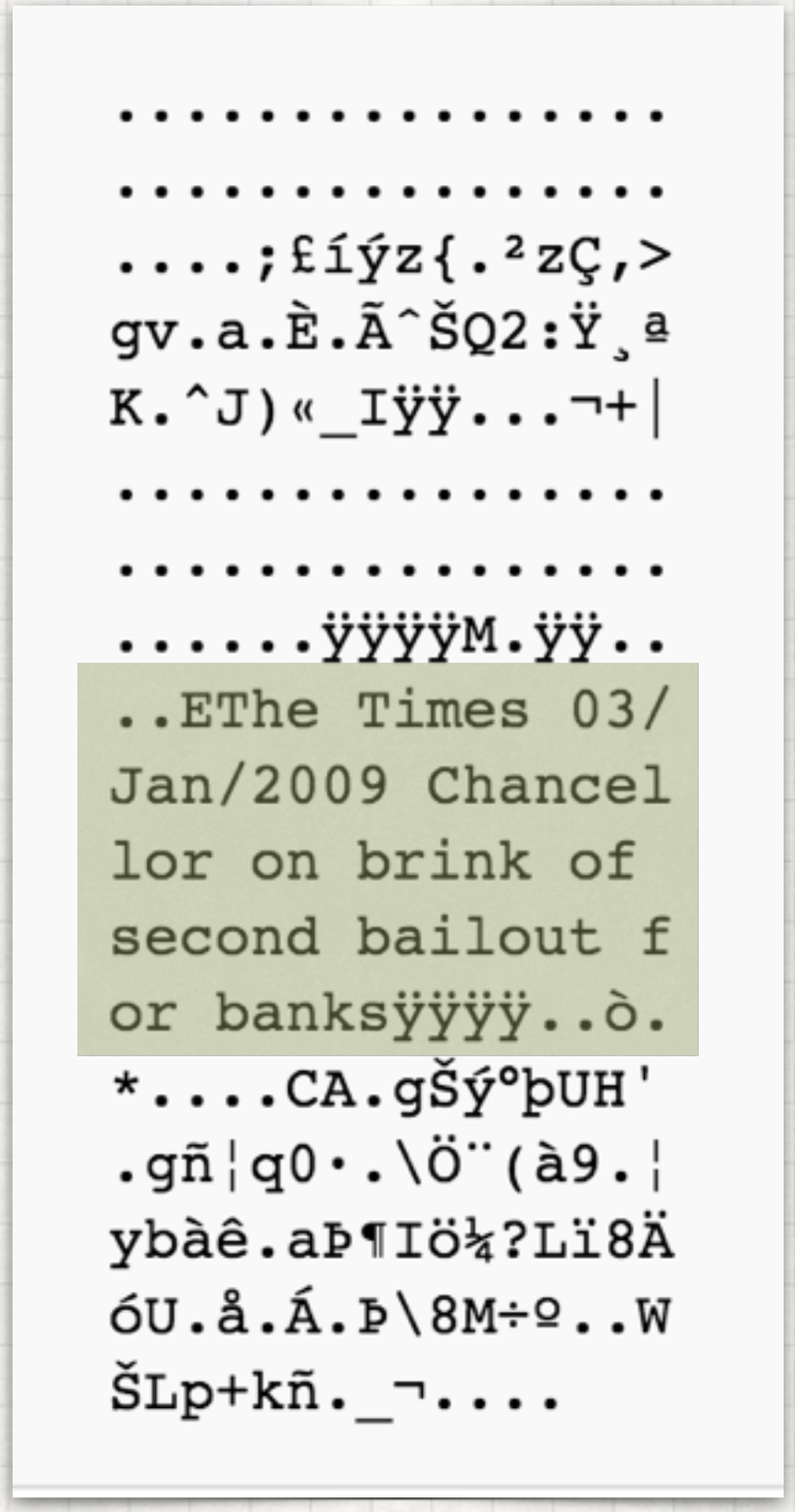
WHAT IS "BLOCKCHAIN"?

SATOSHI
NAKAMOTO

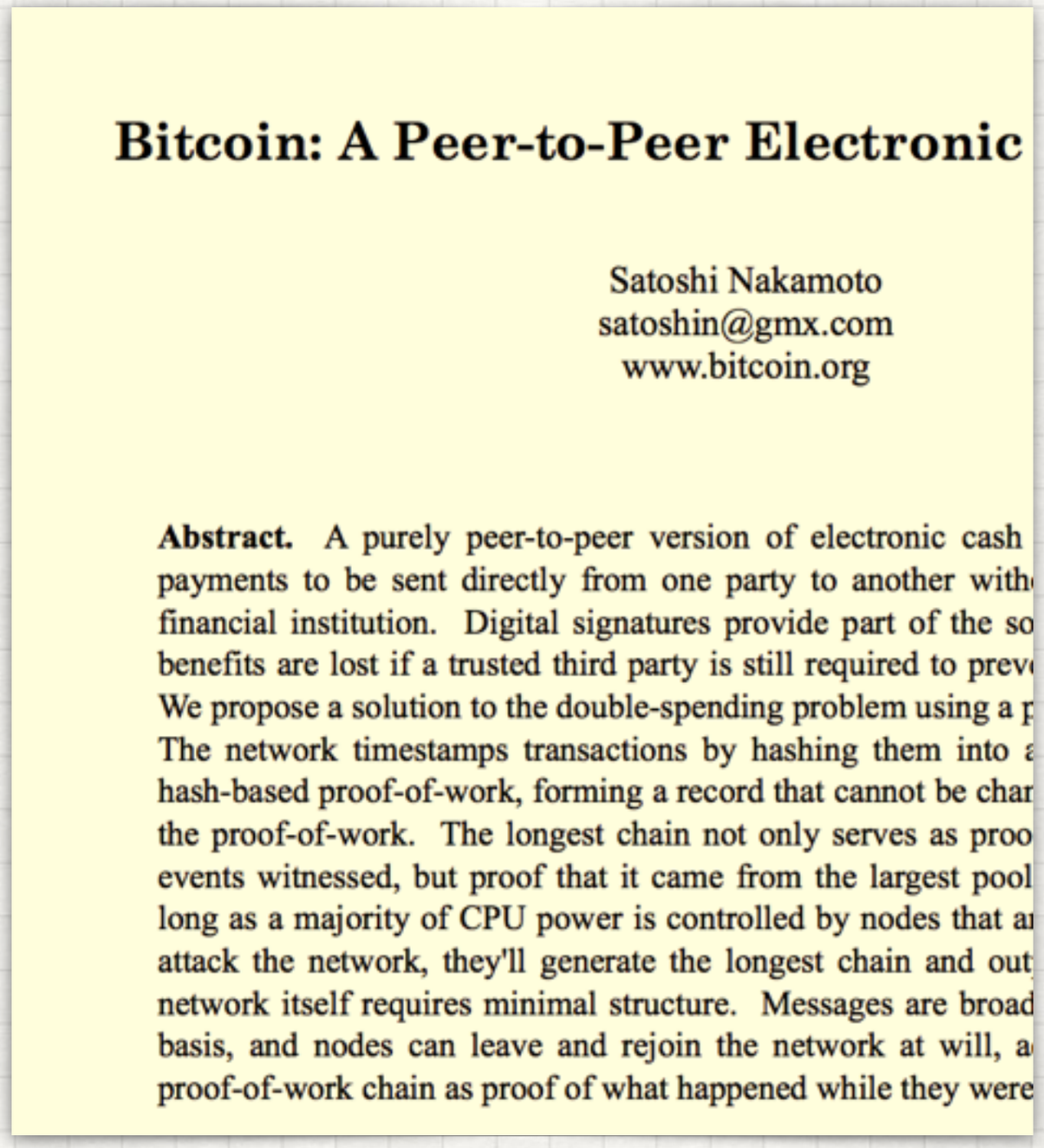
GENESIS BLOCK



BITCOIN

A PEER-TO-PEER ELECTRONIC CASH SYSTEM

- “chain of blocks”
  - immutable Merkle trees
- censorship resistance
  - P2P communication
- coordination
  - Byzantine General
  - Prisoner’s Dilemme
- compliance protocol
  - incentivized validation
  - prevent starvation of resources



Bitcoin: A Peer-to-Peer Electronic

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

Abstract. A purely peer-to-peer version of electronic cash
payments to be sent directly from one party to another with
financial institution. Digital signatures provide part of the so
benefits are lost if a trusted third party is still required to prev
We propose a solution to the double-spending problem using a p
The network timestamps transactions by hashing them into a
hash-based proof-of-work, forming a record that cannot be char
the proof-of-work. The longest chain not only serves as proo
events witnessed, but proof that it came from the largest pool
long as a majority of CPU power is controlled by nodes that a
attack the network, they'll generate the longest chain and out
network itself requires minimal structure. Messages are broad
basis, and nodes can leave and rejoin the network at will, a
proof-of-work chain as proof of what happened while they were

BUILDING ON THE SHOULDERS OF GIANTS

PREREQUISITE COMPONENTS

- Databases
  - SQL
  - NoSQL
  - Big Data
- Asymmetric cryptography
  - Hash trees
  - PGP
- Peer-to-peer networks
  - DHT (distributed hash tables)
  - BitTorrent

“

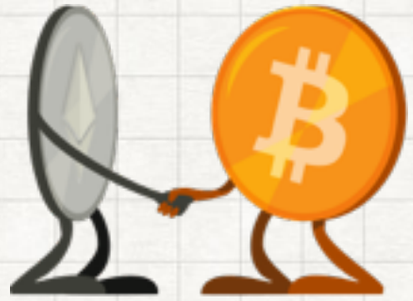
GOVERNMENTS ARE GOOD AT CUTTING OFF THE HEADS OF A CENTRALLY CONTROLLED NETWORKS LIKE NAPSTER, BUT PURE P2P NETWORKS LIKE GNUTELLA AND TOR SEEM TO BE HOLDING THEIR OWN.

— *Satoshi Nakamoto*

”

FIRST, BUT NO LONGER UNIQUE

- Litecoin / 4x faster
- Namecoin / DNS
- Dogecoin / fun
- DASH / private
- BitMessage / messaging
- Ethereum / flexible



DISTRIBUTED IMMUTABLE LEDGER

- no central point of control
  - tolerates partial connectivity
  - resilient to individual failure
- tamper resistant
  - non-repudiation
  - difficult to censor
- account of entry
  - real-time validation
  - machine-processed settlement

KEY BENEFITS

- Auditable
  - Cryptographic receipts
  - Triple entry accounting
- Protocol enforces compliance
  - Reduce bad actors
  - Egalitarian usage
- Distributed trust
  - Remove central point of failure
  - Spread trust among participants (instead of concentrating in single entity)

STRONG USE CASES

- Coordinating action between untrusted actors
  - Increased speed
  - Lower cost
- M2M transactions
  - Internet of Things
  - Microtransactions / pay per usage
- Shared real-time state
  - Instant data portability
  - Fast convergence to consistent view

TAYLOR GERRING

DIRECTOR OF TECHNOLOGY
ETHEREUM FOUNDATION

@TaylorGerring

taylor.gerring@gmail.com

https://blockchainconsulting.expert