bitcoin`s Sound Money Properties Series

#6 Easily Verifiable & Can’t be Counterfeited

with @SimplestBTCBook and @DJSATOSHI18

- PORTABLE, DURABLE, DIVISIBLE, FUNGIBLE
- TRULY SCARCE
- DISTRIBUTED & DECENTRALIZED
- CENSORSHIP RESISTANT & UNCONFISCATABLE
- IMMUTABLE & INCORRUPTIBLE
- EASILY VERIFIABLE & CAN'T BE COUNTERFEITED
- PERMISSIONLESS, FRICTIONLESS & PEER-TO-PEER
- NEUTRAL & VOLUNTARY
- TRANSPARENT, OPEN-SOURCE & AUDITABLE
- BORDERLESS
- PROVIDES SETTLEMENT FINALITY
- PSUEDONYMOUS & TRUSTLESS
- SECURE & SCALABLE
- DISINFLATIONARY/DEFLATIONARY

TO VERIFY

Definition

1 : to establish the truth, accuracy, or reality of

- merriamwebster.com

TO COUNTERFEIT

Definition

1: to make in imitation of something else with intent to deceive

- merriamwebster.com

Bitcoin is

EASY to VERIFY

and

IMPOSSIBLE to counterfeit

Why is this important?

- When transacting, we want to be sure that the medium of exchange we are using is ‘**verifiably** the real thing’, since this assure us that it will be accepted by others in the future, when we wish to trade it for goods and services.

- In addition, we want to be certain that it is truly scarce so that we know it will maintain, or increase in, it’s purchasing power over time.

- In order for us to trust its scarcity, we need to know it **cannot be counterfeited.**

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 breaches of that trust.

Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve.

We have to trust them with our privacy, trust them not to let identity thieves drain our accounts.

~ Satoshi Nakamoto 2009-02-11

Bitcoin cannot be counterfeited because of
Proof of Work, being
the cryptography used in the protocol,
the time stamping in the time chain
and the consensus rules.

With the Byzantine General's Problem
(previously though unsolvable) being solved by Satoshi,
bitcoin became impossible to counterfeit.

The Byzantine General 's Problem

- The Byzantine generals' problem in the field of computer science, tells of two generals planning to attack an enemy city.
- To win the battle, each general must attack from a different side of the city.
- The issue at hand is a timing or synchronization problem coupled with trust, because both armies need to attack simultaneously.
- While each general can send a messenger to the other, to attempt to coordinate the attack, neither can be sure that the message they receive is accurate, since the messengers could have been compromised along the way, and the generals would have no way of knowing if this was the case.
- This represents the problem of how to achieve consensus and trust in a trustless, decentralized system.

On October 31, 2008, Satoshi wrote in the Cryptographers mailing list:

I’ve been working on a new electronic cash system that’s fully peer-to-peer, with no trusted third party

The main properties:

- Double-spending is prevented with a peer-to-peer network.
- No mint or other trusted parties.
- Participants can be anonymous.
- New coins are made from Hashcash style proof-of-work.
- The proof-of-work for new coin generation also powers the network to prevent double-spending.

I’ve developed a new open source P2P e-cash system called Bitcoin. It’s completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper:
Download Bitcoin v0.1 at http://www.bitcoin.org

~ Satoshi Nakamoto 2009-02-11 22:27:00 UTC Posted on metzdowd.com, an early cryptography mailing list

Proof-of-work also solves the problem of determining representation in majority decision making.

If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs.

Proof-of-work is essentially one-CPU-one-vote.

The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it.

If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains.

~ Satoshi Nakamoto

What makes bitcoin verifiable?

- Thousands of people worldwide run bitcoin nodes at home on a small raspberry pi or laptop.

- These nodes form a gossip network, sending and receiving the latest updates from the timechain in real time.

- Each node checks that each transaction and block meets the rules of the protocol.

- If a transaction or block attempts to break the rules, the nodes with reject it.

- When you run a node, you are able to easily verify for yourself the exact amount of bitcoin that have been mined, as well as the exact amount that can ever be mined.

- You can also use your node to verify any transactions you send or receive, to make sure they are actually there!

What makes bitcoin Impossible to Counterfeit?

- Unlike with fiat money, it isn’t possible to counterfeit bitcoin due to the characteristics of its protocol.
- These characteristics prevent a double spend attack, in which a user attempts to generate two or more transactions from the same UTXO.
- If a network attack was attempted, it would be known to all nodes, who would reject the block containing the double spend.
- A 51% attack would be required to successfully double spend a transaction, and this would require the counterfeiter to control more than 51% of the CPU power of the entire Bitcoin network.
- This would mean that a user would have control of the power of millions of ASICS, which is practically impossible.

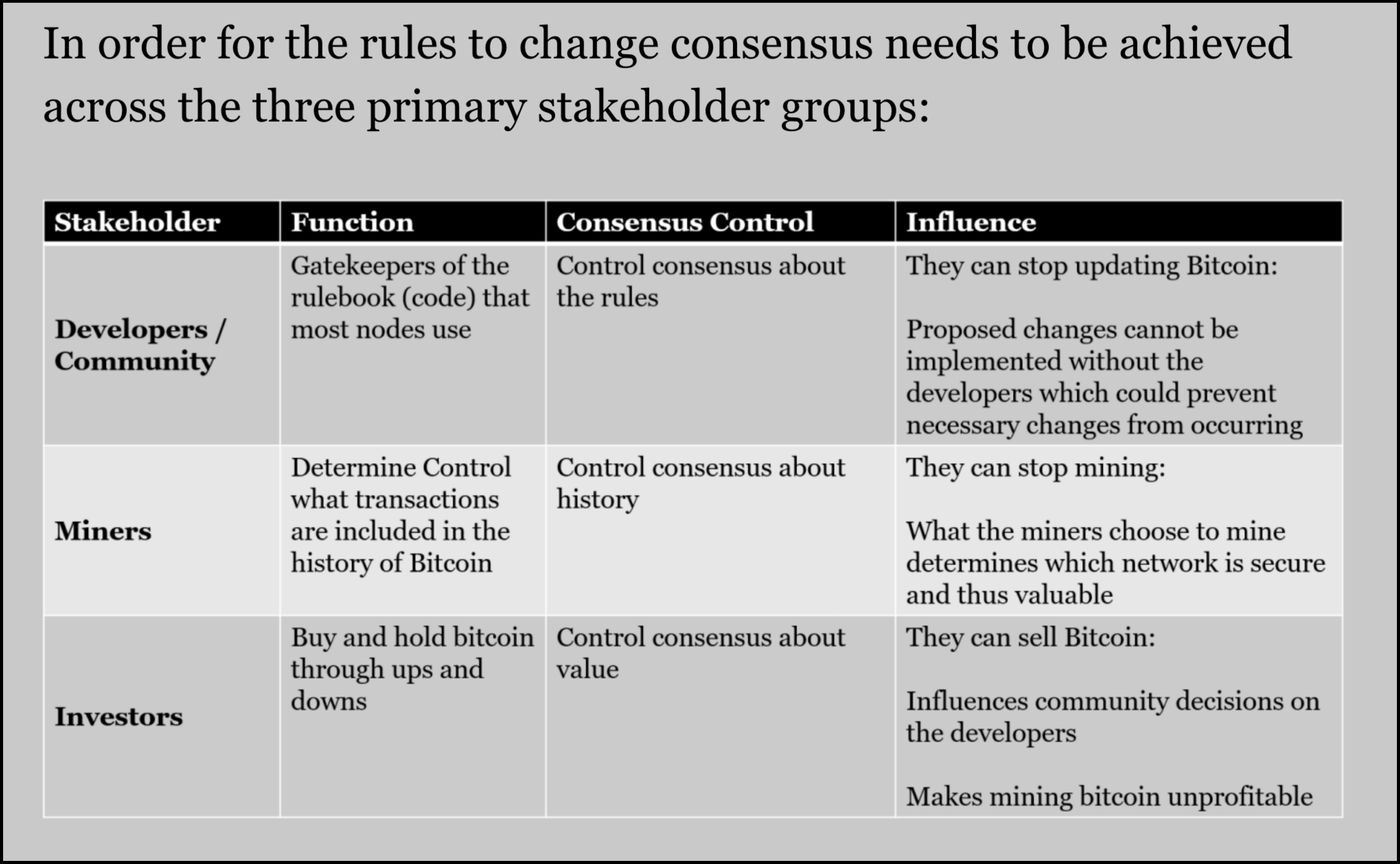
- Security lies in cryptography and in the control of the private key, which allows you to sign and broadcast your transactions to the network.

- In the case of legal tender, to avoid counterfeiting, the monetary authority must constantly improve the paper technology, printing techniques or security markings.

- This leaves us, as Satoshi clearly pointed out, at the mercy of a third party whom we must trust.

- With all the money printing, in the form of QE especially since 2009, it could be argued that the fiat we use is in fact, counterfeit, since it is produced

In Bitcoin, Decentralized Consensus Prevents Counterfeiting



In order for the rules to change consensus needs to be achieved across the three primary stakeholder groups:

Stakeholder	Function	Consensus Control	Influence
Developers / Community	Gatekeepers of the rulebook (code) that most nodes use	Control consensus about the rules	They can stop updating Bitcoin: Proposed changes cannot be implemented without the developers which could prevent necessary changes from occurring
Miners	Determine Control what transactions are included in the history of Bitcoin	Control consensus about history	They can stop mining: What the miners choose to mine determines which network is secure and thus valuable
Investors	Buy and hold bitcoin through ups and downs	Control consensus about value	They can sell Bitcoin: Influences community decisions on the developers Makes mining bitcoin unprofitable

From: Eric Takes site, yakes.io

He ought to find it more profitable to play by the rules, such rules that favor him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

~ Satoshi Nakamoto

Thank you for listening!

We appreciate any feedback, correction or suggestions to improve this deck!