What is a blockchain?

Ricardo Pérez-Marco

(CNRS, IMJ-PRG, Labex Réfi & MME-DII)

Blockchain : émergence d'une nouvelle forme de confiance numérique

Journée SIF

November 14, 2016

What is a blockchain?

Blockchain definition

Blockchain definition

We propose the following general definition:

Blockchain definition

We propose the following general definition:

Definition

A blockchain is a decentralized database.

Blockchain definition

We propose the following general definition:

Definition

A blockchain is a decentralized database.

Blockchain definition

We propose the following general definition:

Definition

A blockchain is a decentralized database.

Decentralized: All entities and individuals writing or amending the database have the same rights and obligations. They do follow the same pre-established rules.

Blockchain definition

We propose the following general definition:

Definition

A blockchain is a decentralized database.

Decentralized: All entities and individuals writing or amending the database have the same rights and obligations. They do follow the same pre-established rules.

Basic example: Bitcoin's blockchain is the blockchain where all bitcoin transactions are recorded.

Blockchain definition

We propose the following general definition:

Definition

A blockchain is a decentralized database.

Decentralized: All entities and individuals writing or amending the database have the same rights and obligations. They do follow the same pre-established rules.

Basic example: Bitcoin's blockchain is the blockchain where all bitcoin transactions are recorded.

Theorem

Transparency Theorem: *An electronic decentralized currency must rely on a blockchain.*

Private blockchain

We can restrict the notion to decentralization among a predefined class of agents.

Private blockchain

We can restrict the notion to decentralization among a predefined class of agents.

In that case there is no pure decentralization and a central authority issues the right to participate in the database.

Private blockchain

We can restrict the notion to decentralization among a predefined class of agents.

In that case there is no pure decentralization and a central authority issues the right to participate in the database.

Definition

A private or confederate “blockchain” is a decentralized database among a predefined class of agents.

Private blockchain

We can restrict the notion to decentralization among a predefined class of agents.

In that case there is no pure decentralization and a central authority issues the right to participate in the database.

Definition

A private or confederate “blockchain” is a decentralized database among a predefined class of agents.

Private blockchain

We can restrict the notion to decentralization among a predefined class of agents.

In that case there is no pure decentralization and a central authority issues the right to participate in the database.

Definition

A private or confederate “blockchain” is a decentralized database among a predefined class of agents.

This is closer to a standard database than to a blockchain.

Poperties and Corollaries

- A blockchain is **open** and **permissionless**, i.e. anyone respecting the rules and formats can write on it .

Poperties and Corollaries

- A blockchain is **open** and **permissionless**, i.e. anyone respecting the rules and formats can write on it .

Decentralisation imposes that there cannot be a central authority issuing “writing or editing permission”.

Poperties and Corollaries

- A blockchain is **open** and **permissionless**, i.e. anyone respecting the rules and formats can write on it .

Decentralisation imposes that there cannot be a central authority issuing “writing or editing permission”.

- A blockchain is governed by **automatic rules** defined by a protocol.

Poperties and Corollaries

- A blockchain is **open** and **permissionless**, i.e. anyone respecting the rules and formats can write on it .

Decentralisation imposes that there cannot be a central authority issuing “writing or editing permission”.

- A blockchain is governed by **automatic rules** defined by a protocol.

If the rules were not automatic, action from an external authority would be needed and decentralization would be broken.

Antifragility

Antifragility

- **Antifragile systems** benefit from catastrophic events (Taleb).

Antifragility

- **Antifragile systems** benefit from catastrophic events (Taleb).
- A blockchain is **antifragile**.

Antifragility

- **Antifragile systems** benefit from catastrophic events (Taleb).
- A blockchain is **antifragile**.

Centralization is fragile since it has a central point of failure. Decentralized structures, through more inefficient, are more resilient.

Antifragility

- **Antifragile systems** benefit from catastrophic events (Taleb).
- A blockchain is **antifragile**.

Centralization is fragile since it has a central point of failure. Decentralized structures, through more inefficient, are more resilient.

- Private or confederate blockchain are **fragile**.

Antifragility

- **Antifragile systems** benefit from catastrophic events (Taleb).
- A blockchain is **antifragile**.

Centralization is fragile since it has a central point of failure. Decentralized structures, through more inefficient, are more resilient.

- Private or confederate blockchain are **fragile**.

Byzantine Generals Problem

Byzantine Generals Problem

Problem: How to reach an honest consensus and prevent malicious attacks?

Byzantine Generals Problem

Problem: How to reach an honest consensus and prevent malicious attacks?

Byzantine Generals Problem (BGP)

Byzantine Generals Problem

Problem: How to reach an honest consensus and prevent malicious attacks?

Byzantine Generals Problem (BGP)

The situation can be described as the siege of a city by a group of generals of the Byzantine army. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach an agreement.

Byzantine Generals Problem

Problem: How to reach an honest consensus and prevent malicious attacks?

Byzantine Generals Problem (BGP)

The situation can be described as the siege of a city by a group of generals of the Byzantine army. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach an agreement.

Nakamoto Byzantine Generals Problem

Nakamoto Byzantine Generals Problem (NBGP)

Nakamoto Byzantine Generals Problem

Nakamoto Byzantine Generals Problem (NBGP)

The number of generals is not fixed. Anyone can participate in the decision network.

Nakamoto Byzantine Generals Problem

Nakamoto Byzantine Generals Problem (NBGP)

The number of generals is not fixed. Anyone can participate in the decision network.

Definition

A **Decentralized Consensus Protocol (DCP)** is a solution to NBGP.

Thermodynamic conjecture

Thermodynamic conjecture

- The protocol running a blockchain solves NBGP.

Thermodynamic conjecture

- The protocol running a blockchain solves NBGP.

This is necessary to make sure that a minority cannot corrupt the database.

Thermodynamic conjecture

- The protocol running a blockchain solves NBGP.

This is necessary to make sure that a minority cannot corrupt the database. Only known solution to NBGP is based on PoW (to defend from a Sybil attack).

Thermodynamic conjecture

- The protocol running a blockchain solves NBGP.

This is necessary to make sure that a minority cannot corrupt the database. Only known solution to NBGP is based on PoW (to defend from a Sybil attack).

- No non-PoW solution to NBGP is known, thus security relies on a PoW.

Thermodynamic conjecture

- The protocol running a blockchain solves NBGP.

This is necessary to make sure that a minority cannot corrupt the database. Only known solution to NBGP is based on PoW (to defend from a Sybil attack).

- No non-PoW solution to NBGP is known, thus security relies on a PoW.

Thermodynamical Conjecture: There is no solution to NBGP without external input of energy.

Thermodynamic conjecture

- The protocol running a blockchain solves NBGP.

This is necessary to make sure that a minority cannot corrupt the database. Only known solution to NBGP is based on PoW (to defend from a Sybil attack).

- No non-PoW solution to NBGP is known, thus security relies on a PoW.

Thermodynamical Conjecture: There is no solution to NBGP without external input of energy.

Thermodynamic proof: We cannot have an isolated system with decreasing entropy.

Strong Thermodynamic Conjecture

Strong Thermodynamic Conjecture

Strong Thermodynamic Conjecture

- The protocol running a blockchain establishes a chronology.

Strong Thermodynamic Conjecture

- The protocol running a blockchain establishes a chronology.

Incompatible changes of the same data must be resolved by prioritizing one of the changes. This cannot rely on an external clock or decentralization would be lost. Therefore there is an internal chronology of modifications of the database.

Strong Thermodynamic Conjecture

- The protocol running a blockchain establishes a chronology.

Incompatible changes of the same data must be resolved by prioritizing one of the changes. This cannot rely on an external clock or decentralization would be lost. Therefore there is an internal chronology of modifications of the database.

Strong Thermodynamical Conjecture: There is no protocol establishing an internal chronology of a system without external input of energy.

Universal blockchain

Universal blockchain

Not every blockchain is composed by blocks...but...

Universal blockchain

Not every blockchain is composed by blocks...but...

- Associated to a blockchain B there is a universal blockchain $\tilde{B}$ composed by a sequence of cryptographically linked ordered blocks.

Universal blockchain

Not every blockchain is composed by blocks...but...

- Associated to a blockchain B there is a universal blockchain $\tilde{B}$ composed by a sequence of cryptographically linked ordered blocks.

This is a standard construction of universal objects in category theory. We consider the class of blockchains with morphisms $A \to B$ if the blockchain B can be obtained from A by removing data. The universal blockchain is the blockchain which contains as data all the chronological modifications of the blockchain.

Monetary Theorem

- The security of a PoW blockchain relies on a cryptocurrency.

Monetary Theorem

- The security of a PoW blockchain relies on a cryptocurrency.

There is a converse to the *Transparency Theorem*:

Monetary Theorem

- The security of a PoW blockchain relies on a cryptocurrency.

There is a converse to the *Transparency Theorem*:

Theorem

Monetary Theorem: *A PoW blockchain relies on a cryptocurrency.*

Monetary Theorem

- The security of a PoW blockchain relies on a cryptocurrency.

There is a converse to the *Transparency Theorem*:

Theorem

Monetary Theorem: *A PoW blockchain relies on a cryptocurrency.*

Monetary Theorem

- The security of a PoW blockchain relies on a cryptocurrency.

There is a converse to the *Transparency Theorem*:

Theorem

Monetary Theorem: *A PoW blockchain relies on a cryptocurrency.*

Security relies on PoW, the miners must be compensated for their use of energy. Compensation must be compatible with decentralization. The token that the miners receive in exchange of their energy is transferable and valuable outside system to pay for energy. It is a cryptocurrency and the payment is regulated by a smart contract.

Monetary Theorem

- The security of a PoW blockchain relies on a cryptocurrency.

There is a converse to the *Transparency Theorem*:

Theorem

Monetary Theorem: *A PoW blockchain relies on a cryptocurrency.*

Security relies on PoW, the miners must be compensated for their use of energy. Compensation must be compatible with decentralization. The token that the miners receive in exchange of their energy is transferable and valuable outside system to pay for energy. It is a cryptocurrency and the payment is regulated by a smart contract.

The blockchain is **autonomous** if the cryptocurrency is internal to the system.

Blockchain time

Blockchain time

Blockchain time

- The precision of bitcoin blockchain time $\Delta t \sim 10\text{min}$.

Blockchain time

- The precision of bitcoin blockchain time $\Delta t \sim 10\text{min}$.

This is so because we adjust the difficulty.

Blockchain time

- The precision of bitcoin blockchain time $\Delta t \sim 10\text{min}$.

This is so because we adjust the difficulty.

- Without difficulty adjustment, the precision of blockchain time $\Delta t \sim 1/H$, where H is the hashrate of the network.

Blockchain time

- The precision of bitcoin blockchain time $\Delta t \sim 10\text{min}$.

This is so because we adjust the difficulty.

- Without difficulty adjustment, the precision of blockchain time $\Delta t \sim 1/H$, where H is the hashrate of the network.
- H is proportional to the external input of energy,

$$H = k \,.\, \Delta E$$

Heisenberg Uncertainty Principle

Heisenberg Uncertainty Principle

Heisenberg Uncertainty Principle

Theorem

Heisenberg Uncertainty Principle

$$\Delta t \,.\, \Delta E \sim h = 1/k \,.$$

Thank you for your attention!!