bitcoin`s

Sound Money Properties Series

#12: Pseudonymous & Trustless

with @SimplestBTCBook & @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

PSEUDONYMOUS

Definition of pseudonymous

1 **:** bearing or using a fictitious name

- merriamwebster.com

PSEUDONYMOUS VS ANONYMOUS

- Pseudonymous means that a person is using a false name or an alias.
- Anonymous means that a person's identity is completely unknown.
- In other words, pseudonymous is a partial disguise, while anonymous is a complete disguise.
- While both terms refer to concealing one's identity, pseudonymous means using a false name or alias, while anonymous means not revealing any identifying information at all.
- Using a pseudonym does not necessarily mean that a person's identity is completely hidden, as it may still be possible to track them down through other means.

BITCOIN IS PSEUDONYMOUS

- Bitcoin is Pseudonymous
- Sending and receiving bitcoins is like writing under a pseudonym.
- If an author’s pseudonym is ever linked to their identity, everything they ever wrote under that pseudonym will now be linked to them.
- In Bitcoin, your pseudonym is the address to which you receive Bitcoin.
- Every transaction involving that address is stored forever in the blockchain.
- If your address is ever linked to your identity, every transaction will be linked to you.

- Bitcoin Anonymity - Is Bitcoin Anonymous?
- From: buybitcoinworldwide.com

- In the original whitepaper, it was recommended that Bitcoin users use a new address for each transaction to avoid the transactions being linked to a common owner.

As an additional firewall, a new (address) should be used for each transaction to keep them from being linked to a common owner....The risk is that if the owner of a (address) is revealed, linking could reveal other transactions that belonged to the same owner.

- Satoshi Nakamoto Inventor, Bitcoin

- This would be the equivalent of writing many books under different pseudonyms. If one of your pseudonyms is linked to you, the others are still secret.

- Bitcoin Anonymity - Is Bitcoin Anonymous?
- From: buybitcoinworldwide.com

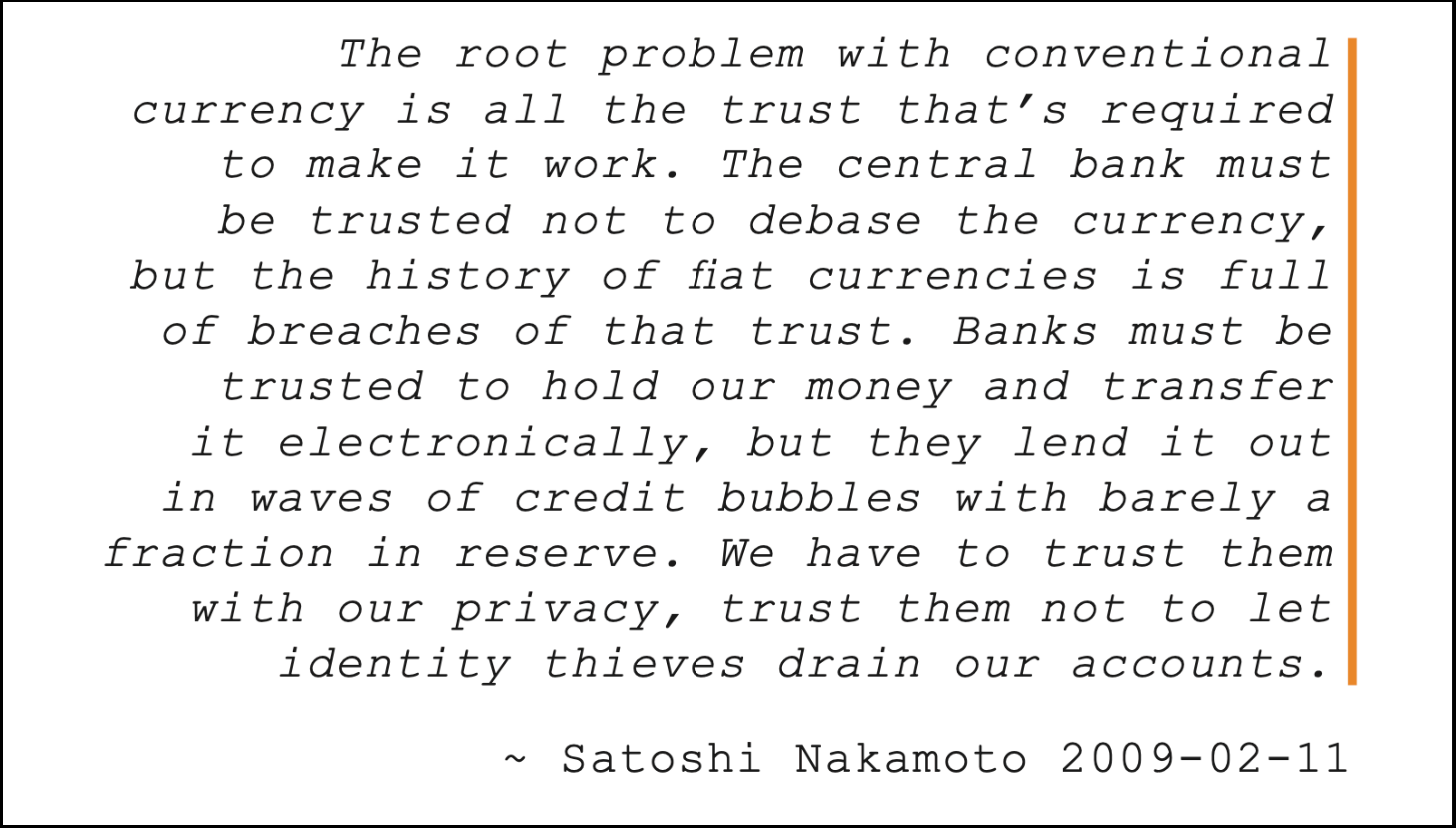
TRUSTLESS

Definition of trustless

: without trust

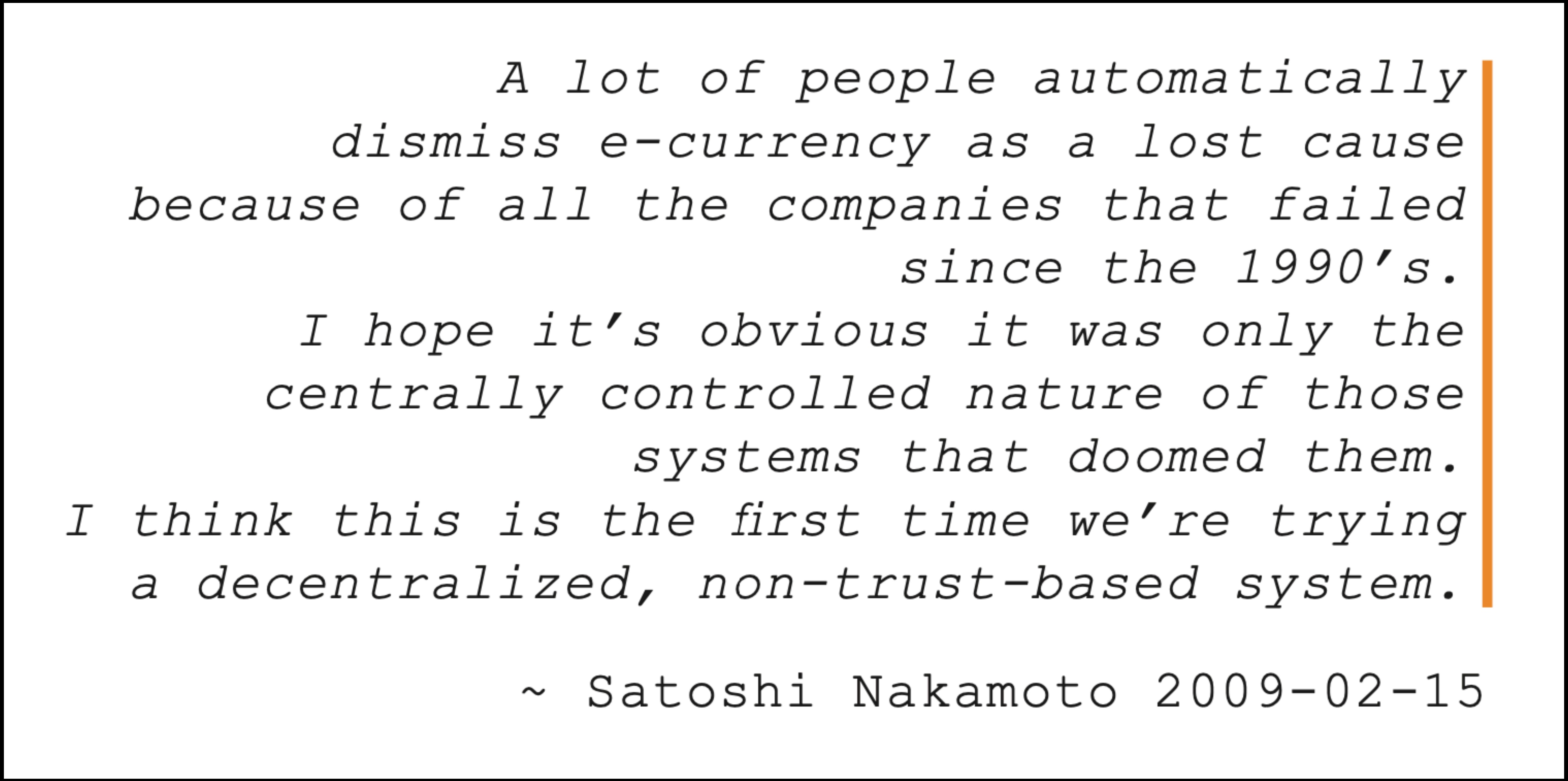
With regard to bitcoin, trustless means no single party needs to be trusted because a majority of nodes (parties) agree by reaching consensus.

SATOSHI ON THE ISSUE OF TRUST



> *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



> *A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990's.*
>
> *I hope it's obvious it was only the centrally controlled nature of those systems that doomed them.*
>
> *I think this is the first time we're trying a decentralized, non-trust-based system.*

~ Satoshi Nakamoto 2009-02-15

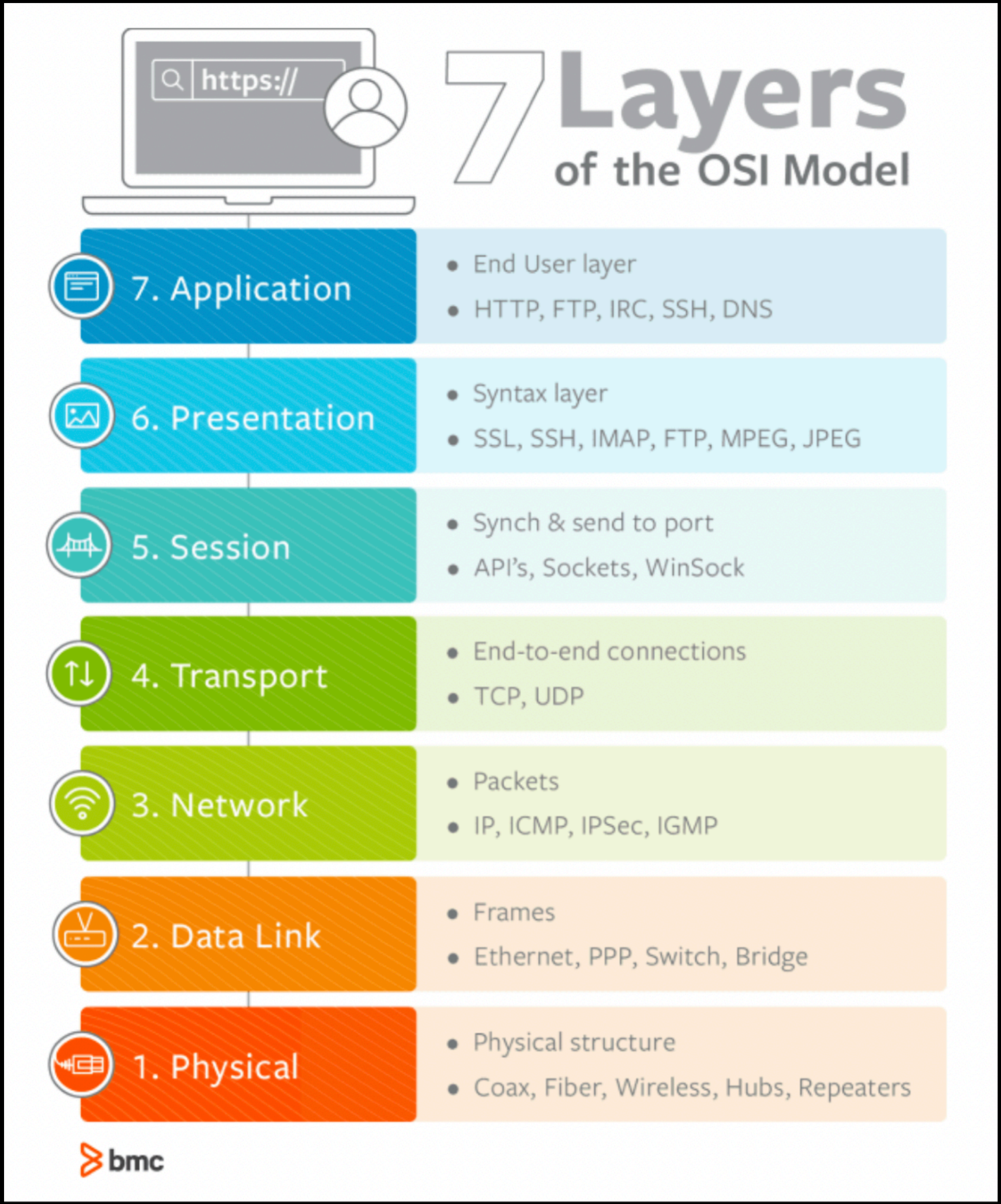
BITCOIN IS TRUSTLESS

- By replacing reliance on third parties in a trustless way, Bitcoin adds a layer of non-intermediated trust to the infrastructure of the internet.

- From: Bitcoin’s Trustless Nature Adds Trust To The Internet
An article in Bitcoin Magazine By Stephen Thompson

Bitcoin As A New Trust Layer For The Internet

The internet currently has seven layers as expressed in this model below. This is the Open Systems Interconnections model (OSI).



7 Layers of the OSI Model

7. Application
- End User layer
- HTTP, FTP, IRC, SSH, DNS

6. Presentation
- Syntax layer
- SSL, SSH, IMAP, FTP, MPEG, JPEG

5. Session
- Synch & send to port
- API's, Sockets, WinSock

4. Transport
- End-to-end connections
- TCP, UDP

3. Network
- Packets
- IP, ICMP, IPSec, IGMP

2. Data Link
- Frames
- Ethernet, PPP, Switch, Bridge

1. Physical
- Physical structure
- Coax, Fiber, Wireless, Hubs, Repeaters

THE IRONY:
BY BEING TRUSTLESS, BITCOIN CREATES TRUST

- The Bitcoin network is a trust protocol and we see it as the essential trust layer for the internet.

- The Bitcoin protocol is a set of rules that govern the network and protect it from attacks, like tampering with the blockchain, double-spending or spamming the network.

- We consider Bitcoin as a much-needed trust layer for the internet because it is *trustless*.

- How can this be?

- "Trustless" means that there are no entities that users have to trust in order to get their information from one node to another and its eventual confirmation onto the network.

- From: Bitcoin's Trustless Nature Adds Trust To The Internet
An article in Bitcoin Magazine By Stephen Thompson

- Instead, the *decentralized nature and transparency* of the network is the base on which Bitcoin's trust protocol sits.

- Bitcoin's own trust protocol runs on two levels: the transaction level, where users in a transaction swap their public keys and then sign transactions with their private keys so that both users can know that the transaction was genuine; the network level where thousands of nodes and miners confirm that the transaction was not spent twice and then broadcast to the blockchain.

- From: Bitcoin's Trustless Nature Adds Trust To The Internet
An article in Bitcoin Magazine By Stephen Thompson

- When we say bitcoin is trustless, we mean that one is able to transact value, to send and receive bitcoin, without trusting a third party to verify or process the transactions.

- Unlike banks or other financial institutions that hold one’s money, have operating hours, can freeze or close accounts, can demand to know where one’s money comes from or is going to, bitcoin runs on code that is maintained by thousands of individual nodes that are run ad hoc, by thousands of people globally.

- These nodes all carry a copy of the bitcoin timechain, or ledger, and compare notes every ten minutes, to be sure that all transactions are valid.

- No specific humans are necessary or need to be trusted to be good actors. No one can censor your transactions, manipulate the data or otherwise control the flow of value.

- Bitcoin runs 24/7, everywhere.

BITCOIN IS SOVEREIGN BANKING FOR ANYONE, ANYWHERE

- Anyone, anywhere with a smartphone and cell service can simply download a bitcoin wallet, and immediately start receiving bitcoin whether they worked for it, bought it or were gifted it.

- No name, address, ID, passport, approval or permission needed.

- No need to trust anyone to hold or protect or preserve your wealth.

- Remember: Being your own bank means securing your own savings and wealth.

- Secure your seed! Stamp it into metal and hide it well! Make at least two copies and hide them in geographically distributed places.

WHY ARE PSEUDONYMITY AND TRUSTLESSNESS IMPORTANT PROPERTIES OF SOUND MONEY?

- When we need to provide all of our personal information to a third party, and when we need to request permission to spend our own money, we are not free or sovereign.

- When others have the power to prevent us from transacting and fulfilling our needs, we are not free or sovereign.

- When we must trust that another is holding our money safely, and not rehypothecating or inflating/debasing it, we can never know for certain what is happening to our purchasing power, and therefore we cannot plan for the future.

WHY ARE PSEUDONYMITY AND TRUSTLESSNESS IMPORTANT PROPERTIES OF SOUND MONEY? Cont..

- On the other hand, when money is pseudonymous and trustless, it can be used by anyone, anywhere, without needing permission from anyone.
- No one can stop another from transacting freely, and from spending their stored energy when and how they wish.
- For money to be truly sound, and to work for everyone, everywhere, it needs to be pseudonymous and trustless in order to facilitate freedom and sovereignty into the future.

Thanks for listening!

Feedback always welcome!

Next week we will discuss how bitcoin is

SECURE & SCALABLE