Applications

LSB paper which defines a lightweight scalable blockchain for IoT security and privacy contends that conventional security and privacy methods tend to be ineffective in IoT because of challenges such as resource consumption, centralization and lack of privacy. That is to say, most IoT devices suffer from limited resources which is incompatible with the requirements of complex security solutions. Furthermore, current IoT ecosystems use centralized communication models which is not scalable enough for billions of devices and also creates a bottleneck and point of failure. Blockchain is an effective technology for overcoming these security and privacy challenges that emerge from connecting billions of devices to the Internet of Things. However, current blockchain instantiations have some limitations to be readily adopted in the IoT context. Complex consensus algorithms in blockchain are far beyond the capabilities of most IoT devices. In addition, most IoT devices have limited bandwidth connections and processing capabilities which cause scalability and overhead problems. Latency in blockchain is another parameter that cannot be reasonable in the most IoT applications since they have stricter delay requirements. Finally, the number of transactions in the IoT ecosystem would far exceed such limits in blockchain due to extensive interactions between various entities.

LSB tries to addresses the mentioned challenges by a framework which consists of two main tiers namely, smart home and overlay. To optimize resource consumption, IoT devices in the local smart home get benefits from a local private immutable ledger of local transactions which is managed centrally. Symmetric encryption is used to encrypt transactions in this tier. The overlay tier consists of capable nodes that collaboratively manage a public blockchain which stores overlay transactions. To ensure scalability, the overlay nodes are organized as clusters and only the cluster heads are responsible for managing the public blockchain. At the end, a distributed throughput management mechanism has been introduced to dynamically adjust certain system parameters to ensure that the throughput of the public blockchain does not deviate from the transaction load in the network. In LSB, the flow of data to and from IoT devices is kept separate from the transaction flow which causes optimal unicast routing of data packets and resulting in reduced delays.

Privacy preserving energy transactions (PETra) is another approach which tries to utilize combination of IoT devices and blockchain technology. PETra claims that this approach is a secure and safe solution for transactive microgrids that enables consumers to trade energy without sacrificing their privacy. PETra can be built on distributed ledgers of blockchain and provide anonymity for communication, bidding and trading. The distributed ledger in the transactive microgrid system model of PETra permanently stores transactions that specify energy trades and change regulatory policies for the microgrid. In order to enhance fault tolerance, the ledger should be distributed. A distributed ledger can be implemented using blockchains with proof of stake consensus or a practical Byzantine fault tolerance algorithm. PETra also utilizes a bid storage service for the sake of scalability that enables prosumers (nodes that can produce and consume simultaneously) to find trade partners. This service relieves prosumers from

contacting a large number of potential trade partners since they only communicate with the service to discover trade partners. To measure the prosumers' energy production and consumption, a smart meter must be deployed at each prosumer. Microgrid controller is another component in the transactive microgrid system model which is used to regulate the total load that the microgrid should present to the distribution system.