IEEE SmartComp, 19 June 2018

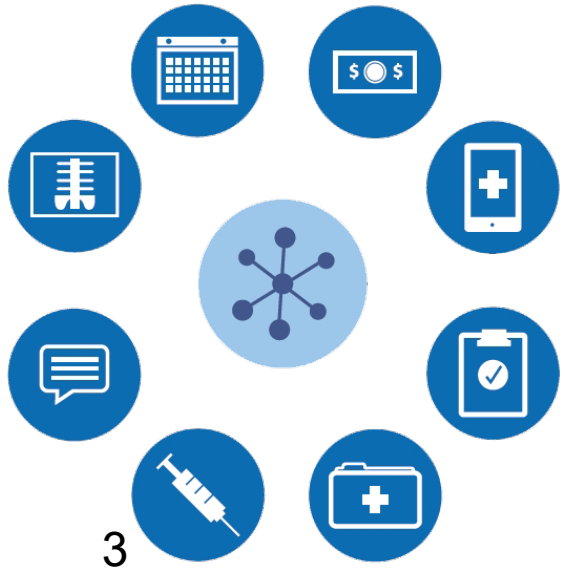
BlockHIE: a BLOCkchain-based platform for Healthcare Information Exchange

Shan Jiang*, Jiannong Cao*, Hanqing Wu*, Yanni Yang*,
Mingyu Ma*, Jianfei He†
*The Hong Kong Polytechnic University, Hong Kong, China
†Huawei Technologies Co. Ltd., Shenzhen, China

Table of Contents

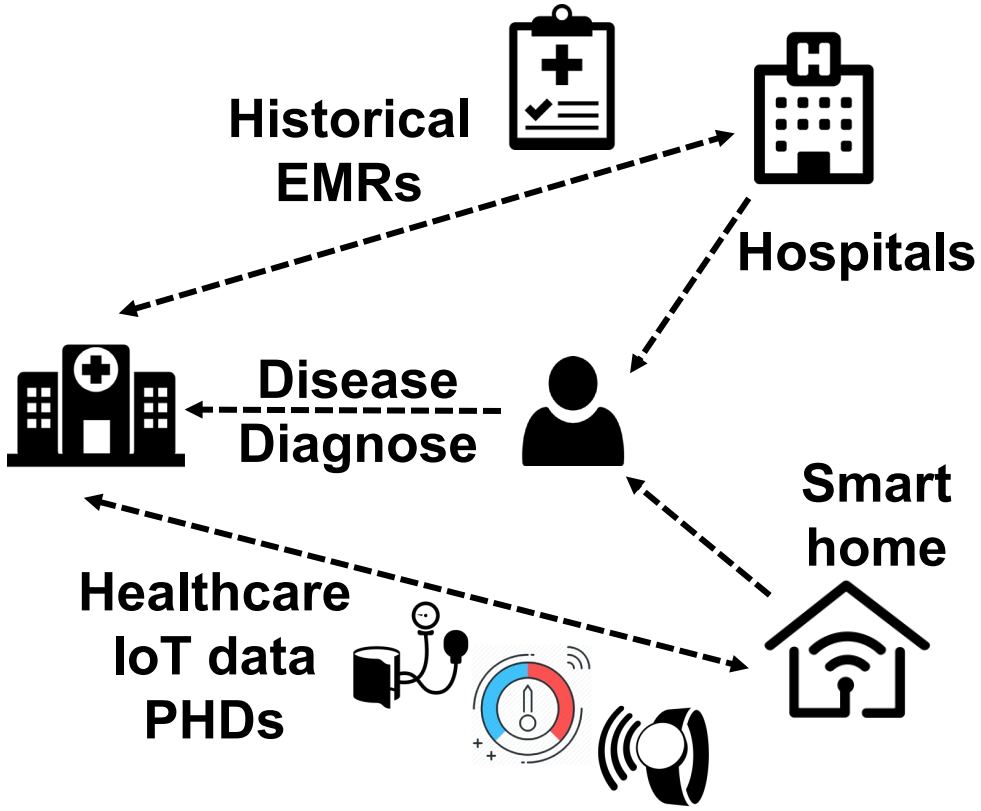
Healthcare Information Exchange

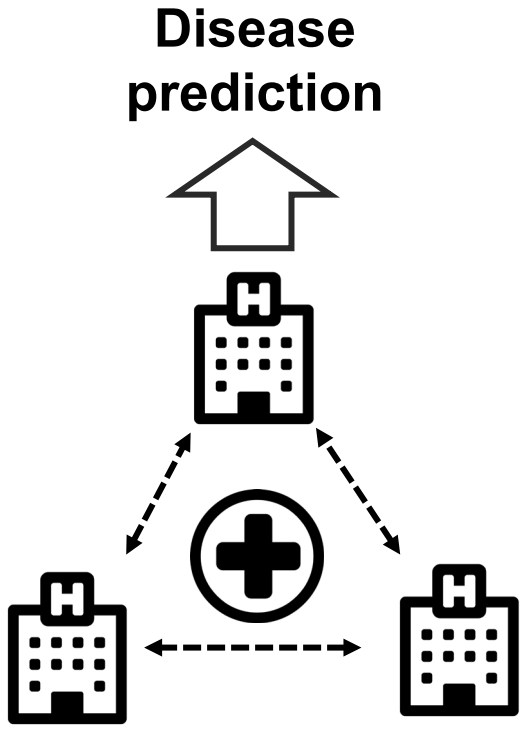
- HIE
  - mobilization of health care information electronically across organizations within a region, community or hospital system.
- Goal
  - facilitate access to and retrieval of clinical data
  - provide safer and more timely, efficient, effective, and equitable patient-centered care.



Healthcare Information Exchange

- Healthcare data sharing and exchange





- EMR: Electronic medical records
- PHD: Personal healthcare data

Existing Solutions

- Cloud service providers (CSPs) propose various schemes for reliable data storage and efficient data processing.
- CSPs have been taking great responsibilities to provide a controlled, cross-domain and flexible HIE platform.

- However, CSPs are unwilling to share their data.
- Risky if the healthcare is exposed to the malicious users unexpectedly

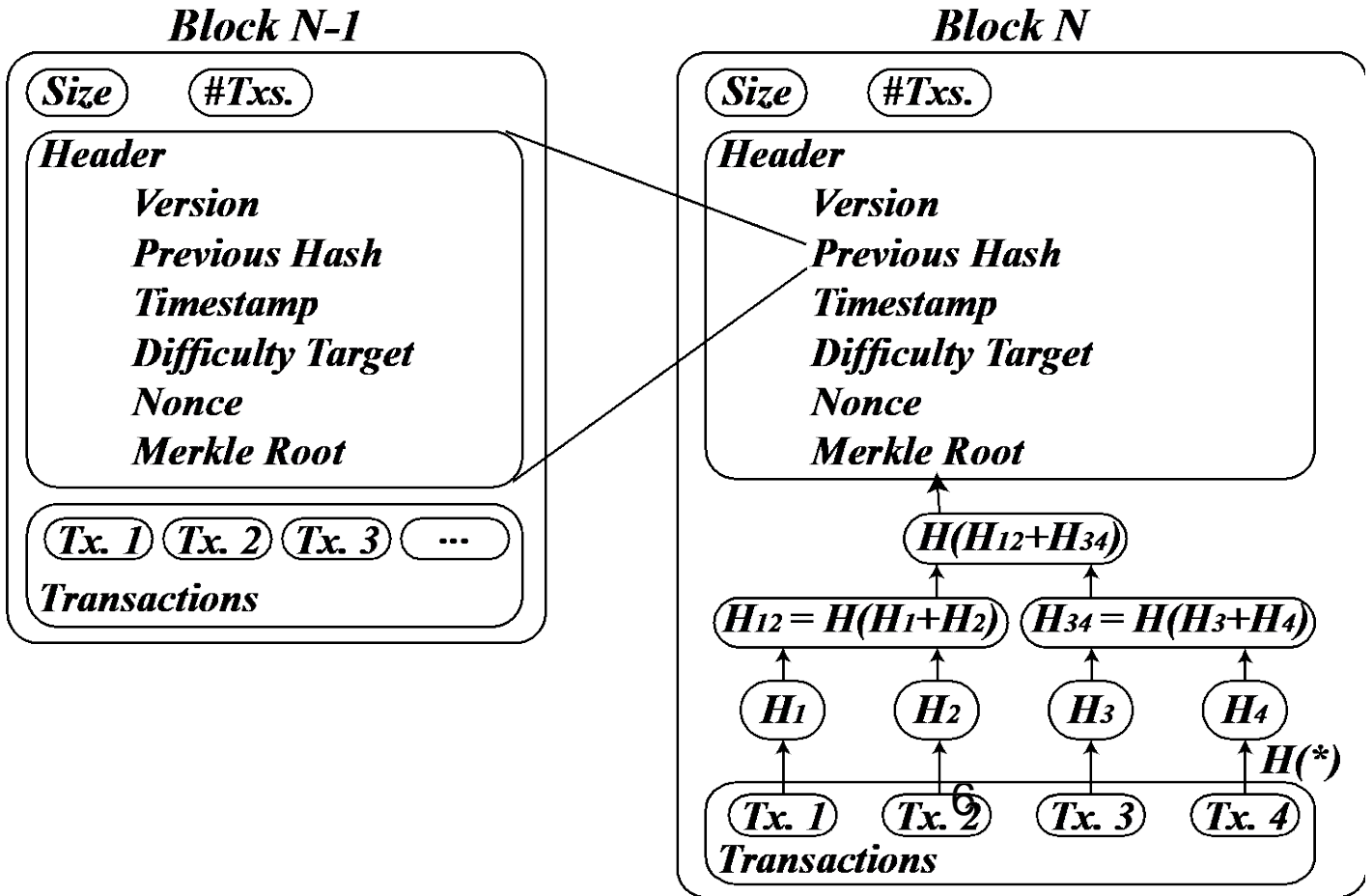
Blockchain - Distributed Ledger Technology

- A Blockchain is an append-only data structure, to store a continuously growing list of transactions.

Decentralization: removal of third party

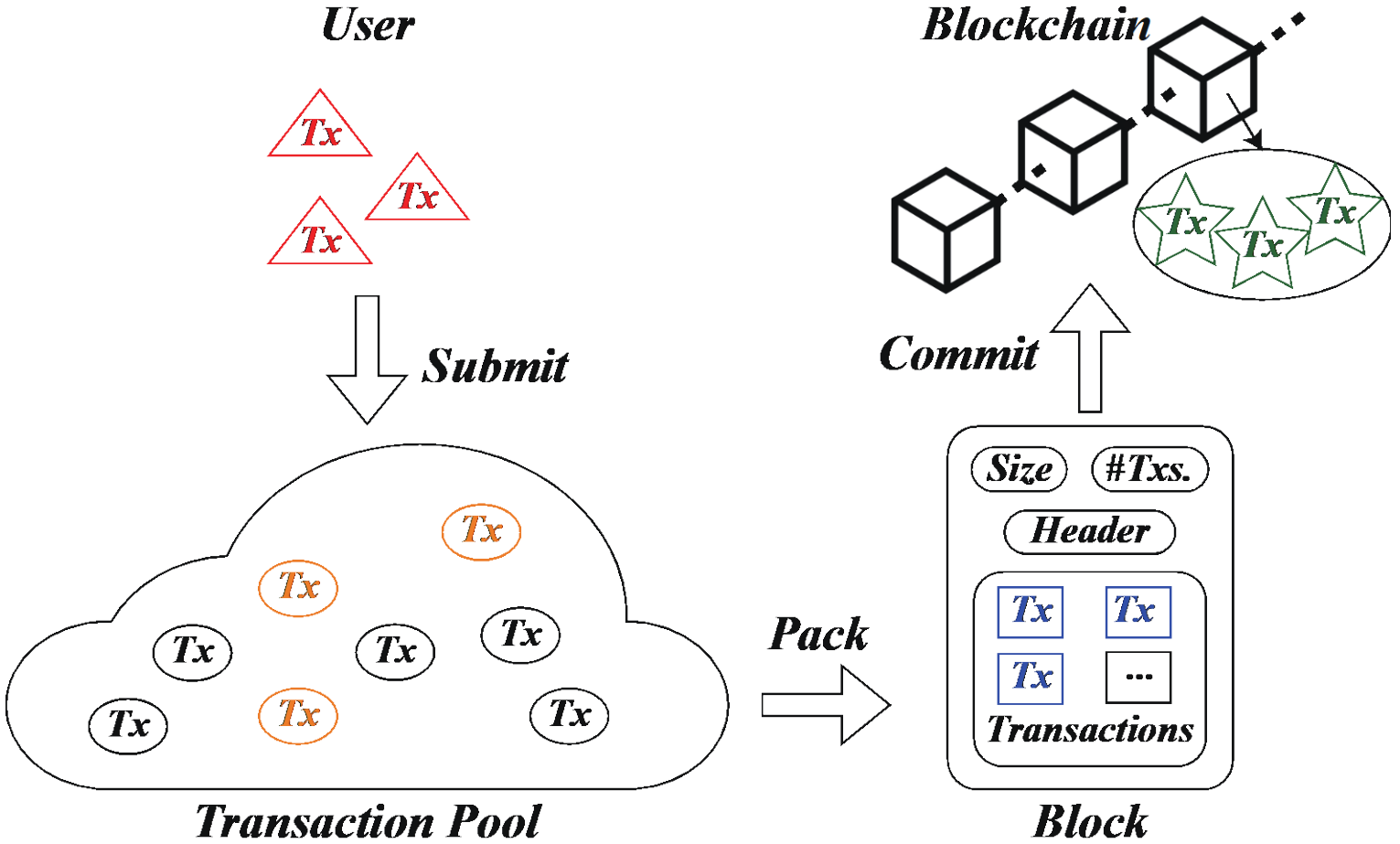
Transparency: visible to everyone

Immutability: once stored, cannot be changed



Distributed Consensus

- Consensus algorithm
  - members need to agree on a certain state of the Blockchain

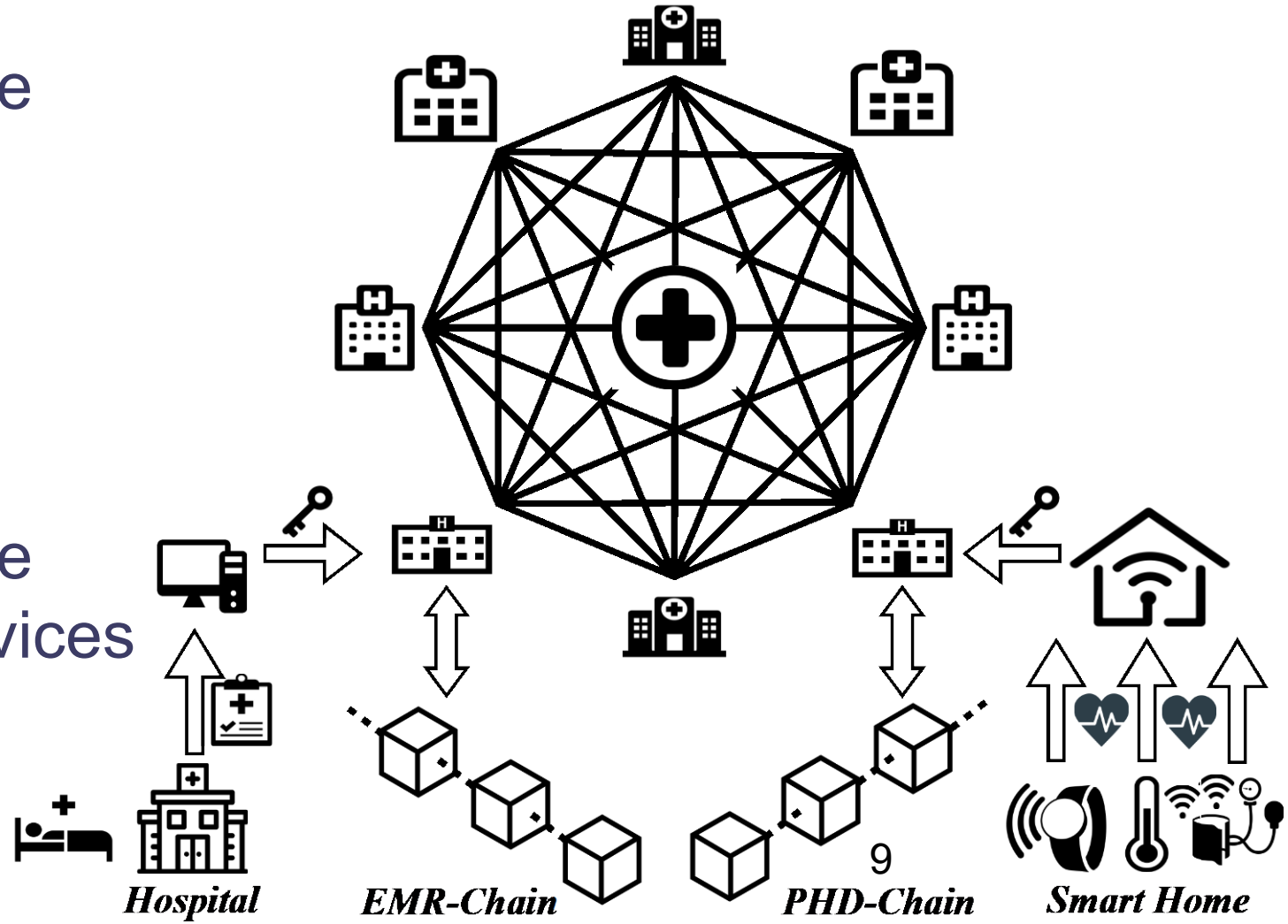


Requirements to Publish and Share Data

Requirements	EMR	PHD
privacy	high	moderate
authenticability	High	low
throughput	moderate	high
latency	moderate	moderate
fairness	moderate	moderate

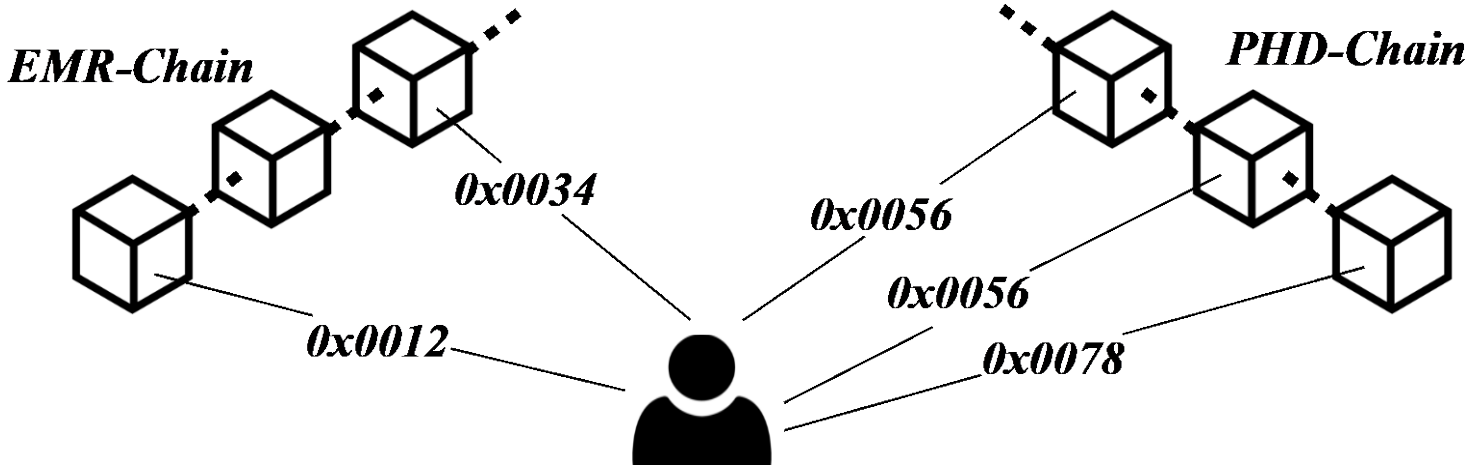
BlockHIE System Architecture

- Blockchain network
  - store and share healthcare data
- Medical institutions
  - submit diagnostic records
- Individuals
  - store and share healthcare data generated by IoT devices



Two Loosely-coupled Blockchains

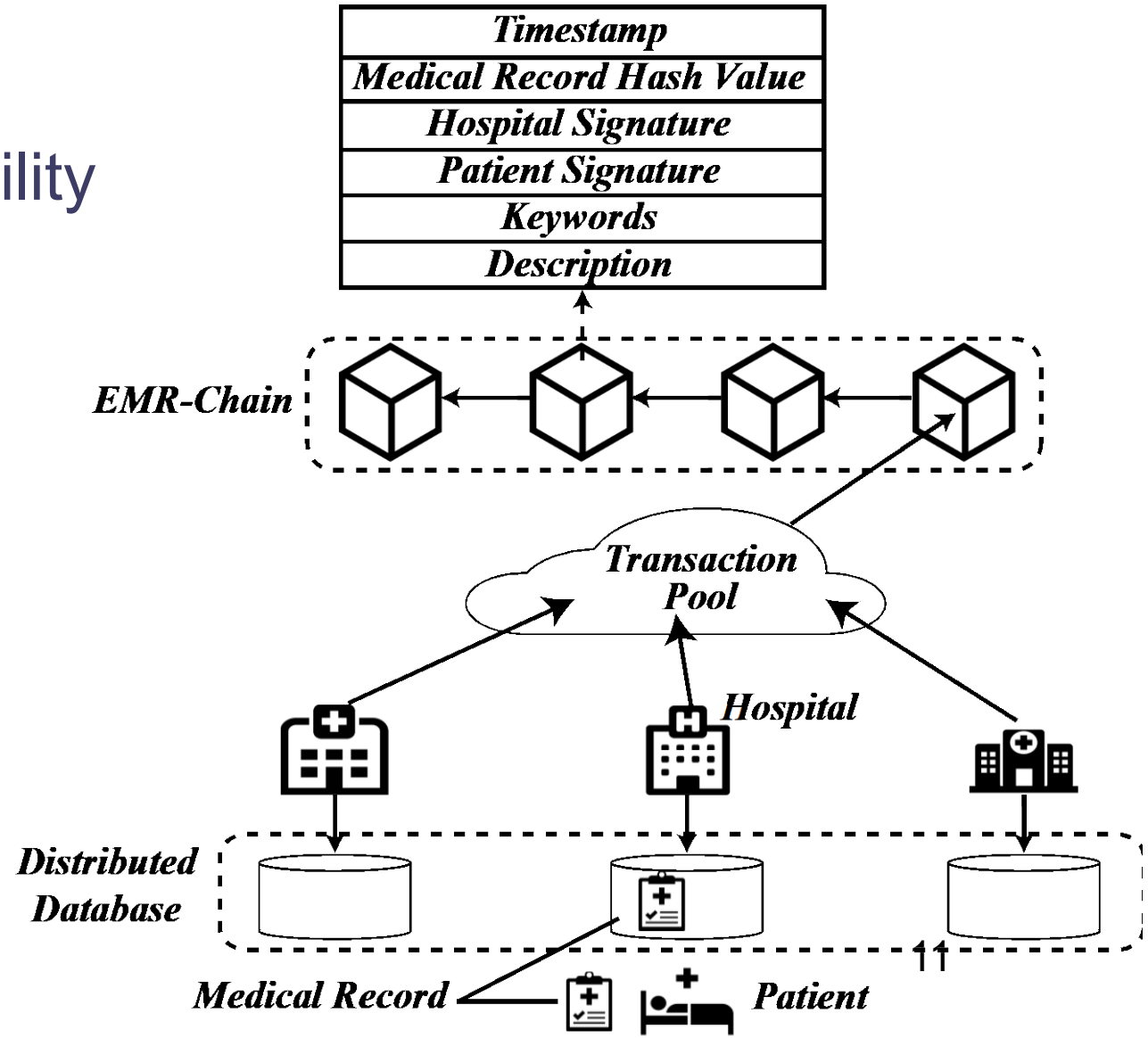
- Propose to store and EMR and PHD with two loosely-coupled Blockchains: EMR-Chain and PHD-Chain.



- Coupled when user publish data on both chains
- Identities of the same person can be different
  - EMR-Chain: unique record identifier
  - PHD-Chain: unique device identifier

Mechanism and Structure of EMR-Chain

- Key requirements
  - Privacy and Authenticability
- Generate three copies
  - Hospital database
    - full copy
  - Patient
    - full copy
  - Blockchain Network
    - proof-of-existence copy



Fairness-based Transaction Packing Algorithm

- Fairness-based packing algorithms in Blockchain
  - Data sharing applications can have different requirements, e.g., maximum throughput, maximum fairness
  - Propose algorithms to balance the throughput and fairness

$$t_i = e_i - s_i$$

- Fairness: $$\mathcal{J}(x_1, x_2, \cdots, x_n) = \frac{(\sum_{i=1}^{n} t_i)^2}{n \cdot \sum_{i=1}^{n} t_i^2}$$

- Pack the TXs with top-m waiting times

Fairness-based Transaction Packing Algorithm

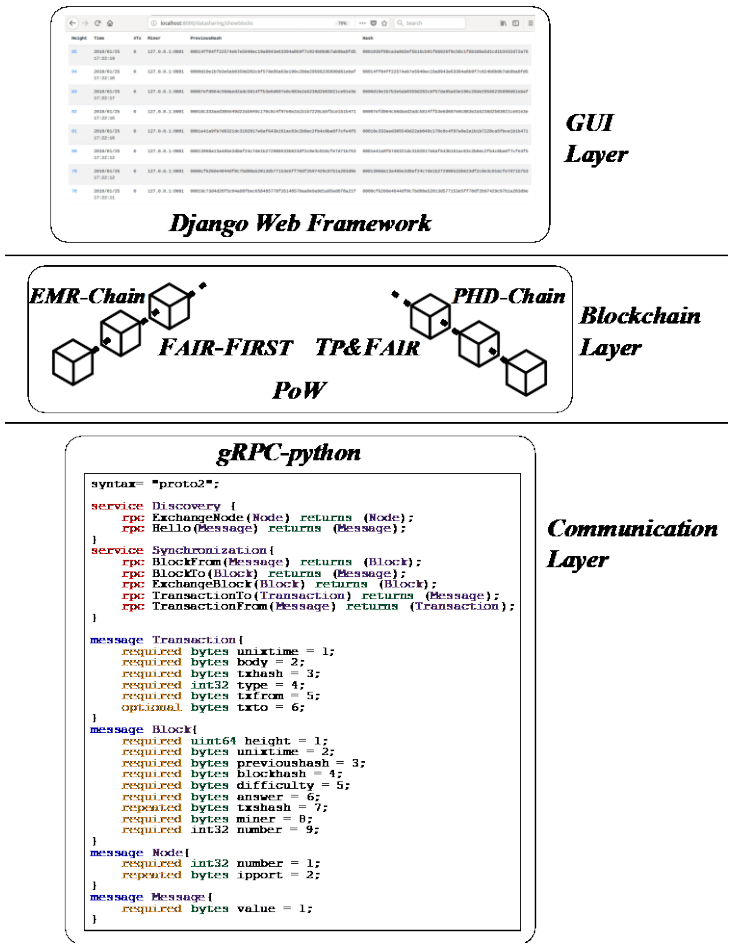
- APP-Kth -SUM: An approaximate algorithm to find the subset of size m with k-th largest sum in a set X of n positive real numbers
- EMR-Chain
  - TP&FAIR
  - high throughput and moderate fairness
- PHD-Chain
  - FAIR-FIRST
  - High fairness

Algorithm 2 Throughput-first and fairness-first packing algorithm running on node i

procedure TP&FAIR(X)
  $m \leftarrow$ the maximum number of transactions in a block
  $X' \leftarrow$ APP-KTH-SUM($X, |X|, m, i$)
  return X'
end procedure
procedure FAIR-FIRST(X)
  $m \leftarrow$ the maximum number of transactions in a block
  $X' \leftarrow$ APP-KTH-SUM($X, |X|, m, 1$)
  return X'
end procedure

BlocHIE Implementation

- Implement BlocHIE in a minimal-viable-product version
- Three layers
  - Communication layer
  - Blockchain layer
  - GUI layer




```
syntax= "proto2";

service Discovery {
     rpc ExchangeNode(Node) returns (Node);
     rpc Hello(Message) returns (Message);
}
service Synchronization{
     rpc BlockFrom(Message) returns (Block);
     rpc BlockTo(Block) returns (Message);
     rpc ExchangeBlock(Block) returns (Block);
     rpc TransactionTo(Transaction) returns (Message);
     rpc TransactionFrom(Message) returns (Transaction);
}

message Transaction{
     required bytes unixtime = 1;
     required bytes body = 2;
     required bytes txhash = 3;
     required int32 type = 4;
     required bytes txfrom = 5;
     optional bytes txto = 6;
}
message Block{
     required uint64 height = 1;
     required bytes unixtime = 2;
     required bytes previoushash = 3;
     required bytes blockhash = 4;
     required bytes difficulty = 5;
     required bytes answer = 6;
     repeated bytes txshash = 7;
     required bytes miner = 8;
     required int32 number = 9;
}
message Node{
     required int32 number = 1;
     repeated bytes ipport = 2;
}
message Message{
     required bytes value = 1;
}
```

Communication Layer

- Implemented using gRPC-python
- Two services
  - Discovery
    - peer discovery service
    - greet static nodes
    - exchange the connectivity info
  - Synchronization
    - synchronization service
    - remote procedure calls

gRPC-python

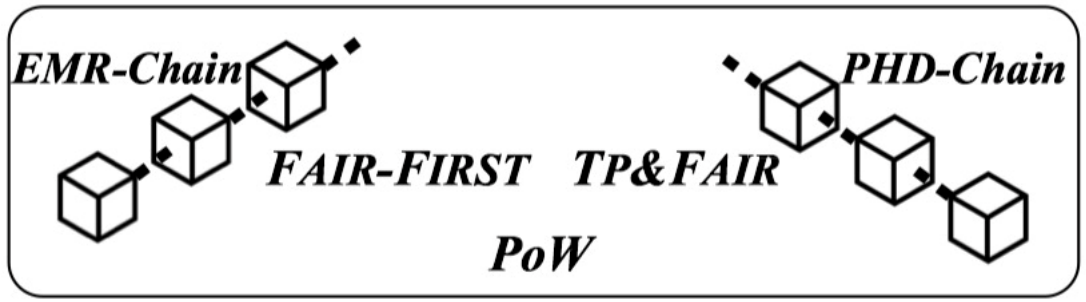
```
syntax= "proto2";

service Discovery {
    rpc ExchangeNode(Node) returns (Node);
    rpc Hello(Message) returns (Message);
}
service Synchronization{
    rpc BlockFrom(Message) returns (Block);
    rpc BlockTo(Block) returns (Message);
    rpc ExchangeBlock(Block) returns (Block);
    rpc TransactionTo(Transaction) returns (Message);
    rpc TransactionFrom(Message) returns (Transaction);
}

message Transaction{
    required bytes unixtime = 1;
    required bytes body = 2;
    required bytes txhash = 3;
    required int32 type = 4;
    required bytes txfrom = 5;
    optional bytes txto = 6;
}
message Block{
    required uint64 height = 1;
    required bytes unixtime = 2;
    required bytes previoushash = 3;
    required bytes blockhash = 4;
    required bytes difficulty = 5;
    required bytes answer = 6;
    repeated bytes txshash = 7;
    required bytes miner = 8;
    required int32 number = 9;
}
message Node{
    required int32 number = 1;
    repeated bytes ipport = 2;
}
message Message{
    required bytes value = 1;
}
```

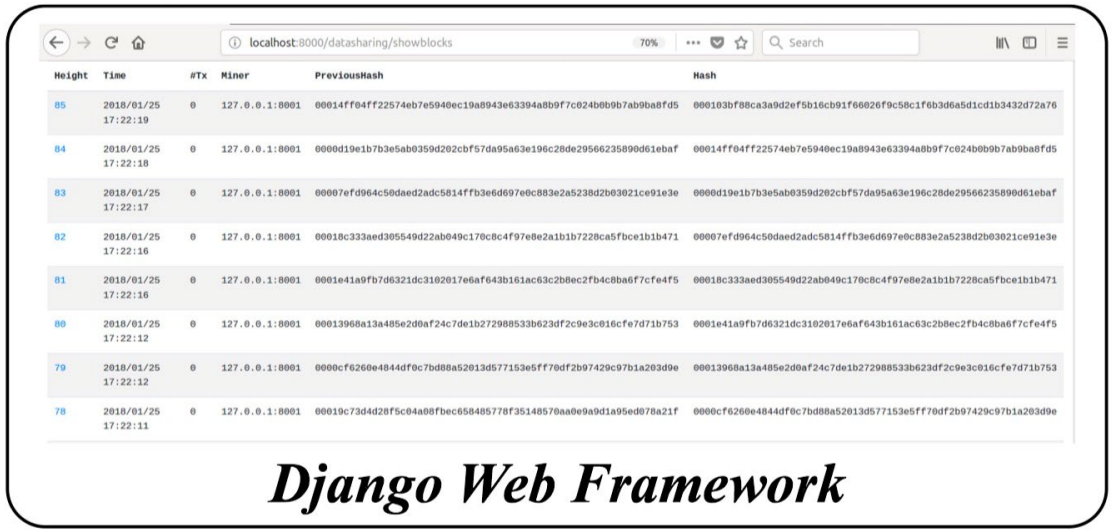
Blockchain Layer

- EMR-Chain
  - FAIR-FIRST packing algorithm
- PHD-Chain
  - TP&FAIR packing algorithm
- Block Committing Algorithm
  - PoW



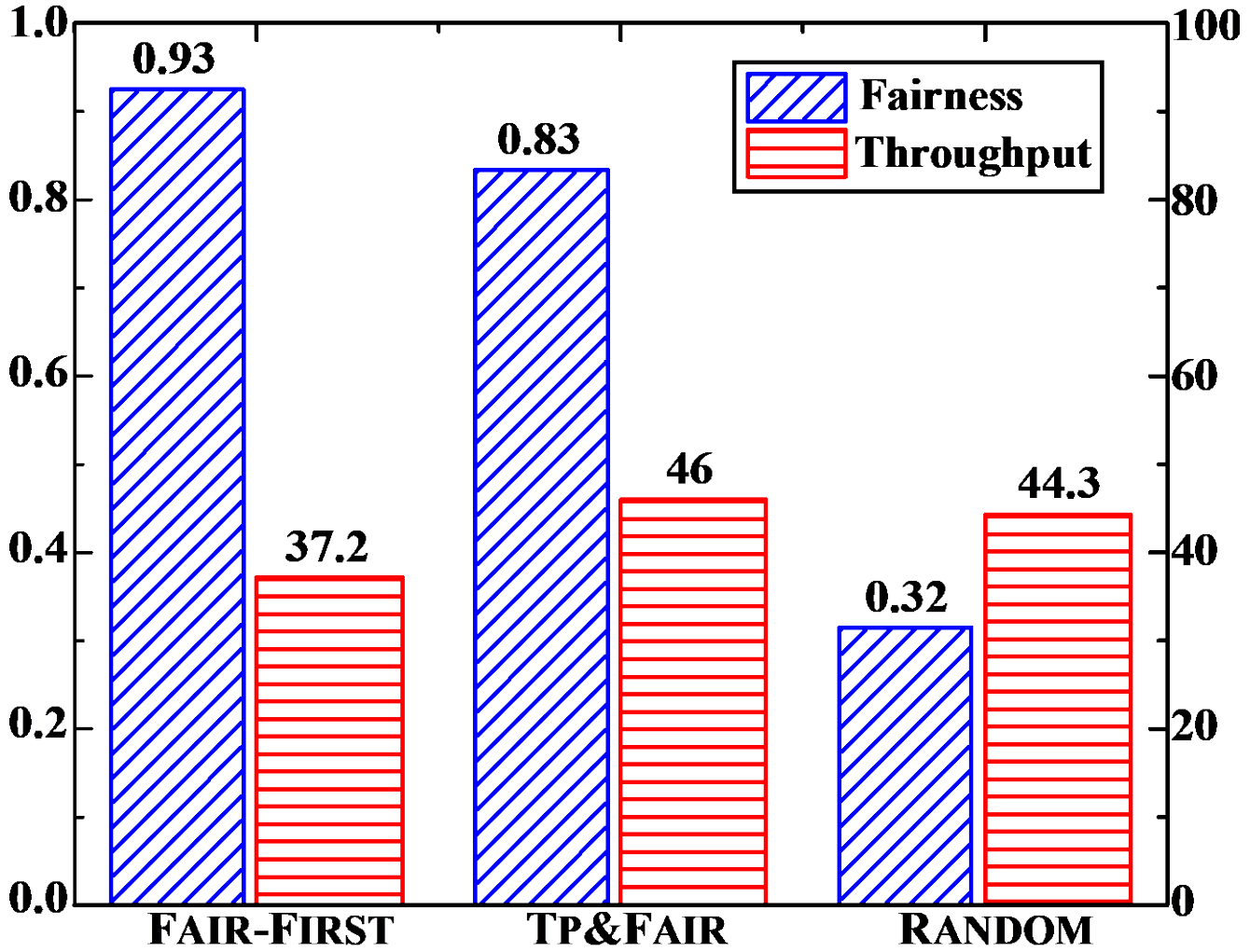
GUI Layer

- Django web framework
- Open HTTP port and present HTML pages
- Submit data following the HTTP protocol



BlocHIE Evaluation

- Deployed BlocHIE with 8 nodes with tx frequency at 7 tx/s/node.



Conclusion

1. Analyzed the requirements for storing and sharing EMRs and PHD
2. Propose two loosely-coupled Blockchain, EMR-Chain and PHD-Chain
3. Combine off-chain storage and on-chain verification in EMR-Chain
4. Propose two fairness-based transaction packing algorithms, FAIR-FIRST and TP&FAIR
5. Implement the BlocHIE in a minimal-viable-product way
6. Evaluate the proposed packing algorithms extensively

Acknowledgments

- This work is supported by Huawei Technologies Co. Ltd. with project code P15-0540 and RGC CRF with project number CityU C1008-16G.

References

- [1] B. E. Dixon and C. M. Cusack, “Measuring the value of health information exchange,” in Health Information Exchange. Elsevier, 2016, pp. 231–248.
- [2] X. Liu, K. Li, G. Min, Y. Shen, A. X. Liu, and W. Qu, “Completely pinpointing the missing rfid tags in a time-efficient way,” IEEE Transactions on Computers, vol. 64, no. 1, pp. 87–96, 2015.
- [3] S. Jiang, J. Cao, Y. Liu, J. Chen, and X. Liu, “Programming large-scale multi-robot system with timing constraints,” in Computer Communication and Networks (ICCCN), 2016 25th International Conference on. IEEE, 2016, pp. 1–9.
- [4] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, “The internet of things for health care: a comprehensive survey,” IEEE Access, vol. 3, pp. 678–708, 2015.
- [5] F. S. Collins and H. Varmus, “A new initiative on precision medicine,” New England Journal of Medicine, vol. 372, no. 9, pp. 793–795, 2015.
- [6] J. Zhou, Z. Cao, X. Dong, and X. Lin, “Tr-mabe: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems,” in INFOCOM. IEEE, 2015, pp. 2398–2406.

[7] N. Grozev and R. Buyya, “Inter-cloud architectures and application brokering: taxonomy and survey,” Software: Practice and Experience, vol. 44, no. 3, pp. 369–390, 2014.

References

- [8] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
- [9] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, vol. 151, 2014.
- [10] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, “Blockchain-based dynamic key management for heterogeneous intelligent transportation systems,” IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1832–1843, 2017.
- [11] H. Hou, “The application of blockchain technology in e-government in china,” in ICCCN. IEEE, 2017, pp. 1–4.
- [12] M. Turkanovi´c, M. H¨olbl, K. Koˇsiˇc, M. Heriˇcko, and A. Kamiˇs “Eductx: A blockchain-based higher education credit platform,” IEEE Access, 2018.
- [13] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, “Medshare: Trust-less medical data sharing among cloud service providers via blockchain,” IEEE Access, vol. 5, pp. 14 757–14 767, 2017.
- [14] Z. Shae and J. J. Tsai, “On the design of a blockchain platform for clinical trial and precision medicine,” in ICDCS. IEEE, 2017, pp. 1972–1980.
- [15] M. Jakobsson and A. Juels, “Proofs of work and bread pudding protocols,” in Secure Information Networks. Springer, 1999, pp. 258–272.

References

- [16] “Nxt: The blockchain application platform via proof-of-stake,” https://nxtplatform.org/, accessed: 2018-01-28.
- [17] “Slimcoin: A peer-to-peer crypto-currency with proof-of-burn,” https://slimcoin-project.github.io/, accessed: 2018-01-28.
- [18] “Litecoin: Open source p2p digital currency,” https://litecoin.org/, accessed: 2018-01-26.
- [19] “Cryptonight hash function,” https://cryptonote.org/cns/cns008.txt, accessed: 2018-01-28.
- [20] “Monero [xmr]: a brand new uprising cryptocurrency which originates from bitmonero,” http://dogecoin.com/, accessed: 2018-01-28.
- [21] R. Jain, D.-M. Chiu, and W. R. Hawe, A quantitative measure of fairness and discrimination for resource allocation in shared computer system. Eastern Research Laboratory, Digital Equipment Corporation Hudson, MA, 1984, vol. 38.
- [22] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer et al., “On scaling decentralized blockchains,” in International Conference on Financial Cryptography and Data Security. Springer, 2016, pp. 106–125.
- [23] A. Gervais, G. O. Karame, K. W¨ust, V. Glykantzis, H. Ritzdorf, and S. Capkun, “On the security and performance of proof of work blockchains,” in CCS. ACM, 2016, pp. 3–16.


thank
you!