Understanding Blockchain: Definitions, Properties, Architecture, and Comparisons

Mohammad H. Tabatabaei

Advisors: Roman Vitenberg, Hein Melling

University of Oslo, University of Stavanger

Motivation:

- Not having a clear definition and knowledge of blockchain systems in the state-of-the-art
- The area is highly volatile: old definitions are no longer relevant
- No taxonomies in existence

Contributions:

- Defining the main attributes of the blockchain systems
- Defining representative attributes and properties of each layer in a layered blockchain architecture
- Defining the roles of various entities in blockchain systems and interactions between them
- Investigating representative blockchain systems to compare them based on the layers' attributes

Blockchain Definitions*:

1. Blockchain is a system that uses the data structure of bitcoin but extends the functionality.
2. Blockchain is a system that maintains a chain of blocks.
3. Blockchain is a system that maintains a ledger of all transactions
4. Blockchain is a system with distributed non-trusting parties collaborating without a trusted intermediary.
5. Blockchain is a system that uses smart contracts.

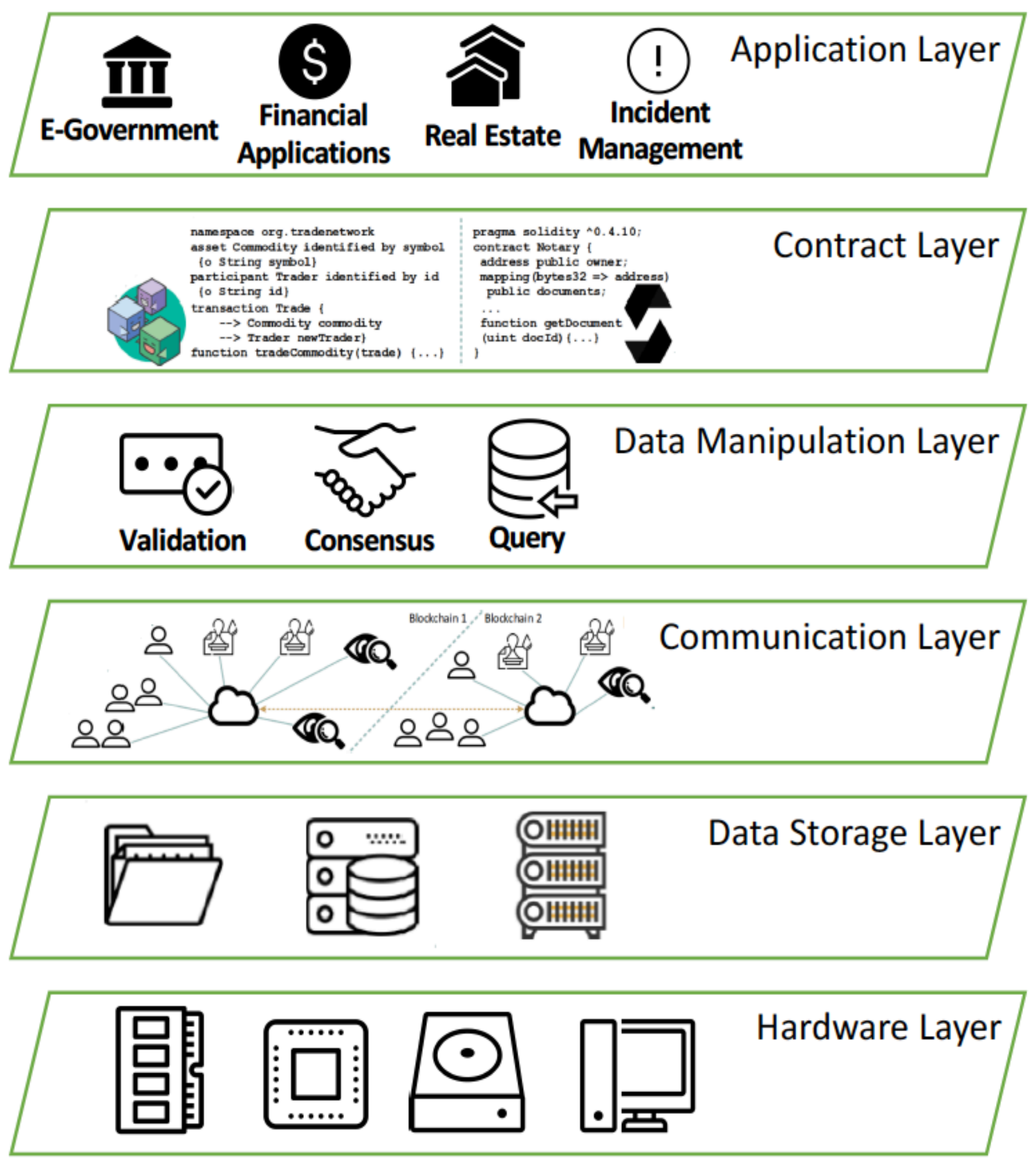
*Jacobsen, Hans Arno; Sadoghi, Mohammad; Tabatabaei, Mohammad Hossein; Vitenberg, Roman; Zhang, Kaiwen. Blockchain Landscape and AI Renaissance: The Bright Path Forward. I: Proceedings of the 19th International Middleware Conference. Association for Computing Machinery (ACM) 2018 ISBN 978-1-4503-5702-9. p. -

Five Pillars of Blockchain Systems:

The followings are inherent blockchain properties. There are also other properties present in blockchain systems, but they are not specific to this technology.

1. **Lack of trusted third party:** There is no hierarchy of authority, and all decisions are made by consensus between the participants, without a central intermediator.
2. **Verifiability**: More than just one trusted authority could be allowed to verify the correctness of the transactions, blocks, and states of the system.
3. **Transparency**: The content of transactions, states of them, and associations of the transactions with identities are open to viewing
4. **Immutability**: Blockchain's data is protected against any modification by misbehave or unconscious participants.
5. **Traceability**: Providing an easy way to identify the origin of data, its creator, and its lifecycle.

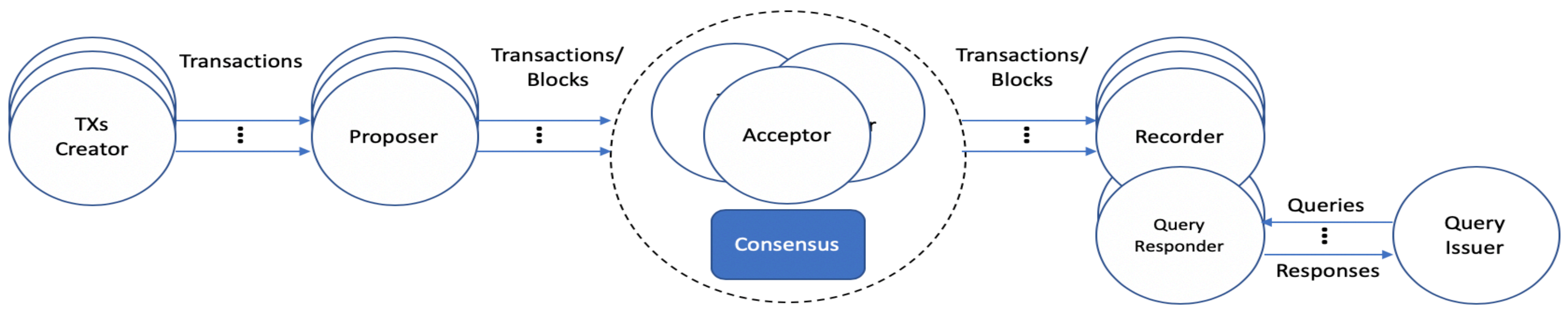
Blockchain Architecture:



```
namespace org.tradenetwork
asset Commodity identified by symbol
 {o String symbol}
participant Trader identified by id
 {o String id}
transaction Trade {
    --> Commodity commodity
    --> Trader newTrader}
function tradeCommodity(trade) {...}
```

```
pragma solidity ^0.4.10;
contract Notary {
 address public owner;
 mapping(bytes32 => address)
  public documents;
 ...
 function getDocument
 (uint docId) {...}
}
```

Blockchain Roles:



Mapping Roles to Entities:

Blockchain Systems	Transactions Creator	Proposer	Acceptor	Recorder	Query Responder	Query Issuer
Bitcoin	Bitcoin Nodes	Miners	Bitcoin Full Nodes	Bitcoin Full Nodes	Dedicated Services	Everyone
Ethereum	Ethereum Nodes	Miners	Ethereum Full Nodes	Ethereum Full Nodes	Dedicated Services	Everyone
Hyperledger Fabric	Application Clients	Orderers	Peers	Peers	Peers	Application Clients
IOTA	IOTA Nodes	IOTA Nodes	IOTA Nodes	IOTA Full Nodes	Dedicated Services	Everyone

Comparing blockchain systems based on the layers' attributes:

- Two tables below are samples of our results (Comparisons for data storage layer, data manipulation layer, contract layer, and application layer are given in our paper)
- Negative and positive points of the systems can be inferred from the tables in order to identify the gaps

Hardware Layer of Different Blockchains:

Blockchain Systems	Limiting Resource	Crypto Puzzle Solving Device	Additional Hardware for Security
Bitcoin	Processor	ASIC	Hardware-based Trusted Execution Environment
Ethereum	Memory Bandwidth	GPU	Hardware-based Trusted Execution Environment
Hyperledger Fabric	Application Dependent	No Device	Application Dependent
IOTA	Processor & Network Bandwidth	Proprietary Processor (JINN - in progress)	Not Applicable

Communication Layer of Different Blockchains:

Blockchain Systems	Granularity	Protocol	Ordering Guarantees	Privacy & Security Guarantees	Propagation Time
Bitcoin	Whole Network	Push-gossiping Inventory & Pull by Nodes	No Guarantee	No Guaranty	About 12.6 seconds
Ethereum	Whole Network	Push-flooding	No Guarantee	Encrypted and authenticated messages	No studies conducted
Hyperledger Fabric	Per Channel	Push-gossiping and Pull-gossiping blocks	Atomic Communication	Authenticated channels	Application dependent
IOTA	Whole Network	Push-flooding	No Guarantee	Encrypted data streams (MAM Protocol)	No studies conducted

Future Works:

- To find the fields that are still open for further studies by analyzing the layered features of the mentioned blockchain systems
- To do experiments on the representative blockchain systems and compare them based on the quantified attributes such as throughput, latency, and storage overhead
- To identify unresolved technical challenges in the current blockchain implementations based on the experiments