On instabilities of the Bitcoin protocol

Ricardo Pérez-Marco

@rperezmarco

CNRS, IMJ-PRG, Univ. Paris 7

Breaking Bitcoin

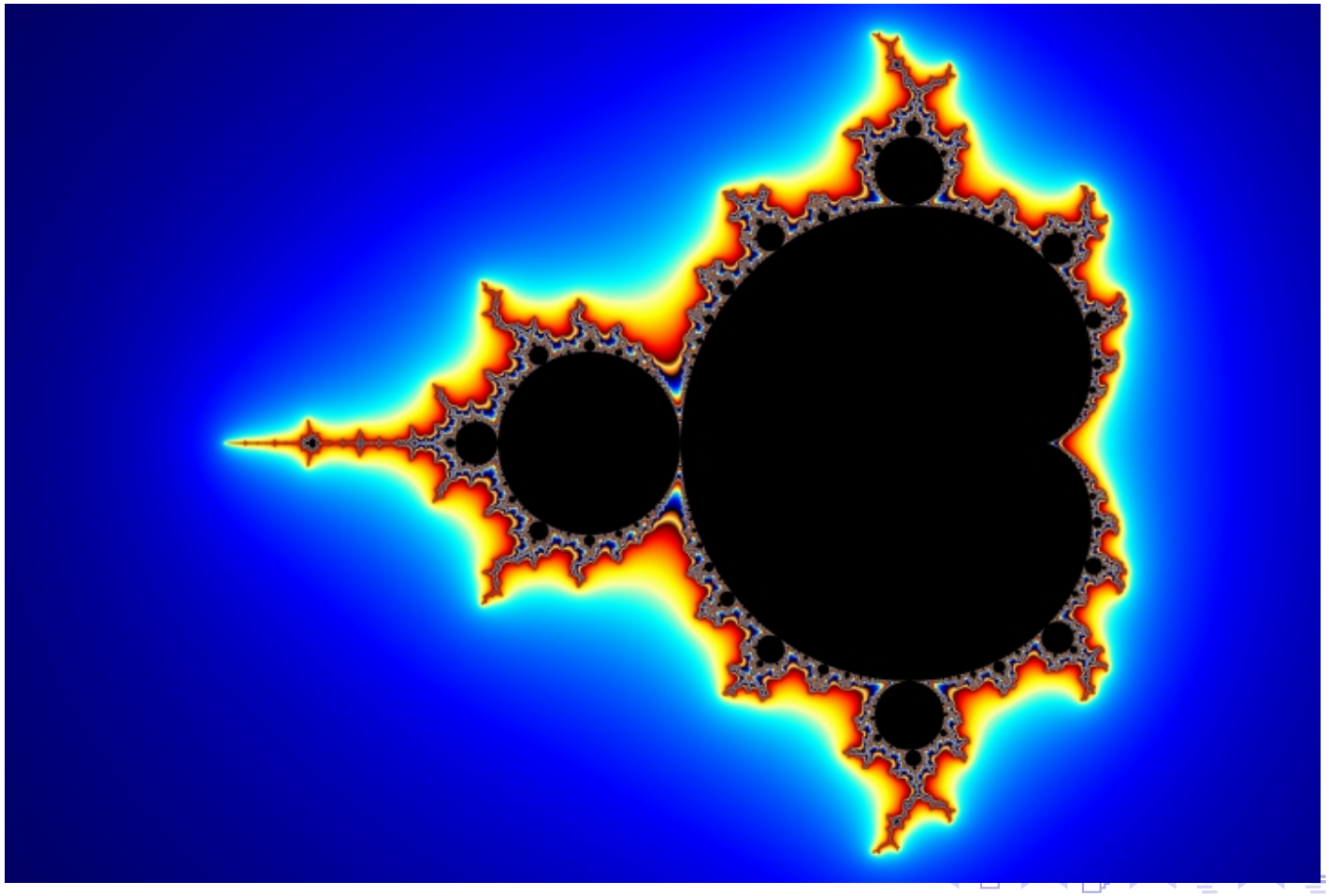
Paris

September 10, 2017

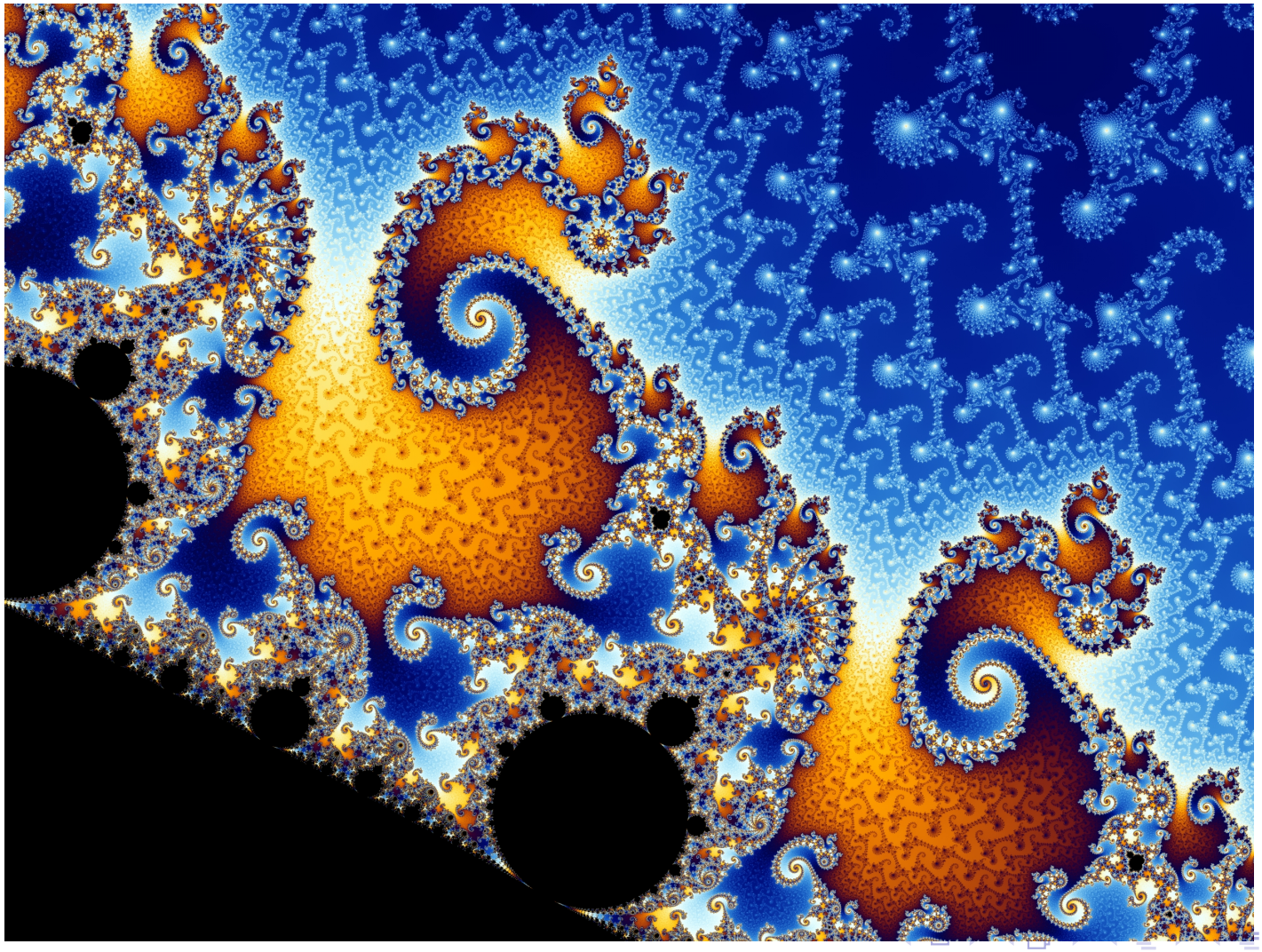
On instabilities of the Bitcoin protocol

The Mandelbrot set

Iteration of $x \mapsto x^2 + c$

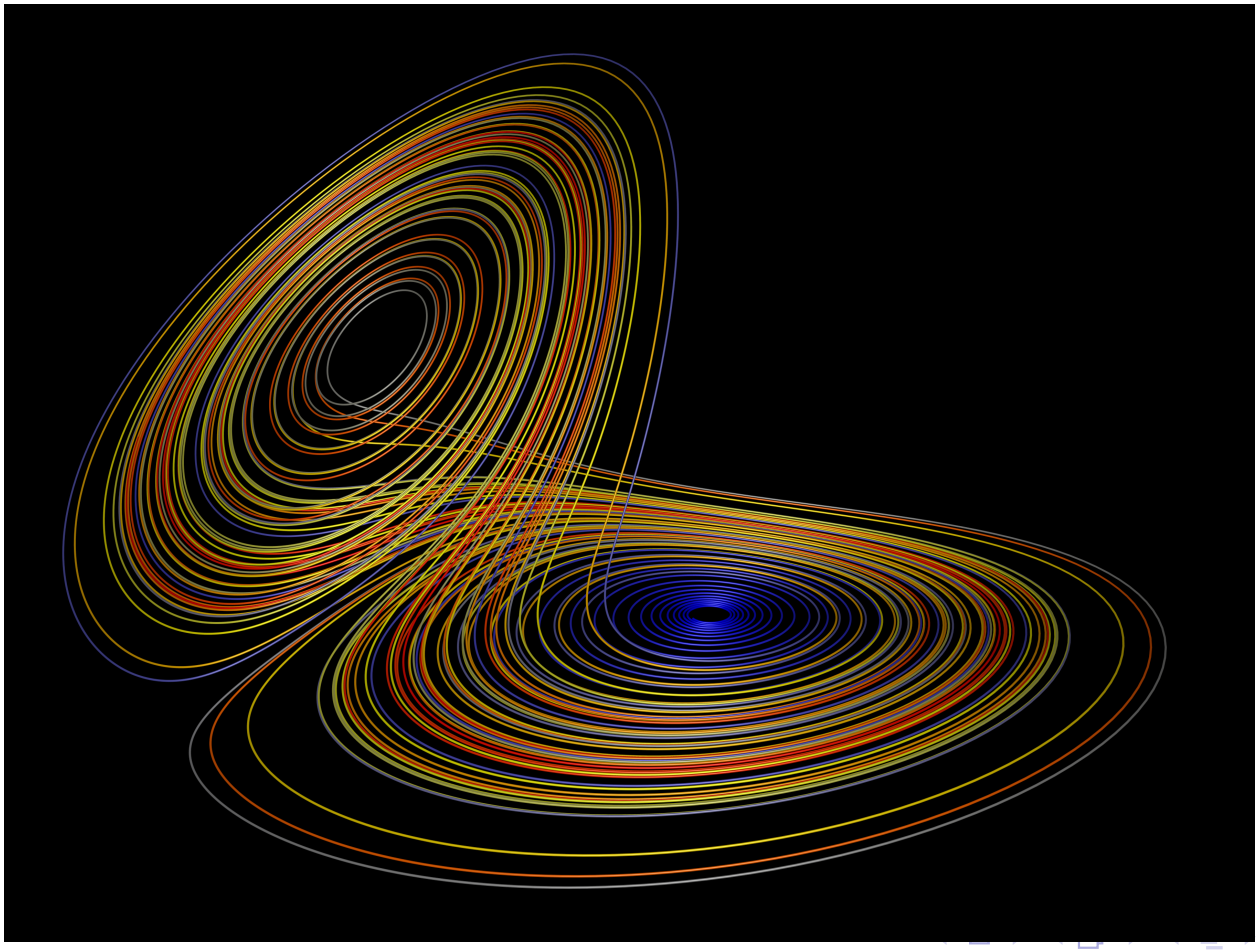


Details of the Mandelbrot set

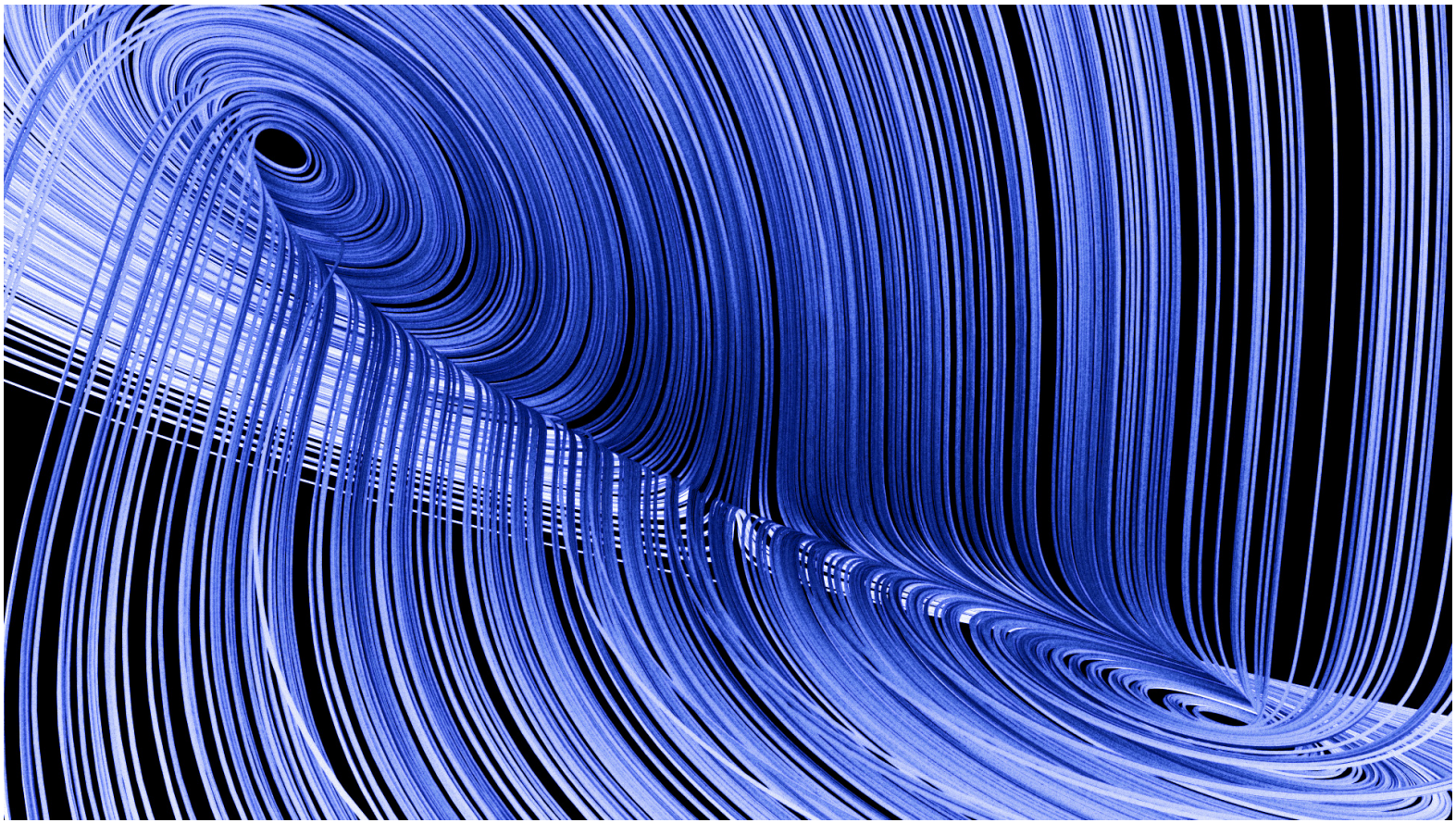


The Lorentz Attractor

Simple meteorological model.



Details of the Lorentz Attractor



The Butterfly Effect

Butterfly effect

A tiny change on initial conditions may produce large deviations on the long term behavior.

The Butterfly Effect

Butterfly effect

A tiny change on initial conditions may produce large deviations on the long term behavior.

Example

Something as small as the flutter of a butterfly's wing can cause a tornado in another part of the Earth.

Dynamical Instability

Definition

Dynamical Instability: Anything that can change the steady evolution of a Dynamical System.

Dynamical Instability

Definition

Dynamical Instability: Anything that can change the steady evolution of a Dynamical System.

Dynamical Instability

Definition

Dynamical Instability: Anything that can change the steady evolution of a Dynamical System.

This “change” can have different natures: Catastrophic, mildly disfunctioning, operating abnormaly,...

Some examples

- The stability of the Solar System.

Some examples

- The stability of the Solar System.
- Hydrodynamical stability and turbulence.

Some examples

- The stability of the Solar System.
- Hydrodynamical stability and turbulence.
- Competing species in biology.

Some examples

- The stability of the Solar System.
- Hydrodynamical stability and turbulence.
- Competing species in biology.
- Stability of the Financial System.

Some examples

- The stability of the Solar System.
- Hydrodynamical stability and turbulence.
- Competing species in biology.
- Stability of the Financial System.
- In particular, stability of the Monetary System.

Some examples

- The stability of the Solar System.
- Hydrodynamical stability and turbulence.
- Competing species in biology.
- Stability of the Financial System.
- In particular, stability of the Monetary System.
- Stability of the Bitcoin Protocol.

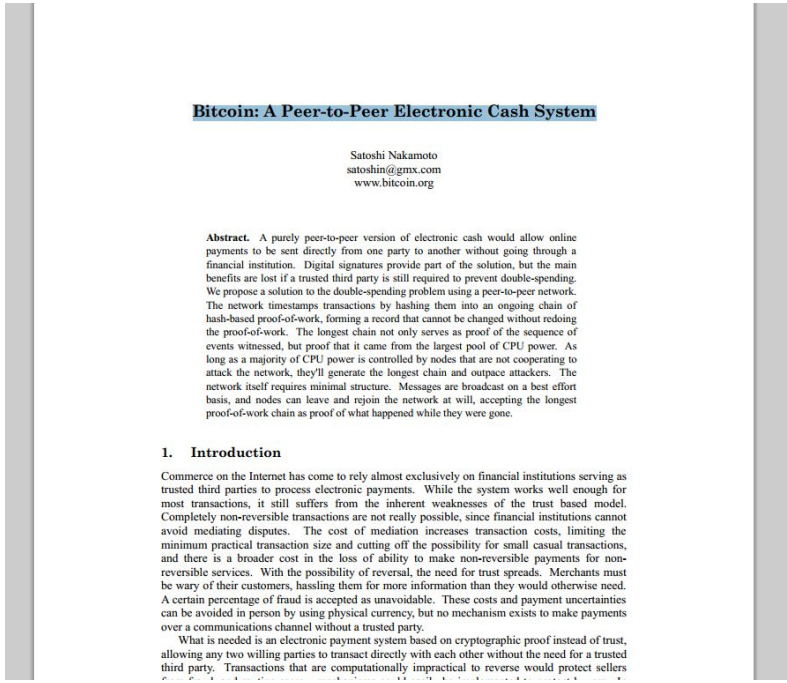
The Bitcoin Dynamical System

On 1/3/2009 the Bitcoin Dynamical System is launched.

The Bitcoin Dynamical System

On 1/3/2009 the Bitcoin Dynamical System is launched.

S. Nakamoto, 11/1/2008



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers

Basic stability question:

How likely is the Bitcoin network be able to survive over the long run?

Basic stability question:

How likely is the Bitcoin network be able to survive over the long run?

Basic stability question:

How likely is the Bitcoin network be able to survive over the long run?

To answer this question we need to analyze all possible risks: Threats, possible bugs, hacks, social attacks (see Alyse Killeen's talk), etc

Basic stability question:

How likely is the Bitcoin network be able to survive over the long run?

To answer this question we need to analyze all possible risks: Threats, possible bugs, hacks, social attacks (see Alyse Killeen's talk), etc

There are some general arguments that give an useful insight.

Lindy Effect

A quantitative version of the “test of time”.

Lindy Effect

A quantitative version of the “test of time”.

Lindy Effect

Future life expectancy is proportional to its current age.

Goldman (1964), Mandelbrot (1984), Taleb (2007),...

Lindy Effect

A quantitative version of the “test of time”.

Lindy Effect

Future life expectancy is proportional to its current age.

Goldman (1964), Mandelbrot (1984), Taleb (2007),...

Lindy Effect

A quantitative version of the “test of time”.

Lindy Effect

Future life expectancy is proportional to its current age.

Goldman (1964), Mandelbrot (1984), Taleb (2007),...

Approximate and very general.

Lindy Effect

A quantitative version of the “test of time”.

Lindy Effect

Future life expectancy is proportional to its current age.

Goldman (1964), Mandelbrot (1984), Taleb (2007),...

Approximate and very general.

Applies to new technologies...and to cryptocurrencies.

Lindy Effect

A quantitative version of the “test of time”.

Lindy Effect

Future life expectancy is proportional to its current age.

Goldman (1964), Mandelbrot (1984), Taleb (2007),...

Approximate and very general.

Applies to new technologies...and to cryptocurrencies.

Example: Bitcoin’s life expectancy is 4 times larger than ETH life expectancy.

Idea for a definite BIP proposal

Corollary

Resilience improves with time.

Idea for a definite BIP proposal

Corollary

Resilience improves with time.

Idea for a definite BIP proposal

Corollary

Resilience improves with time.

If it ain't broke, don't fix it!

Idea for a definite BIP proposal

Corollary

Resilience improves with time.

If it ain't broke, don't fix it!

Idea for a definite BIP proposal

Corollary

Resilience improves with time.

If it ain't broke, don't fix it!

Definite BIP

Don't touch the Bitcoin protocol unless there is an obvious bug or a direct threat.

Idea for a definite BIP proposal

Corollary

Resilience improves with time.

If it ain't broke, don't fix it!

Definite BIP

Don't touch the Bitcoin protocol unless there is an obvious bug or a direct threat.

Idea for a definite BIP proposal

Corollary

Resilience improves with time.

If it ain't broke, don't fix it!

Definite BIP

Don't touch the Bitcoin protocol unless there is an obvious bug or a direct threat.

And this is a BIP since Bitcoin improves along with its lifetime...

Antifragility

Antifragile System (Taleb, 2012)

An evolving Dynamical System that increases in capability, resilience, or robustness as a result of stressors, shocks, volatility, noise, mistakes, faults, attacks, or failures

Antifragility

Antifragile System (Taleb, 2012)

An evolving Dynamical System that increases in capability, resilience, or robustness as a result of stressors, shocks, volatility, noise, mistakes, faults, attacks, or failures

Antifragility

Antifragile System (Taleb, 2012)

An evolving Dynamical System that increases in capability, resilience, or robustness as a result of stressors, shocks, volatility, noise, mistakes, faults, attacks, or failures

Decentralized systems are more antifragile than centralized systems that have a “central point of failure”.

Antifragility

Antifragile System (Taleb, 2012)

An evolving Dynamical System that increases in capability, resilience, or robustness as a result of stressors, shocks, volatility, noise, mistakes, faults, attacks, or failures

Decentralized systems are more antifragile than centralized systems that have a “central point of failure”.

“What doesn’t kill you makes you stronger”

Good and bad hard forks

Question

Are hard forks a disruption or a feature of the Bitcoin protocol?

Good and bad hard forks

Question

Are hard forks a disruption or a feature of the Bitcoin protocol?

Good and bad hard forks

Question

Are hard forks a disruption or a feature of the Bitcoin protocol?

- "Unity gives strength": A hard fork splits the hashrate of the network. Security is directly proportional to hashrate. Thus a hard fork is negative from this point of view.

Good and bad hard forks

Question

Are hard forks a disruption or a feature of the Bitcoin protocol?

- "Unity gives strength": A hard fork splits the hashrate of the network. Security is directly proportional to hashrate. Thus a hard fork is negative from this point of view.
- There are also "hidden costs" (see Jimmy Song's talk)

Good and bad hard forks

Question

Are hard forks a disruption or a feature of the Bitcoin protocol?

- "Unity gives strength": A hard fork splits the hashrate of the network. Security is directly proportional to hashrate. Thus a hard fork is negative from this point of view.
- There are also "hidden costs" (see Jimmy Song's talk)

But things are far more subtle...

Hard forks and prize

- The market price should reflect if a hard fork is bad.

Hard forks and prize

- The market price should reflect if a hard fork is bad.
- More precisely, if the sum of the capitalization of the two resulting coins is much lower than the prefork capitalization, the market has decided that the fork is bad.

Hard forks and prize

- The market price should reflect if a hard fork is bad.
- More precisely, if the sum of the capitalization of the two resulting coins is much lower than the prefork capitalization, the market has decided that the fork is bad.
- One may argue that this sum of capitalizations must always be lower, because it cannot be always higher or a succession of forks will keep increasing wealth (!)

Hard forks and prize

- The market price should reflect if a hard fork is bad.
- More precisely, if the sum of the capitalization of the two resulting coins is much lower than the prefork capitalization, the market has decided that the fork is bad.
- One may argue that this sum of capitalizations must always be lower, because it cannot be always higher or a succession of forks will keep increasing wealth (!)
- But this turns out to be empirically false as observed for the Bitcoin's BTC/BCH fork and the previous ETH/ETC fork !

Hard forks and prize

- The market price should reflect if a hard fork is bad.
- More precisely, if the sum of the capitalization of the two resulting coins is much lower than the prefork capitalization, the market has decided that the fork is bad.
- One may argue that this sum of capitalizations must always be lower, because it cannot be always higher or a succession of forks will keep increasing wealth (!)
- But this turns out to be empirically false as observed for the Bitcoin's BTC/BCH fork and the previous ETH/ETC fork !
- What's going on?

Uncertainty and prize

- Why the sum of capitalizations after fork increases? Where is this wealth coming from?

Uncertainty and prize

- Why the sum of capitalizations after fork increases? Where is this wealth coming from?
- Market prize factors all future expectations. When there is a conflict on the future evolution of the protocol, this causes tensions between two camps that impact the prize.

Uncertainty and prize

- Why the sum of capitalizations after fork increases? Where is this wealth coming from?
- Market prize factors all future expectations. When there is a conflict on the future evolution of the protocol, this causes tensions between two camps that impact the prize.
- There is a hidden cost for conflict. The price is high.

Uncertainty and prize

- Why the sum of capitalizations after fork increases? Where is this wealth coming from?
- Market prize factors all future expectations. When there is a conflict on the future evolution of the protocol, this causes tensions between two camps that impact the prize.
- There is a hidden cost for conflict. The price is high.
- The fork resolves the tension when each camp gets their choice blockchain with the version of the protocol they like.

Uncertainty and prize

- Why the sum of capitalizations after fork increases? Where is this wealth coming from?
- Market prize factors all future expectations. When there is a conflict on the future evolution of the protocol, this causes tensions between two camps that impact the prize.
- There is a hidden cost for conflict. The price is high.
- The fork resolves the tension when each camp gets their choice blockchain with the version of the protocol they like.
- Once the tension is resolved, the uncertainty leaves and the market price adjusts.

- These are healthy hard forks if they are done for good reasons.

- These are healthy hard forks if they are done for good reasons.
- This is a powerful tool for resolution of conflicts which is implicit in the Bitcoin protocol.

- These are healthy hard forks if they are done for good reasons.
- This is a powerful tool for resolution of conflicts which is implicit in the Bitcoin protocol.

A classical instability

- If an agent controls more than 50% of the hashrate, the network is unstable (Nakamoto).

A classical instability

- If an agent controls more than 50% of the hashrate, the network is unstable (Nakamoto).
- Computation of the probability of a double spend attack.

A classical instability

- If an agent controls more than 50% of the hashrate, the network is unstable (Nakamoto).
- Computation of the probability of a double spend attack.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

"assuming the honest blocks took the average expected time per block"

Correct computation

Join work with Cyril Grunspan, ArXiv:1702.02867, 2017.

Correct computation

Join work with Cyril Grunspan, ArXiv:1702.02867, 2017.

Theorem

Let $0 < q < 1/2$ *be the relative hash power of the group of the attackers, and* $p = 1 - q$. *After* z *blocks have been validated by the honest miners, the probability of success of the attackers is*

$$P(z) = I_{4pq}(z, 1/2) \ ,$$

where $I_x(a, b)$ *is the Regularized Incomplete Beta Function*

$$I_x(a, b) = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} \int_0^x t^{a-1}(1-t)^{b-1}\, dt \ .$$

Corollary

A Corollary (that everyone knew)

Corollary

A Corollary (that everyone knew)

Corollary

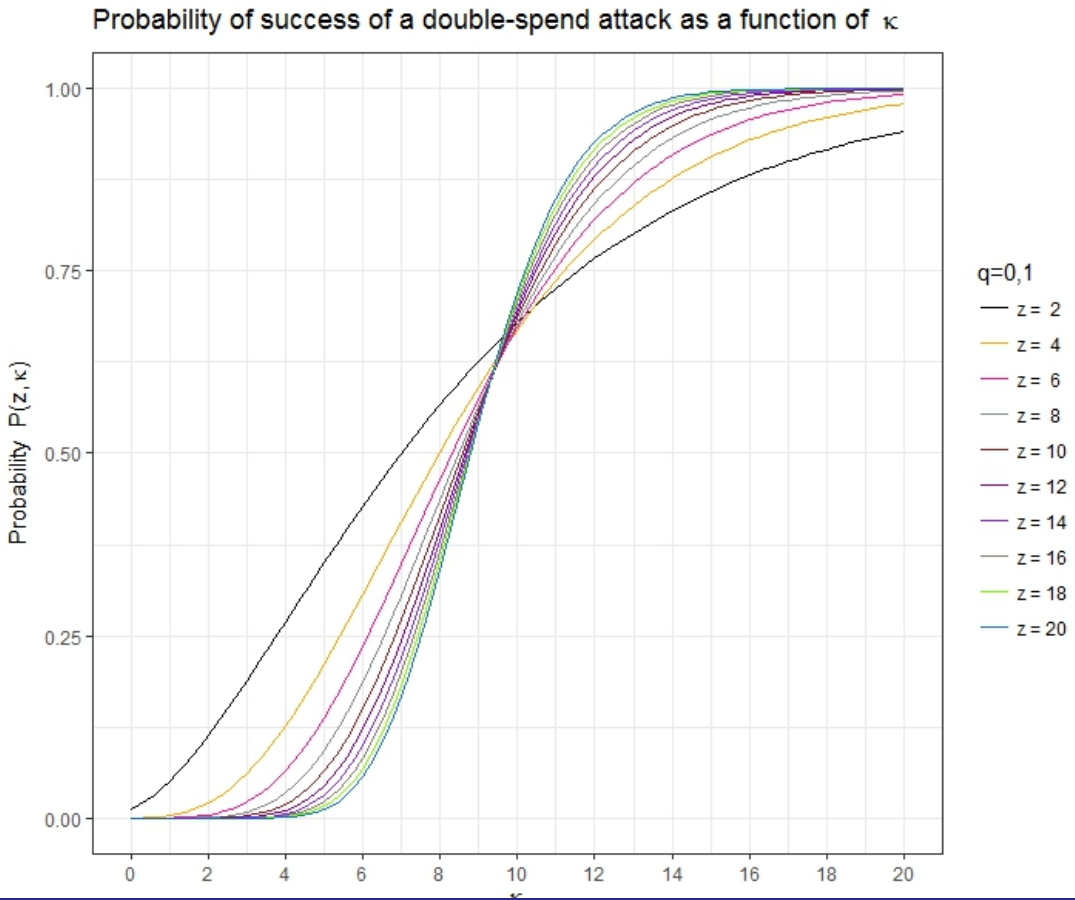
The probability of a double spend decreases exponentially with the number of confirmations.

A more precise probability

The parameter κ measures the deviation from average time validation of honest blocks ($\kappa = 1$ is Satoshi's assumption).

A more precise probability

The parameter κ measures the deviation from average time validation of honest blocks ($\kappa = 1$ is Satoshi's assumption).



A new type of instability

- Decentralization: Bitcoin Protocol must self-regulate.

A new type of instability

- Decentralization: Bitcoin Protocol must self-regulate.
- Participating agents follow the rules of the protocol because of self-economic interest.

A new type of instability

- Decentralization: Bitcoin Protocol must self-regulate.
- Participating agents follow the rules of the protocol because of self-economic interest.
- Example: A miner must mine on top of the largest work blockchain.

A new type of instability

- Decentralization: Bitcoin Protocol must self-regulate.
- Participating agents follow the rules of the protocol because of self-economic interest.
- Example: A miner must mine on top of the largest work blockchain.
- If a miner just mined a block, but he realizes than just before another block has propagated on the network, will he start mining on top of the network blockchain?

A new type of instability

- Decentralization: Bitcoin Protocol must self-regulate.
- Participating agents follow the rules of the protocol because of self-economic interest.
- Example: A miner must mine on top of the largest work blockchain.
- If a miner just mined a block, but he realizes than just before another block has propagated on the network, will he start mining on top of the network blockchain?
- The answer depends on the miner's hashrate.

Catch-up mining

- Let $E_n^m(q, v)$ be the EV (Expected Value) of the optimal strategy to overcome m blocks delay in n steps for a reward v (includes block rewards, plus fees, plus a possible double spend). When $E_n^m(q, v) > 0$ the strategy is profitable.

Catch-up mining

- Let $E_n^m(q, v)$ be the EV (Expected Value) of the optimal strategy to overcome m blocks delay in n steps for a reward v (includes block rewards, plus fees, plus a possible double spend). When $E_n^m(q, v) > 0$ the strategy is profitable.
- The map $v \mapsto E_n^m(q, v)$ is a continuous increasing convex affine by pieces function.

Catch-up mining

- Let $E_n^m(q, v)$ be the EV (Expected Value) of the optimal strategy to overcome m blocks delay in n steps for a reward v (includes block rewards, plus fees, plus a possible double spend). When $E_n^m(q, v) > 0$ the strategy is profitable.
- The map $v \mapsto E_n^m(q, v)$ is a continuous increasing convex affine by pieces function.

Theorem

If $q > 0.42$, $m = 2$, and $b > 0$ is the block reward, then $\lim_{n \to +\infty} E_n^2(q, 3b) > 0$.

Catch-up mining

- Let $E_n^m(q, v)$ be the EV (Expected Value) of the optimal strategy to overcome m blocks delay in n steps for a reward v (includes block rewards, plus fees, plus a possible double spend). When $E_n^m(q, v) > 0$ the strategy is profitable.
- The map $v \mapsto E_n^m(q, v)$ is a continuous increasing convex affine by pieces function.

Theorem

If $q > 0.42$, $m = 2$, and $b > 0$ is the block reward, then $\lim_{n \to +\infty} E_n^2(q, 3b) > 0$.

Catch-up mining

• Let $E_n^m(q, v)$ be the EV (Expected Value) of the optimal strategy to overcome m blocks delay in n steps for a reward v (includes block rewards, plus fees, plus a possible double spend). When $E_n^m(q, v) > 0$ the strategy is profitable.

• The map $v \mapsto E_n^m(q, v)$ is a continuous increasing convex affine by pieces function.

Theorem

If $q > 0.42$, $m = 2$, and $b > 0$ is the block reward, then $\lim_{n\to+\infty} E_n^2(q, 3b) > 0$.

• If $v > 3b$, considering block fees or possible rewards for double spends, the minimal value for q is lower.

Why this happens?

Why this happens?

- If the hashrate is over 42% of the total hashrate, following the optimal strategy and with unlimited resources, he has a positive return expectation of catch-up, mining on top of his mined block.

Why this happens?

- If the hashrate is over 42% of the total hashrate, following the optimal strategy and with unlimited resources, he has a positive return expectation of catch-up, mining on top of his mined block.
- Quick explanation: If the miner mines 2 consecutive blocks before the rest of the network, although it is less probable, he will cash the reward corresponding to 3 blocks: The 2 mined blocks plus the invalidate one.

Why this happens?

- If the hashrate is over 42% of the total hashrate, following the optimal strategy and with unlimited resources, he has a positive return expectation of catch-up, mining on top of his mined block.
- Quick explanation: If the miner mines 2 consecutive blocks before the rest of the network, although it is less probable, he will cash the reward corresponding to 3 blocks: The 2 mined blocks plus the invalidate one.

Catch-up mining instability

When a miner refuses to mine on top of the network blockchain and mines on top on blocks that he has secretly validated.

Why this happens?

- If the hashrate is over 42% of the total hashrate, following the optimal strategy and with unlimited resources, he has a positive return expectation of catch-up, mining on top of his mined block.
- Quick explanation: If the miner mines 2 consecutive blocks before the rest of the network, although it is less probable, he will cash the reward corresponding to 3 blocks: The 2 mined blocks plus the invalidate one.

Catch-up mining instability

When a miner refuses to mine on top of the network blockchain and mines on top on blocks that he has secretly validated.

Why this happens?

- If the hashrate is over 42% of the total hashrate, following the optimal strategy and with unlimited resources, he has a positive return expectation of catch-up, mining on top of his mined block.
- Quick explanation: If the miner mines 2 consecutive blocks before the rest of the network, although it is less probable, he will cash the reward corresponding to 3 blocks: The 2 mined blocks plus the invalidate one.

Catch-up mining instability

When a miner refuses to mine on top of the network blockchain and mines on top on blocks that he has secretly validated.

Sorry for the formulas...

Sorry for the formulas...

and thank you for your attention!!