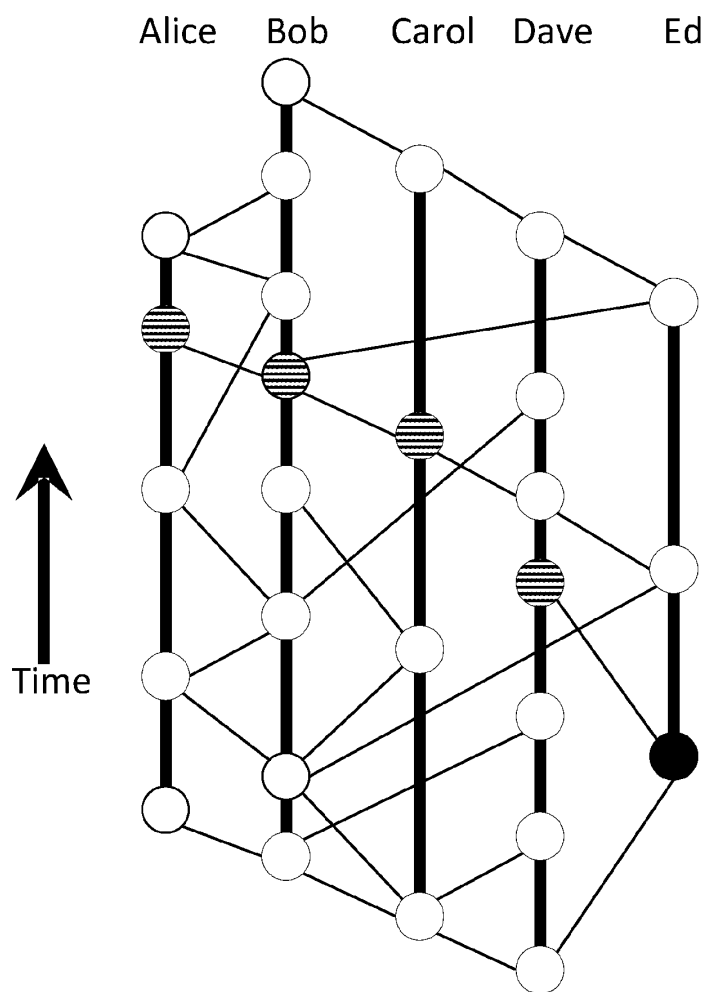


FIG. 5

640

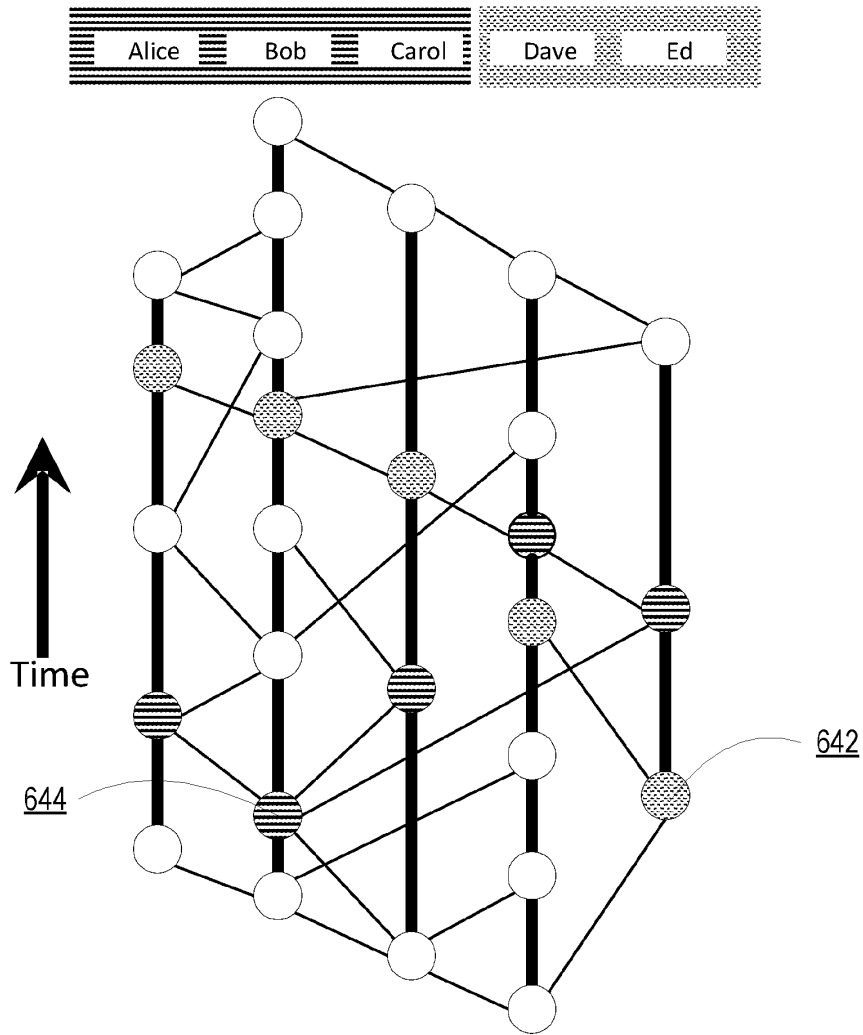


FIG. 6

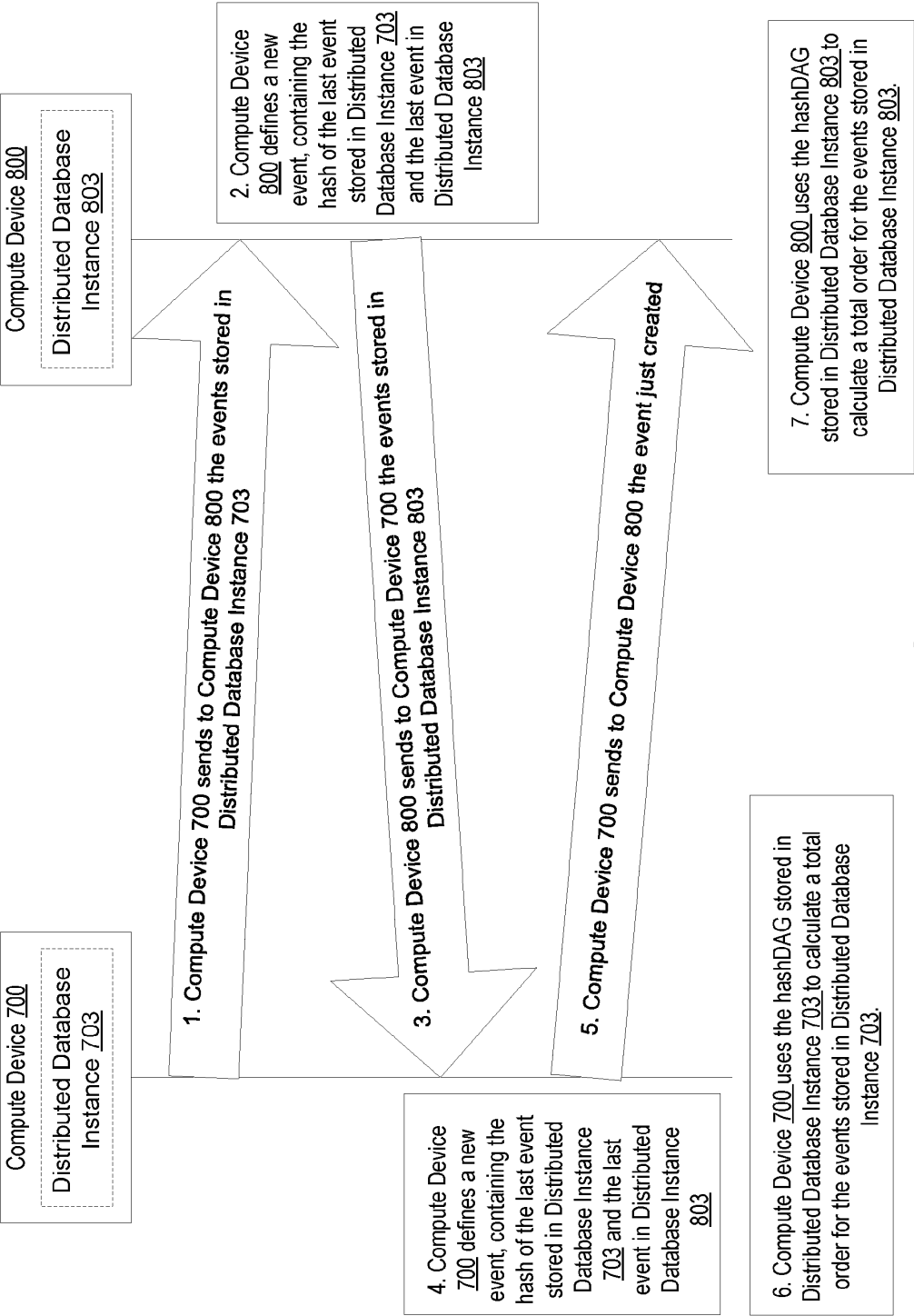


FIG. 7

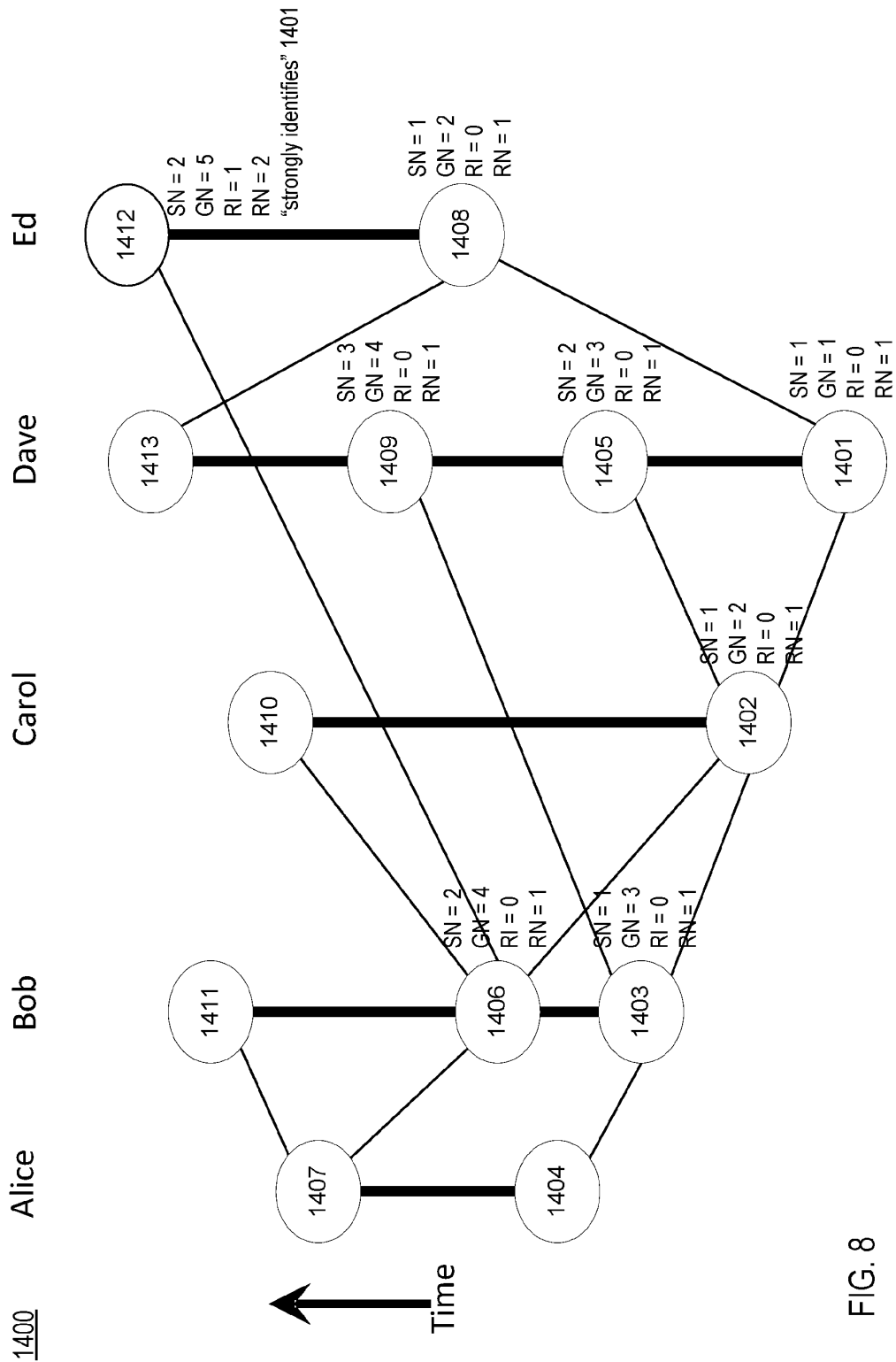
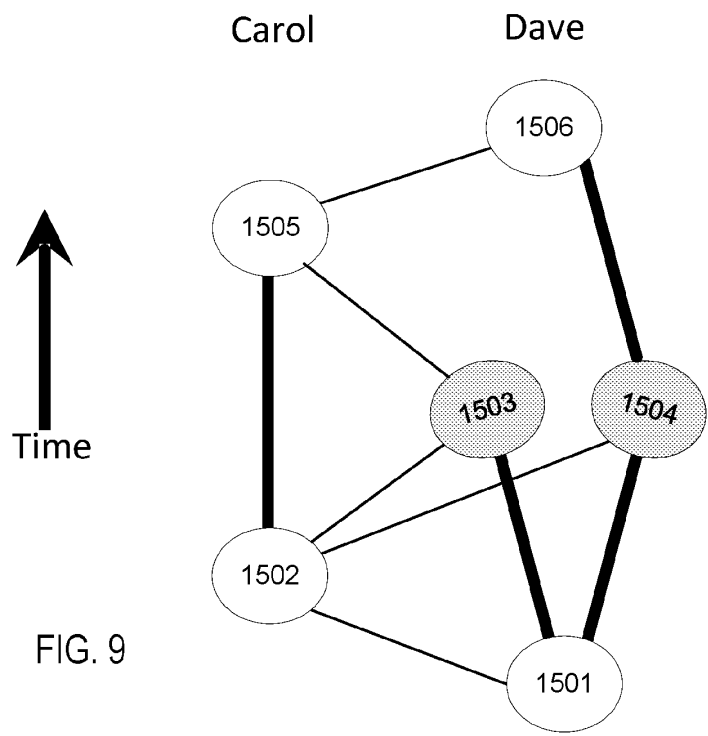


FIG. 8



An event is a tuple $e = \{d, h, t, c, s\}$ where:

$d = data(e)$ = the “payload” data, which may include transactions.
 $h = hashes(e)$ = a list of hashes of the event’s parents, self-parent first.
 $t = time(e)$ = creator’s claimed date and time of the event’s creation.
 $c = creator(e)$ = creator’s ID number.
 $s = sig(e)$ = creator’s digital signature of $\{d, h, t, c\}$.
 n = the number of members in the population
 $m = 1 + \lfloor 2n/3 \rfloor$
 $first$ = the unique event that has no parents
 E = the set of all events
 T = set of all possible $(time, date)$ pairs
 $\mathbb{B} = \{true, false\}$
 $\mathbb{N} = \{0, 1, 2, \dots\}$
 $ancestor : E \times E \rightarrow B$
 $selfAncestor : E \times E \rightarrow B$
 $see : E \times E \rightarrow B$
 $stronglySee : E \times E \rightarrow B$
 $parentRound : E \rightarrow \mathbb{N}$
 $witness : E \rightarrow \mathbb{B}$
 $round : E \rightarrow \mathbb{N}$
 $roundDiff : E \times E \rightarrow \mathbb{I}$
 $votes : E \times E \times \mathbb{B} \rightarrow \mathbb{N}$
 $voteFraction : E \times E \rightarrow \mathbb{R}$
 $vote : E \times E \rightarrow \mathbb{B}$
 $decide : E \times E \rightarrow \mathbb{B}$
 $allFamous : \mathbb{I} \rightarrow 2^E$
 $famous : E \rightarrow \mathbb{B}$
 $roundReceived : E \rightarrow \mathbb{N}$
 $timeReceived : E \rightarrow T$

FIG. 10A

$$\begin{aligned}
\text{ancestor}(x, y) &::= (x = y) \vee (\exists z \in \text{parents}(x) : \text{ancestor}(z, y)) \\
\text{selfAncestor}(x, y) &::= \text{ancestor}(x, y) \wedge ((\text{selfParent}(x) = y) \vee \text{selfAncestor}(\text{selfParent}(x), y)) \\
\text{see}(x, y) &::= \text{ancestor}(x, y) \wedge \neg(\exists u, b, c \in E : \\
&\quad (\text{ancestor}(y, u) \wedge \text{ancestor}(y, b) \wedge c \in \text{parents}(x) \wedge c \in \text{parents}(b)) \wedge \\
&\quad \text{creator}(u) = \text{creator}(b) = \text{creator}(c)) \\
\text{stronglySee}(x, y) &::= \text{see}(x, y) \wedge (\exists S \in 2^E : (|S| = m) \wedge (z \in S \iff (\text{see}(x, z) \wedge \text{see}(z, y)))) \\
\text{parentRound}(x) &::= \begin{cases} 0 & \text{if } x = \text{first} \\ \max_{y \in \text{parents}(x)} \text{round}(y) & \text{otherwise} \end{cases} \\
\text{witness}(x) &::= \exists S \in 2^E : (|S| = m \wedge \\
&\quad (\forall y \in S : (\text{round}(y) = \text{parentRound}(x) \wedge \text{stronglySee}(x, y)))) \\
\text{round}(x) &::= \begin{cases} 1 + \text{parentRound}(x) & \text{if witness}(x) \\ \text{parentRound}(x) & \text{otherwise} \end{cases} \\
\text{roundDiff}(x, y) &::= \text{round}(x) - \text{round}(y) \\
\text{votes}(x, y, v) &::= |\{z \in E : (\text{see}(x, z) \wedge \text{roundDiff}(x, z) = 1 \wedge \\
&\quad \text{stronglySee}(x, z) \wedge \text{vote}(z, y) = v)\}| \\
\text{voteFraction}(x, y) &::= \text{votes}(x, \text{true}) / (\text{votes}(x, \text{true}) + \text{votes}(x, \text{false})) \\
\text{vote}(x, y) &::= \begin{cases} \text{see}(x, y) & \text{if roundDiff}(x, y) = 1 \\ (\text{voteFraction}(x, y) \geq 1/2) & \text{if } (\text{roundDiff}(x, y) \bmod 5 \neq 1) \vee \\ & |\text{voteFraction}(x, y) - 1/2| > 1/6 \\ (1 = \text{LSB}(\text{signature}(x))) & \text{otherwise} \end{cases} \\
\text{decide}(x, y) &::= \text{vote}(x, y) \wedge (\text{roundDiff}(x, y) \bmod 5 \neq 1) \wedge (\text{voteFraction}(x, y) > 2/3) \\
\text{allFamous}(r) &::= \{x \in E : \text{famous}(x) \wedge \text{round}(x) = r\} \\
\text{famous}(x) &::= \text{witness}(x) \wedge \exists y \in E : \text{decide}(y, x) \\
\text{roundReceived}(x) &::= \min_{\text{ens}}(|\{y \in E : \text{round}(y) = r \wedge \text{famous}(y) \wedge \text{see}(y, x)\}| / \\
&\quad |\{y \in E : \text{round}(y) = r \wedge \text{famous}(y)\}|) \geq 1/2 \\
\text{timeReceived}(x) &::= \text{median}(\{\text{time}(y) : y \in E \wedge \text{see}(y, x) \wedge \\
&\quad (\exists z \in E : \text{round}(z) = \text{roundReceived}(x) \wedge \text{selfAncestor}(z, y)) \wedge \\
&\quad \neg(\exists w \in E : \text{selfAncestor}(y, w) \wedge \text{see}(w, x))\})
\end{aligned}$$

FIG. 10B

An event is a tuple $e = \{d, h, t, c, s\}$ where:

d	$= data(e)$	$=$ the “payload” data, which may include transactions.
h	$= hashes(e)$	$=$ a list of hashes of the event’s parents, self-parent first.
t	$= time(e)$	$=$ creator’s claimed date and time of the event’s creation.
i	$= creator(e)$	$=$ creator’s ID number.
s	$= sig(e)$	$=$ creator’s digital signature of $\{d, h, t, c\}$.
n	$=$	the number of members in the population
c	$=$	frequency of coin rounds (e.g., $c = 6$)
E	$=$	(the set of all events) $\cup \{\emptyset\}$
T	$=$	set of all possible $(time, date)$ pairs
$\mathbb{B}$	$=$	$\{true, false\}$
$\mathbb{N}$	$=$	$\{0, 1, 2, \dots\}$
parents	$:$	$E \rightarrow 2^E$
selfParent	$:$	$E \rightarrow E$
ancestor	$:$	$E \times E \rightarrow \mathbb{B}$
selfAncestor	$:$	$E \times E \rightarrow \mathbb{B}$
see	$:$	$E \times E \rightarrow \mathbb{B}$
stronglySee	$:$	$E \times E \rightarrow \mathbb{B}$
parentRound	$:$	$E \rightarrow \mathbb{N}$
roundInc	$:$	$E \rightarrow \mathbb{B}$
round	$:$	$E \rightarrow \mathbb{N}$
witness	$:$	$E \rightarrow \mathbb{B}$
roundDiff	$:$	$E \times E \rightarrow \mathbb{I}$
votes	$:$	$E \times E \times \mathbb{B} \rightarrow \mathbb{N}$
fractTrue	$:$	$E \times E \rightarrow \mathbb{R}$
decide	$:$	$E \times E \rightarrow \mathbb{B}$
vote	$:$	$E \times E \rightarrow \mathbb{B}$
famous	$:$	$E \rightarrow \mathbb{B}$
roundReceived	$:$	$E \rightarrow \mathbb{N}$
timeReceived	$:$	$E \rightarrow T$

FIG. 11A

$\text{parents}(x)$	$\equiv$	set of parents of event x
$\text{selfParent}(x)$	$\equiv$	the self-parent of event x , or $\emptyset$ if none
$\text{ancestor}(x, y)$	$\equiv$	$(x \neq \emptyset) \wedge ((x = y) \vee (\exists z \in \text{parents}(x) : \text{ancestor}(z, y)))$
$\text{selfAncestor}(x, y)$	$\equiv$	$(x \neq \emptyset) \wedge ((x = y) \vee \text{selfAncestor}(\text{selfParent}(x), y))$
$\text{see}(x, y)$	$\equiv$	$\text{ancestor}(x, y) \wedge \neg(\exists a, b \in E : \text{creator}(y) = \text{creator}(a) = \text{creator}(b) \wedge$ $\text{ancestor}(x, a) \wedge \text{ancestor}(x, b) \wedge \neg \text{selfAncestor}(a, b) \wedge \neg \text{selfAncestor}(b, a))$
$\text{stronglySee}(x, y)$	$\equiv$	$\text{see}(x, y) \wedge (\exists S \in 2^E : (S > 2n/3) \wedge (x \in S \iff (\text{see}(x, x) \wedge \text{see}(x, y))))$
$\text{parentRound}(x)$	$\equiv$	$\max(\{0\} \cup \{\text{round}(y) y \in \text{parents}(x)\})$
$\text{roundInc}(x)$	$\equiv$	$\exists S \in 2^E : (S > 2n/3 \wedge$ $(\forall y \in S : (\text{round}(y) = \text{parentRound}(x) \wedge \text{stronglySee}(x, y))))$
$\text{round}(x)$	$\equiv$	$\text{parentRound}(x) + \begin{cases} 1 & \text{if } \text{roundInc}(x) \\ 0 & \text{otherwise} \end{cases}$
$\text{witness}(x)$	$\equiv$	$(\text{selfParent}(x) = \emptyset) \vee (\text{round}(x) > \text{round}(\text{selfParent}(x)))$
$\text{roundDiff}(x, y)$	$\equiv$	$\text{round}(x) - \text{round}(y)$
$\text{votes}(x, y, v)$	$\equiv$	$ \{z \in E \mid \text{roundDiff}(x, z) = 1 \wedge \text{stronglySee}(x, z) \wedge \text{vote}(z, y) = v\} $
$\text{fractTrue}(x, y)$	$\equiv$	$\frac{\text{votes}(x, y, \text{true})}{(\text{votes}(x, y, \text{true}) + \text{votes}(x, y, \text{false}))}$
$\text{decide}(x, y)$	$\equiv$	$(x \neq \emptyset) \wedge (\text{roundDiff}(x, y) > 1) \wedge (\text{decide}(\text{selfParent}(x), y) \vee$ $(\text{witness}(x) \wedge (\text{roundDiff}(x, y) \bmod c \neq 1) \wedge \neg(\frac{1}{3} \leq \text{fractTrue}(x, y) \leq \frac{2n}{3})))$
$\text{vote}(x, y)$	$\equiv$	$\begin{cases} \text{vote}(\text{selfParent}(x), y) & \text{if } (\neg \text{witness}(x)) \vee \text{decide}(\text{selfParent}(x), y) \\ 1 = \text{middleBit}(\text{signature}(x)) & \text{if } \text{witness}(x) \\ & \wedge \neg \text{decide}(\text{selfParent}(x), y) \\ & \wedge (\text{roundDiff}(x, y) \neq 1) \\ & \wedge (\text{roundDiff}(x, y) \bmod c = 1) \\ \text{fractTrue}(x, y) \geq \frac{1}{2} & \text{otherwise} \end{cases}$
$\text{famous}(x)$	$\equiv$	$\text{witness}(x) \wedge \exists y \in E : \text{decide}(y, x) \wedge \text{vote}(y, x)$
$\text{roundReceived}(x)$	$\equiv$	$\min_{y \in E} \frac{ \{y \in E \mid (\text{round}(y) = x) \wedge \text{famous}(y) \wedge \text{see}(y, x)\} }{ \{y \in E \mid (\text{round}(y) = x) \wedge \text{famous}(y)\} } \geq 1/2$
$\text{timeReceived}(x)$	$\equiv$	$\text{median}(\{\text{time}(y) \mid y \in E \wedge \text{see}(y, x) \wedge$ $(\exists z \in E : \text{round}(z) = \text{roundReceived}(x) \wedge \text{selfAncestor}(z, y)) \wedge$ $\neg(\exists w \in E : \text{selfAncestor}(y, w) \wedge \text{see}(w, x))\})$

FIG. 11B

An event is a tuple $e = \{d, h, t, i, s\}$ where:

d	$= data(e)$	$=$ the “payload” data, which may include transactions.
h	$= hashes(e)$	$=$ a list of hashes of the event’s parents, self-parent first.
t	$= time(e)$	$=$ creator’s claimed date and time of the event’s creation.
i	$= creator(e)$	$=$ creator’s ID number.
s	$= sig(e)$	$=$ creator’s digital signature of $\{d, h, t, i\}$.
$parents(x)$	$=$	set of events that are parents of event x
$selfParent(x)$	$=$	the self-parent of event x , or $\emptyset$ if none
n	$=$	the number of members in the population
c	$=$	frequency of coin rounds (such as $c = 10$)
E	$=$	the set of all events in the hashgraph
E_0	$=$	$E \cup \{\emptyset\}$
$\mathbb{T}$	$=$	set of all possible $(time, date)$ pairs
$\mathbb{B}$	$=$	$\{true, false\}$
$\mathbb{N}$	$=$	$\{1, 2, 3, \dots\}$
$parents$	$:$	$E \rightarrow 2^E$
$selfParent$	$:$	$E \rightarrow E_0$
$ancestor$	$:$	$E \times E \rightarrow \mathbb{B}$
$selfAncestor$	$:$	$E \times E \rightarrow \mathbb{B}$
$manyCreators$	$:$	$2^E \rightarrow \mathbb{B}$
see	$:$	$E \times E \rightarrow \mathbb{B}$
$stronglySee$	$:$	$E \times E \rightarrow \mathbb{B}$
$parentRound$	$:$	$E \rightarrow \mathbb{N}$
$roundInc$	$:$	$E \rightarrow \mathbb{B}$
$round$	$:$	$E \rightarrow \mathbb{N}$
$witness$	$:$	$E \rightarrow \mathbb{B}$
$diff$	$:$	$E \times E \rightarrow \mathbb{I}$
$votes$	$:$	$E \times E \times \mathbb{B} \rightarrow \mathbb{N}$
$fractTrue$	$:$	$E \times E \rightarrow \mathbb{R}$
$decide$	$:$	$E \times E \rightarrow \mathbb{B}$
$copyVote$	$:$	$E \times E \rightarrow \mathbb{B}$
$vote$	$:$	$E \times E \rightarrow \mathbb{B}$
$famous$	$:$	$E \rightarrow \mathbb{B}$
$uniqueFamous$	$:$	$E \rightarrow \mathbb{B}$
$roundsDecided$	$:$	$\mathbb{N} \rightarrow \mathbb{B}$
$roundReceived$	$:$	$E \rightarrow \mathbb{N}$
$timeReceived$	$:$	$E \rightarrow \mathbb{T}$

FIG. 12A

$$\begin{aligned}
\text{ancestor}(x, y) &= x = y \vee \exists z \in \text{parents}(x), \text{ancestor}(z, y) \\
\text{selfAncestor}(x, y) &= x = y \vee (\text{selfParent}(x) \neq \emptyset \wedge \text{selfAncestor}(\text{selfParent}(x), y)) \\
\text{manyCreators}(S) &= |S| > 2n/3 \wedge \forall x, y \in S, (x \neq y \implies \text{creator}(x) \neq \text{creator}(y)) \\
\text{see}(x, y) &= \text{ancestor}(x, y) \wedge \neg(\exists a, b \in E, \text{creator}(y) = \text{creator}(a) = \text{creator}(b) \wedge \\
&\quad \text{ancestor}(x, a) \wedge \text{ancestor}(x, b) \wedge \neg \text{selfAncestor}(a, b) \wedge \neg \text{selfAncestor}(b, a)) \\
\text{stronglySee}(x, y) &= \text{see}(x, y) \wedge (\exists S \subseteq E, \text{manyCreators}(S) \\
&\quad \wedge (z \in S \implies (\text{see}(x, z) \wedge \text{see}(z, y)))) \\
\text{parentRound}(x) &= \max(\{1\} \cup \{\text{round}(y) \mid y \in \text{parents}(x)\}) \\
\text{roundInc}(x) &= \exists S \subseteq E, \text{manyCreators}(S) \\
&\quad \wedge (\forall y \in S, \text{round}(y) = \text{parentRound}(x) \wedge \text{stronglySee}(x, y)) \\
\text{round}(x) &= \text{parentRound}(x) + \begin{cases} 1 & \text{if } \text{roundInc}(x) \\ 0 & \text{otherwise} \end{cases} \\
\text{witness}(x) &= (\text{selfParent}(x) = \emptyset) \vee (\text{round}(x) > \text{round}(\text{selfParent}(x))) \\
\text{diff}(x, y) &= \text{round}(x) - \text{round}(y) \\
\text{votes}(x, y, v) &= |\{z \in E \mid \text{diff}(x, z) = 1 \wedge \text{witness}(z) \wedge \text{stronglySee}(x, z) \wedge \text{vote}(z, y) = v\}| \\
\text{fractTrue}(x, y) &= \frac{\text{votes}(x, y, \text{true})}{(\text{votes}(x, y, \text{true}) + \text{votes}(x, y, \text{false}))} \\
\text{decide}(x, y) &= (\text{selfParent}(x) \neq \emptyset \wedge \text{decide}(\text{selfParent}(x), y)) \vee (\wedge \text{witness}(x) \wedge \text{witness}(y) \\
&\quad \wedge \text{diff}(x, y) > 1 \wedge (\text{diff}(x, y) \bmod c > 0) \wedge (\exists v \in B, \text{votes}(x, y, v) > \frac{2n}{3})) \\
\text{copyVote}(x, y) &= (\neg \text{witness}(x)) \vee (\text{selfParent}(x) \neq \emptyset \wedge \text{decide}(\text{selfParent}(x), y)) \\
\text{vote}(x, y) &= \begin{cases} \text{vote}(\text{selfParent}(x), y) & \text{if } \text{copyVote}(x) \\ 1 - \text{middleBit}(\text{signature}(x)) & \text{if } \neg \text{copyVote}(x) \\ \quad \wedge (\text{diff}(x, y) \bmod c = 0) \\ \quad \wedge (\frac{1}{3} \leq \text{fractTrue}(x, y) \leq \frac{2}{3}) \\ \text{fractTrue}(x, y) \geq \frac{1}{2} & \text{otherwise} \end{cases} \\
\text{famous}(x) &= \exists y \in E, \text{decide}(y, x) \wedge \text{vote}(y, x) \\
\text{uniqueFamous}(x) &= \text{famous}(x) \wedge \neg \exists y \in E, y \neq x \wedge \text{famous}(y) \\
&\quad \wedge \text{round}(x) = \text{round}(y) \wedge \text{creator}(x) = \text{creator}(y) \\
\text{roundsDecided}(r) &= \forall x \in E, ((\text{round}(x) \leq r \wedge \text{witness}(x)) \implies \exists y \in E, \text{decide}(y, x)) \\
\text{roundReceived}(x) &= \min(\{r \in \mathbb{N} \mid \text{roundsDecided}(r) \wedge (\forall y \in E, \\
&\quad (\text{round}(y) = r \wedge \text{uniqueFamous}(y)) \implies \text{ancestor}(y, x)\}) \\
\text{timeReceived}(x) &= \text{median}(\{\text{time}(y) \mid y \in E \wedge \text{ancestor}(y, x) \wedge \\
&\quad (\exists z \in E, \text{round}(z) = \text{roundReceived}(x) \wedge \text{uniqueFamous}(z) \\
&\quad \wedge \text{selfAncestor}(z, y)) \wedge \neg(\exists w \in E, \text{selfAncestor}(y, w) \wedge \text{ancestor}(w, x))\})
\end{aligned}$$

FIG. 12B

An event is a tuple $x = \{p, h, t, i, s\}$ where:

p = payload(x) = the “payload” data, such as a list of transactions
 h = hashes(x) = a list of hashes of the event’s parents, self-parent first
 t = time(x) = creator’s claimed date and time of the event’s creation
 i = creator(x) = creator’s ID number
 s = signature(x) = creator’s digital signature of $\{p, h, t, i\}$

selfParent(x) = the self-parent of event x , or $\emptyset$ if none
 otherParent(x) = the other-parent of event x , or $\emptyset$ if none
 parents(x) = the set of events that are parents (self or other) of event x
 stake(m) = The amount of stake that member m has, or 0 if $m = \emptyset$
 c = frequency of coin rounds (such as $c = 10$)
 $\mathbb{T}$ = set of all possible (time, date) pairs
 E = the set of all events in the hashgraph
 E_0 = $E \cup \{\emptyset\}$
 M = the set of all members (participating computers),
 TotalStake = total stake of the population (where member m has stake(m))
 $\mathbb{N}$ = $\{0, 1, 2, 3, \dots\}$
 $\mathbb{I}$ = $\{\dots - 2, -1, 0, 1, 2, \dots\}$
 $\mathbb{B}$ = $\{\text{true}, \text{false}\}$

The function `weightedMedian( $S$ )` returns the *weighted median* of a set S of (x_i, s_i) pairs. It is defined as the middle of a sorted list of x values, where each x_i is repeated s_i times. If there are two middle values, it is the minimum of them.

Two such lists are compared by *extended weighted median* by comparing elements in position $\{0, 1, -1, 2, -2, 3, -3, \dots\}$ until an unequal element is found, where position 0 is the middle element.

FIG. 13A

$\text{gen}(x)$	=	The generation of event x .
$\text{ancestor}(x, y)$	=	can x reach y by following 0 or more parent edges?
$\text{selfAncestor}(x, y)$	=	can x reach y by following 0 or more selfParent edges?
$\text{supermajority}(x)$	=	is number x is more than 2/3 of the total stake?
$\text{parentRound}(x)$	=	the maximum created round of all parents of x (or 1 if there are none)
$\text{lastSee}(x, m)$	=	The most recent event created by member m that is an ancestor of x .
$\text{seeThru}(x, m, m')$	=	The latest witness that event x can see that is created by m , and is seen through an event created by m' .
$\text{stronglySeeP}(x, m)$	=	The witness created by m in round $\text{parentRound}(x)$ that x can strongly see.
$\text{round}(x)$	=	The created round for event x .
$\text{firstSelfWitnessS}(x)$	=	The first witness that is a self ancestor of x in the same round as x .
$\text{firstWitnessS}(x)$	=	The first witness that is an ancestor of x in the same round as x .
$\text{stronglySeeS1}(x, m)$	=	The witness created by m in round $\text{round}(x) - 1$ that x can strongly see.
$\text{firstSee}(x, m)$	=	The most recent witness created by member m that is an ancestor of x .
$\text{witness}(x)$	=	true if x has a greater created round than its selfParent
$\text{diff}(x, y)$	=	$\text{round}(x) - \text{round}(y)$
$\text{votes}(x, y, v)$	=	the total stake of creators of votes equal to v about the fame of witness y collected by witness x from witnesses in the previous round
$\text{decide}(x, y)$	=	true iff x (or its self ancestor) "decided" for the election for witness y (and therefore that member will never change its vote about y again)
$\text{copyVote}(x, y)$	=	true iff x should simply copy its selfParent's vote about the fame of witness y (or x is not a witness, or has already decided earlier)
$\text{witnessR}(x, r)$	=	the witness in round r that is a self-ancestor of the witness x .
$\text{firstVote}(x, y)$	=	the first vote by x in the voting for the fame of y . It is true iff y is a self-ancestor of an event x can lastSee.
$\text{coin}(x)$	=	a pseudorandom boolean as a function of x . An attacker must not be able to guess it before knowing x . There must exist an ϵ such that the probabilities of true and of false are both greater than ϵ . In the implementation shown here, this is derived from the signature of x .
$\text{vote}(x, y)$	=	the vote by witness x about the fame of witness y (true for famous, false for not)
$\text{famous}(x)$	=	true iff x is famous (i.e., had its fame decided by someone, and their vote was true)
$\text{roundsDecided}(r)$	=	true iff all known witnesses had their fame decided, for both round r and all earlier rounds
$\text{received}(x, r)$	=	the set of events that are each a descendant of x and an ancestor of at least one famous witness in round r . If there are multiple by the same creator, then only the one with the earliest creation time is retained (with ties broken by least signature, lexicographically).
$\text{roundReceived}(x)$	=	the round received for event x
$\text{timeReceived}(x)$	=	the consensus timestamp for event x
$\text{before}(x, y)$	=	true iff event x is before event y in the consensus order.

FIG. 13B

IF	: $\mathbb{B} \times \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$
selfParent	: $E \rightarrow E_0$
otherParent	: $E \rightarrow E_0$
parents	: $E \rightarrow 2^E$
stake	: $M \rightarrow \mathbb{N}$
gen	: $E_0 \rightarrow \mathbb{N}$
ancestor	: $E \times E \rightarrow \mathbb{B}$
selfAncestor	: $E \times E \rightarrow \mathbb{B}$
supermajority	: $\mathbb{N} \rightarrow \mathbb{B}$
parentRound	: $E_0 \rightarrow \mathbb{N}$
lastSee	: $E_0 \times M \rightarrow E_0$
seeThru	: $E_0 \times M \rightarrow E_0$
stronglySeeP	: $E_0 \times M \times M \rightarrow E_0$
round	: $E_0 \rightarrow \mathbb{N}$
firstSelfWitnessS	: $E_0 \rightarrow E_0$
firstWitnessS	: $E_0 \rightarrow E_0$
stronglySeeS1	: $E_0 \times M \times M \rightarrow E_0$
firstSee	: $E_0 \times M \rightarrow E_0$
witness	: $E \rightarrow \mathbb{B}$
diff	: $E \times E \rightarrow \mathbb{I}$
votes	: $E \times E \times \mathbb{B} \rightarrow \mathbb{N}$
decide	: $E \times E \rightarrow \mathbb{B}$
copyVote	: $E \times E \rightarrow \mathbb{B}$
witnessR	: $E \times \mathbb{N} \rightarrow E$
firstVote	: $E \times E \rightarrow \mathbb{B}$
coin	: $E \rightarrow \mathbb{B}$
vote	: $E \times E \rightarrow \mathbb{B}$
famous	: $E \rightarrow \mathbb{B}$
roundsDecided	: $\mathbb{N} \rightarrow \mathbb{B}$
received	: $E \times \mathbb{N} \rightarrow 2^E$
roundReceived	: $E \rightarrow \mathbb{N}$
timeReceived	: $E \rightarrow \mathbb{T}$
before	: $E \times E \rightarrow \mathbb{B}$

$$\text{IF}(p, x, y) = \begin{cases} x & \text{if } p \\ y & \text{otherwise} \end{cases}$$

$$\text{gen}(x) = \begin{cases} 0 & \text{if } x = \emptyset \\ 1 & \text{if } \text{parents}(x) = \{\} \\ 1 + \max(\{\text{gen}(y) \mid y \in \text{parents}(x)\}) & \text{otherwise} \end{cases}$$

$$\text{ancestor}(x, y) = x = y \vee \exists z \in \text{parents}(x), \text{ancestor}(z, y)$$

$$\text{selfAncestor}(x, y) = x = y \vee (\text{selfParent}(x) \neq \emptyset \wedge \text{selfAncestor}(\text{selfParent}(x), y))$$

$$\text{supermajority}(x) = (x > (2/3) \text{TotalStake})$$

FIG. 13C

$$\begin{aligned}
\text{parentRound}(x) &= \max(\text{round}(\text{selfParent}(x)), \text{round}(\text{otherParent}(x))) \\
\text{lastSee}(x, m) &= \begin{cases} x & \text{if } m = \text{creator}(x) \\ \emptyset & \text{if } x = \emptyset \vee \text{parents}(x) = \{\} \\ \text{lastSee}(\text{otherParent}(x), m) & \text{if } (\text{round}(\text{lastSee}(\text{otherParent}(x), m)) \\ & > \text{round}(\text{lastSee}(\text{selfParent}(x), m))) \\ & \vee ((\text{gen}(\text{lastSee}(\text{otherParent}(x), m)) \\ & > \text{gen}(\text{lastSee}(\text{selfParent}(x), m))) \\ & \wedge (\text{firstSee}(\text{otherParent}(x), m)) \\ & = \text{firstSee}(\text{selfParent}(x), m))) \\ \text{lastSee}(\text{selfParent}(x), m) & \text{otherwise} \end{cases} \\
\text{seeThru}(x, m, m') &= \begin{cases} \text{firstSelfWitnessS}(\text{selfParent}(x)) & \text{if } m = m' = \text{creator}(x) \\ \text{firstSee}(\text{lastSee}(x, m'), m) & \text{otherwise} \end{cases} \\
\text{stronglySeeP}(x, m) &= \begin{cases} \emptyset & \text{if } x = \emptyset \\ \text{stronglySeeP}(\text{selfParent}(x), m) & \text{if } \emptyset \neq \text{stronglySeeP}(\text{selfParent}(x), m) \\ & \wedge \text{parentRound}(x) \\ & = \text{parentRound}(\text{selfParent}(x)) \\ \text{stronglySeeP}(\text{otherParent}(x), m) & \text{if } \emptyset \neq \text{stronglySeeP}(\text{otherParent}(x), m) \\ & \wedge \text{parentRound}(x) \\ & = \text{parentRound}(\text{otherParent}(x)) \\ \emptyset & \text{if } \text{round}(\text{seeThru}(x, m, m)) \\ & \neq \text{parentRound}(x) \\ \text{seeThru}(x, m, m) & \text{supermajority}(\sum_{m' \in M} (\\ & \text{IF}(\text{seeThru}(x, m, m') \\ & = \text{seeThru}(x, m, m), \\ & \text{stake}(m', 0))) \\ \emptyset & \text{otherwise} \end{cases} \\
\text{round}(x) &= \begin{cases} 0 & \text{if } x = \emptyset \\ 1 & \text{if } \text{parents}(x) = \{\} \\ \text{round}(\text{selfParent}(x)) & \text{if } \text{round}(\text{selfParent}(x)) \\ & > \text{round}(\text{otherParent}(x)) \\ \text{round}(\text{otherParent}(x)) & \text{if } \text{round}(\text{otherParent}(x)) \\ & > \text{round}(\text{selfParent}(x)) \\ \text{parentRound}(x) + 1 & \text{if } \text{supermajority}(\sum_{m' \in M} (\text{stake}(\text{creator}(\text{stronglySeeP}(x, m'))))) \\ \text{parentRound}(x) & \text{otherwise} \end{cases} \\
\text{firstSelfWitnessS}(x) &= \begin{cases} \emptyset & \text{if } x = \emptyset \\ x & \text{if } \text{round}(x) > \text{round}(\text{selfParent}(x)) \\ \text{firstSelfWitnessS}(\text{selfParent}(x)) & \text{otherwise} \end{cases} \\
\text{firstWitnessS}(x) &= \begin{cases} \emptyset & \text{if } x = \emptyset \\ x & \text{if } \text{round}(x) > \text{parentRound}(x) \\ \text{firstWitnessS}(\text{selfParent}(x)) & \text{if } \text{round}(x) = \text{round}(\text{selfParent}(x)) \\ \text{firstWitnessS}(\text{otherParent}(x)) & \text{otherwise} \end{cases} \\
\text{stronglySeeS1}(x, m) &= \text{stronglySeeP}(\text{firstWitnessS}(x), m) \\
\text{firstSee}(x, m) &= \text{firstSelfWitnessS}(\text{lastSee}(x, m))
\end{aligned}$$

FIG. 13D

$$\begin{aligned}
\text{witness}(x) &::= (\text{selfParent}(x) = \emptyset) \vee (\text{round}(x) > \text{round}(\text{selfParent}(x))) \\
\text{diff}(x, y) &::= \text{round}(x) - \text{round}(y) \\
\text{votes}(x, y, v) &::= \sum \{ \text{stake}(m) \mid m \in M \wedge v = \text{vote}(\text{stronglySeeS1}(x, m), y) \} \\
\text{decide}(x, y) &::= (\text{selfParent}(x) \neq \emptyset \wedge \text{decide}(\text{selfParent}(x), y)) \\
&\quad \vee (\text{witness}(x) \wedge \text{witness}(y) \wedge \text{diff}(x, y) > d \wedge (\text{diff}(x, y) \bmod c > 0) \\
&\quad \wedge (\text{supermajority}(\text{votes}(x, y, \text{true})) \vee \text{supermajority}(\text{votes}(x, y, \text{false})))) \\
\text{copyVote}(x, y) &::= (\neg \text{witness}(x)) \vee (\text{selfParent}(x) \neq \emptyset \wedge \text{decide}(\text{selfParent}(x), y)) \\
\text{witnessR}(x, r) &::= \begin{cases} \emptyset & \text{if } \text{round}(x) < r \\ x & \text{if } \text{round}(x) = r \\ \text{witnessR}(\text{firstSelfWitnessS}(\text{selfParent}(x)), r) & \text{otherwise} \end{cases} \\
\text{firstVote}(x, y) &::= (y = \text{witnessR}(\text{firstSee}(x, \text{creator}(y)), \text{round}(y))) \\
\text{coin}(x) &::= (1 = \text{middleBit}(\text{signature}(x))) \\
\text{vote}(x, y) &::= \begin{cases} \text{vote}(\text{selfParent}(x), y) & \text{if } \text{copyVote}(x, y) \\ \text{firstVote}(x, y) & \text{if } \text{diff}(x, y) = 1 \\ \text{coin}(x) & \text{if } (\text{diff}(x, y) \bmod c = 0) \\ & \wedge \neg \text{supermajority}(\text{votes}(x, y, \text{true})) \\ & \wedge \neg \text{supermajority}(\text{votes}(x, y, \text{false})) \\ \text{votes}(x, y, \text{true}) \geq \text{votes}(x, y, \text{false}) & \text{otherwise} \end{cases} \\
\text{famous}(x) &::= \exists y \in E, \text{decide}(y, x) \wedge \text{vote}(y, x) \\
\text{roundsDecided}(r) &::= \forall x \in E, ((\text{round}(x) \leq r \wedge \text{witness}(x)) \implies \exists y \in E, \text{decide}(y, x)) \\
\text{received}(x, r) &::= \{ y \in E \mid \exists z \in E, \text{round}(z) = r \wedge \text{famous}(z) \wedge \text{ancestor}(z, y) \wedge \text{ancestor}(y, x) \\
&\quad \wedge \neg \exists y' \in E, (\text{creator}(y') = \text{creator}(y) \wedge \text{ancestor}(x, y') \wedge \text{ancestor}(y', x) \wedge \\
&\quad (\text{time}(y') < \text{time}(y) \vee (\text{time}(y') = \text{time}(y) \wedge \text{signature}(y') < \text{signature}(y))) \} \\
\text{roundReceived}(x) &::= \min(\{ r \in \mathbb{N} \mid \text{supermajority}(\Sigma \{ \text{stake}(\text{creator}(e)) \mid e \in \text{received}(x, r) \}) \}) \\
\text{timeReceived}(x) &::= \text{weightedMedian}(\{ (\text{time}(y), \text{stake}(\text{creator}(y))) \mid y \in \text{received}(x, r) \}) \\
\text{before}(x, y) &::= \begin{cases} \text{roundReceived}(x) < \text{roundReceived}(y) & \text{if } \text{roundReceived}(x) \\ & \neq \text{roundReceived}(y) \\ \text{timeReceived}(x) < \text{timeReceived}(y) & \text{if } \text{timeReceived}(x) \\ & \neq \text{timeReceived}(y) \\ f(x) < f(y) & \text{otherwise} \end{cases}
\end{aligned}$$

The consensus order is determined by sorting by $\text{before}(x, y)$, where f is any total order, such as sorting by the extended weighted median of the received times, then breaking ties by generation, then breaking ties by whitened signature (signature XORed with all signatures of famous witnesses in the received round).

FIG. 13E

Address Book 1400

Compute Device	Public Key	Stake
110	A	100
120	B	50
130	C	30
140	D	75

FIG. 14

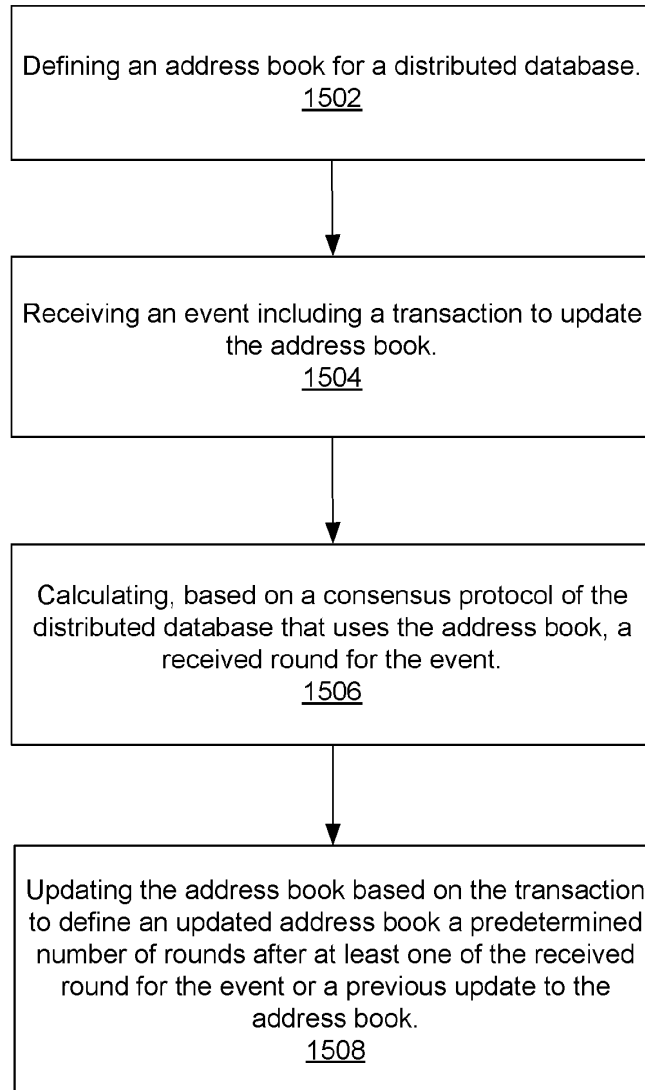
1500

FIG. 15

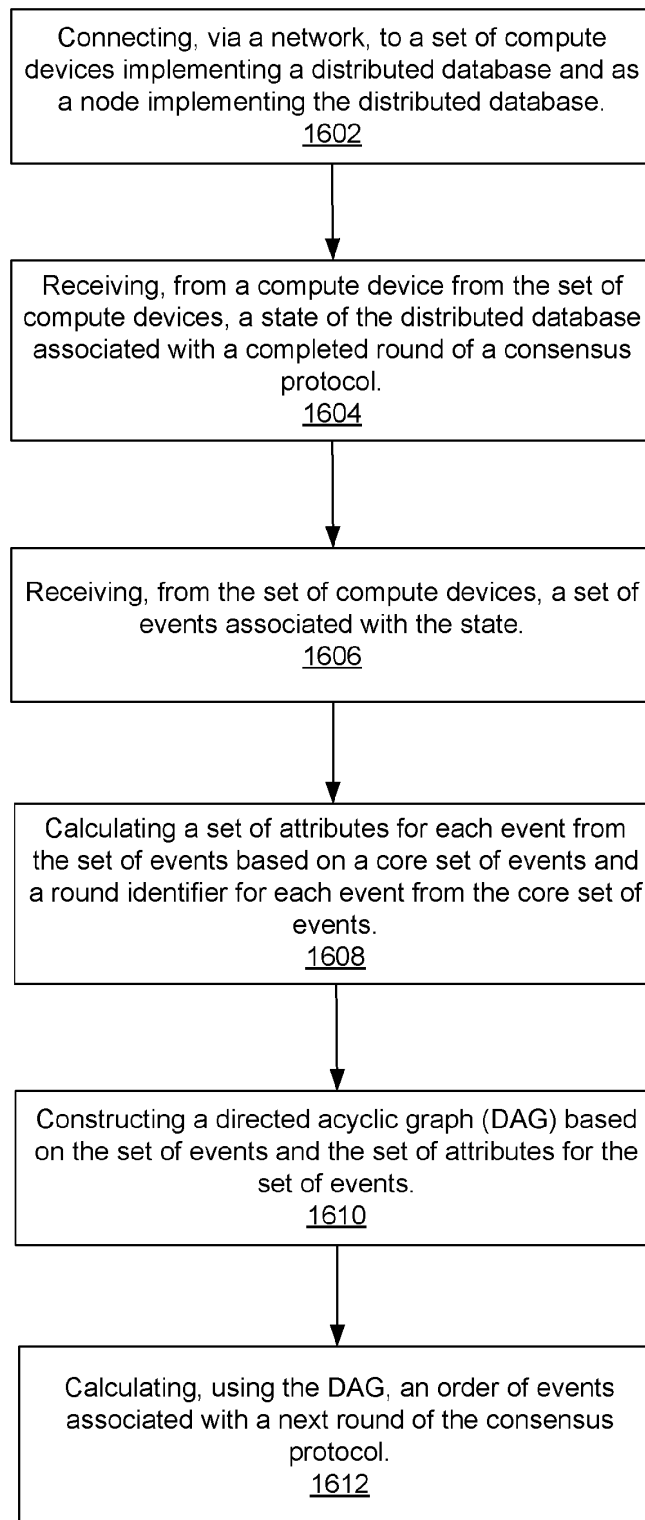
1600

FIG. 16