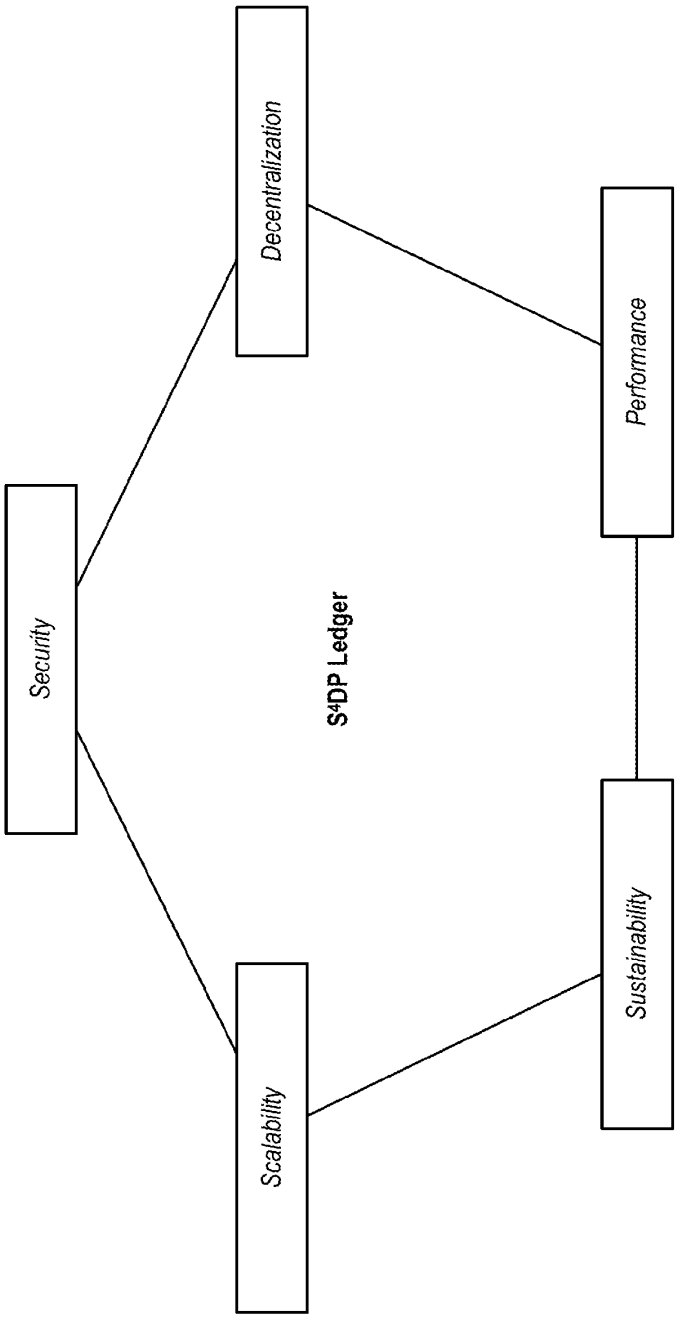

Decentralization
Performance
Security
S⁴DP Ledger
Sustainability
Scalability

FIG. 1

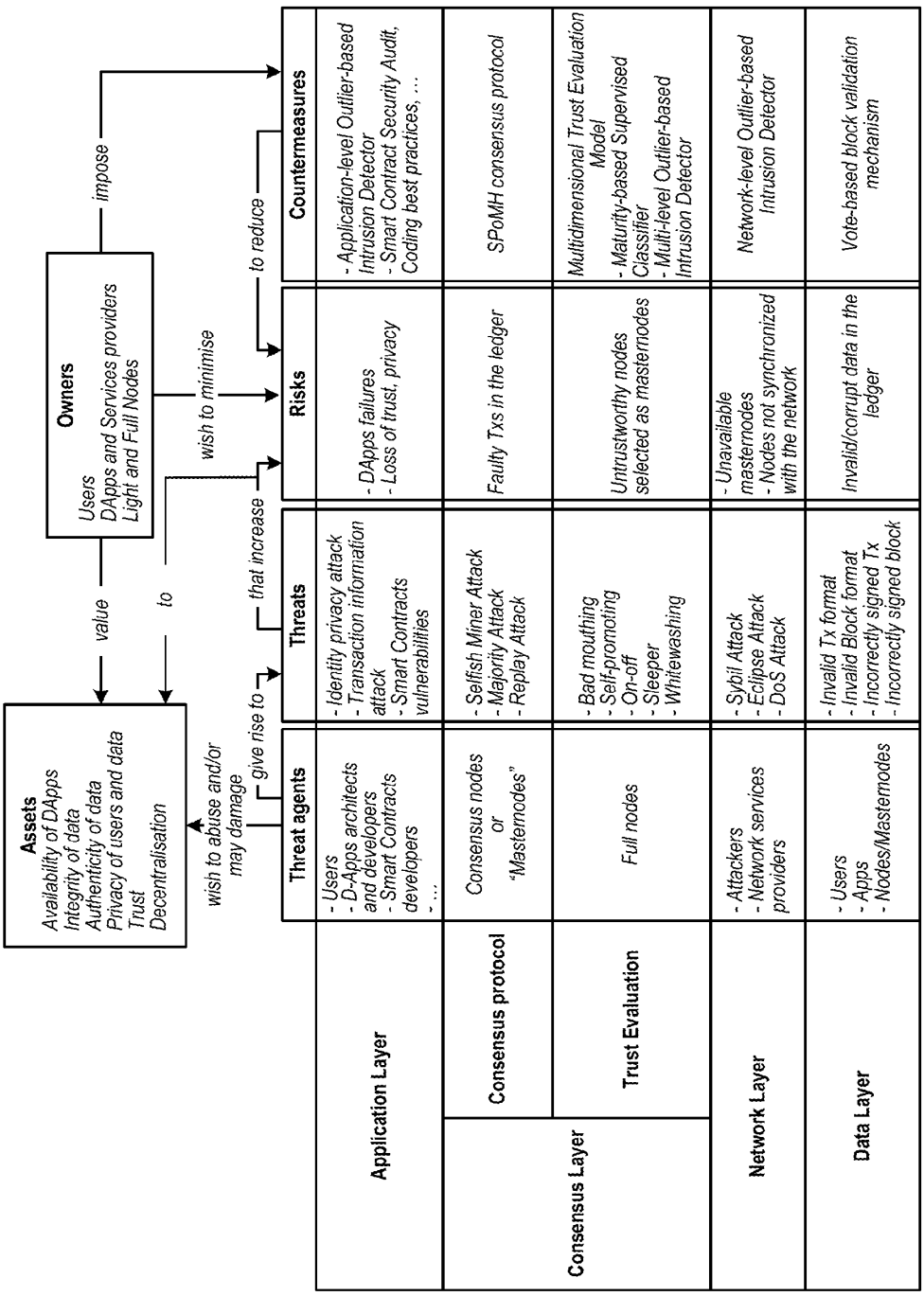

Assets
Availability of DApps
Integrity of data
Authenticity of data
Privacy of users and data
Trust
Decentralisation
value
to
Owners
Users
DApps and Services providers
Light and Full Nodes
impose
wish to minimise
to reduce
wish to abuse and/or
may damage
give rise to
that increase
Threat agents
Threats
Risks
Countermeasures
Application Layer
- Users
- D-Apps architects and developers
- Smart Contracts developers
- ...
- Identity privacy attack
- Transaction information attack
- Smart Contracts vulnerabilities
- DApps failures
- Loss of trust, privacy
- Application-level Outlier-based Intrusion Detector
- Smart Contract Security Audit, Coding best practices, ...
Consensus Layer
Consensus protocol
Consensus nodes or "Masternodes"
- Selfish Miner Attack
- Majority Attack
- Replay Attack
Faulty Txs in the ledger
SPoMH consensus protocol
Trust Evaluation
Full nodes
- Bad mouthing
- Self-promoting
- On-off
- Sleeper
- Whitewashing
Untrustworthy nodes selected as masternodes
Multidimensional Trust Evaluation Model
- Maturity-based Supervised Classifier
- Multi-level Outlier-based Intrusion Detector
Network Layer
- Attackers
- Network services providers
- Sybil Attack
- Eclipse Attack
- DoS Attack
- Unavailable masternodes
- Nodes not synchronized with the network
Network-level Outlier-based Intrusion Detector
Data Layer
- Users
- Apps
- Nodes/Masternodes
- Invalid Tx format
- Invalid Block format
- Incorrectly signed Tx
- Incorrectly signed block
Invalid/corrupt data in the ledger
Vote-based block validation mechanism

FIG. 2

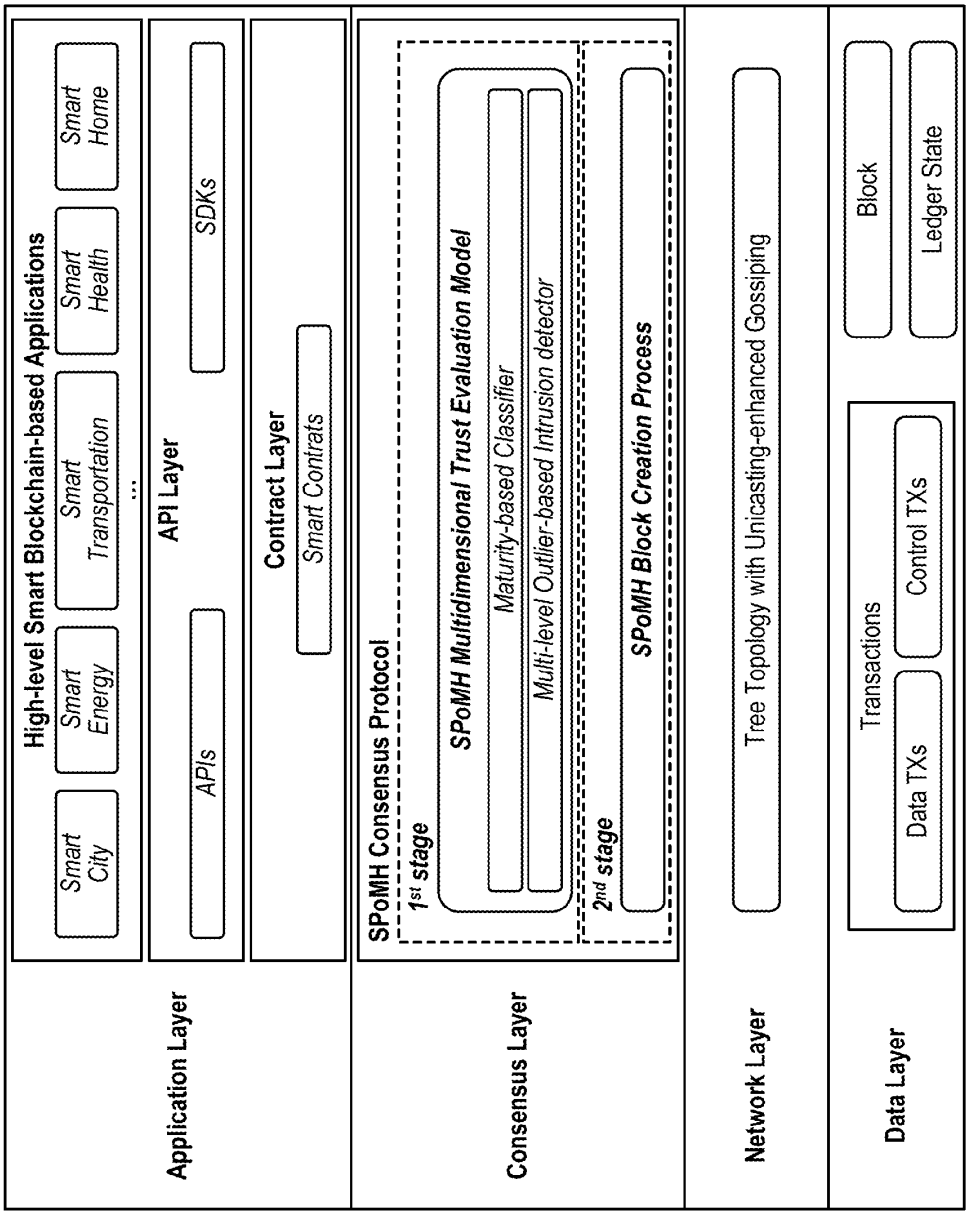

Application Layer
High-level Smart Blockchain-based Applications
Smart City
Smart Energy
Smart Transportation
...
Smart Health
Smart Home
API Layer
APIs
SDKs
Contract Layer
Smart Contrats
Consensus Layer
SPoMH Consensus Protocol
1st stage
SPoMH Multidimensional Trust Evaluation Model
Maturity-based Classifier
Multi-level Outlier-based Intrusion detector
2nd stage
SPoMH Block Creation Process
Network Layer
Tree Topology with Unicasting-enhanced Gossiping
Data Layer
Transactions
Data TXs
Control TXs
Block
Ledger State

FIG. 3

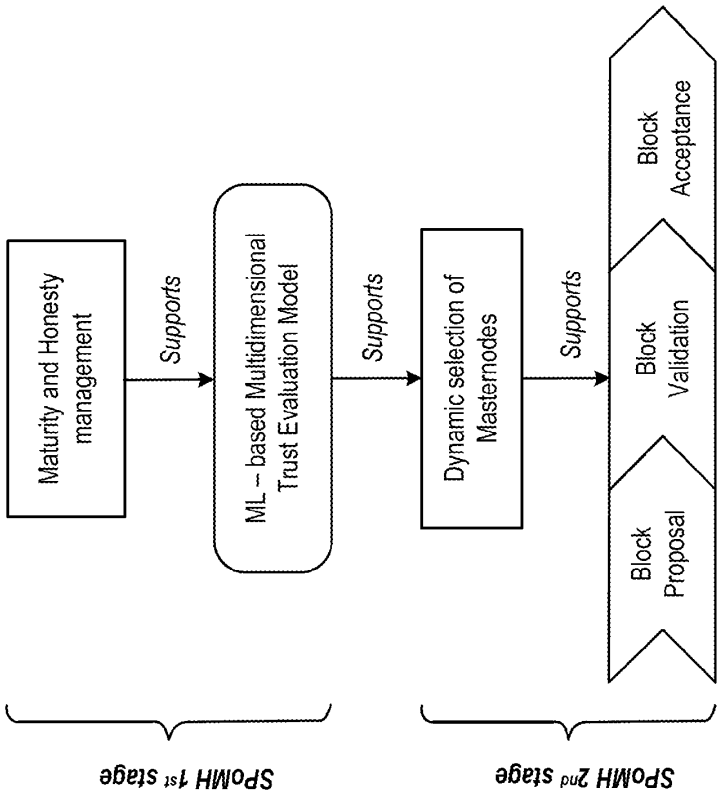

Maturity and Honesty management
Supports
ML – based Multidimensional Trust Evaluation Model
Supports
Dynamic selection of Masternodes
Supports
Block Proposal
Block Validation
Block Acceptance
SPoMH 1st stage
SPoMH 2nd stage

FIG. 4

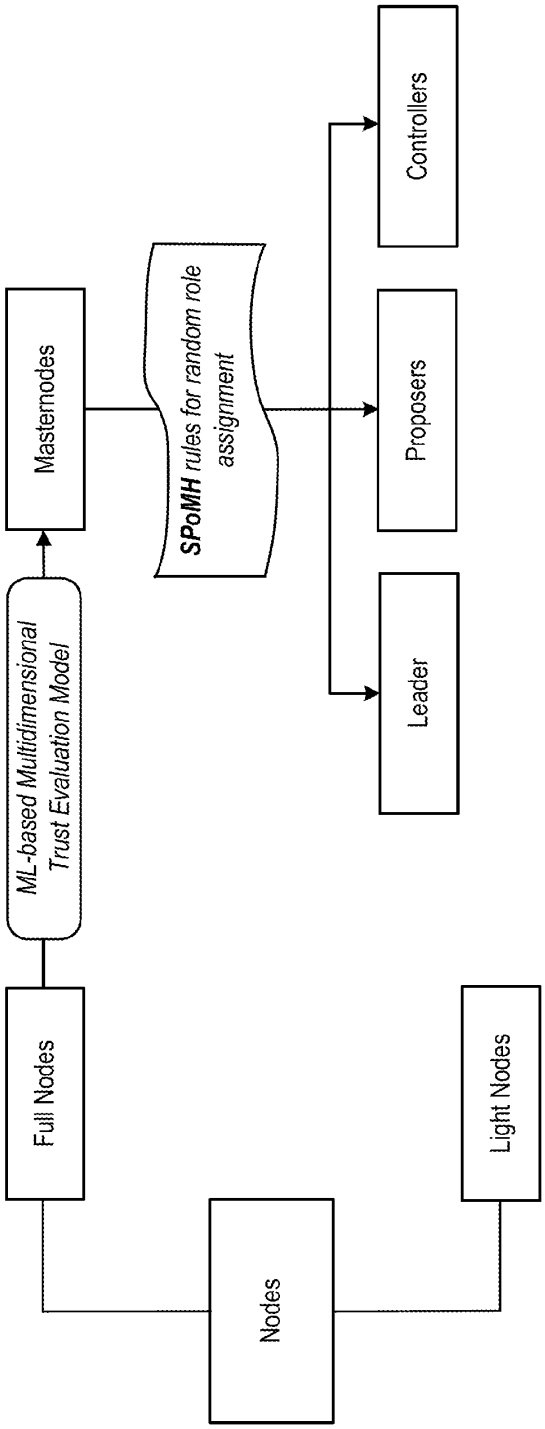

Nodes
Full Nodes
Light Nodes
ML-based Multidimensional Trust Evaluation Model
Masternodes
SPoMH rules for random role assignment
Controllers
Proposers
Leader

FIG. 5

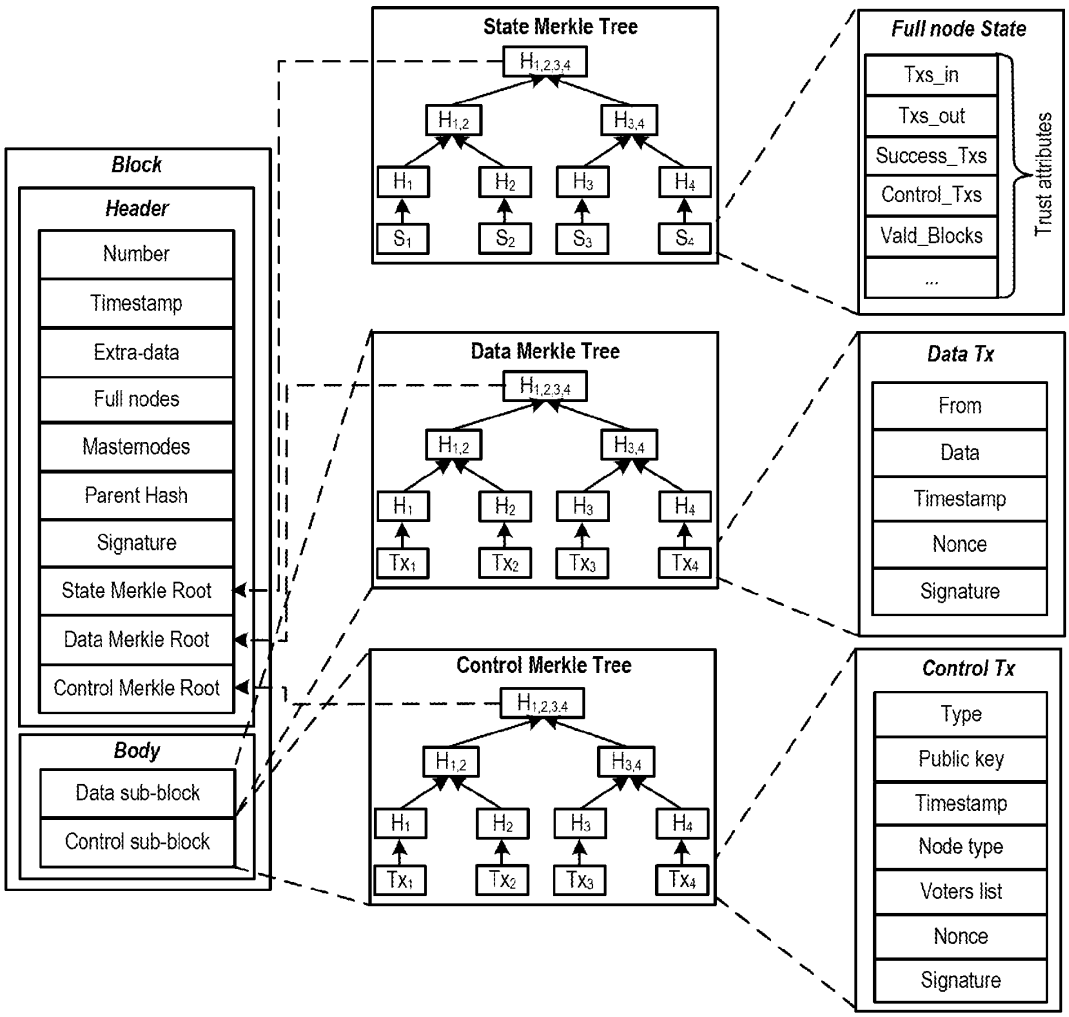

Block
Header
Number
Timestamp
Extra-data
Full nodes
Masternodes
Parent Hash
Signature
State Merkle Root
Data Merkle Root
Control Merkle Root
Body
Data sub-block
Control sub-block
State Merkle Tree
H1,2,3,4
H1,2
H3,4
H1
H2
H3
H4
S1
S2
S3
S4
Data Merkle Tree
Tx1
Tx2
Tx3
Tx4
Control Merkle Tree
Full node State
Txs_in
Txs_out
Success_Txs
Control_Txs
Vald_Blocks
...
Trust attributes
Data Tx
From
Data
Timestamp
Nonce
Signature
Control Tx
Type
Public key
Timestamp
Node type
Voters list
Nonce
Signature

FIG. 6

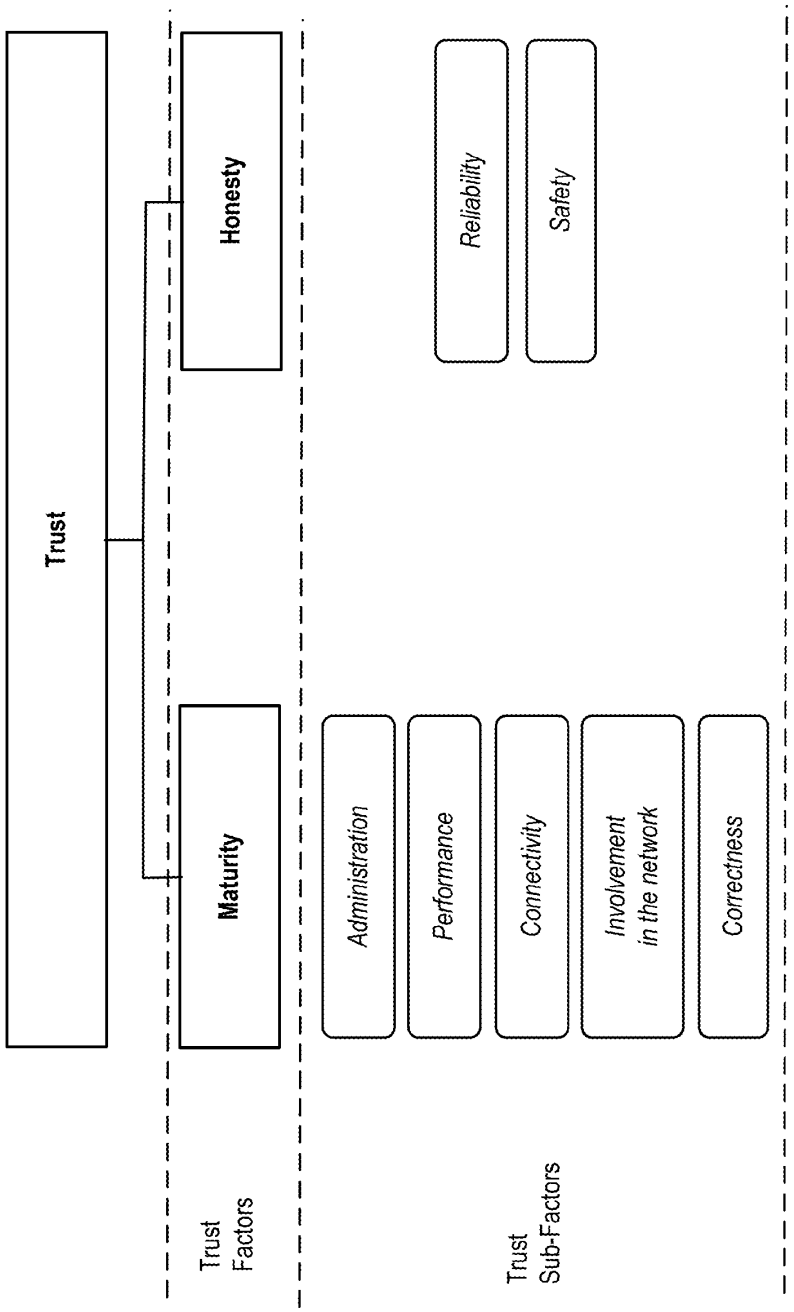

Trust
Honesty
Maturity
Reliability
Safety
Administration
Performance
Connectivity
Involvement in the network
Correctness
Trust Factors
Trust Sub-Factors

FIG. 7

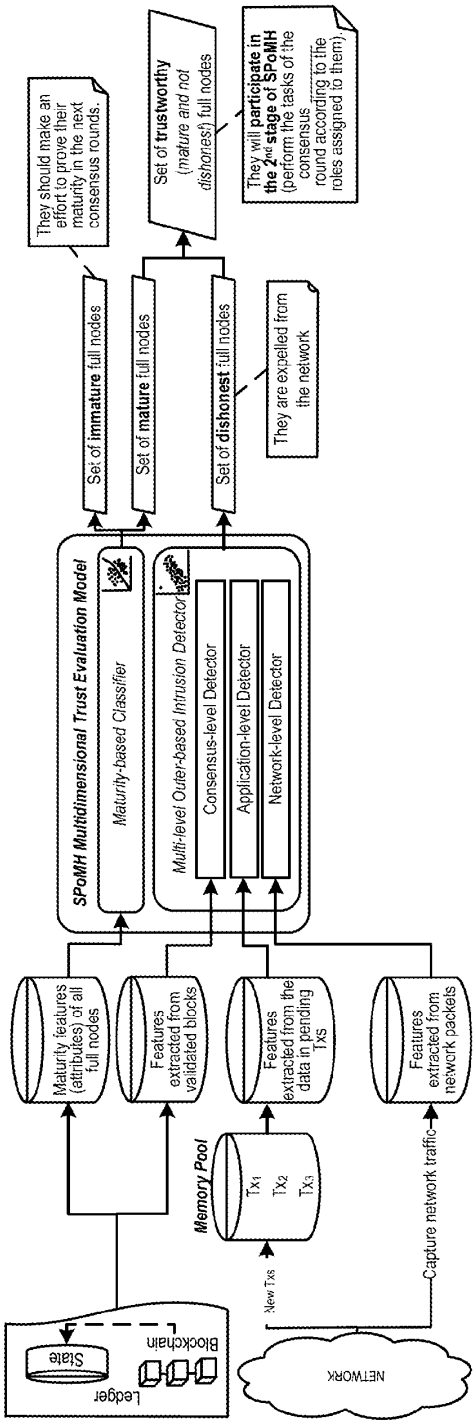

They should make an effort to prove their maturity in the next consensus rounds.
Set of trustworthy (mature and not dishonest) full nodes
They will participate in the 2nd stage of SPoMH (perform the tasks of the consensus round according to the roles assigned to them).
Set of immature full nodes
Set of mature full nodes
Set of dishonest full nodes
They are expelled from the network
SPoMH Multidimensional Trust Evaluation Model
Maturity-based Classifier
Multi-level Outer-based Intrusion Detector
Consensus-level Detector
Application-level Detector
Network-level Detector
Maturity features (attributes) of all full nodes
Features extracted from validated blocks
Features extracted from the data in pending Txs
Features extracted from network packets
Memory Pool
Tx1
Tx2
Tx3
New Txs
Capture network traffic
Blockchain
State
Ledger
NETWORK

FIG. 8

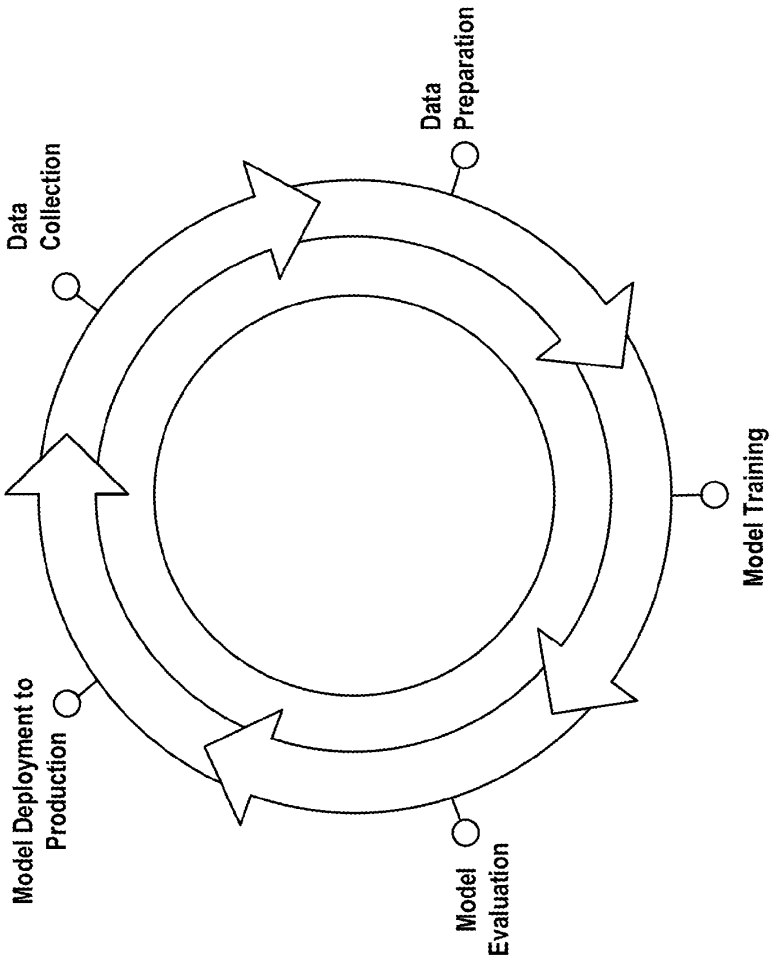

Data Preparation
Model Training
Model Evaluation
Model Deployment to Production
Data Collection

FIG. 9

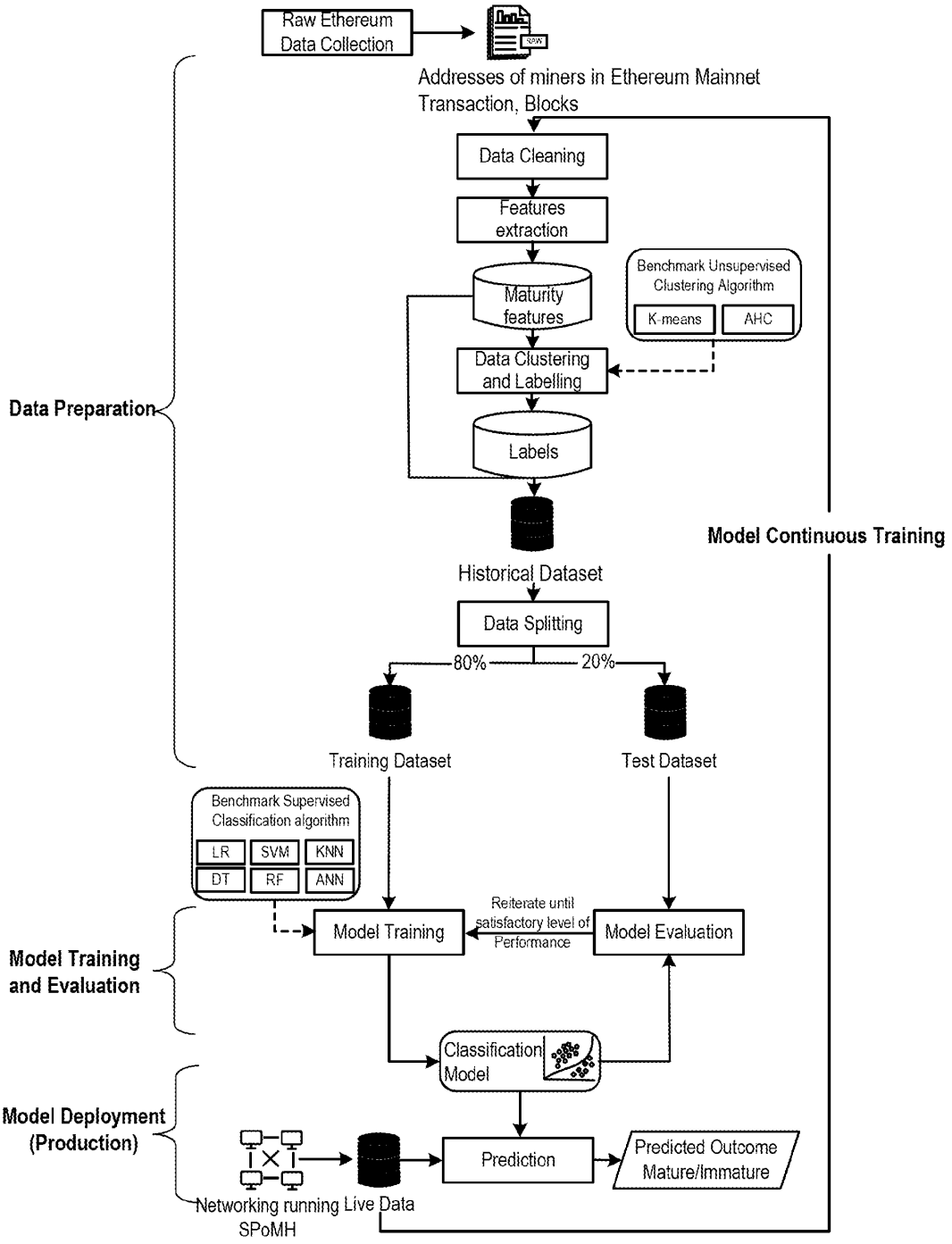

Raw Ethereum Data Collection
Addresses of miners in Ethereum Mainnet
Transaction, Blocks
Data Cleaning
Features extraction
Benchmark Unsupervised Clustering Algorithm
K-means
AHC
Maturity features
Data Clustering and Labelling
Labels
Historical Dataset
Data Splitting
80%
20%
Training Dataset
Test Dataset
Benchmark Supervised Classification algorithm
LR
SVM
KNN
DT
RF
ANN
Model Training
Reiterate until satisfactory level of Performance
Model Evaluation
Classification Model
Prediction
Predicted Outcome Mature/Immature
Networking running Live Data SPoMH
Data Preparation
Model Training and Evaluation
Model Deployment (Production)
Model Continuous Training

FIG. 10

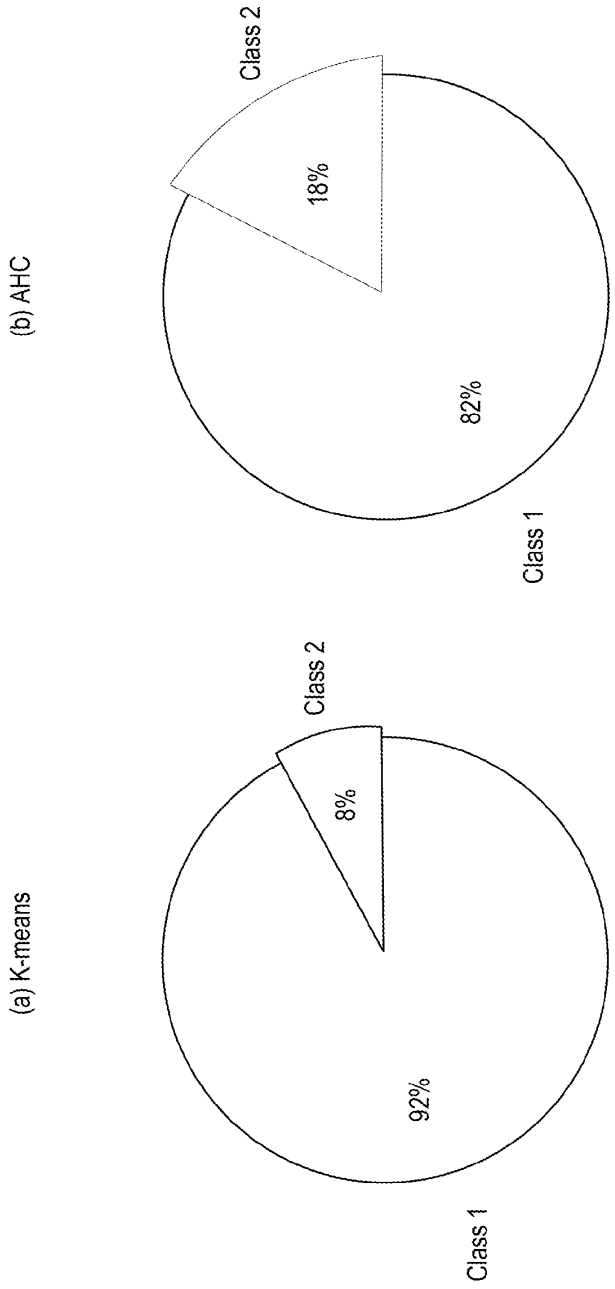


FIG. 11

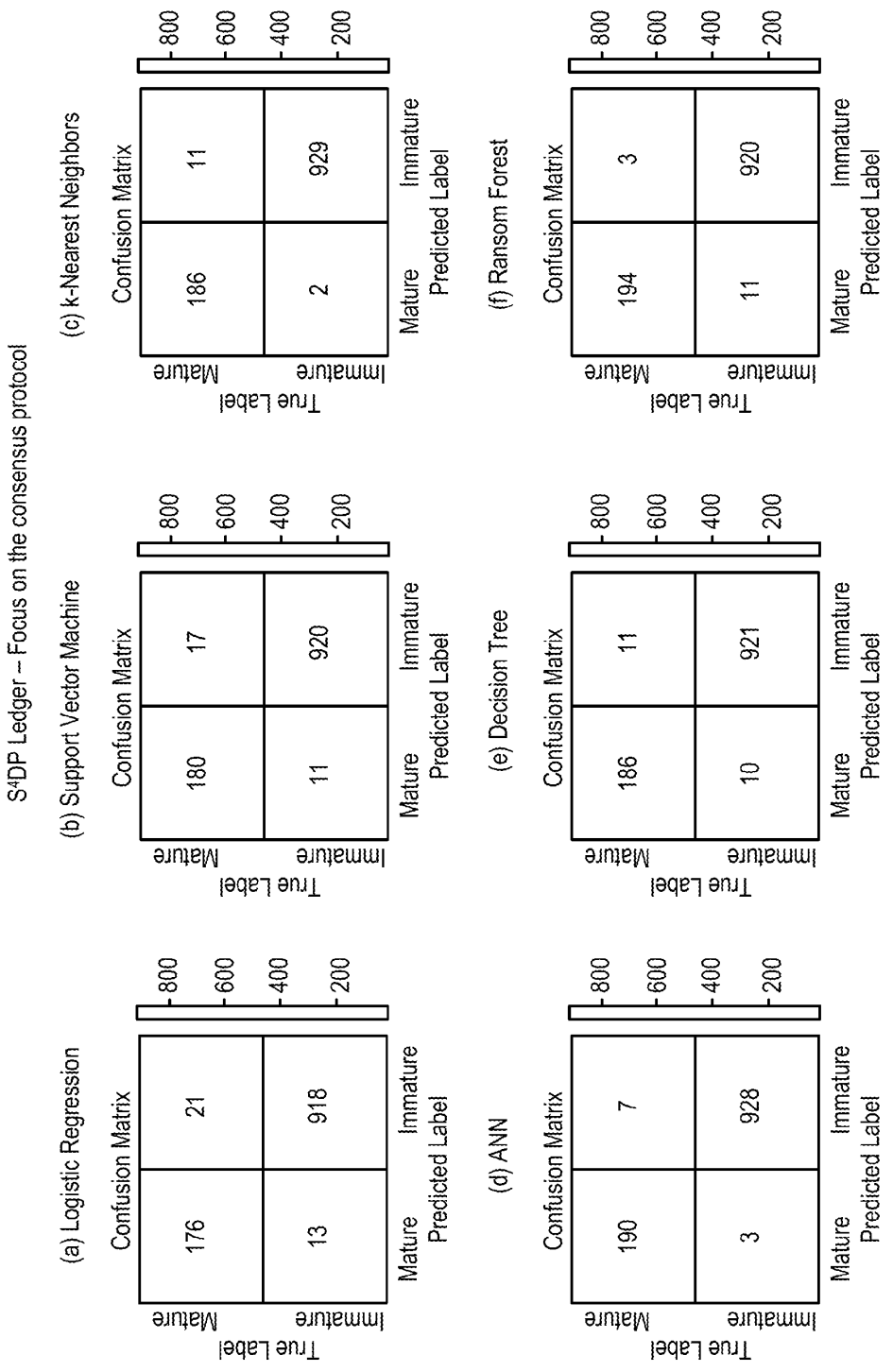

S4DP Ledger – Focus on the consensus protocol
(a) Logistic Regression
Confusion Matrix
176
21
13
918
True Label
Mature
Immature
Mature
Immature
Predicted Label
800
600
400
200
(b) Support Vector Machine
Confusion Matrix
180
17
11
920
True Label
Mature
Immature
Mature
Immature
Predicted Label
800
600
400
200
(c) k-Nearest Neighbors
Confusion Matrix
186
11
2
929
True Label
Mature
Immature
Mature
Immature
Predicted Label
800
600
400
200
(d) ANN
Confusion Matrix
190
7
3
928
True Label
Mature
Immature
Mature
Immature
Predicted Label
800
600
400
200
(e) Decision Tree
Confusion Matrix
186
11
10
921
True Label
Mature
Immature
Mature
Immature
Predicted Label
800
600
400
200
(f) Ransom Forest
Confusion Matrix
194
3
11
920
True Label
Mature
Immature
Mature
Immature
Predicted Label
800
600
400
200

FIG. 12

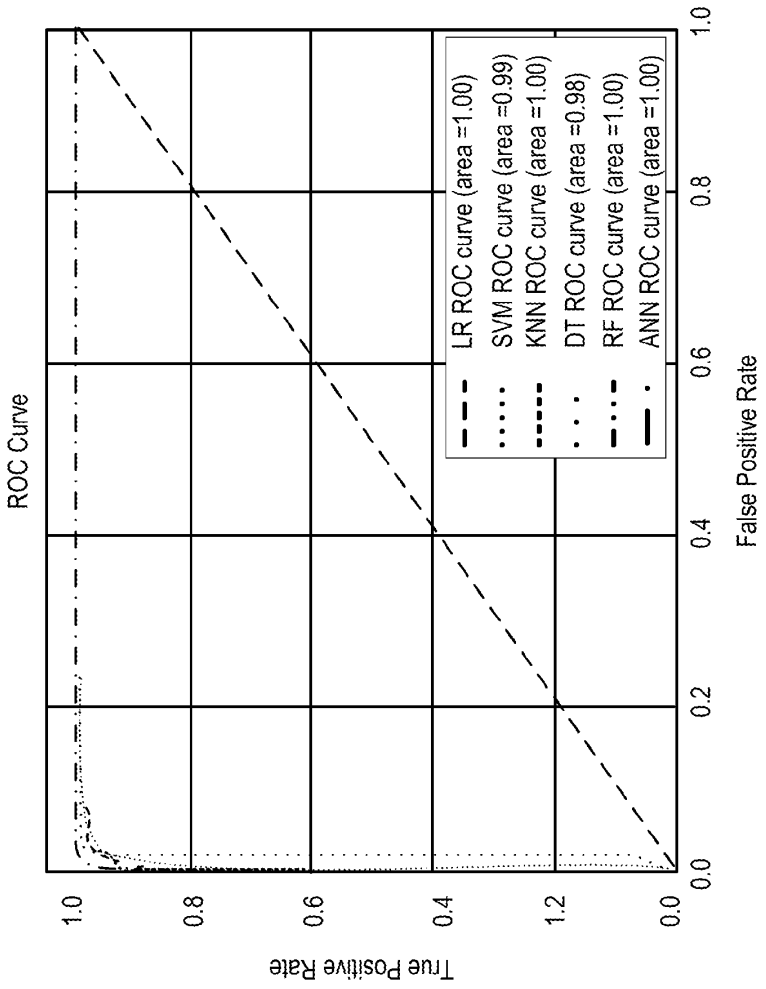

ROC Curve
True Positive Rate
False Positive Rate
0.0
0.2
0.4
0.6
0.8
1.0
1.2
LR ROC curve (area =1.00)
SVM ROC curve (area =0.99)
KNN ROC curve (area =1.00)
DT ROC curve (area =0.98)
RF ROC curve (area =1.00)
ANN ROC curve (area =1.00)

FIG. 13

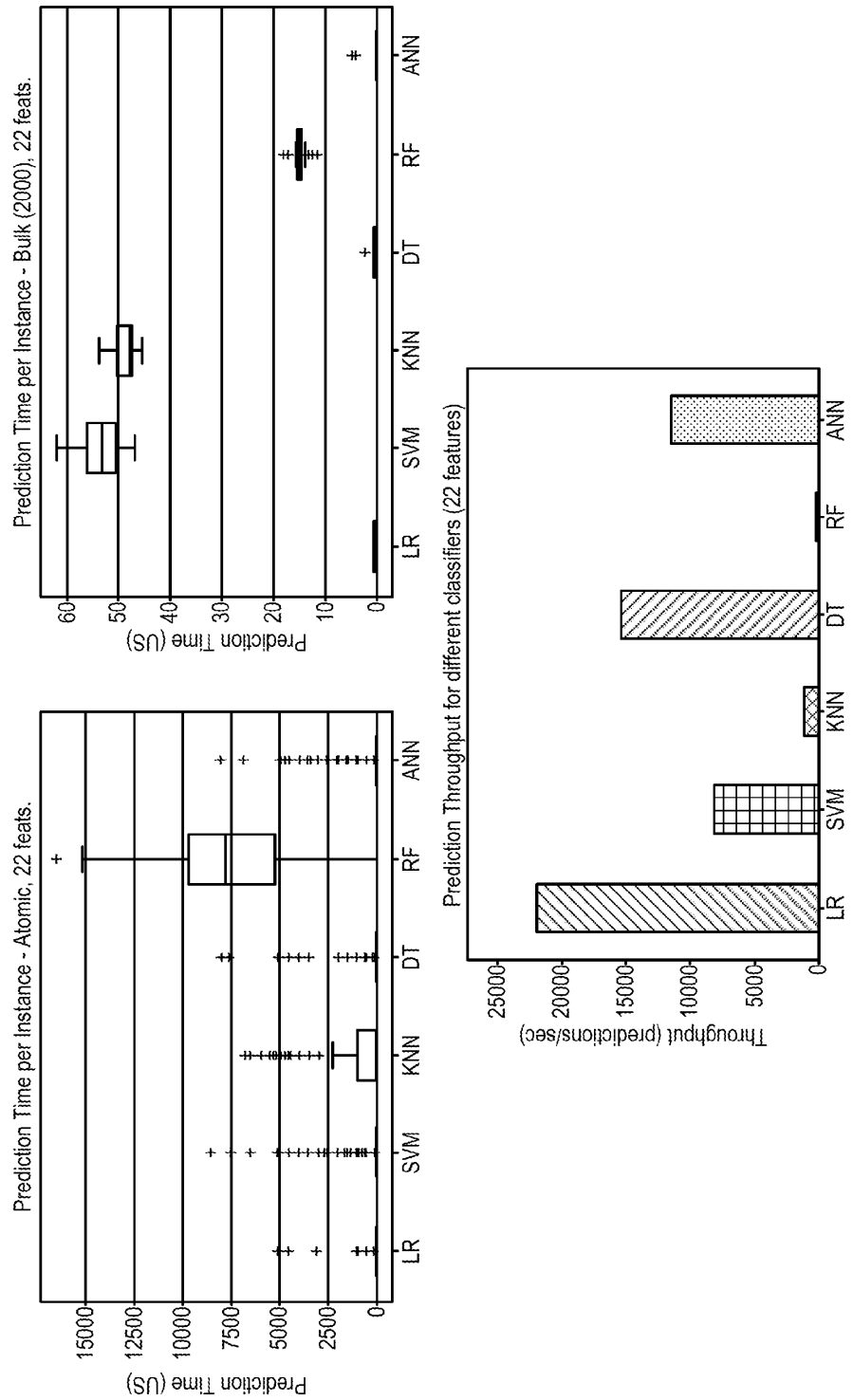

Prediction Time per Instance - Bulk (2000), 22 feats.
Prediction Time (uS)
0
10
20
30
40
50
60
LR
SVM
KNN
DT
RF
ANN
Prediction Time per Instance - Atomic, 22 feats.
Prediction Time (uS)
0
2500
5000
7500
10000
12500
15000
LR
SVM
KNN
DT
RF
ANN
Prediction Throughput for different classifiers (22 features)
Throughput (predictions/sec)
0
5000
10000
15000
20000
25000
LR
SVM
KNN
DT
RF
ANN

FIG. 14

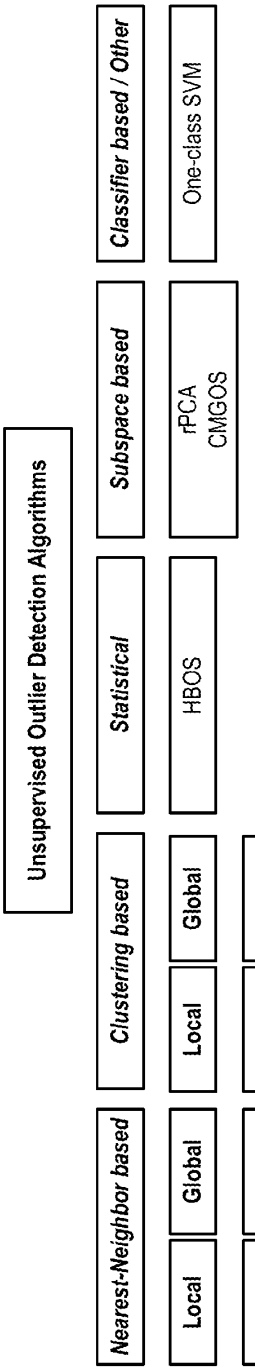

Unsupervised Outlier Detection Algorithms
Nearest-Neighbor based
Clustering based
Statistical
Subspace based
Classifier based / Other
Local
Global
Local
Global
K-NN
K^th-NN
LOF
COF
INFLO
LoOP
LOCI
aLOCI
CBLOF
uCBLOF
LDCOF
CMGOS
HBOS
rPCA
CMGOS
One-class SVM

FIG. 15

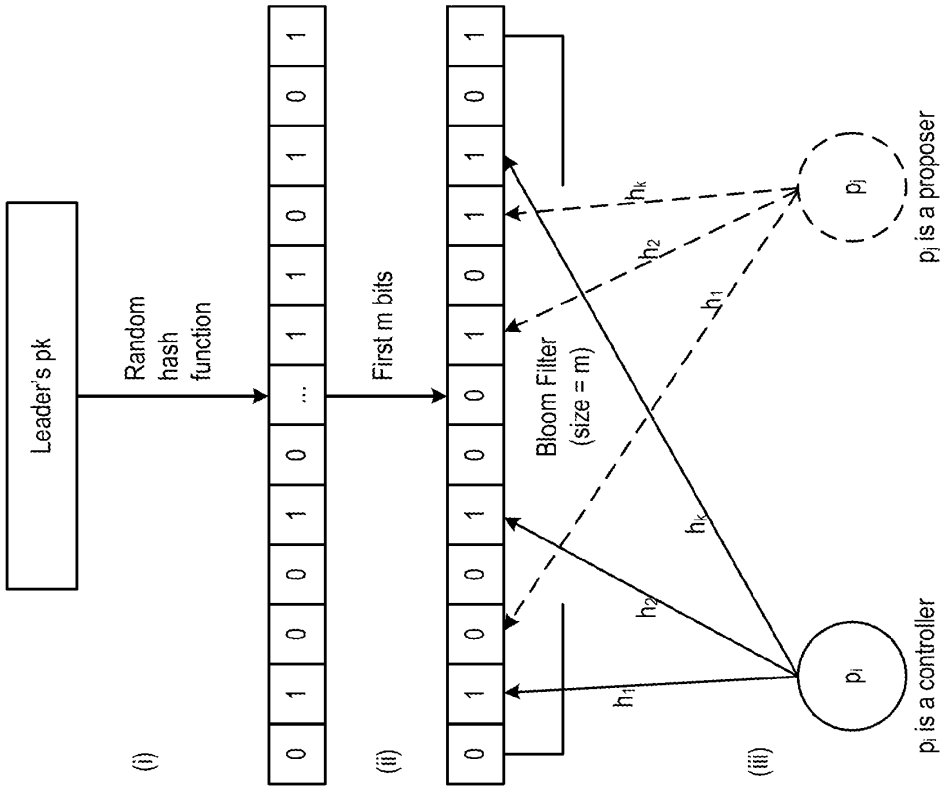

Leader's pk
Random hash function
(i)
0 1 0 0 0 1 ... 1 1 0 1 0 1
First m bits
(ii)
0 1 0 0 0 1 0 0 1 1 0 1
Bloom Filter (size = m)
h_k
h_2
h_1
p_j
p_j is a proposer
h_k
h_2
h_1
p_i
p_i is a controller
(iii)

FIG. 16

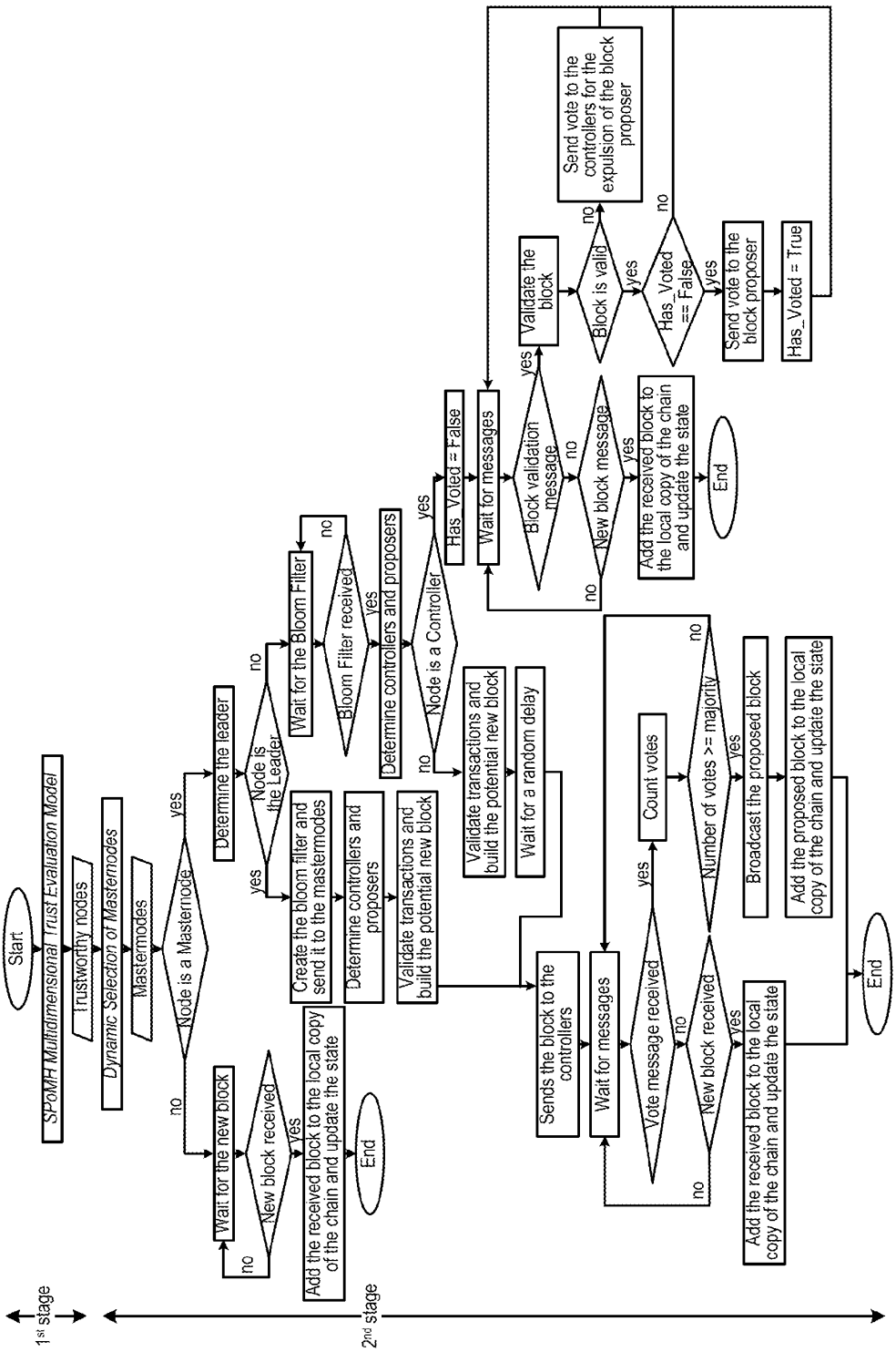

1st stage
2nd stage
Start
SPoMH Multidimensional Trust Evaluation Model
Trustworthy nodes
Dynamic Selection of Mastermodes
Mastermodes
Node is a Mastermode
yes
no
Wait for the new block
New block received
no
yes
Add the received block to the local copy of the chain and update the state
End
Determine the leader
Node is the Leader
yes
no
Create the bloom filter and send it to the mastermodes
Wait for the Bloom Filter
Bloom Filter received
no
yes
Determine controllers and proposers
Determine controllers and proposers
Validate transactions and build the potential new block
Node is a Controller
yes
no
Validate transactions and build the potential new block
Wait for a random delay
Has_Voted = False
Wait for messages
Block validation message
yes
no
New block message
yes
no
Add the received block to the local copy of the chain and update the state
End
Validate the block
Block is valid
yes
no
Send vote to the controllers for the expulsion of the block proposer
Has_Voted == False
yes
no
Send vote to the block proposer
Has_Voted = True
Sends the block to the controllers
Wait for messages
Vote message received
yes
no
Count votes
Number of votes >= majority
yes
no
Broadcast the proposed block
Add the proposed block to the local copy of the chain and update the state
New block received
yes
no
Add the received block to the local copy of the chain and update the state
End

FIG. 17

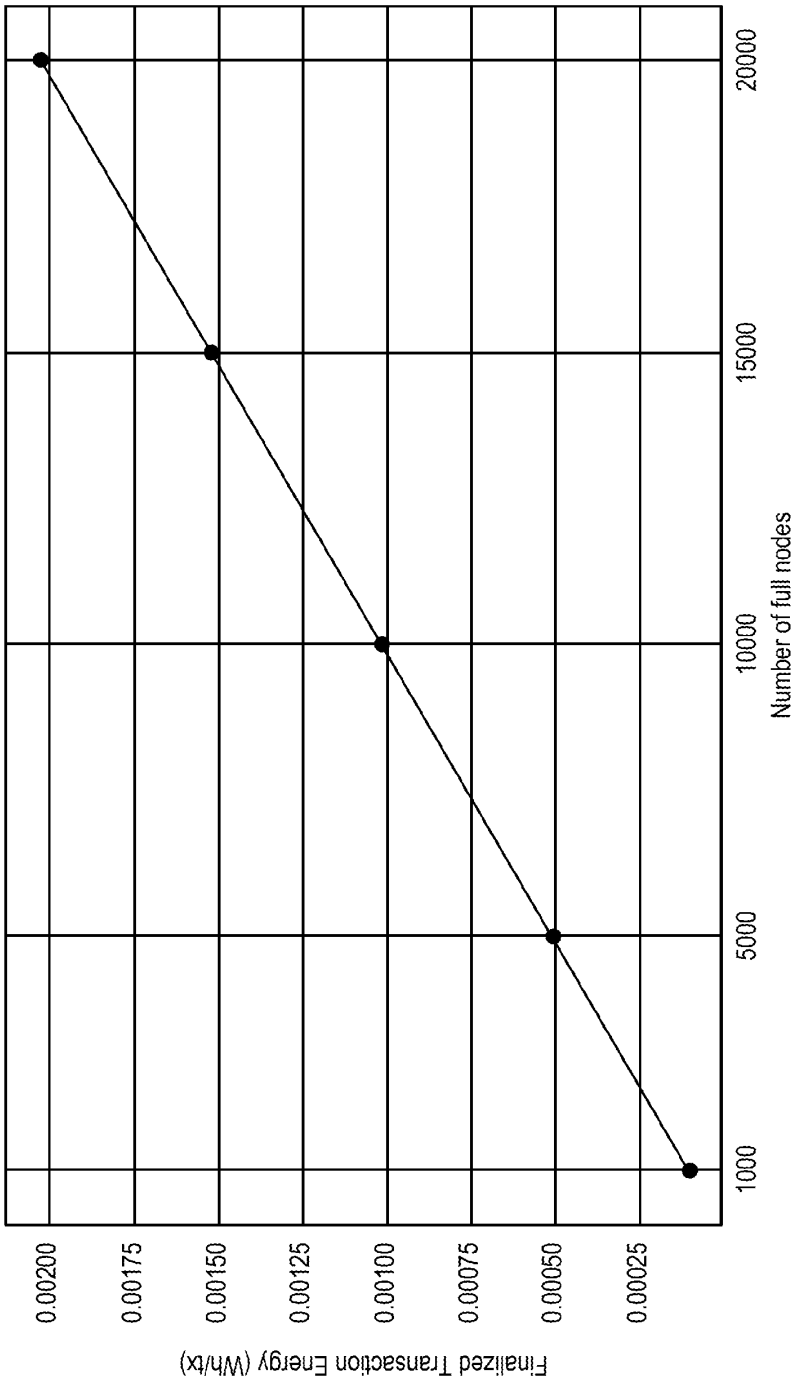

Finalized Transaction Energy (Wh/tx)
0.00200
0.00175
0.00150
0.00125
0.00100
0.00075
0.00050
0.00025
1000
5000
10000
15000
20000
Number of full nodes

FIG. 18

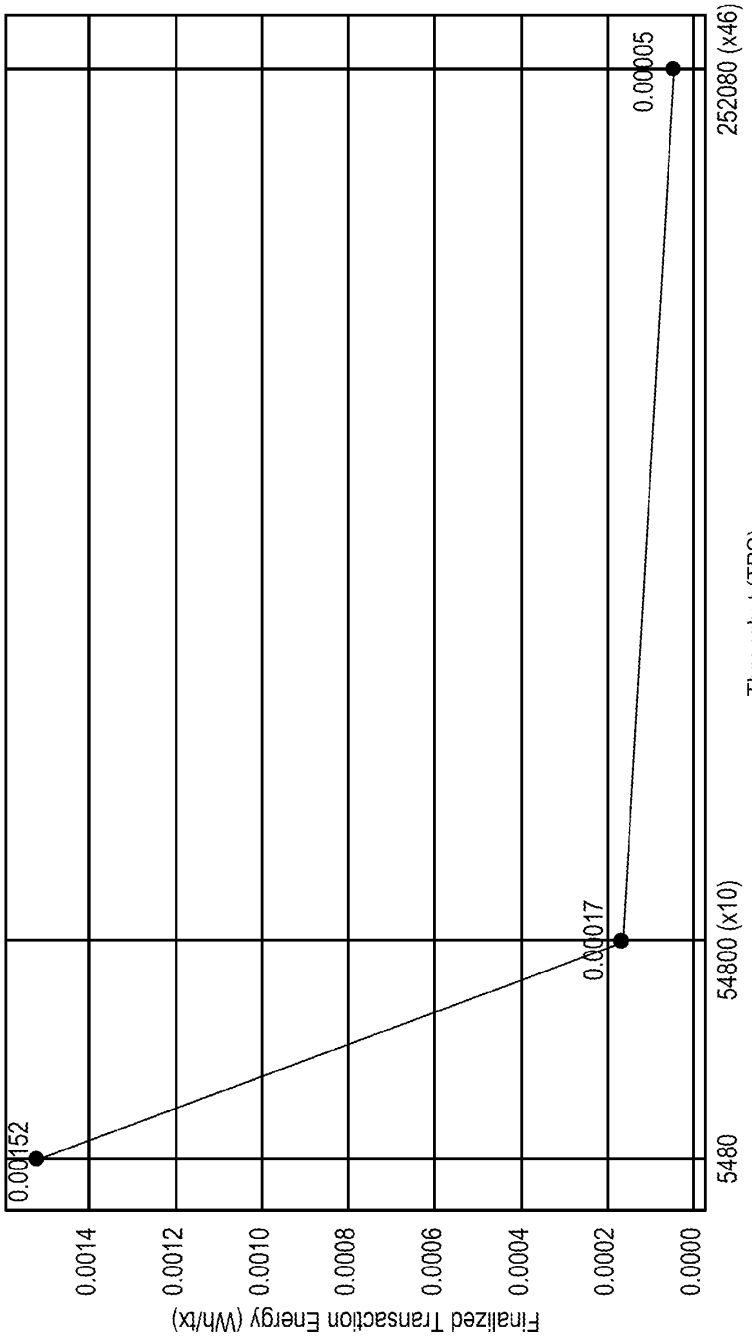

Finalized Transaction Energy (Wh/tx)
0.0014
0.0012
0.0010
0.0008
0.0006
0.0004
0.0002
0.0000
0.00152
0.00017
0.00005
5480
54800 (x10)
252080 (x46)
Throughut (TPS)

FIG. 19

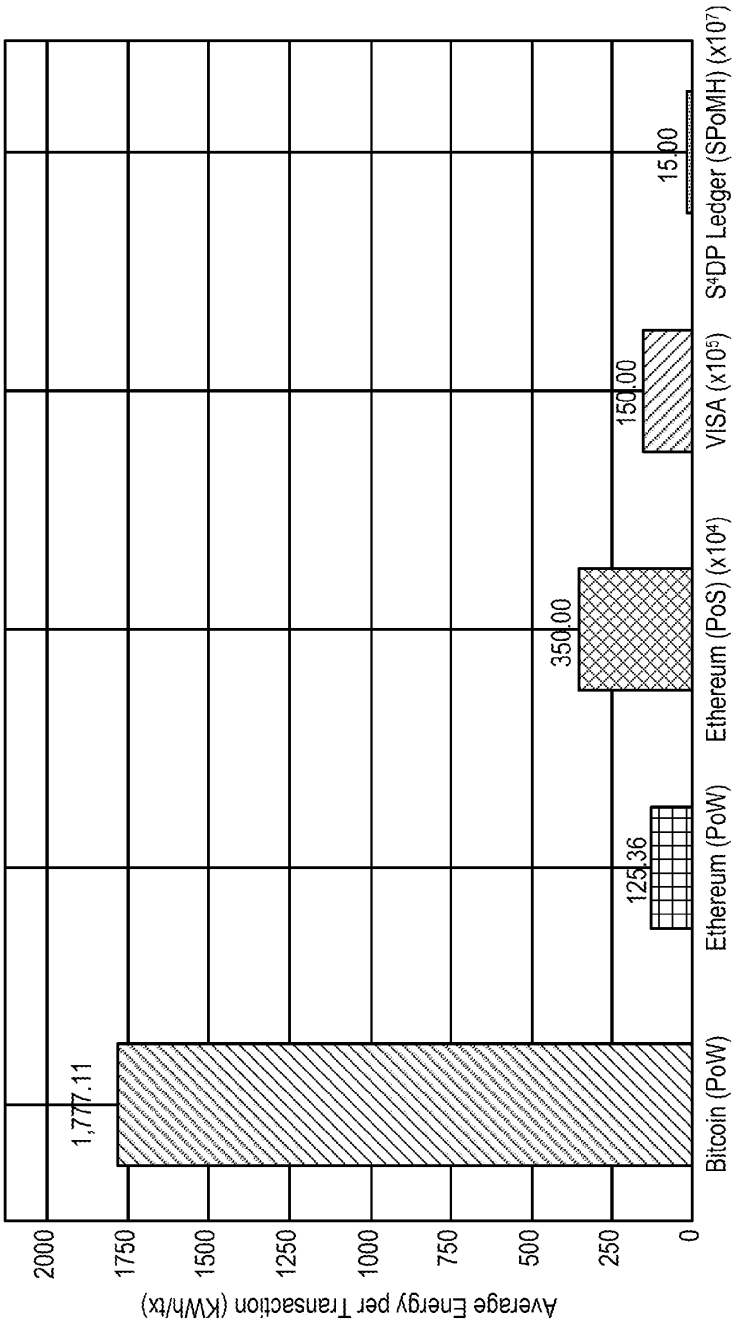

Average Energy per Transaction (KWh/tx)
2000
1750
1500
1250
1000
750
500
250
0
1,777.11
125.36
350.00
150.00
15.00
Bitcoin (PoW)
Ethereum (PoW)
Ethereum (PoS) (x10⁴)
VISA (x10⁵)
S⁴DP Ledger (SPoMH) (x10⁷)

FIG. 20

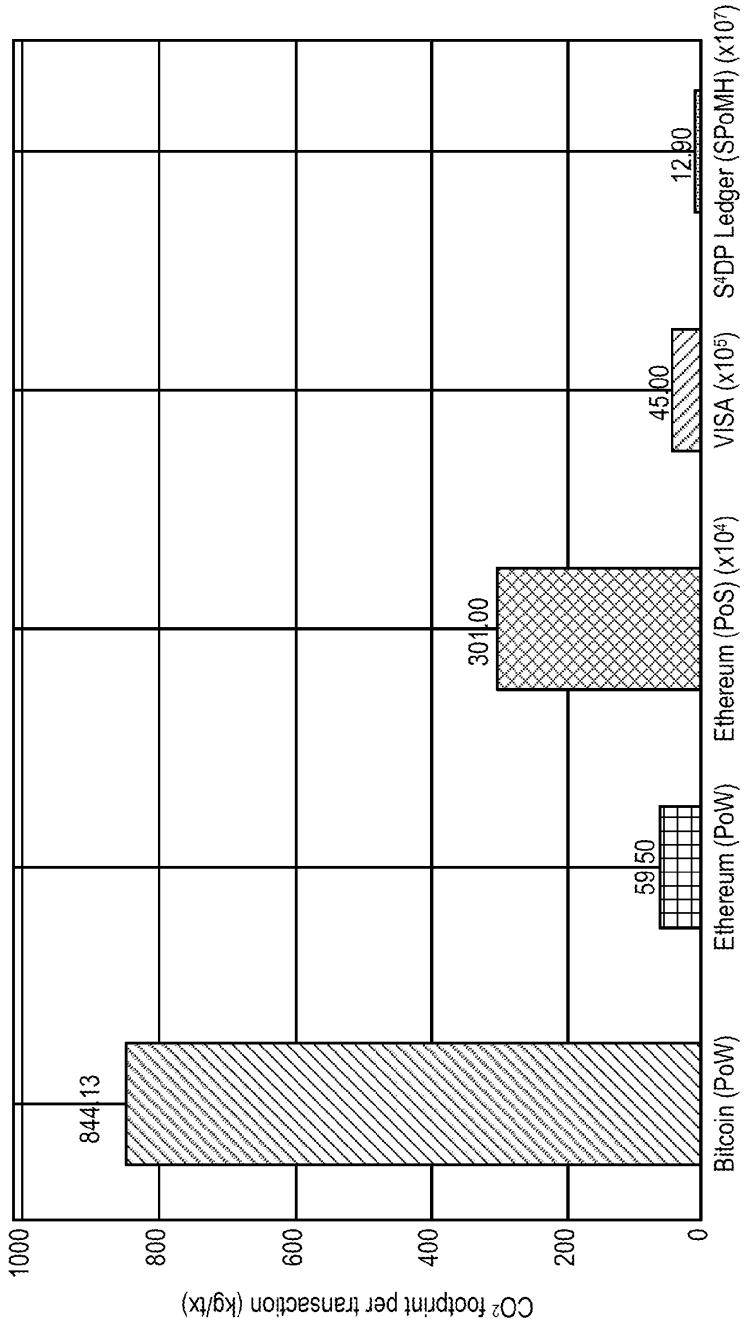

CO² footprint per transaction (kg/tx)
1000
800
600
400
200
0
844.13
59.50
301.00
45.00
12.90
Bitcoin (PoW)
Ethereum (PoW)
Ethereum (PoS) (x10⁴)
VISA (x10⁵)
S⁴DP Ledger (SPoMH) (x10⁷)

FIG. 21

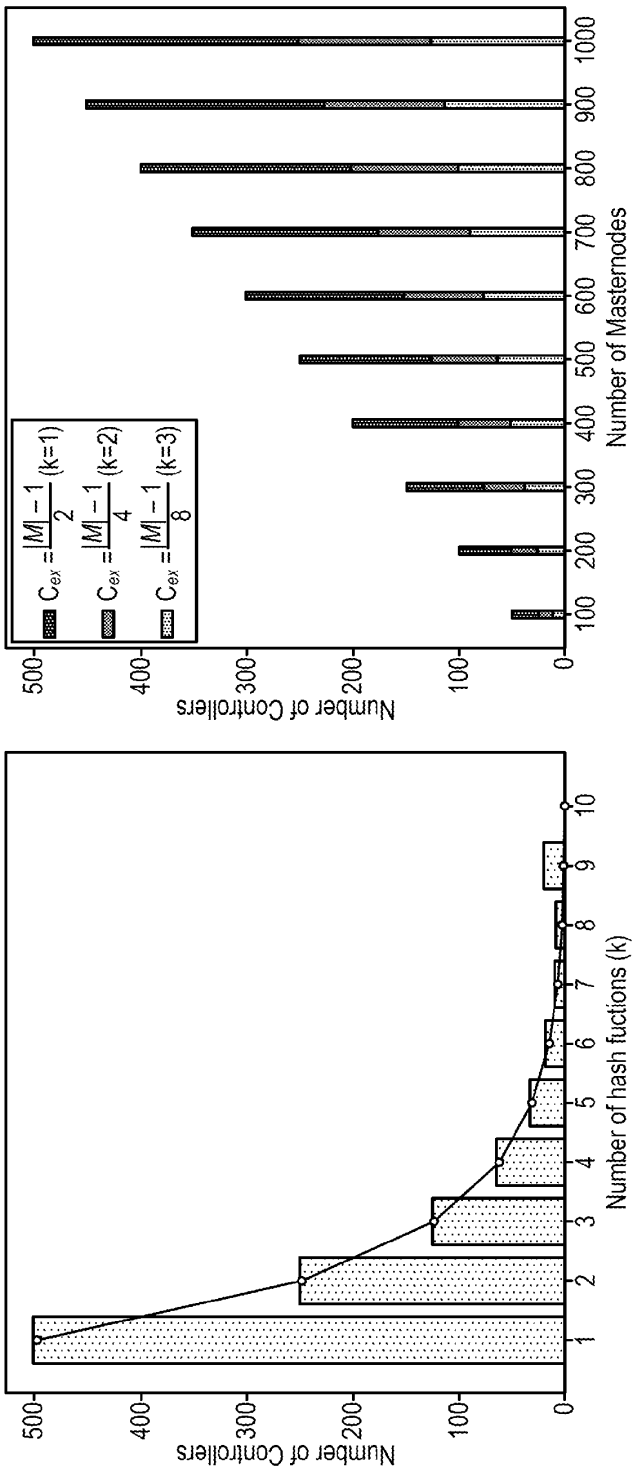

Number of Controllers
0
100
200
300
400
500
Number of Masternodes
100
200
300
400
500
600
700
800
900
1000
$C_{ex} = \frac{|M|-1}{2}$ (k=1)
$C_{ex} = \frac{|M|-1}{4}$ (k=2)
$C_{ex} = \frac{|M|-1}{8}$ (k=3)
Number of Controllers
0
100
200
300
400
500
Number of hash fuctions (k)
1
2
3
4
5
6
7
8
9
10

FIG. 22

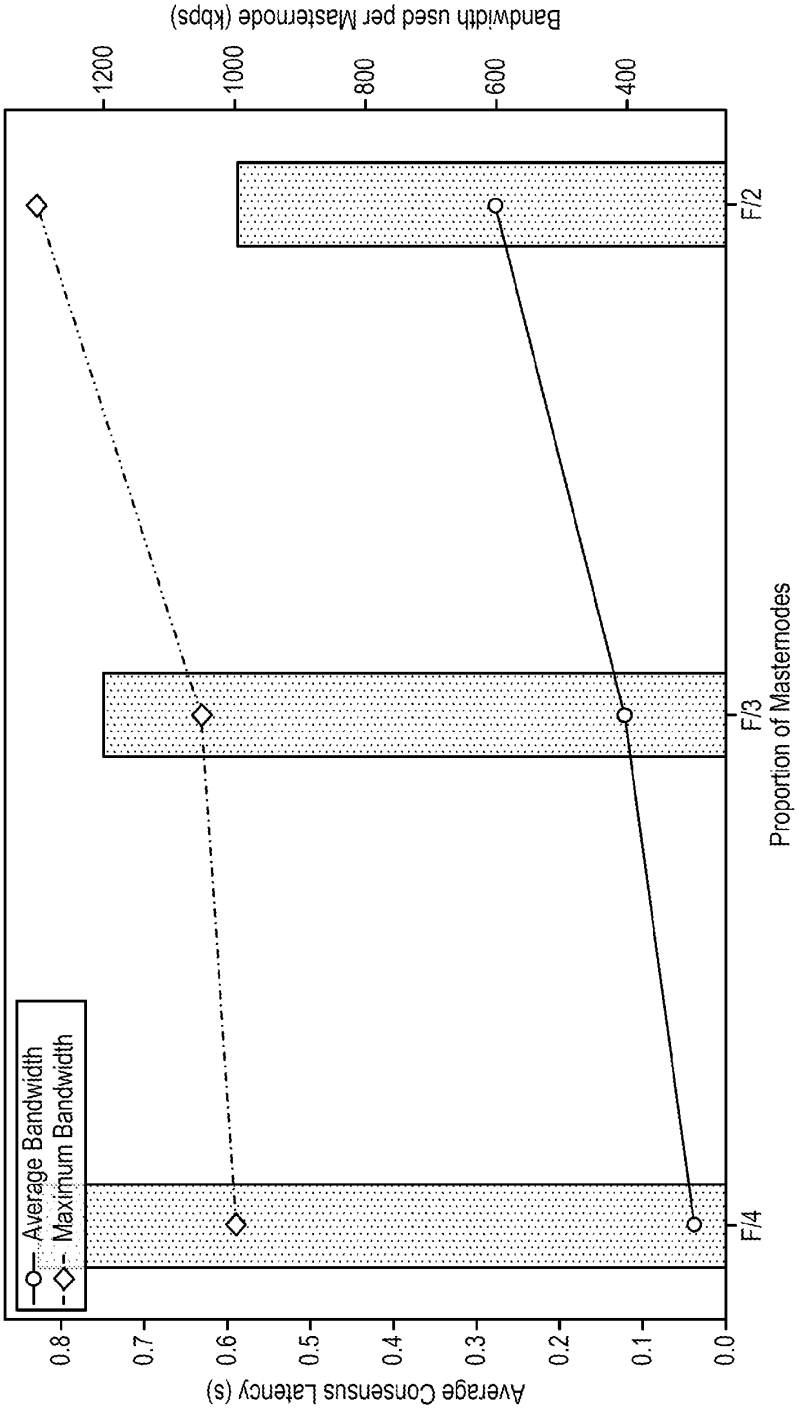

Bandwidth used per Mastermode (kbps)
1200
1000
800
600
400
Average Consensus Latency (s)
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
Average Bandwidth
Maximum Bandwidth
F/4
F/3
F/2
Proportion of Mastermodes

FIG. 23

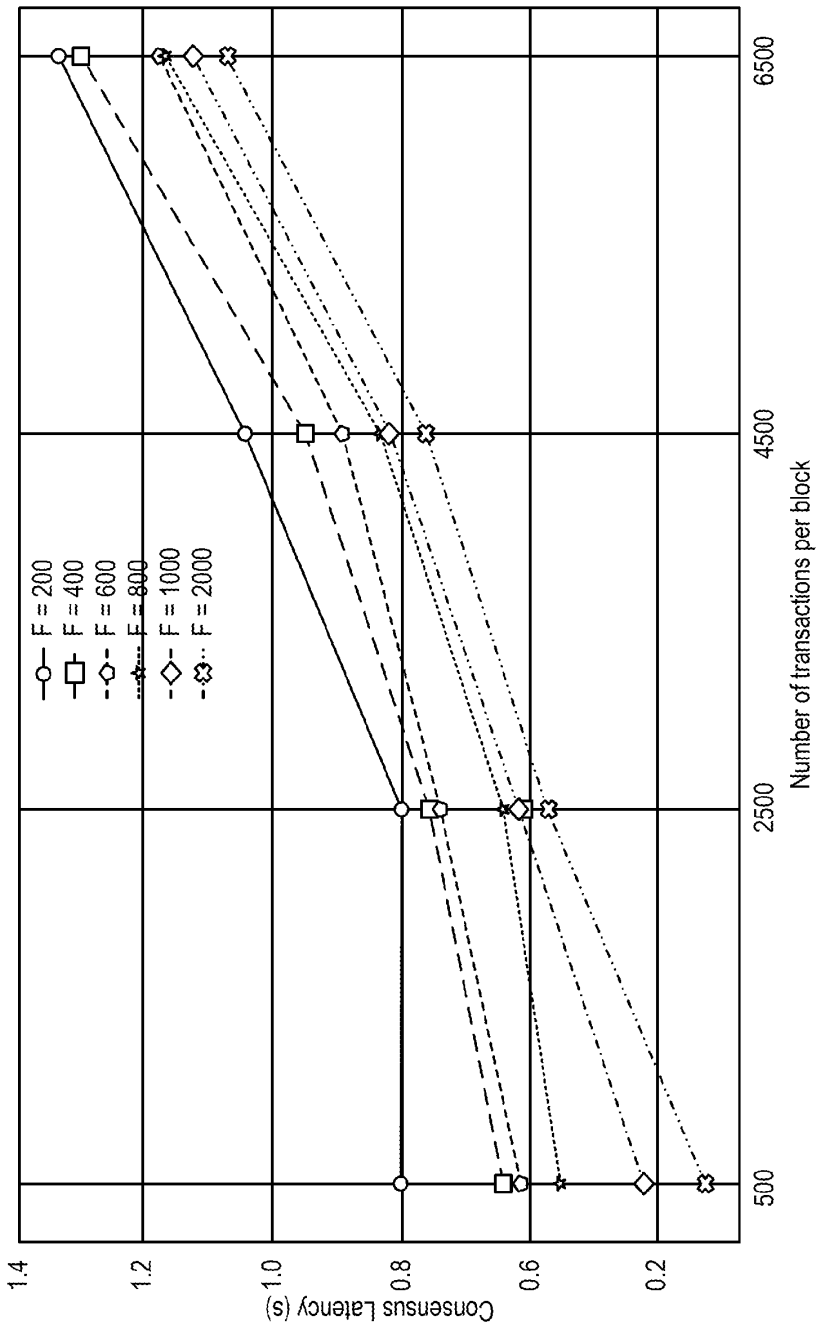

Consensus Latency (s)
1.4
1.2
1.0
0.8
0.6
0.2
500
2500
4500
6500
Number of transactions per block
F = 200
F = 400
F = 600
F = 800
F = 1000
F = 2000

FIG. 24

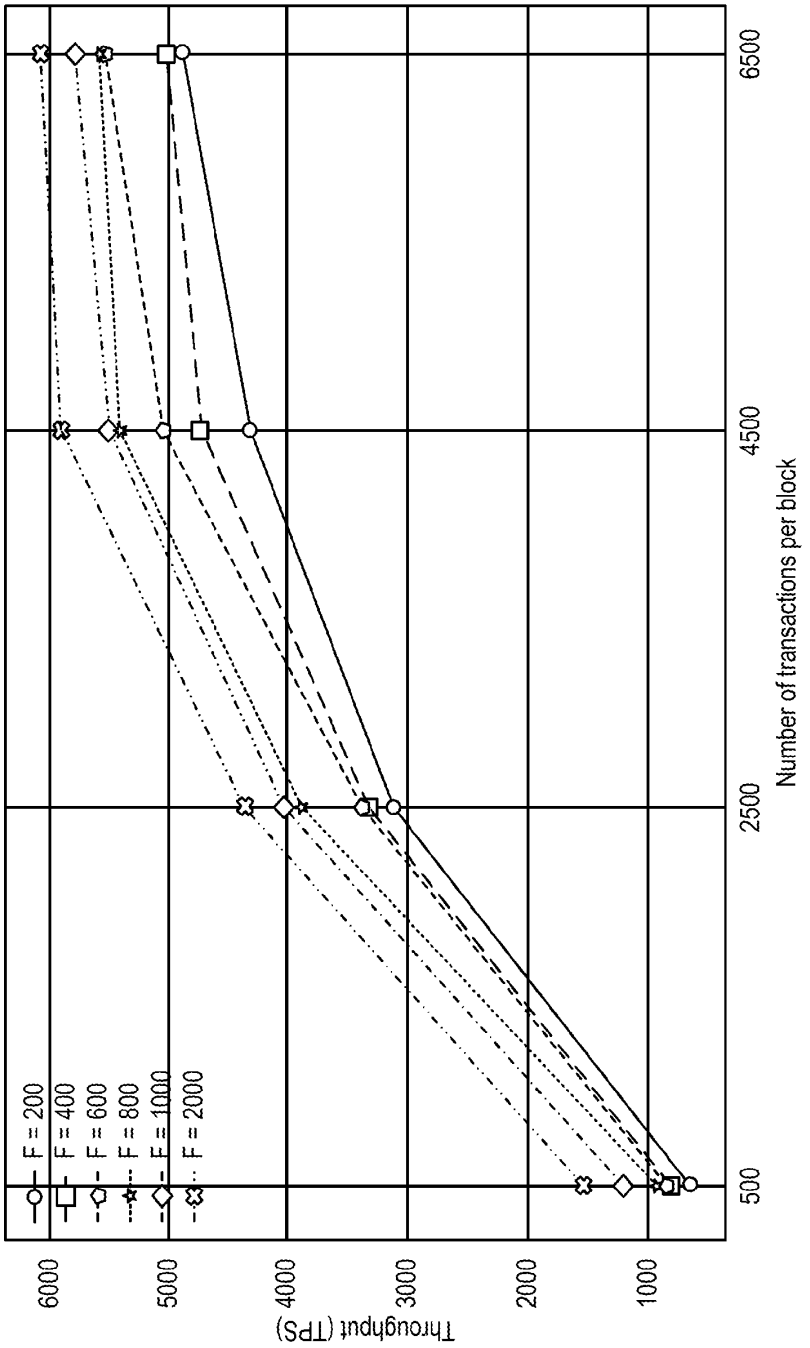

Throughput (TPS)
6000
5000
4000
3000
2000
1000
500
2500
4500
6500
Number of transactions per block
F = 200
F = 400
F = 600
F = 800
F = 1000
F = 2000

FIG. 25

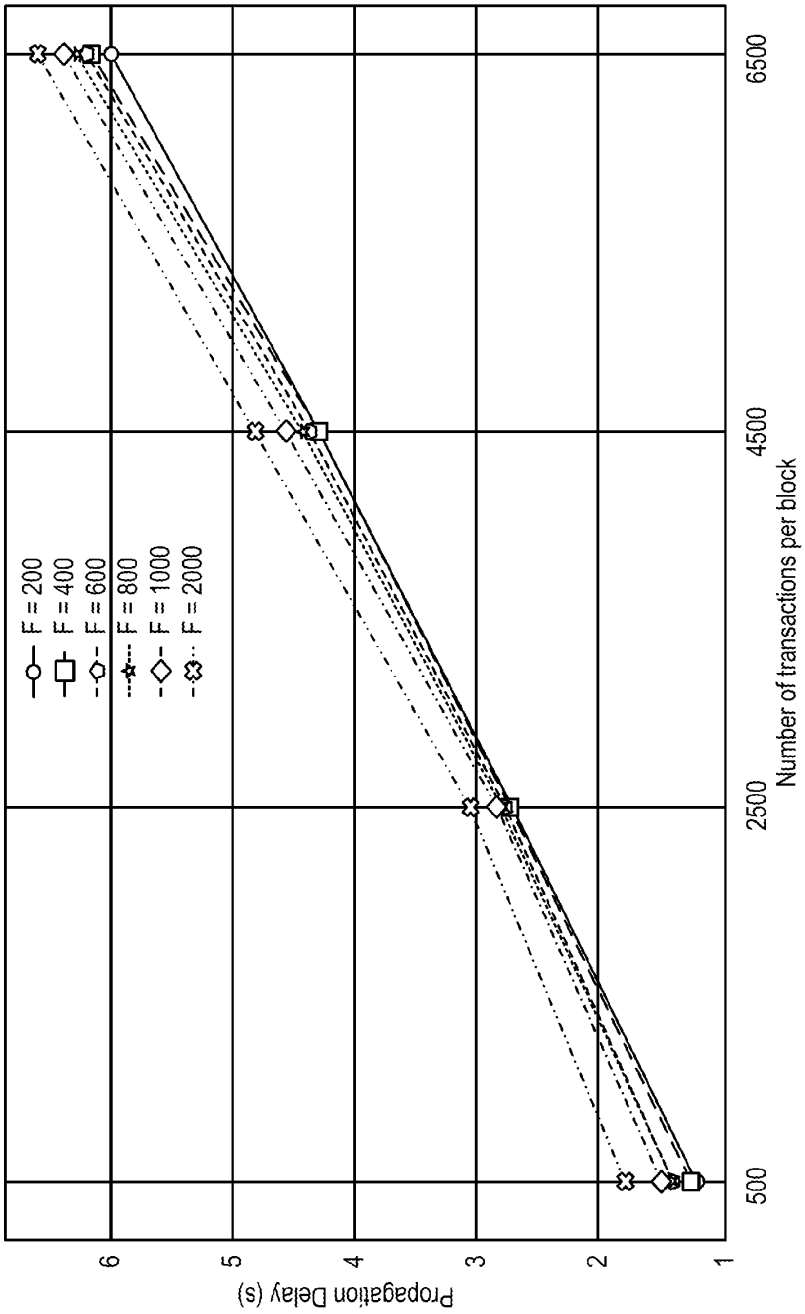

Propagation Delay (s)
1
2
3
4
5
6
500
2500
4500
6500
Number of transactions per block
F = 200
F = 400
F = 600
F = 800
F = 1000
F = 2000

FIG. 26