Blockchains and Smart Contracts for the internet of Things.

This first paper presents whether blockchain and smart contracts can be used for the Internet of things (IoT). This paper presents how IoT combines with blockchain technology: (i) facilitates the sharing of services and resources to creates services between devices, and (ii) allow the users to verify cryptographically different time-consuming workflows. Also presents different problems before using a blockchain network in an IoT as transactional privacy to the expected value of the traded digital assets. One problem of centralized models in IoT is that they have a high maintenance cost, using blockchain technology they can use a trustless peer-to-peer model that can operate transparently and can distribute data. Blockchain and IoT allows sharing services and properties as in (i) Slock.it that works on smart electronics locks, or (ii) at the energy sector that provides a peer-to-peer market where machines can buy and sell energy automatically based on user-defined criteria. The blockchain solution provides lower transaction processing throughput higher latencies. This problem is more important in public networks where proof-of-work mechanisms are deployed. Also, in a blockchain each node performs the same task, where no parallel task execution is possible. Also maintaining privacy, confidentiality and deciding on the miner set are complicated issues to perform on blockchains-IoT. Finally, they pointed out that legal enforceability of smart contracts is limited, and including references to the actual real-world contract in the smart contracts is needed.

LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy

Blockchain is computationally expensive, and also has limited scalability. Also has significant bandwidth overheads which delays are not suitable to the IoT context. Lightweight Scalable Blockchain (LSB) achieves decentralization by forming an overlay network where high resource devices manage a public blockchain that ensures end-to-end privacy and security. LSB also incorporates different optimizations that includes algorithms for lightweight consensus, distributed trust and throughput management. This paper presents a framework based on blockchain to preserve security and privacy for IoT that uses a smart home setting. Also they planned to use this framework to a broad range of IoT applications. In addition, this framework is tailored to meet the specific requirements of IoT devices and applications with optimizations that includes a lightweight consensus algorithm, a distributed trust method, a distributed throughput management strategic and a separation of the transaction traffic from the data flow. This paper presents a time-based consensus algorithm that must ensure that a block generator is selected randomly among nodes and is limited in the number of blocks it can generate.

Providing Privacy, Safety, and Security in IoT-Based Transactive Energy Systems using Distributed Ledgers

This paper presents decentralized IoT solutions where local communities can use transactive energy microgrids where users can trade energy with each other. However, there are problems like find an efficient way of providing security, safety and privacy in a decentralized and transactive energy system. This system is a set of market-based construct for dynamically balancing the demand and supply across the electrical infrastructure. In a distributed market, there is a problem in which erroneous and/or

malicious transactions can create a gap between demand and supply can destabilize the system. The analysis performed in this paper in a distributed IoT infrastructure focuses on different privacy challenges as: (i) leakage of energy usage patterns to other consumers, (ii) inference of future states of a consumer, and (iii) personally identifiable information. The authors present the called Privacy-preserving Energy Transactions (PETra) to provide privacy to the consumers in a transactive energy IoT system without compromising grid safety and security. Finally, this solution provides: (i) communication anonymity, (ii) transaction anonymity, and (iii) bidding anonymity.