Demo:Towards the Development of a Differentially Private Lightweight and Scalable Blockchain for IoT (Under review)

Abdur R. Shahid[§], Niki Pissinou, Laurent Njilla, Edwin Aguilar, and Eric Perez

***Abstract*—In this work, we demonstrate the design and implementation of a novel privacy-preserving blockchain for the resource-constrained Internet of Things (IoT). Blockchain, by design, ensures trust, provides built-in integrity of information and security of immutability in an IoT system without the need of a centralized entity. However, its slow transaction rate, lack of transaction privacy, and high resource consumption are three of the major hindrances to the practical realization of blockchain in IoT. While directed acyclic graphs (DAG)-based blockchain variants (e.g., hashgraph) improve the transaction rate, the other two problems remain open. To this end, we designed and constructed the prototype of a blockchain by utilizing the benefits of high transaction rate and miner-free transaction validation process from hashgraph. The proposed blockchain, coined as PrivLiteChain, implements the concept of local differential privacy to provide transaction privacy and temporal constraint to the lifecycle of the blockchain to make it lightweight.**

***Index Terms*—Blockchain, Storage, Local Differential Privacy, IoT.**

I. Introduction

Blockchain is a distributed peer-to-peer (P2P) way of recording digital interactions in a way that it provides built-in integrity of information, and security of immutability by design, making it very useful to ensure trust, security, and transparency in P2P trustless networks of devices. Blockchain, from its inception as the backbone technology of bitcoin, has evolved significantly in the last few years. With its highly significant features, it has shown serious potential as a key to redesign and improve wireless sensor networks (WSN)-based Internet of Things (IoT). Such a consideration is quite promising, as the existing centralized architecture for IoT systems is incapable of handling the fast-paced growth of IoT. Despite that, tapping into the benefit of blockchain is not straightforward as the state-of-the-art implementation of blockchains are slow in transaction processing, resource-heavy, and lack transaction privacy.

Over the years, several alternatives have proposed with improved transaction rate, including directed acyclic graphs (DAG)-based hashgraph [1]. Hashgraph uses gossip protocol to establish consensus in the network where a node chooses multiple other nodes in the network to share all its information on the historical, as well as new, transactions. The receiver nodes repeatedly do the same, which forms "gossip about gossip". Such a gossip mechanism impressively eliminates the need for vote casting or miner selection process, subsequently yields high transaction rates. For instance, where bitcoin and ethereum's blockchains can process 5 and 15 transactions per second respectively, with enough computing resources, it is possible to yield a throughput of thousands of transactions per second with hashgraph [1], [2]. Babble blockchain [3] is an improvement of hashgraph which projects a hashgraph onto a blockchain to achieve an immutable ordered list of transactions while maintaining the high transaction rate. Despite this, babble is not suitable for resource-constrained IoT devices as it requires high storage capacity and cannot guarantee the privacy of the data of devices shared in the network.

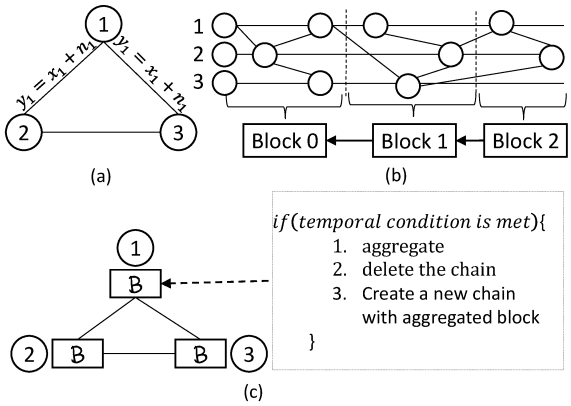


Fig. 1. Fundamental concepts implemented in PrivLiteChain: (a) local differential privacy in transaction, (b) babble hashgraph as the core blockchain, and (c) temporal constraint on the lifecycle of the blockchain.

We address the gap between blockchain, resource-constrained IoT, and privacy by developing PrivLiteChain, a babble-based lightweight blockchain platform with a focus on wireless sensor network-driven IoT systems. It is a part of our long term research goal to develop a lightweight, scalable, secure, and privacy-preserving blockchain platform for resource-constrained mobile IoT systems [4], [5]. It exemplifies the effectiveness of our proposed spatiotemporal mobility-based lightweight blockchain technique, Sensor-Chain [4].

The system of PrivLiteChain is built around three important concepts: local differential privacy (LDP) to achieve transaction privacy, babble's hashgraph blockchain to achieve scalability, and controlled lifecycle of the blockchain to make it lightweight (Figure 1). In the current implementation, PrivLiteChain supports 1-dimensional sensor data, such as environmental data (e.g., temperature and humidity). We also

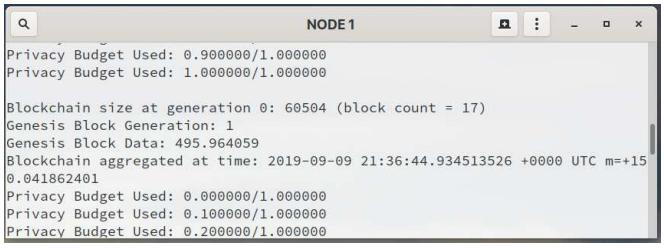
A.R. Shahid, N. Pissinou, E. Aguilar, and E. Perez were with the School of Computing and Information Sciences, Florida International University, Miami, FL. L.Njilla was with the Cyber Assurance Branch, Air Force Research Laboratory, Rome, NY. [§]Corresponding e-mail: ashah044@fiu.edu.

consider each node is connected with all the other nodes in the network and transactions are happened in the form of sensed data broadcast. The sharing of private data over the blockchain can reveal privacy sensitive information about a node [6] for which it is important to privatized the data using LDP before it is released from a node. In a LDP setting, the original sensed data is made obfuscated by adding properly scaled statistical noise to it such that an adversary cannot identify the original data from all the possible values. Theoretically, a mechanism $\mathcal{M}$ satisfies ϵ-LDP ($\epsilon \geq 0$), if and only if for any input x and x', we have, $\forall y \in Range(\mathcal{M}) : \Pr[\mathcal{M}(x) = y] \leq e^{\epsilon}\Pr[\mathcal{M}(x') = y]$. In PrivLiteChain, we implemented Laplace mechanism to achieve ϵ-LDP. If i-th node's original sensed data is x_i, then the broadcasted data (transaction) is $y_i = x_i + n_i$ where n_i is a random noise drawn from Laplace distribution [7] (Figure 1(a)). This transaction is gossiped among the nodes in the network and mapped in the blockchain (the detail of the mechanism can be found in [3]). With each new release of noisy data for the same sensed original data (x_i) the privacy continues to degrade, which refers to the concept of privacy budget ϵ_{total}. It defines the maximum amount of privacy leakage for an original sensed data. Once the privacy budget is completely consumed, a node needs to opt out from making transactions for certain amount of time. The third and final concept that we implemented in PrivLiteChain is a temporal constraint-based lifecycle controlling mechanism. We introduced this concept in our previous work on the design of lightweight blockchain [5]. A temporal constraint, T_{chain}, is a limit on for how long a the blockchain can grow overtime. Let the time of genesis block creation and current time are t_{gen} and t_{cur}, and $(t_{cur} - t_{gen}) \geq T_{chain}$. Then, at time t_{cur}, the data over the blockchain is aggregated locally using a lightweight aggregation method, the existing blockchain is deleted, and a new chain is started with a genesis block containing the aggregated information. The privacy budget ϵ_{total} of each node is reset at each aggregation.

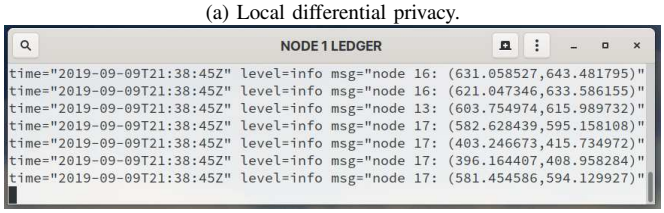
II. Demonstration

In this section, we demonstrate how PrivLiteChain achieves local differential privacy, scalability, and lightweight-ness. The current implementation of it is a permissioned one where every node knows the participants in the network in advance. The screenshots of the demo are presented in Figure 2. A video on the demo can be found at https://youtu.be/0Wcgsqtjvhs. The demonstration will use a laptop where the nodes will communicate with each other over TCP connections.

PrivLiteChain will be demonstrated in three phases. First, we will show the original babble blockchain for 20 nodes and how it processes the transactions in the hashgraph. The nodes generate the transactions at 50% probability. This phase generates some important statistics on babble blockchain, including the size of the blockchain, average transaction rate, average transactions in waiting pool, average block size (in bytes), average number of transactions per block, and block creation rate.



(a) Local differential privacy.



(b) Timed transactions in the network.

Fig. 2. screenshots of PrivLiteChain: (a) Differentially private transactions with privacy budget 1 and $\epsilon = 0.1$. (b) Transactions in the ledger of node 1 where "node $i : (x_i, y_i)$" refers to the i-th node's orginal sensed data and noisy data, respectively.

In the second phase, we will demonstrate the application of Laplace mechanism to achieve LDP in the process of transaction generation. We will demonstrate it with privacy budget, $\epsilon_{total} = 1$. Figure 2(a) shows the privacy budget consumption by node 1 for each transaction. Figure 2(b) presents the original sensed data and its corresponding noisy data in a transaction.

In the final and third phase, we demonstrate the application of temporal constraint on the lifecycle of blockchain. We will use $T_{chain} = 150$ seconds in the setting. In this phase, the demonstration will generate the statistics on the size of PrivLiteChain. Figure 2(a) shows some important information on the aggregation.

References

[1] L. Baird, "The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance," *Swirlds Tech Reports SWIRLDS-TR-2016-01, Tech. Rep.*, 2016.

[2] A. Anjum, M. Sporny, and A. Sill, "Blockchain standards for compliance and trust," *IEEE Cloud Computing*, vol. 4, no. 4, pp. 84–90, 2017.

[3] M. Networks, "Introduction - babble 0 documentation," 2017. [Online]. Available: http://docs.babble.io/en/latest/index.html

[4] A. R. Shahid, N. Pissinou, C. Staier, and R. Kwan, "Sensor-Chain: a lightweight scalable blockchain framework for internet of things," in *The 2019 IEEE International Conference on Internet of Things (iThings-2019)*, Atlanta, USA, Jul. 2019.

[5] A. R. Shahid, N. Pissinou, L. Njilla, S. Alemany, A. Imteaj, and K. Makki, "Quantifying location privacy in permissioned blockchain-based internet of things (iot)," in *The 16th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (Mobiquitous-2019)*, Houston, USA, Nov. 2019.

[6] C. Roulin, A. Dorri, R. Jurdak, and S. Kanhere, "On the activity privacy of blockchain for iot," *arXiv preprint arXiv:1812.08970*, 2018.

[7] W.-S. Choi, M. Tomei, J. R. S. Vicarte, P. K. Hanumolu, and R. Kumar, "Guaranteeing local differential privacy on ultra-low-power systems," in *2018 ACM/IEEE 45th Annual International Symposium on Computer Architecture (ISCA)*. IEEE, 2018, pp. 561–574.