Jon Gulson

112 Followers · About Follow

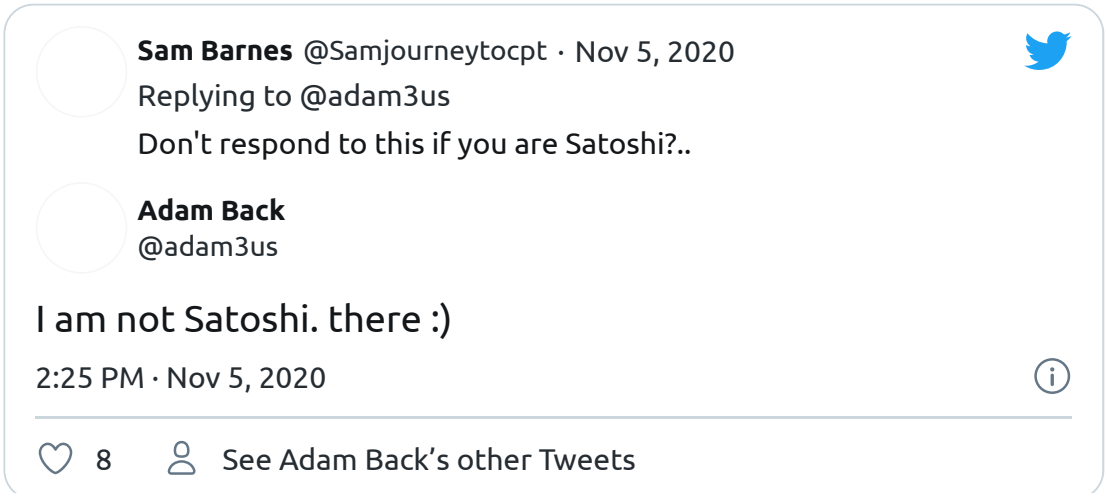
"Chancellor Nash" by @ormpho

19 Reasons John F Nash Jr. was Satoshi Nakamoto

Jon Gulson Nov 12 · 6 min read

One of the usual suspects for the identity of Satoshi Nakamoto is Adam Back, because bitcoin describes itself as a proof of work system similar to Back's Hashcash.

However, Back denies he is Satoshi Nakamoto:



Another candidate for Satoshi has been named as John Forbes Nash Jr., the mathematician who had a Hollywood film *A Beautiful Mind (2001)* made about his life.

Hal Finney was aware of Nash:

> **John Nash, proto-Extropian?**
>
> I've just started reading Sylvia Nasar's biography of mathematician John Nash, A Beautiful Mind, on which the current...

Following on from the idea of "*proto-Extropian*" — and given Nash's work in cryptography, mathematics, game theory, and economics — there are 19 compelling reasons to believe Nash was Satoshi:

1. The shared characteristic of decentralisation in Nash and Satoshi systems

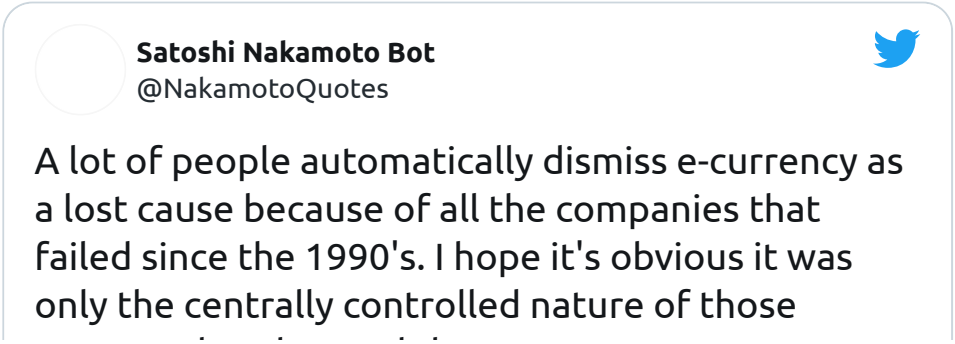
A quirk of bitcoin is it's commonly championed for the characteristic of *decentralisation*, yet its white paper doesn't reference this characteristic in such popular terms.

Rather, it speaks to decentralisation in reference to solving the problem of double-spending (fraud) and removing a trusted central mint by which the entire money system depends (Bitcoin: A Peer-to-Peer Electronic Cash System, section 2).

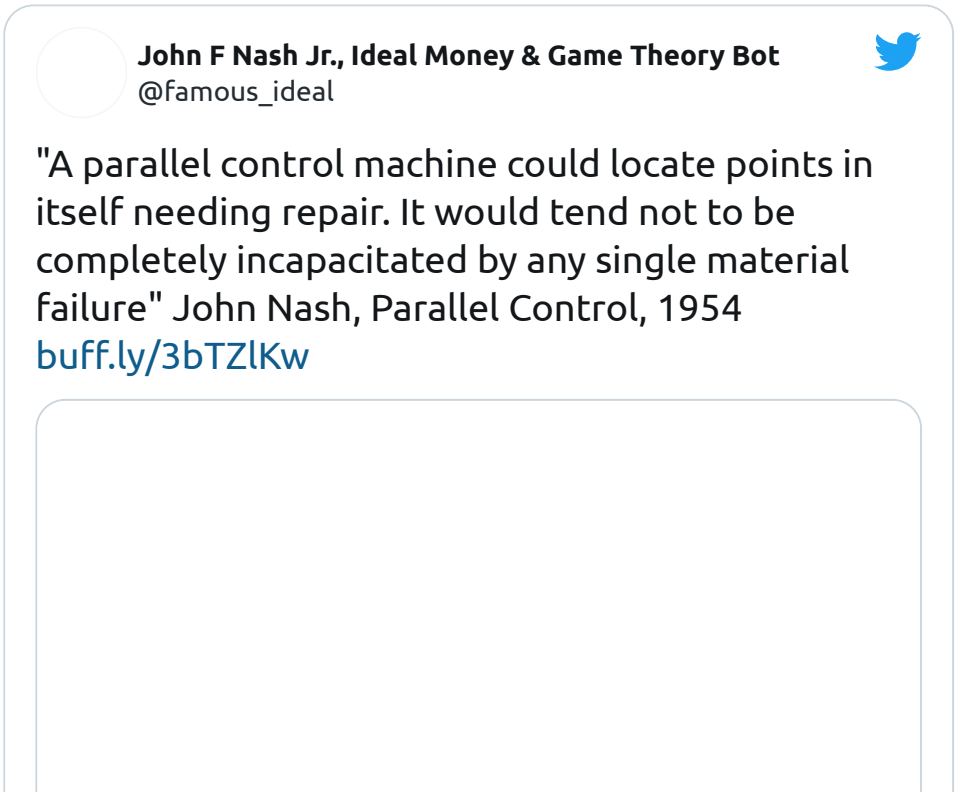
With regard to decentralisation, and in 1954, John Nash had a futuristic idea for "electronic brains" of the future:

> "the idea is to decentralise control with several different control units capable of directing various simultaneous operations and interrelating them when appropriate" John Nash, Parallel Control, 1954

Satoshi in his bitcoin talk forum posts, refers to the decentralised nature of bitcoin:

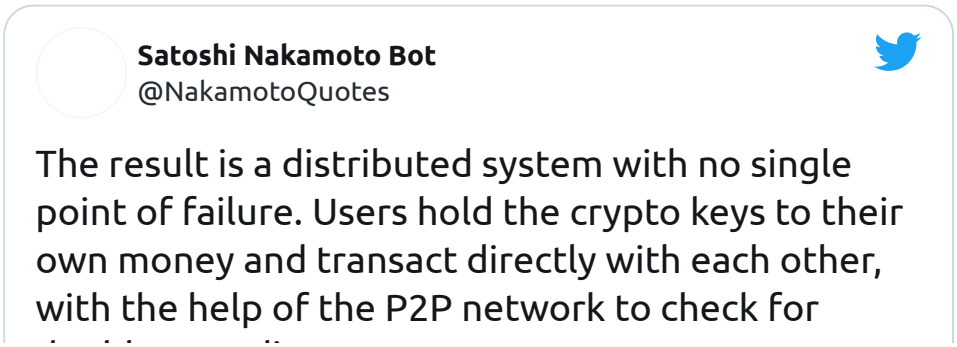


Satoshi



Nash

Satoshi says this on the same subject:



Satoshi

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"Perhaps this type of machine organization would have the most value for very large machines intended to have a wide range of applicability" John Nash, Parallel Control, 1954 buff.ly/3bTZlKw

Nash

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"Now we can see how the large parallel control machine capable of handling several problems simultaneously would have an advantage. The interpretation program would only need be represented once." John Nash, Parallel Control, 1954 buff.ly/3bTZlKw

Nash

As did Satoshi for his bitcoin system:

> “The design supports a tremendous variety of possible transaction types that I designed years ago.” Satoshi Nakamoto, 17 June 2010

3. The shared method of problem solving

Nash on problem solving:

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"The mathematician should have to do little more than state the problem and general method of computation in almost ordinary mathematical style" John Nash, Parallel Control, 1954
buff.ly/3bTZlKw

Satoshi on the two problems the bitcoin proof of work computation solves:

> "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." Bitcoin: A Peer-to-Peer Electronic Cash System, Abstract.

> "The proof-of-work also solves the problem of determining representation in majority decision making." Bitcoin: A Peer-to-Peer Electronic Cash System, Section 4

Trial, error, and chance also feature in the Nash and Satoshi methodology:

> **John F Nash Jr., Ideal Money & Game Theory Bot**
> @famous_ideal
>
> Ultimately trial and error processes, combined with search or association processes, abstraction processes, and learning or conditioning processes should lead to the learning machine or even to the genuine thinking machine - John Nash, Parallel Control buff.ly/3bTZlKw

10:16 PM · Oct 10, 2020

2 See John F Nash Jr., Ideal Money & Game Theory Bot's other…

Nash

Satoshi Nakamoto Bot
@NakamotoQuotes

The proof-of-work is a Hashcash style SHA-256 collision finding. It's a memoryless process where you do millions of hashes a second, with a small chance of finding one each time.

12:13 AM · Nov 14, 2020

12 See Satoshi Nakamoto Bot's other Tweets

Satoshi

4. Nash and Satoshi's convergent thinking on inflation

John Nash's work on Ideal Money was based on the idea that a money should ideally be inflation-free, but realised this might cause a problem if it didn't circulate:

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"There is a problem for the issuer of a currency, whether in coinage, paper, or "electronic" form, that if this currency (or money) is TOO GOOD then it could be exploited by all sorts of parties and interests that might simply wish to ...store wealth" buff.ly/2UX4cEM

10:44 PM · Mar 26, 2020

5 See John F Nash Jr., Ideal Money & Game Theory Bot's other…

So John Nash introduced a steady and constant inflation rate which would be more or less as good as to be free of inflation:

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"to improve the conditions under which agreements for long term lending and borrowing would be made a money would be more or less equivalently good if it had a completely steady and constant rate of inflation." John Nash, Ideal Money, 2002 buff.ly/3eDxjo2

The parallel with bitcoin is clear:

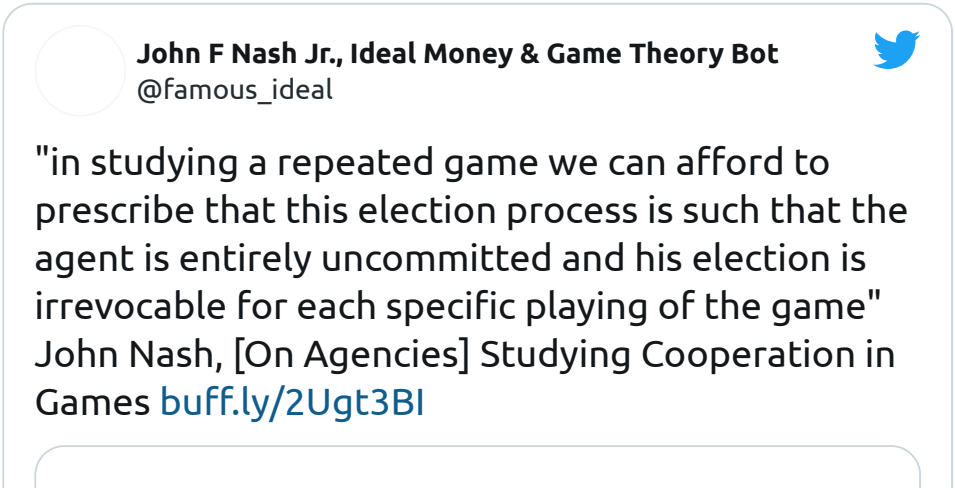
> "The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended." Bitcoin: A Peer-to-Peer Electronic Cash System, Section 6

5. "Uncommitted agency" in Nash and Satoshi systems

Satoshi on bitcoin nodes:

> "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." Bitcoin: A Peer-to-Peer Electronic Cash System, Abstract.

John Nash, in his Agencies Method, which evolved concurrently to his work on Ideal Money, developed an election procedure in respect to experimental studies on coalitions and coalition formation, the results of which were found to be "computationally heavy" and analogous to a scheme of "robotic attorney agents":



Nash

6. Similar indications on the value of contracts

Satoshi on contracts:

> “The design supports a tremendous variety of possible transaction types that I designed years ago. Escrow transactions, bonded contracts, third party arbitration, multi-party signature, etc. If Bitcoin catches on in a big way, these are things we’ll want to explore in the future, but they all had to be designed at the beginning to make sure they would be possible later.” Satoshi Nakamoto, 17 June 2010

Nash on the application of “ideal money” in contracts:

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"...our first ideas about Ideal Money is that of the importance of the comparative quality of the money used in an economic society to the possible precision, as an indicator of quality, of the contracts for performances of future contractual

Nash

7. Nash and Satoshi's shared distrust of central banks

Satoshi on central banks:

Satoshi Nakamoto Bot
@NakamotoQuotes

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of

Satoshi

Bitcoin

Nash on debt pardoning:

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"A debt pardoner is an agency or authority that can pardon the "sins" of the overindebted... Banks can thus sometimes be saved from failing. The government of a country that issues the locally accepted currency also thus pardons its own "sins" " Nash, 2002 buff.ly/2vorGIR

10:18 PM · Jun 21, 2020

3 See John F Nash Jr., Ideal Money & Game Theory Bot's other…

Nash

Nash on "Keynesians":

John F Nash Jr., Ideal Money & Game Theory Bot

called "the Keynesians" in that while they have claimed to be operating for high and noble objectives of general welfare what is clearly true is that they have made it easier for governments to "print money" buff.ly/2OEahlI

Nash

"...a "Keynesian" would favor the existence of a "manipulative" state establishment of central bank and treasury which would continuously seek to achieve "economic welfare" objectives with comparatively little regard for the long term reputation of the national currency.." John Nash, Ideal Money, 2003

Satoshi Nakamoto Bot
@NakamotoQuotes

Those coins can never be recovered, and the total

prints money and the value of existing money goes

8. Citations in common on the idea of “collectibles” and “hoarding”

Satoshi Nakamoto Bot
@NakamotoQuotes

Lost coins only make everyone else's coins worth slightly more. Think of it as a donation to everyone.

3:51 PM · Jan 21, 2020

Satoshi

Satoshi Nakamoto Bot
@NakamotoQuotes

Bitcoins have no dividend or potential future dividend, therefore not like a stock. More like a collectible or commodity.

Satoshi

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

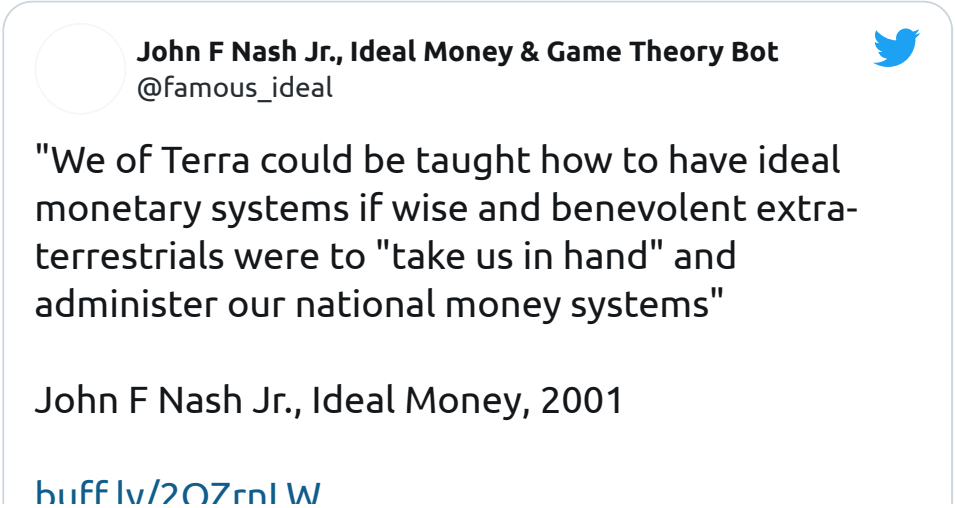
"My opinion now is that it is desirable that a standard for a comparatively "ideal" currency should be structured so that the form of money established would have some attractiveness for "hoarding" " - John Nash, Ideal Money, 2010
buff.ly/3hcXFyH

Nash

9. The Extra-Terrestrial

“Proto-Extropian”

Satoshi

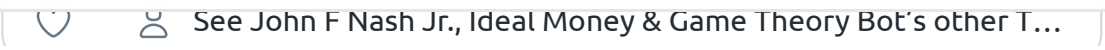


Nash

10. Nash and Satoshi's shared belief in "new money"

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

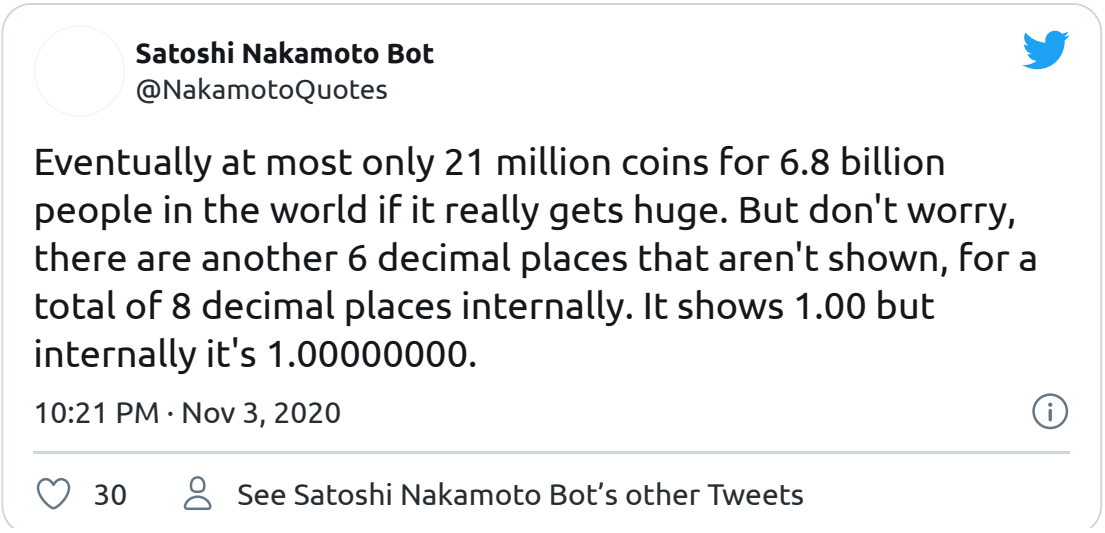
One obvious solution for these problems of equity relating to debtors and creditors would be to have, somehow, a scheme that would gradually "phase in" a version of "ideal" money while some sort of typical "20th century money" would be gradually phased out buff.ly/3hcXFyH



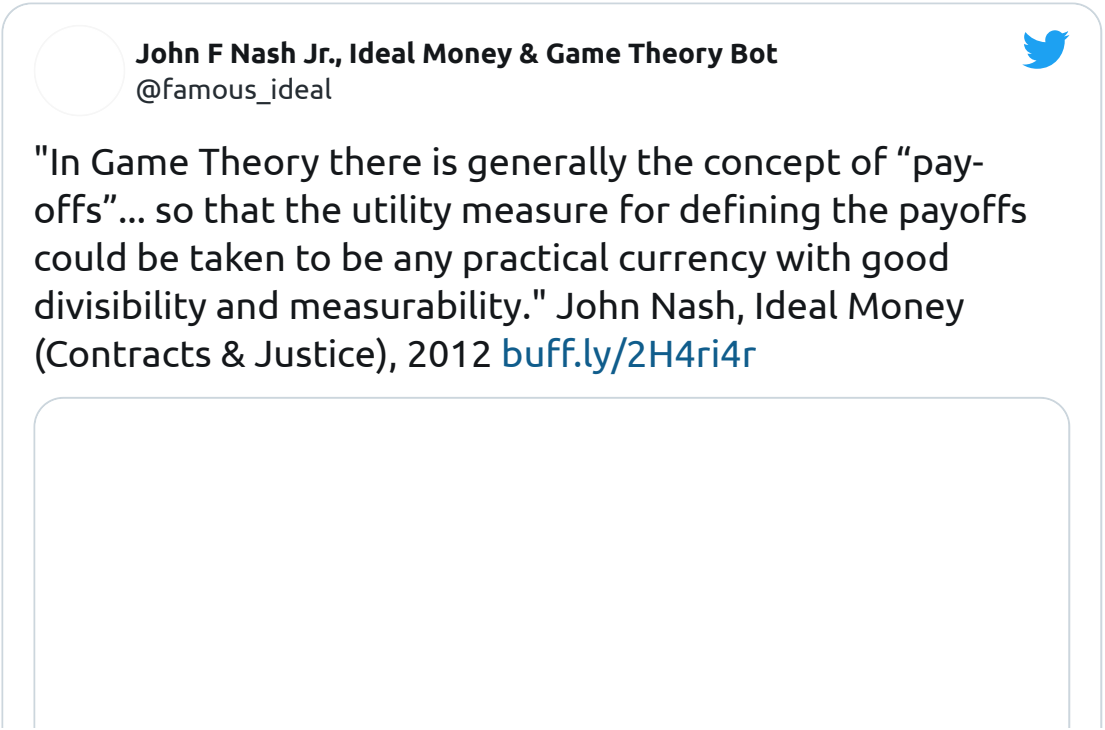
Nash

> “I’ve been working on a new electronic cash system that’s fully peer-to-peer, with no trusted third party.” Satoshi Nakamoto, 31 October, 2008

And on the internally divisible nature of the new money:



Satoshi



10:21 AM · Jun 15, 2020

1 See John F Nash Jr., Ideal Money & Game Theory Bot's other…

Nash

11. "Difficulty" ,"adjustment", "the moving average", as axioms in Nash and Satoshi systems

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"if a "miracle energy source" were found, and thus if a good index is constructed it should not be expected to be valid, as initially defined, into all eternity. It would instead be appropriate for it to be regularly readjusted.." Nash, Mumbai, 2002 buff.ly/2OEahlI

Satoshi Nakamoto Bot
@NakamotoQuotes

As computers get faster and the total computing proof-of-worker applied to creating bitcoins increases, the difficulty increases proportionally to keep the total new production constant. Thus, it is known in advance how many new bitcoins will be created every year in the future.

4:16 AM · Nov 25, 2018

59 See Satoshi Nakamoto Bot's other Tweets

Satoshi

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"This index could be constructed by computing a moving average of the index for the base metals computed by pricing them modulo the index of the precious metals" Nash, Ideal Money, 2002
buff.ly/2Ir86hZ

Nash

> To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty

Satoshi

> **John F Nash Jr., Ideal Money & Game Theory Bot**
> @famous_ideal
>
> It seems clear that as soon as the machines become able to solve intellectual problems of the highest difficulty which can be solved by humans they will be able to solve most of the problems enormously faster than a human - John Nash, Parallel Control 1954 buff.ly/3bTZlKw

Nash

12. Uniqueness

"A non-cooperative game does not always have a solution, but when it does the solution is unique. Strong solutions are solutions with special properties. Sub-solutions always exist and have many of the properties of solutions, but lack uniqueness" 1950 buff.ly/37d2gL2

Nash

Satoshi Nakamoto Bot
@NakamotoQuotes

I don't believe a second, compatible implementation of Bitcoin will ever be a good idea. So much of the design depends on all nodes getting exactly identical results in lockstep that a second implementation would be a menace to the network.

10:12 AM · Aug 17, 2020

12 See Satoshi Nakamoto Bot's other Tweets

Satoshi

13. Shared expectancy in Nash and Satoshi systems

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

quality then, in principle, the people can demand that."
John Nash, Ideal Money and Asymptotically Ideal Money, 2008 buff.ly/2QWOgzt

10:21 AM · Aug 7, 2020

2 See John F Nash Jr., Ideal Money & Game Theory Bot's other…

Nash

Satoshi Nakamoto Bot
@NakamotoQuotes

It might make sense just to get some in case it catches on. If enough people think the same way, that becomes a self fulfilling prophecy.

7:31 PM · Nov 3, 2018

113 26 people are Tweeting about this

Satoshi

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"it is natural to think of the users as having

Nash, Ideal Money & Asymptotically Ideal Money, 2008 buff.ly/2QWOgzt

Nash

Satoshi Nakamoto Bot
@NakamotoQuotes

A rational market price for something that is expected to increase in value will already reflect the present value of the expected future increases. In your head, you do a probability estimate balancing the odds that it keeps increasing.

9:12 AM · Nov 1, 2020

12 See Satoshi Nakamoto Bot's other Tweets

Satoshi

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"Thus an anticipation of an individual is a state of expectation that may involve the certainty of some contingencies and various probabilities of other contingencies."

buff.ly/3gdAlAE

4:08 PM · Dec 5, 2020

2 See John F Nash Jr., Ideal Money & Game Theory Bot's other…

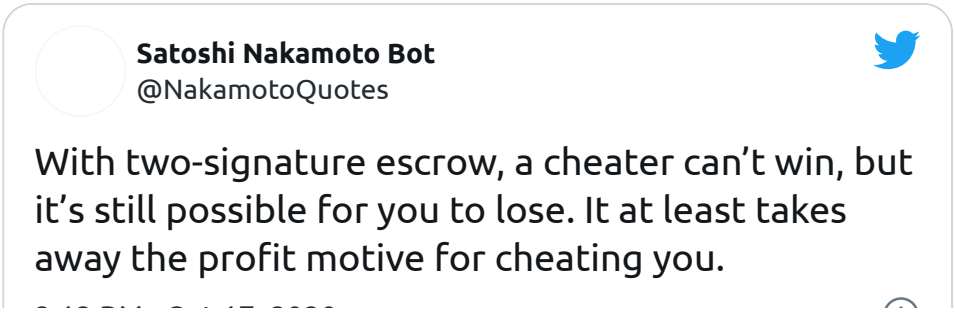
John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"It is not widely advertised by American banking institutions, but the rate of interest that they would pay on deposit or "money market" accounts might be lower than the rational expectation for the rate of inflation relevant for the national currency" buff.ly/3au9ah8

Nash

14. Reoccurring ideas on “law” in Nash and Satoshi systems

The opening passages in the bitcoin white paper uses terminology and descriptions of mediation, disputes, reversibility, trust and fraud, which are all features of litigation. The two problems bitcoin says it solves (double spending, and determining representation in majority decision making) are also representative of legal processes, like escrow and how it can disincentive “cheating”:



Satoshi

With the emphasis on prevention:

Satoshi

Nash’s work in the Ideal Money and Agencies Method had a common focus on the nature and importance of contracts:

analogous to a climate of lawlessness that would make contracts, in general, unreliable." John Nash - Ideal Money, 2008 buff.ly/39DouHi

Nash

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"In principle, coalitions, and specifically coalitions as considered by Von Neumann and Morgenstern in "Theory of Games and Economic Behavior", are things that could be implemented by contracts, like contracts in roman law." John Nash, 2003, buff.ly/2Ugt3BI

Nash

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"the quality of the money unit in terms of which the contract is written makes a big difference in the level of certainty of the contract terms." John Nash, Ideal Money (Relations to Law and Contracts), Lafayette College, 2010 buff.ly/2SrBtVY

Nash

And Nash on the utility of “ideal money” in dispute resolution:

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"Nevertheless, a truly Grand Coalition...is an

Nash, 2015 [in interview with Yanis Varoufakis, on Ideal Money] buff.ly/3dRZ4IL

Nash

15. Common references to gold in Nash and Satoshi systems

> “Our proposal is that a preferable version of a general system for the transferring of utility, thus a “medium of exchange”, would be structured so as to provide a medium with a natural (and reliable!) stability of value. And this stability of value would be particularly of benefit in connection with contracts or exchanges involving long time periods for the complete performance of the contract or exchange.
>
> Classically, when gold or silver was used as the basis of a standard for exchanges, that objective was

2010

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"And (4) It can be recognized as wasteful of labor if gold is accumulated much beyond its various uses and put into storage vaults like in Fort Knox in the USA." John Nash, Ideal Money, 2002

Satoshi Nakamoto Bot
@NakamotoQuotes

The marginal cost of gold mining tends to stay near the price of gold. Gold mining is a waste, but that waste is far less than the utility of having gold available as a medium of exchange. I think the case

“As a thought experiment, imagine there was a base metal as scarce as gold but with the following properties:
- boring grey in colour
- not a good conductor of electricity
- not particularly strong, but not ductile or easily malleable either
- not useful for any practical or ornamental purpose

and one special, magical property:
- can be transported over a communications channel

If it somehow acquired any value at all for whatever reason, then anyone wanting to transfer wealth over a long distance could buy some, transmit it, and have the recipient sell it.” Satoshi Nakamoto, 27 August, 2010

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"Clearly, in terms of this geographical perspective, gold has been historically optimal and that largely because the labor cost of moving it over great distances is so small in relation to the value of what is transported." John Nash, Ideal Money, 2002
buff.ly/3eDxjo2

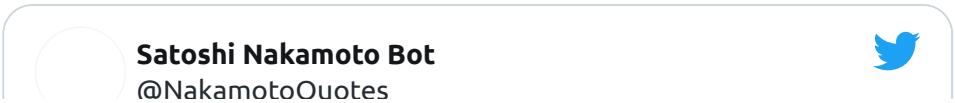
Nash

Is Satoshi referencing pro-cooperative games in relation to gold below?

Satoshi

16. The value of words in Nash and Satoshi systems

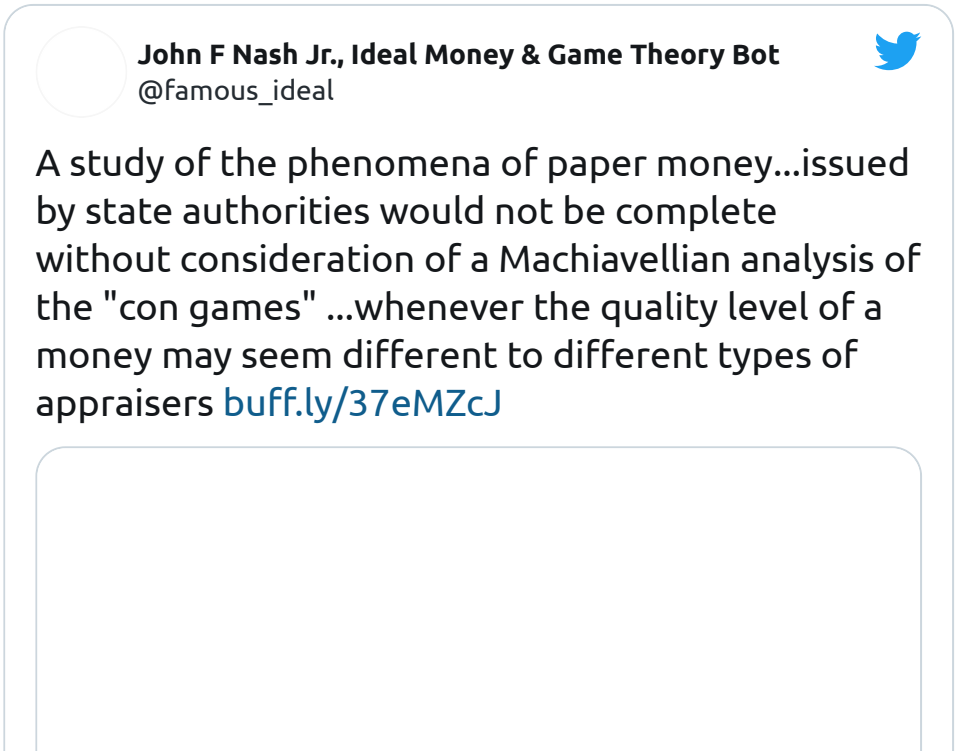
Satoshi on words at work:



have to worry about a chain of custody of communication. It doesn't matter who tells you a longest chain, the proof-of-work speaks for itself.

Satoshi

Nash on “words”:

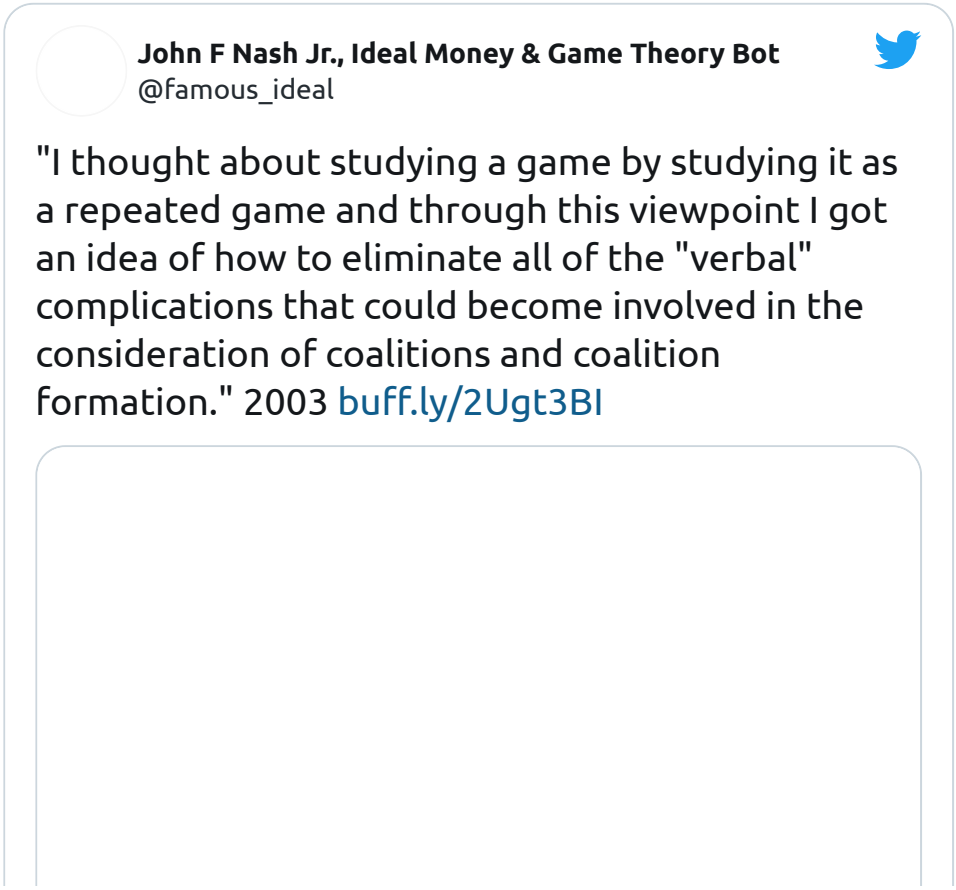


Nash

Satoshi on words:

Satoshi

Nash on verbal complications in contracts:



Nash

17. Proof of work as a solution to Prisoner Dilemma games and the Byzantine Generals' Problem

synchronisation problem, and to knowing what the globally shared view is without having to trust anyone

Satoshi

“The proof-of-work chain is a solution to the Byzantine Generals’ Problem. I’ll try to rephrase it in that context.” Satoshi Nakamoto, 13 November, 2008

John F Nash Jr., Ideal Money & Game Theory Bot
@famous_ideal

"players of a REPEATED game of "prisoners' dilemma" can have a good cooperative equilibrium (in an infinitely repeated game context) where each player has, strategically, a DEMAND that the other player should play in an approved cooperative fashion" 2010 buff.ly/3bny17v

Nash

"If an appropriately honest government-like agency is to issue the actual currency, and to provide for the central bank deposits denominated in terms of that currency, for a money system, then it can also, naturally, compute the indexes that would measure the presence or absence of inflation or deflation." John Nash, Ideal Money, 2011

"By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them...The incentive may help encourage nodes to stay honest." Bitcoin: A Peer-to-Peer Electronic Cash System, Section 6

19. Accepted agency of players in games

"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." Bitcoin: A Peer-to-Peer Electronic Cash System, Section 1

the “agency” of another player or of an existing coalition of players" buff.ly/2SmPsfq

Nash

Bitcoin