Radoslaw Krzeski
Summary of Topic XIiI – Applications

Blockchains and Smart Contracts for the Internet of Things

The text explains a few basic things in the blockchain world: Looking at blockchain as distributable peer-to peer systems and how it uses smart contracts. Further, it looks at how technology facilitates the sharing of services and marketplaces, and how it automates workflows in a cryptographic manner. They also discuss issues such as transactional privacy of the digitized assets.

It begins by explaining what Bitcoin is, how the ledger works, and the problem it solved with double-spending. The node network supplies the underlying network that is required for the decentralized chain, the transaction and consensus system. A few other hashing algorithms mentioned apart from the proof-of work concepts are mentioned; Blake-256, scrypt and Myriad. Other BFT protocols mentioned are Tangaroa (Raft algorithm(Juno)), Tendermint, PBFT, and Sieve in the Hyperledger Fabric project.

The article briefly mentions Nick Szabo as the original creator of the idea behind Smart Contracts. A few key elements are described of these contracts that are of interest:

- The contracts have its own state, can take custody of assets.
- Allows to express business logic
- A proper contract should describe all possible outcomes (how about advanced, arbitrary contracts?)
- It is driven by data and is deterministic (results on different nodes are the same)
- Triggered by messages/transactions
- Resides on the chain and uses cryptographically verifiable traces
- In addition to the possible creation of decentralized autonomous organization, DAO`s

There are also a few distinct categorizations made; whether the network is accessible (permissionless, permissioned), who can transact/mine, and whether it's a transaction or an account-based model.
A network should also be robust, tolerate node failures, identify conflicts and forks, uphold transparency and auditability and make participants who do not trust each other able to trade through necessary means.

An example of the IoT network is made, where multiple devices from a manufacturer use the blockchain to probe for new firmware. It can then propagate into other nodes with time, becoming independent of the manufacturer. I believe we read about a similar scenario in a previous papers, and some of the other examples follow the same pattern. A slightly different example it the transportation chain, where the ability to layer communication between contracts create seemingly efficient and safe environments for trade of goods and transport.

Some issues mentioned were lower transaction processing compared to modern, centralized systems. Sharding and proof-of work are other limiters. Maintaining privacy is another, major issue. Using different keys are a way to mitigate this. The issues of legal enforceability are briefly mentioned towards the end. Work is being on how to "dual-integrate" blockchain with real-life contracts. Lastly, the expected values of tokens, or currency is mentioned, along with a few prerequisites that need to be present for a successful network.

Keywords: decentralized fashion, central authority, trustless networks, Sybil attack, proof of Stake, network entities, Ethereum Improvement Protocol, Elements Alpha experimental chain, complete autonomy.

LSB: A Lightweight Scalable Blockchain for IoT Security and Privacy

This paper focuses on something called a tiered Lightweight Scalable Bitcoin Chain. It is described for a "home setting for broad IoT applications". It has a centralized manager that establishes shared keys for communication, and forms an overlay network with an blockchain connecting devices. A few issues are on how to implement efficiently in the IoT-world: Resource consumption, centralization and the always-present point of privacy. Complex consensus process makes it difficult to process to smaller devices, and scalability is limited when all nodes must do computations. Network overheads are also a major point.

LSD contain mostly by two main tiers, the smart home and overlay (in the article at least). Within these there are to main aspects; transactions and the BlockManager(entity for managing BC). Entities in the local smart home use a local, private Immutable Ledger of local transactions (usually multisig), structurally the same as Bitcoin, but managed centrally. The overlay tier consists of capable nodes, such as SP servers, which manage a public BC that stores overlay transactions. These are organized in clusters, and only so-called Cluster Head are responsible for managing the public BC. A different name used for these is Overlay Block Managers (OBM`s)

The paper proposes a lightweight consensus algorithm that “limits the number of new blocks generated by CH`s within a tunable consensus period” (Page 2 in the paper). Also mentioned by the name of “distributed trust algorithm”.
CH`s also have a trust model implemented, which reduced the amount of blocks they need to verify. A Distributed Throughput Management mechanism will also ensure stability. A few of the key points outlined are:

- A comprehensive tiered network based on BC tech
- LBS is specified for IoT devices and applications
- Resistant to a set of 12 attacks
- Simulations ensure justified design of the network.

When an OBM received a transaction is check if a receiver is present in the cluster, and check a key list. If present, transactions is sent onwards. OBM`s also retain a transaction pool, that when reached full limit, congregate into a block in the chain.
The Smart Home itself is connected to the network by an Internet Gateway, a router. Uses the Diffie-Helman distribution method to give keys to all IoT entities on the network.

The article then dwelves down in large amounts of details that are to comprehensible to summarize. An interesting aspect though was the attacks. Two that stuck out were the attacks when an IoT is either injected into the system with the permission of the home owner. Hackers have and will make sure to use this if the system becomes widely distributed. The other is a node becomes so trusted before it at some point becomes corrupt.
Another note is how heavily this system is supported by insanely educated individuals. If something is developing, then this system is surely it, being well documented and tested.

Keywords: Immutable ledger, Symmetric encryption, Burning Bitcoins,

Providing Privacy, Safety, and Security in IoT-Based Transactive Energy Systems using Distributed Ledgers
The main research question revolves around power grids, and the management of these through the IoT-network, so called transactive microgrids; a new vision of decentralized power-grid operations. A new term mentioned is “prosumers” (who have the capability to generate and store energy), who are entities who trade energy in the microgrid. It argues that the microgrid struggles to main order and sufficient privacy of such a system, not to mention infrastructure stability. The paper continues to describe so called – Privacy-preserving Energy Transactions (PETra`s). It builds on distributed ledgers and blockchains. A few examples are mentioned: Voltron, OpenFMB, RIASPS.

Some major issues discussed in regard to privacy:

- Leakage of energy usage pattern to other prosumers. Required “smart metering”
- Inference of future states of a prosumer (out of the house, evening)
- Personally, identifiable information

Petra solves this by being secure, verifiable, preserves prosumer privacy and enables DSO`s to regulate trading and enforce certain rules (assuming distribution feeder and support exchange of power between them).
A few components are necessary; distributed ledger for recording transactions, a bid storage service, microgrid controller and smart meters. It uses a few defined functions, such as “energy selling/buying workflow” – “mixing service” and decentralized protocols such as CoinShuffle. It is also mentioned da few different transactions, and amongst these assets that are being traded. The article emphasizes privacy and transaction anonymity very heavily, but bypasses some of the more practical issues of implementing such a system.

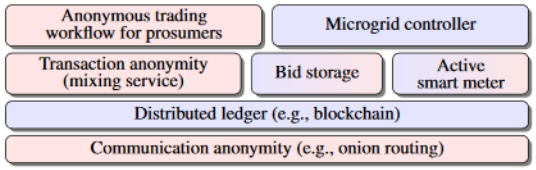

Figure 1. Architecture of a decentralized transactive microgrid with PETra.

Keywords: Distributed System Operators (DSO`s), transactive energy, smart meter/inverter.

References:

Blockchains and Smart Contracts for the Internet of Things

Konstantinos Christidis and Michael Devetsikiotis
http://ieeexplore.ieee.org/document/7467408/

LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy
Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram
https://arxiv.org/abs/1712.02969

Providing Privacy, Safety, and Security in IoT-Based Transactive Energy Systems using Distributed Ledgers
Aron Laszka, Abhishek Dubey, Michael Walker, Douglas Schmidt
https://arxiv.org/abs/1709.09614