Note on blockchain structure and scalability

Bitcoin, Ethereum and IOTA are representatives of the Blockchain ecosystem. This brief note analyzes the evolution of the Blockchain technology infrastructure through the analysis of the aforementioned cryptocurrencies.

Table of Contents

1 Introduction

Nearly 9 years after the launch of the Bitcoin protocol, the term "Blockchain" is widely used to designate a set of technologies, protocols and uses whose primary function is to enable a reliable and secure payment method by using a public and decentralized network of machines (computer, embedded hardware or more generally any machine capable of computing calculations).

To achieve this goal, the Blockchain must overcome a series of challenges: decentralization, scalability, validation speed and security, incentive to expand the network.

Semantically Blockchain comes from Bitcoin and corresponds to the technological choice of the protocol. The term does not correctly represent the various kinds of implementation (altcoins, Ethereum, IOTA ...). However, for the sake of simplicity, we will use the term Blockchain to refer to the technology and the use of the protocol for a payment service

2 A public state machine

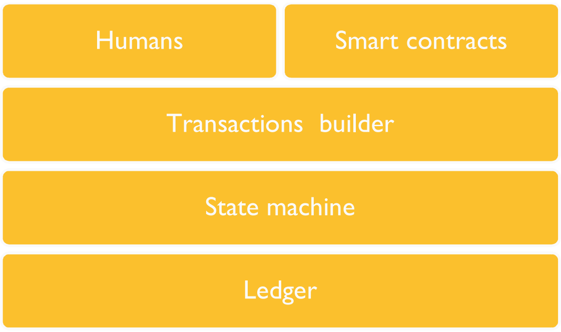
2.1 The concept

Conceptually Blockchain is an immutable state machine, where participants in networks work together to move the system to the next state.

2.2 Requirements

To exist as a publicly accessible entity, a state machine must rely on several services: (1) a set of states, (2) a predefined evolution protocol, (3) transactions.

(1) is usually called the ledger with reference to the accounting ledger (transaction log).
(2) is generally called the consensus.
(3) can be provided by humans or an automated Smart Contract program. Smart contracts are an interesting part of the Blockchain since they allow to see the Blockchain not only as a simple database but also as a computing service.



2.3 A probabilistic approach of security

Decentralized ledger, state machine concepts, computing services are not new concepts. They already existed before and were used in several successful projects.

Blockchain's most innovative concept is the perception of security as a probabilistic function of time. When the information is accessible to the public, it is simply impossible to avoid hacker attacks or attempted fraud. It is part of all human activities. Blockchain solves the problem by creating a system that maintains a version of states with a high probability level of being true.

2.4 The Blockchain history

Even though the blockchain story begins before the appearance of Bitcoin, the well-known blockchain is probably one of the most successful projects of the beginning of this century. Bitcoin introduced the concept of Blockchain in the public scene.

Ethereum brings significant improvements by trying to crystalize all the different altcoins approaches into the concept of smart contract. Smart contracts democratize the concept of Blockchain as a service.

IOTA is one next major evolution of the Blockchain. IOTA differs fundamentally from previous implementations as it comes with a ledger model in the form of a directed acyclic graph (the Tangle). It has been built from the beginning to overcome scalability problems of Bitcoin architecture. The ledger is asynchronous and allows the possibility to have payment with no fees.

	Bitcoin	Ethereum	IOTA
Ledger model	Linked list of blocks	Linked list of blocks	Directed acyclic graph
Transaction model	UTXO model	Account model	Account model
Consensus model	PoW	PoW/PoS	IOTA PoW
Inputs model	humans	Humans and smart contract	Humans and smart contract (future service layer)

2.5 A note on private blockchain

With the success of Bitcoin, many companies have developed so-called private blockchains. However, these blockchains cannot be considered as true blockchain without the concept of public security. Examples include R3 and Hyperledger.

These projects are gaining momentum in corporate and banking area. The reality is that many companies have never changed their information systems until recently. The advent of Bitcoin has put pressure on them to change their system. The decentralized database, microservice architecture or state machine programming (Erlang actor model was created in 1986) has been around for a long time. These projects use the momentum created by Bitcoin for commercial purposes.

3 Ledger models

3.1 A chain of blocks

3.1.1 Description

Bitcoin, Ethereum and most altcoins structure the ledger as a chain of blocks. A blockchain is a standard linked of list of elements called blocks.

Each block contains specific information (the header) (time, nonce, previous block hash or address) and all the transactions.

3.1.2 The lock synchronization problem

Even though there are several machines, the ledger blockchain acts as a synchronization mechanism between all network nodes. It has been modelled around a standard linked list structure. A list cannot be expanded in parallel, otherwise it loses its integrity.

In another area, Python has a similar problem. The Python interpreter is built around the GIL (Global Interpreter Lock). Many attempts to get rid of GIL have failed. It is a fundamental architectural problem. Once it is here, it is hard to get rid of it. The blockchain registry model suffers from the same problem.

3.2 A directed acyclic graph model

3.2.1 Description

IOTA has chosen a different approach than Bitcoin. The ledger is implemented has a directed acyclic graph between transactions. The notion of time is not obviously represented. Every transaction must be validated by two others previously validated transactions. The system is working in an asynchronous way to validate each transaction.

A transaction is never really validated. A transaction is validated on a probability way. The more the transactions get validated, higher the probability that the transaction is correct. This is the main innovation behind the tangle.

3.2.2 A fully parallel structure

On the contrary to list, a directed acyclic graph can be expanded on several points of its structure. It allows multiple entity to work in parallel as soon as they do not work on the same nodes.

4 Transactions models

4.1 The UTXO model

4.1.1 Description

In Bitcoin the state is a collection of Unspent Transactions Outputs (UTXO).

An UTXO is like a physical coin, it has a value and an owner. It can only be spent (destroy). Like a physical coin it is immutable.

It means that several input UTXO may be used in a transaction to make a payment that it in aggregate lower that the value of the inputs. A specific output UTXO will be created with the remaining coins and will be sent back to the owner.

At any time, the wealth of an owner is the sum of all is UTXO.

A transaction is so represented as a function that take UTXO as inputs and send back UTXO as outputs.

4.1.2 Advantage

The UTXO model offers the possibility to a participant to validate multiple independent transactions in parallel. Let's imagine a custody bank that own an omnibus account. With UTXO model, the bank has the possibility to treat simultaneously several customer transactions at the same time.

4.1.3 Disadvantage

In an UTXO model, implementing a wallet is more difficult as the wallet must reconstruct the aggregate value of all UTXO own by the owner.

Another disadvantage is that the parallelism advantage mentioned above can only be achieved if the wallet has been already prepared for multiple execution. Meaning that if one person owns one UTXO and wants to buy two products, it will have first to split is UTXO and then buying the products. This process will necessitate 2 validation steps, identical to treat the transactions on a sequential base.

4.2 The account model

4.2.1 Description

The account model is inspired by the financial industry. In this model the state is composed of accounts. The account model has been introduced by Ethereum as part of the smart contract concept.

There are two kinds of accounts, the external ones or the human's ones and the contract ones. In his documentation Ethereum talk about messages as transactions. This analogy is not anodine as the Ethereum inspired itself from the actor model (implemented in Erlang and democratize with Akka). An account is similar to one actor, it can send and receive messages to other actors. Messages are transactions. Messages represent the state machine function that allows the chain to change of state.

4.2.2 The simplicity as an advantage

Ethereum has been from the ground modelled to be more than a payment infrastructure. It has been made to build an ecosystem of business on it.

Reasoning in term of accounts and message is extremely easy and allows a quick way to model workflows.

4.2.3 The actor model advantage and disadvantage

Ethereum implements a model in between the actor model and the virtual actor model (Orleans, Orbit, Fabrik). The smart contracts live somewhere in the network, they are persistent through to the ledger and they can be trusted to be executed.

This approach offers the possibility to use the Blockchain as a high availability system.

The actor model is a workflow model. Transactions are not able to be run in parallel due to obvious reasons of synchronization.

IOTA threats the problem differently. Each transaction has a probability score, accounts have also a probability score. It is up to the participants to define the trigger of probability with which they are comfortable.

5 Consensus models

5.1 The proof of work

5.1.1 Blockchain validation

Security is achieved in Bitcoin by a race between honest miners and attackers. Validation is implicit in Bitcoin; the longest chain is the valid one.

An attacker will have to maintain a fork of the blockchain and then having a computing capability superior to all the honest nodes in order to corrupt the blockchain (the attacker fork chain becoming then the de facto valid chain).

5.1.2 Vulnerabilities and disadvantages

(1) **Vulnerability to technology shock**. This process is vulnerable to potential sudden jump in processing capability like the one that will come with quantum computer. Obviously, there is always the possibility to change the cryptographic challenge into something else (Proof of stake).

(2) **Important level of energy consumption**. The cryptographic challenge is also debatable as it consumes a lot of computing and electricity power for nothing more than block validation.

(3) **Limitation in response time**. The cryptographic challenge is time consuming and limits the network to support a growing volume of transactions.

(4) **Congestion problem**. The network is not asynchronous and response time of the ledger will increase with an increase of the number of clients

(5) **Fees incentives problem**. The standard proof of works requires special participants (the miners) to be willing to validate and expand the network. These miners receive incentive fees. The level of fees could limit the usage of

the Blockchains because micropayments could simply be too expensive.

5.2 The proof of stake

The proof of stake algorithm replaces the cryptographic challenge by requiring that the validator put collateral in front of each transaction in order to validate a block.

The proof of stake model solved the speed limitation of proof of works. However, the fees problem still exists.

5.3 IOTA proof of work

5.3.1 Validation of transactions

In the consensus model used by IOTA, every participant need to validate 2 transactions in order to send one. Every participant has an economic interest in expanding the network by using it. Fees are not necessary.

5.3.2 A lot of advantages

(1) **Micropayment business**. Transactions without fees can allow the possibility of micropayments.

(2) **Scalability and asynchronous model**. IOTA is scalable. The Tangle is totally asynchronous. There is not distinction between clients and miners. Each participant must validate 2 transactions to send one. Each participant works on one part of the ledger without not being synchronized with the rest of the ledger.

(3) **Avoid congestion**. Every participant improves the security and response time of the network.

(4) **Resistant to technology shock**. Once the network is dense enough and because IOTA has been made to be run on embedded system, the network is resistant to quantum computing.

5.3.3 A dense network is compulsory

People who work with DAG and parallel computing, will always tell you the same. DAGs are fantastic structures because they solve many simple problems. However, the creation of the DAG is the critical point.

IOTA is not immune to this problem. The IOTA model is only secure when the network is sufficiently dense in terms of participants. In the meantime, he will have to rely on the service of a third party to maintain the integrity of the ledger (the coordinator).

6 Conclusion

Bitcoin, Ethereum and IOTA are representative of the evolution of blockchain technology.

Bitcoin is the pioneering project and it is democratizing a publicly decentralized payment network. Ethereum extended the use of Blockchain by introducing smart contracts. By doing so it broadened the possible usage of the Blockchain. It is not anymore an external payment service but an internal tool that allows companies to model products and workflows.

However, Bitcoin and Ethereum suffer from scalability and speed issues inherent to the ledger model as a chain of blocks and the consensus model.

By changing the ledger structure and extending the concept of probabilistic transaction, IOTA is the next step. IOTA solves the problem of scalability and speed of its predecessors. By allowing micropayment activity, it expands the possible use of blockchain technology. However, it must face the problem of building the network (inherent to DAG structure) and the future will validate or not the technological choices.

7 Bibliography

Nakamoto, S. (n.d.). *Bitcoin: A Peer-to-Peer Electronic Cash System.*

Popov, S. (October 1,2017). *The Tangle.*

Wood, D. G. (EIP-150 revision). *Ethereum: A secure decentralised generalised transaction ledger.*