Is Bitcoin Really the Future of Currency

By

Rajarshi Maitra

B.E., Civil - JU

M.Tech, OSE - IITM

Structural Engineer at LTHE

Is Bitcoin Really the Future of Currency

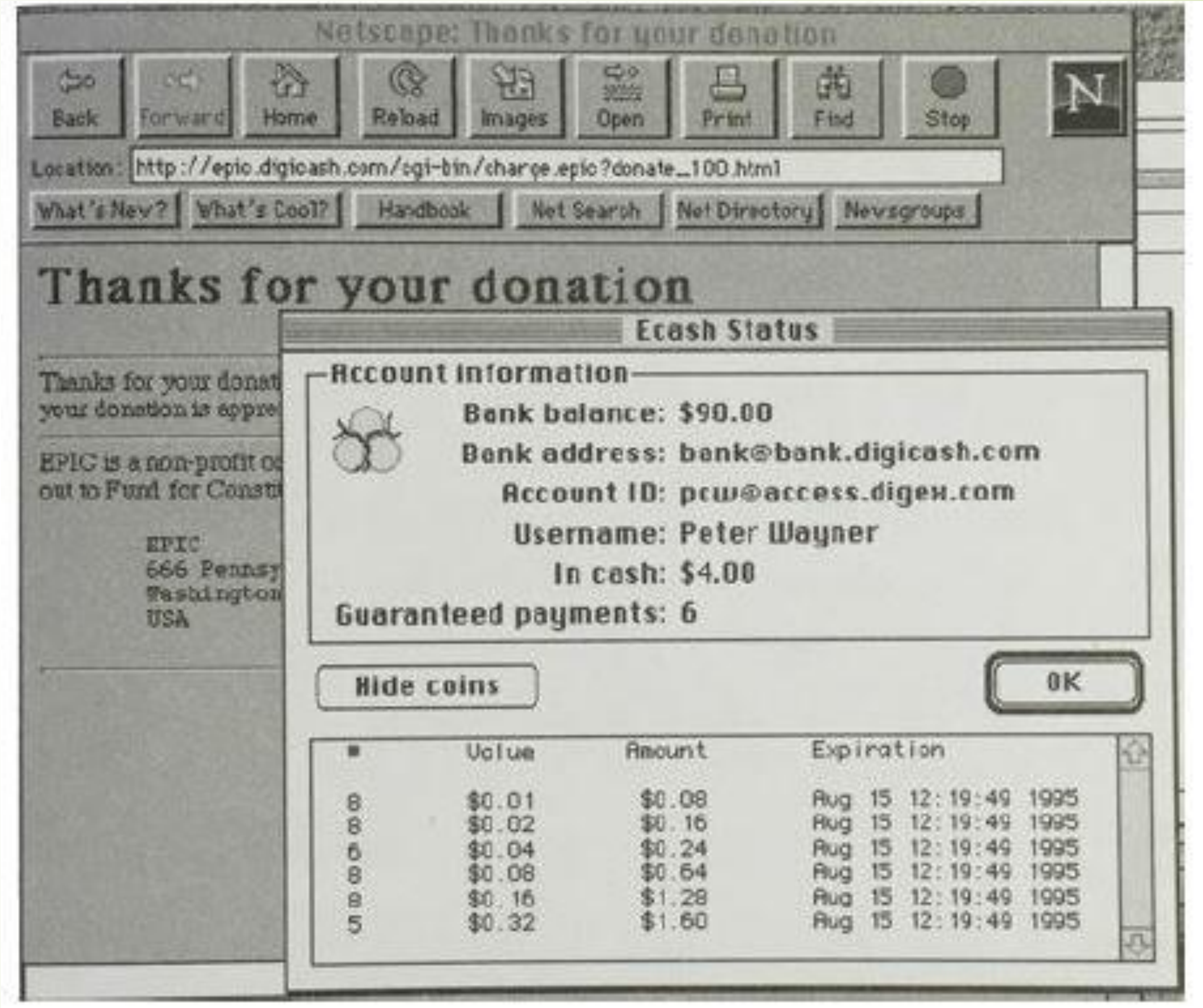
CONTENT

- Brief history of digital money system
- Problem of distributed consensus
- Trustnet Protocol
- Crypto Anarchism and philosophical implications

History

Digi-Cash (David Chaum, 1989)

- 1st Serious Implementation of Digital Currency
- Used "Blind Signature" for end user privacy
- Required a central server for issuance of currency
- Failed due to inadequate adoption of e-commerce



Netscape: Thanks for your donation

Location: http://epic.digicash.com/cgi-bin/charge.epic?donate_100.html

Thanks for your donation

Thanks for your donat
your donation is appre

EPIC is a non-profit o
out to Fund for Constit

EPIC
666 Pennsy
Washington
USA

Ecash Status

Account information

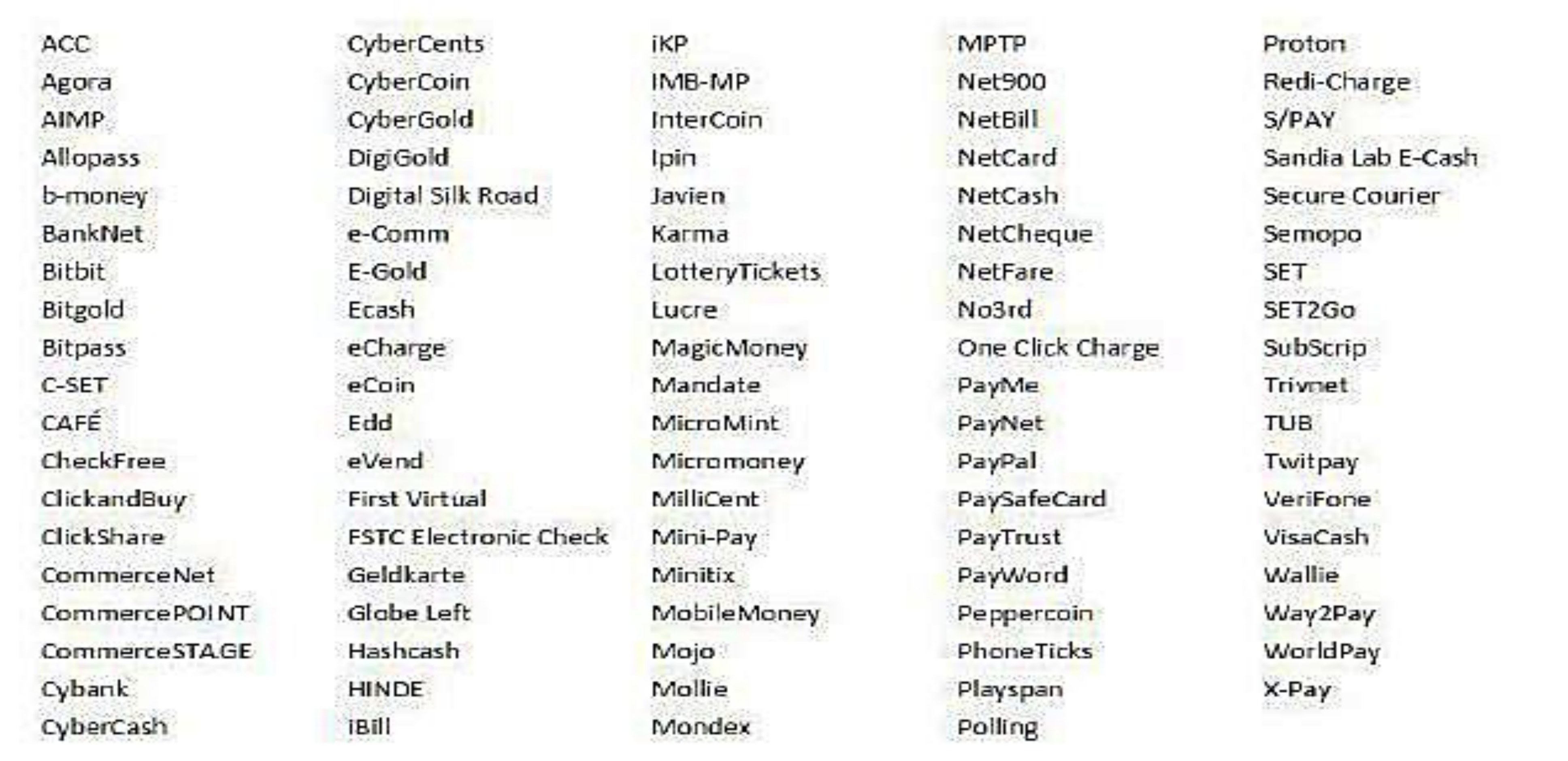
Bank balance: $90.00
Bank address: bank@bank.digicash.com
Account ID: pcw@access.digex.com
Username: Peter Wayner
In cash: $4.00
Guaranteed payments: 6

#	Value	Amount	Expiration
8	$0.01	$0.08	Aug 15 12:19:49 1995
8	$0.02	$0.16	Aug 15 12:19:49 1995
6	$0.04	$0.24	Aug 15 12:19:49 1995
8	$0.08	$0.64	Aug 15 12:19:49 1995
8	$0.16	$1.28	Aug 15 12:19:49 1995
5	$0.32	$1.60	Aug 15 12:19:49 1995

Source : *Bitcoin and Crypto currency technology*, Arvind et.al

History

The Long Road To Bitcoin

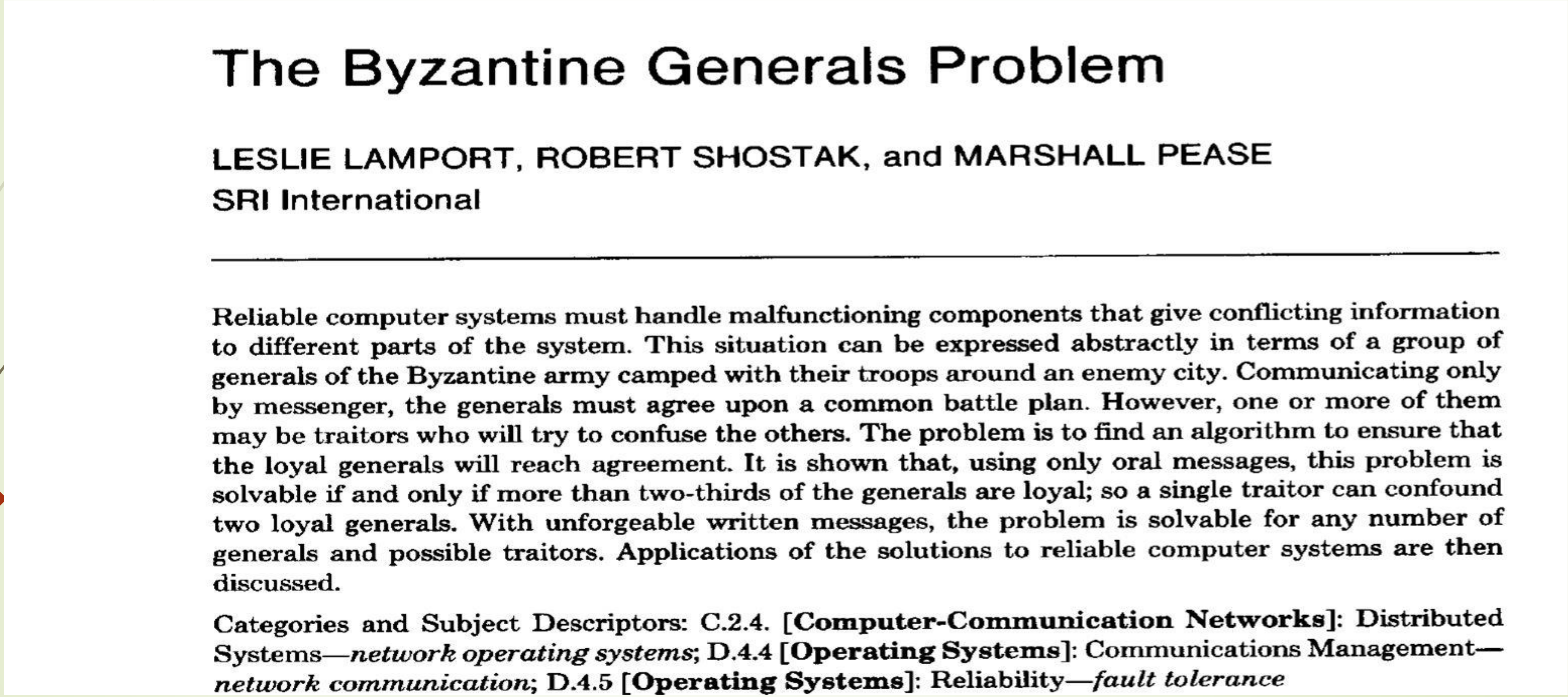


ACC
Agora
AIMP
Allopass
b-money
BankNet
Bitbit
Bitgold
Bitpass
C-SET
CAFÉ
CheckFree
ClickandBuy
ClickShare
CommerceNet
CommercePOINT
CommerceSTAGE
Cybank
CyberCash
CyberCents
CyberCoin
CyberGold
DigiGold
Digital Silk Road
e-Comm
E-Gold
Ecash
eCharge
eCoin
Edd
eVend
First Virtual
FSTC Electronic Check
Geldkarte
Globe Left
Hashcash
HINDE
iBill
iKP
IMB-MP
InterCoin
Ipin
Javien
Karma
LotteryTickets
Lucre
MagicMoney
Mandate
MicroMint
Micromoney
MilliCent
Mini-Pay
Minitix
MobileMoney
Mojo
Mollie
Mondex
MPTP
Net900
NetBill
NetCard
NetCash
NetCheque
NetFare
No3rd
One Click Charge
PayMe
PayNet
PayPal
PaySafeCard
PayTrust
PayWord
Peppercoin
PhoneTicks
Playspan
Polling
Proton
Redi-Charge
S/PAY
Sandia Lab E-Cash
Secure Courier
Semopo
SET
SET2Go
SubScrip
Trivnet
TUB
Twitpay
VeriFone
VisaCash
Wallie
Way2Pay
WorldPay
X-Pay

Source : *Bitcoin and Crypto currency technology*, Arvind et.al

History

The Core Issue:



The Byzantine Generals Problem

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International

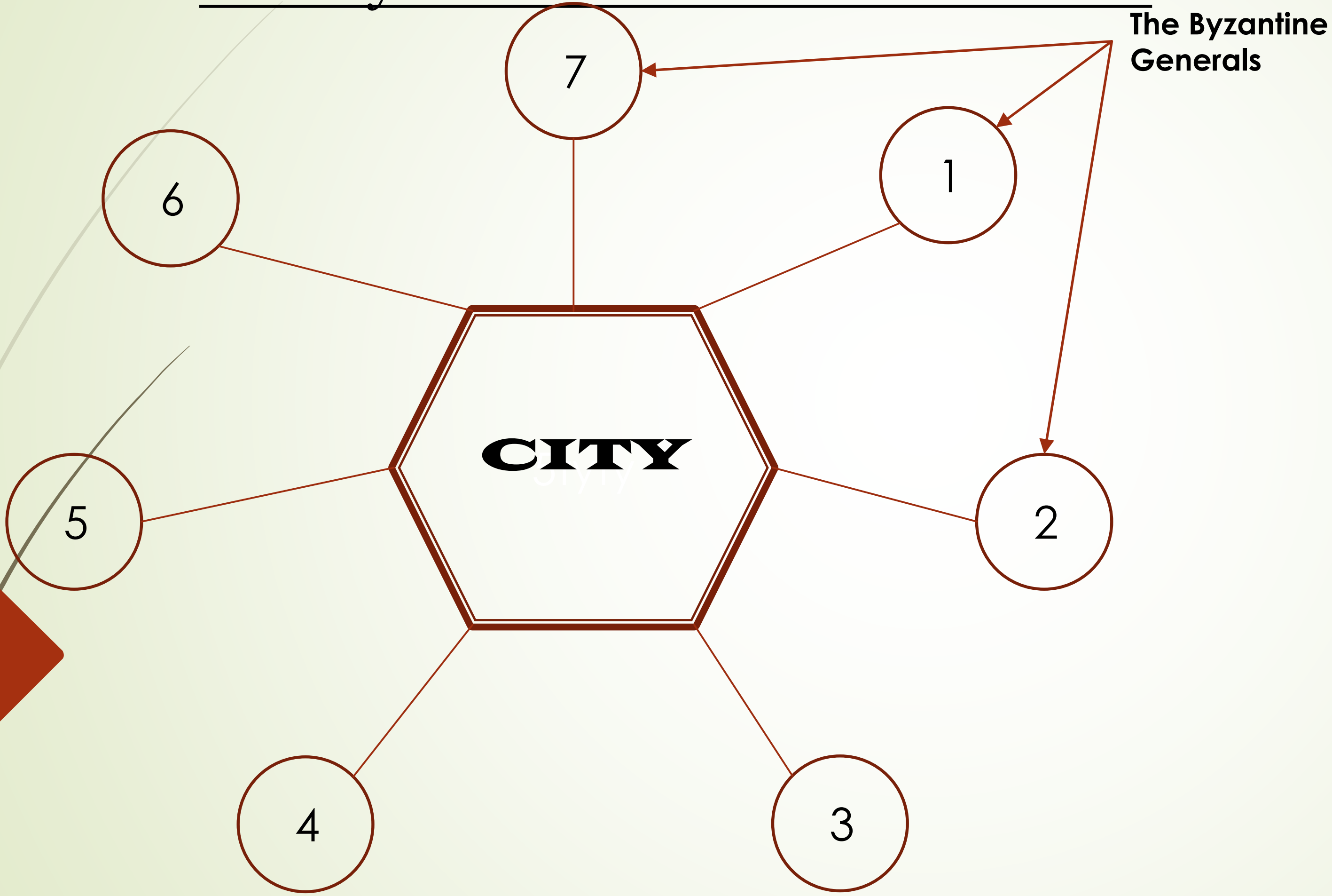
Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed.

Categories and Subject Descriptors: C.2.4. [**Computer-Communication Networks**]: Distributed Systems—*network operating systems*; D.4.4 [**Operating Systems**]: Communications Management—*network communication*; D.4.5 [**Operating Systems**]: Reliability—*fault tolerance*

Source : https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf

History

The Byzantine General's Problem:



Problems:

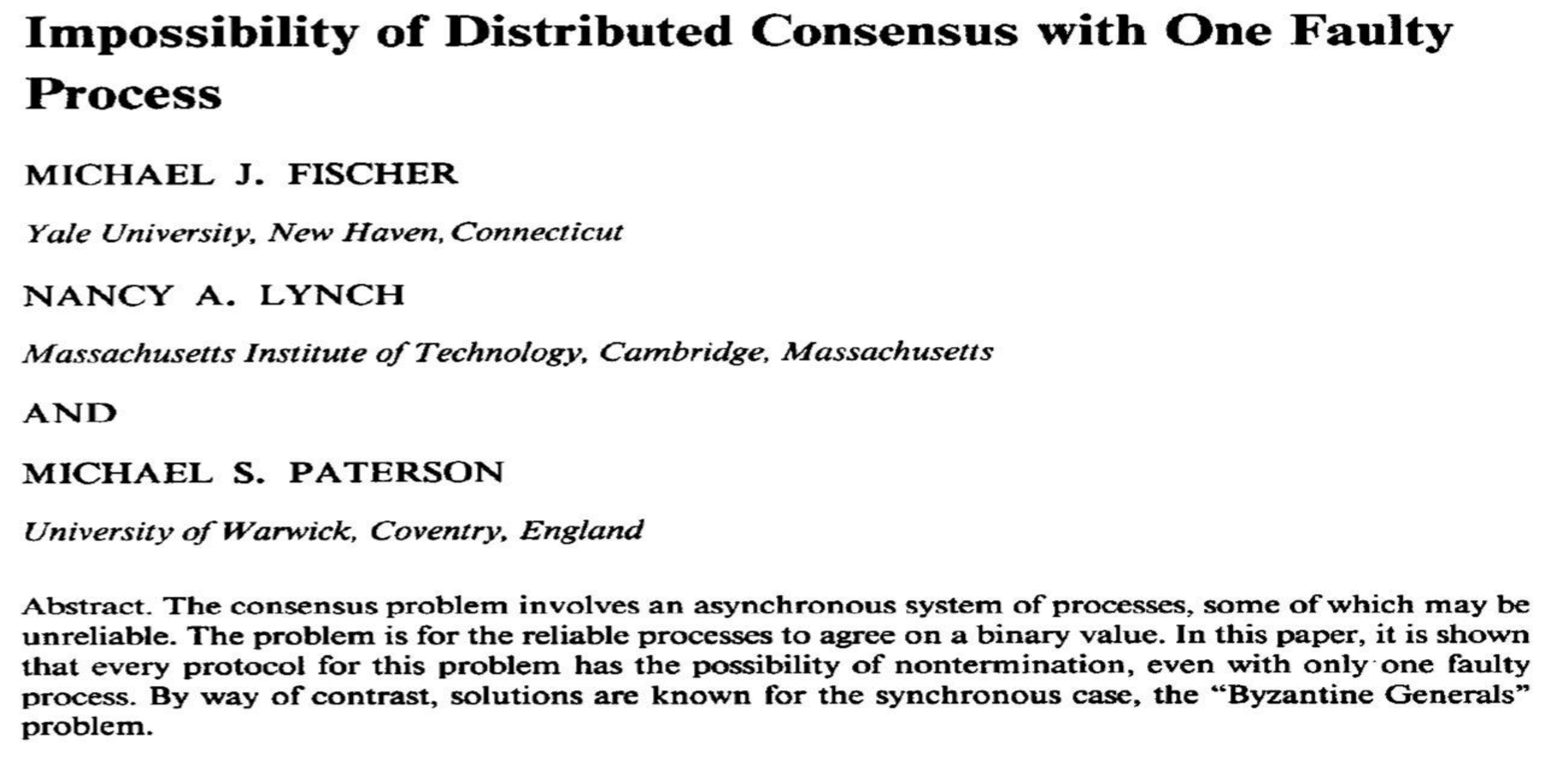
- Capturing messengers/Failure to deliver
- Forging false message by the City
- Dishonest Generals

Goal:

- Reach consensus for attack date and time.
- Trusting other generals (counterparty risk)

History

Some Bad News:



Impossibility of Distributed Consensus with One Faulty Process

MICHAEL J. FISCHER

Yale University, New Haven, Connecticut

NANCY A. LYNCH

Massachusetts Institute of Technology, Cambridge, Massachusetts

AND

MICHAEL S. PATERSON

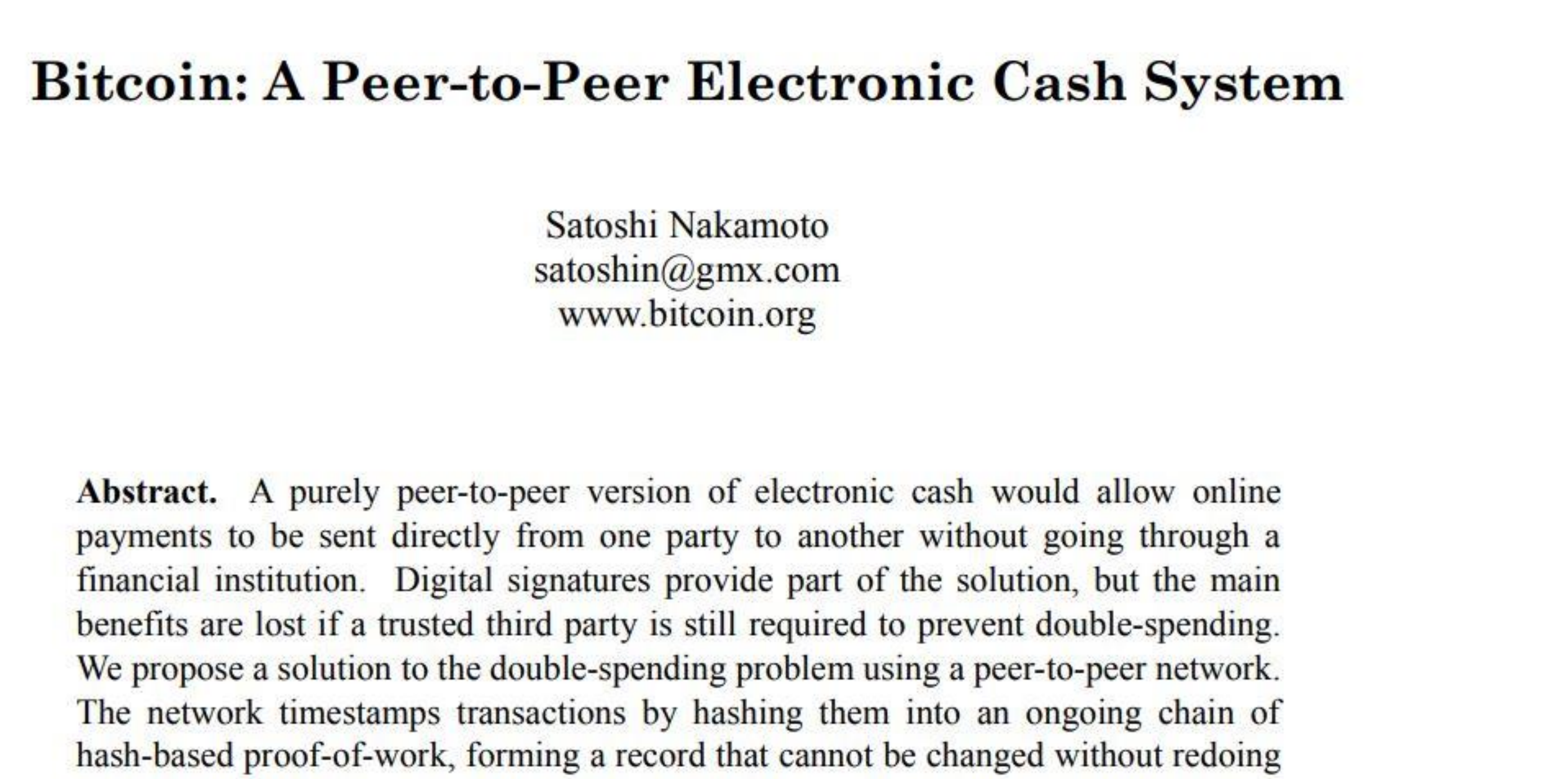
University of Warwick, Coventry, England

Abstract. The consensus problem involves an asynchronous system of processes, some of which may be unreliable. The problem is for the reliable processes to agree on a binary value. In this paper, it is shown that every protocol for this problem has the possibility of nontermination, even with only one faulty process. By way of contrast, solutions are known for the synchronous case, the "Byzantine Generals" problem.

Source : https://groups.csail.mit.edu/tds/papers/Lynch/jacm85.pdf

Trustnet

The Breakthrough:



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

Source : https://bitcoin.org/en/

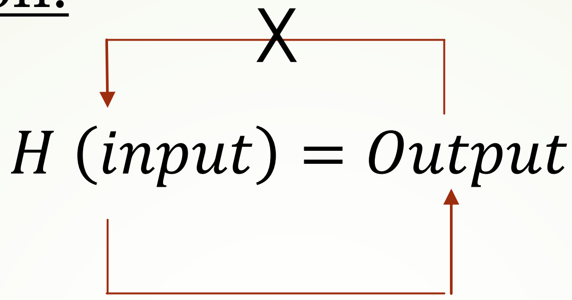
Trustnet

Protocol Outline:

- **Consensus Algorithm** : Proof of Work (PoW) – 1993
- **Hashing Functions** : SHA256, RIPEMD160 – 2001/1992
- **Merkle Tree** – 1979
- **Digital Signature** : ECDSA – 1985
- **Public Key/Private Key Cryptography** – 1976
- **Blockchain** – 1991

-TRUSTNET-

Hashing Function:



$$H\ (input) = Output$$

Characteristics:

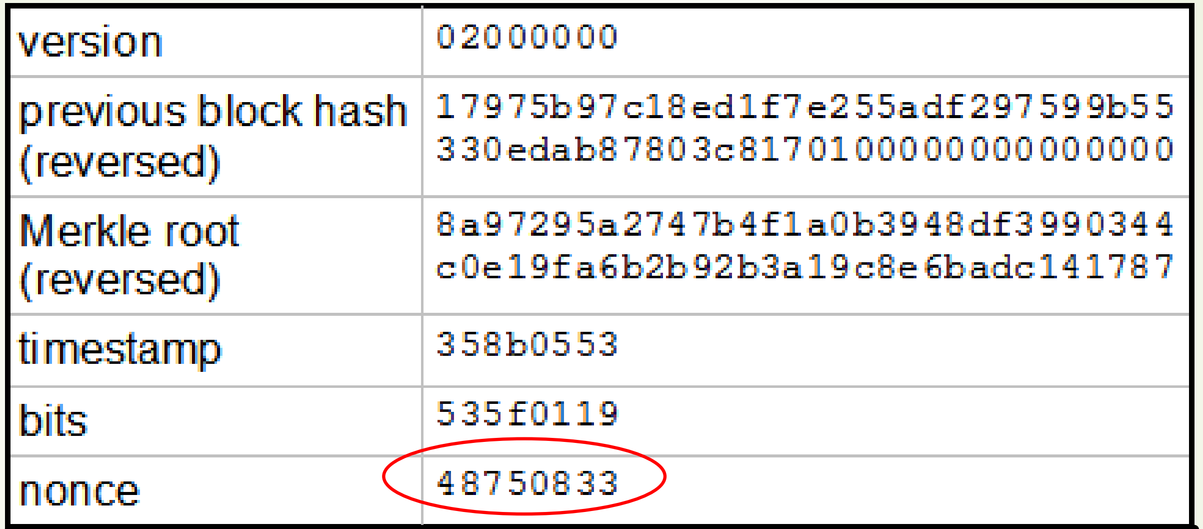
- One way function
- Input can be of any Size
- Output is unique but evenly distributed
- Brute force to obtain input from output

SHA256 (‘I Love Bitcoin1’) = `603c2c0fd8b4ab95cbd8332267a3ad1ec8a3c24d6cc62a33e64c346171db898f`

SHA256 (‘I Love Bitcoin2’) = `7eb9d3b4b24800dfe83f2d1145e023bfed676f3cc4e3124116b6037c7094579a`

Trustnet

Anatomy of a Block:



version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c8170100000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833

Body of Block

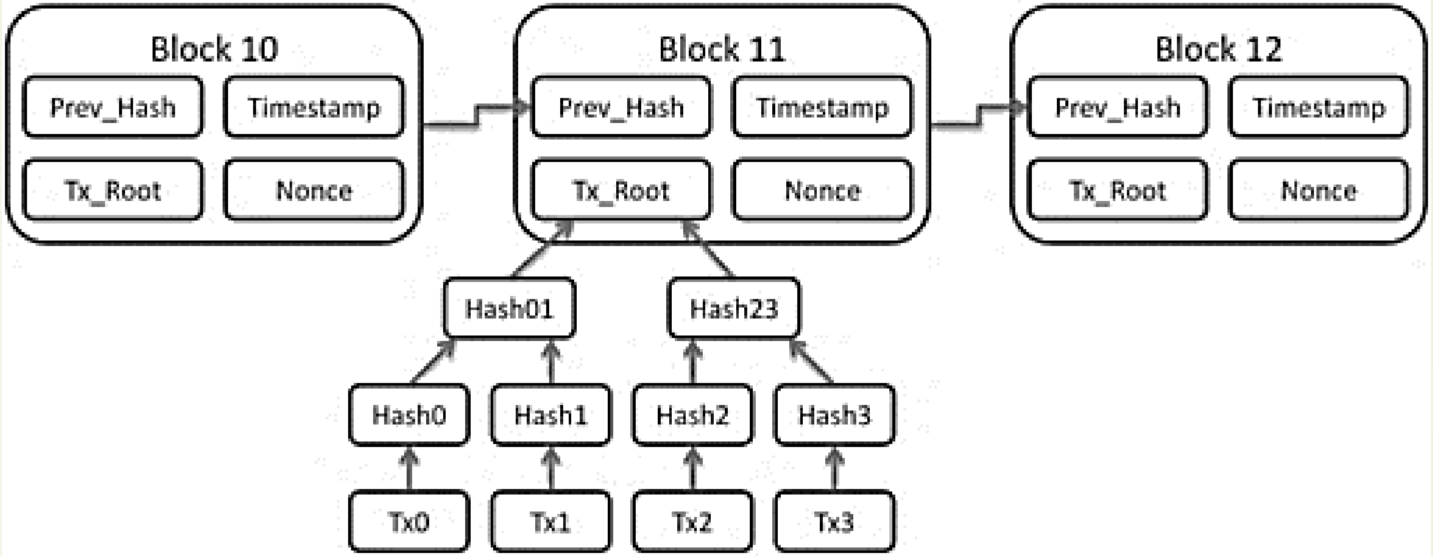
DATA TO ACHIEVE

CONSENSUS

Source : *Bitcoin and Crypto currency technology*, Arvind et.al

Trustnet

Mining:



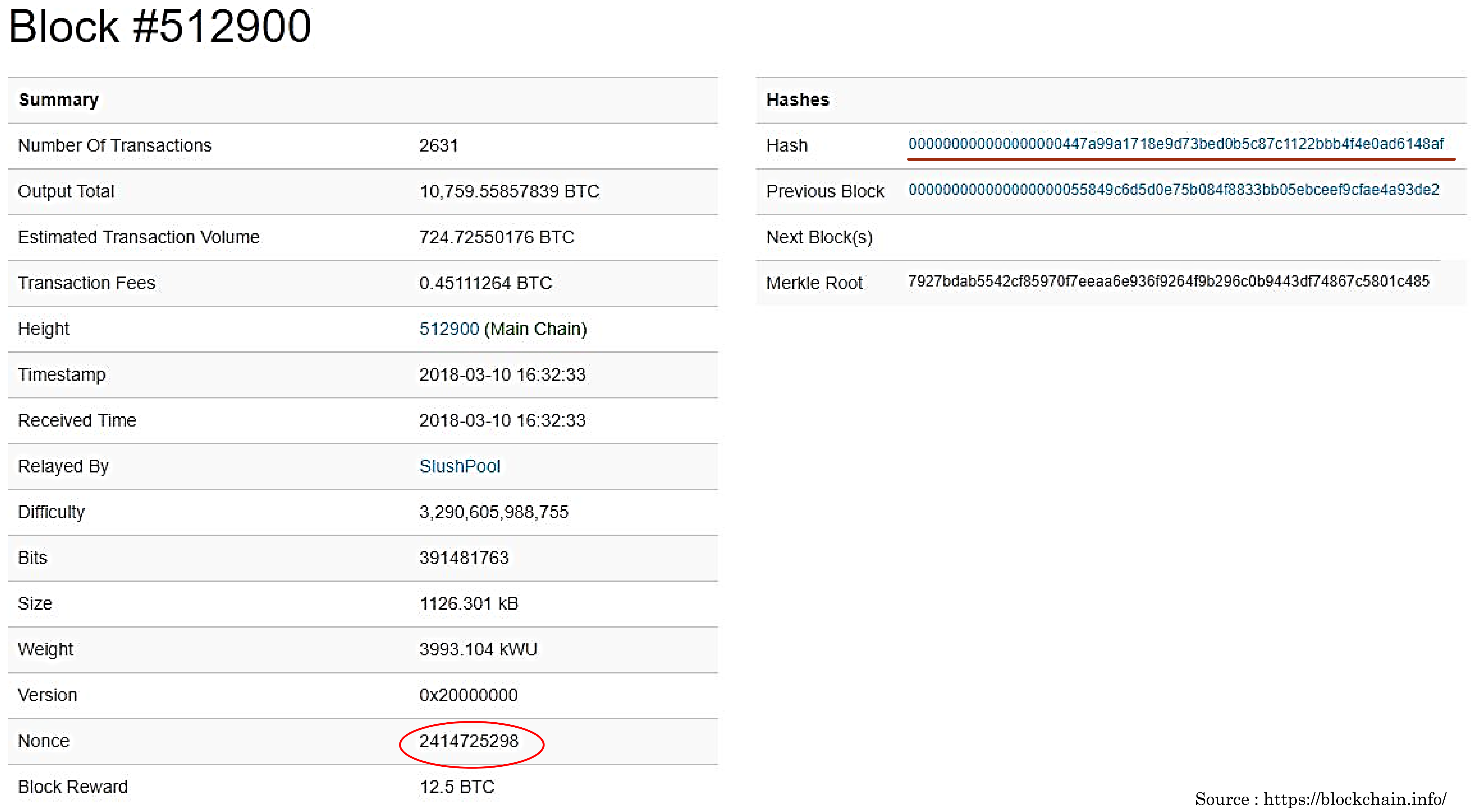
Source : *Bitcoin and Crypto currency technology*, Arvind et.al

Objective:

- Hash (Block Data||nonce) = Output with 1st **n** bits **0** (Difficulty Target)

- Iterate nonce until the above condition is satisfied

- If successful, claim block reward



Block #512900

Summary	
Number Of Transactions	2631
Output Total	10,759.55857839 BTC
Estimated Transaction Volume	724.72550176 BTC
Transaction Fees	0.45111264 BTC
Height	512900 (Main Chain)
Timestamp	2018-03-10 16:32:33
Received Time	2018-03-10 16:32:33
Relayed By	SlushPool
Difficulty	3,290,605,988,755
Bits	391481763
Size	1126.301 kB
Weight	3993.104 kWU
Version	0x20000000
Nonce	2414725298
Block Reward	12.5 BTC

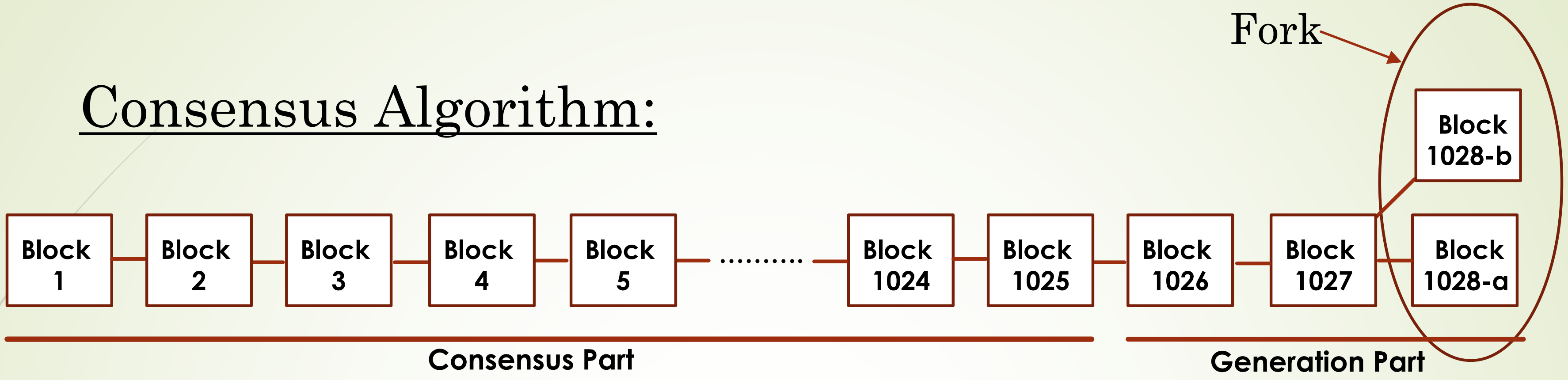
Hashes	
Hash	000000000000000000447a99a1718e9d73bed0b5c87c1122bbb4f4e0ad6148af
Previous Block	000000000000000000055849c6d5d0e75b084f8833bb05ebceef9cfae4a93de2
Next Block(s)	
Merkle Root	7927bdab5542cf85970f7eeaa6e936f9264f9b296c0b9443df74867c5801c485

Source : https://blockchain.info/

Source : https://www.genesis-mining.com/

TRUSTNET

Consensus Algorithm:

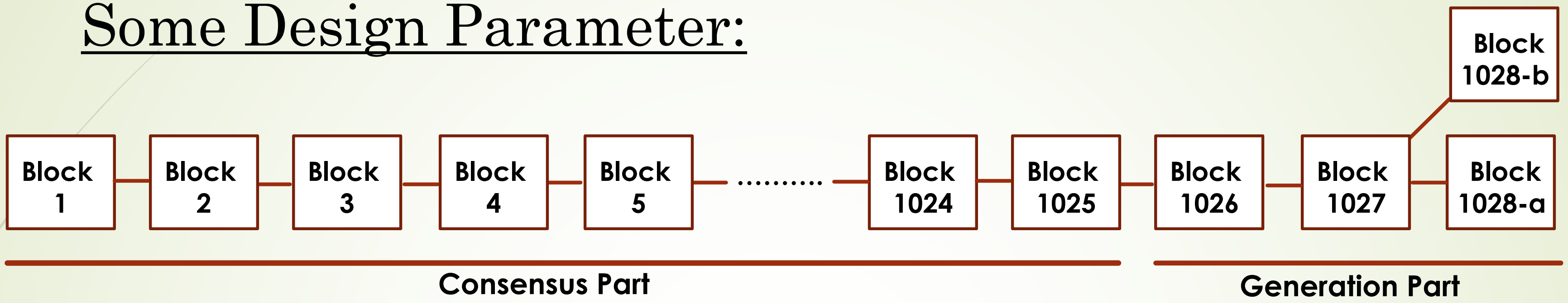


- Mining propagates the chain in time.
- Two blocks on same parents, due to network latency
- Natural forking
- Dispute eventually settles by consensus algorithm
- Local convergence occurs

“Mine on top of the chain containing highest cumulative difficulty”

Trustnet

Some Design Parameter:



Generation Depth:

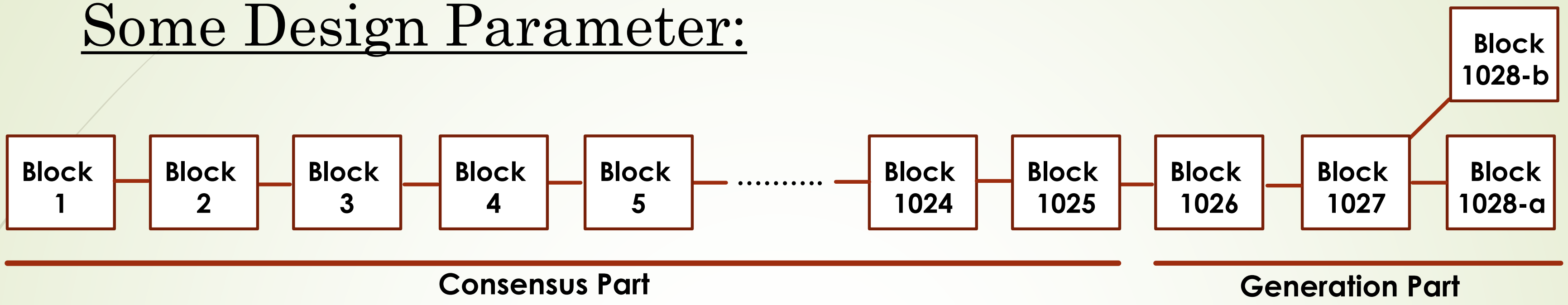
- Probability of fork decreases with depth
- Boundary depends on practical threshold
- In Bitcoin Blockchain – Generation Depth – 6 Blocks

Block Generation Period:

- Dictates amount of fork in generation part
- Statistical average maintained at – 10 minutes

TRUSTNET

Some Design Parameter:

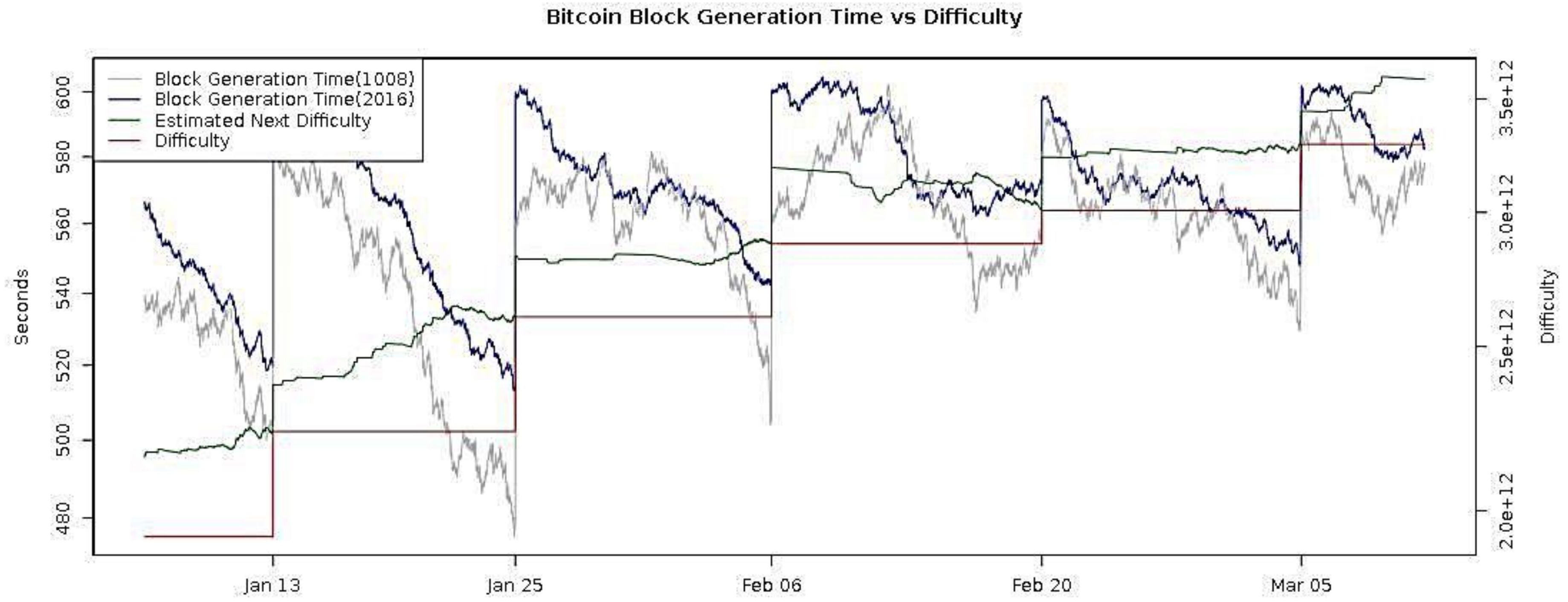


Block 1 — Block 2 — Block 3 — Block 4 — Block 5 — .... — Block 1024 — Block 1025 — Block 1026 — Block 1027 — Block 1028-a

Block 1027 — Block 1028-b

Consensus Part

Generation Part



Bitcoin Block Generation Time vs Difficulty

Source : *Bitcoin and Crypto currency technology*, Arvind et.al

Trustnet

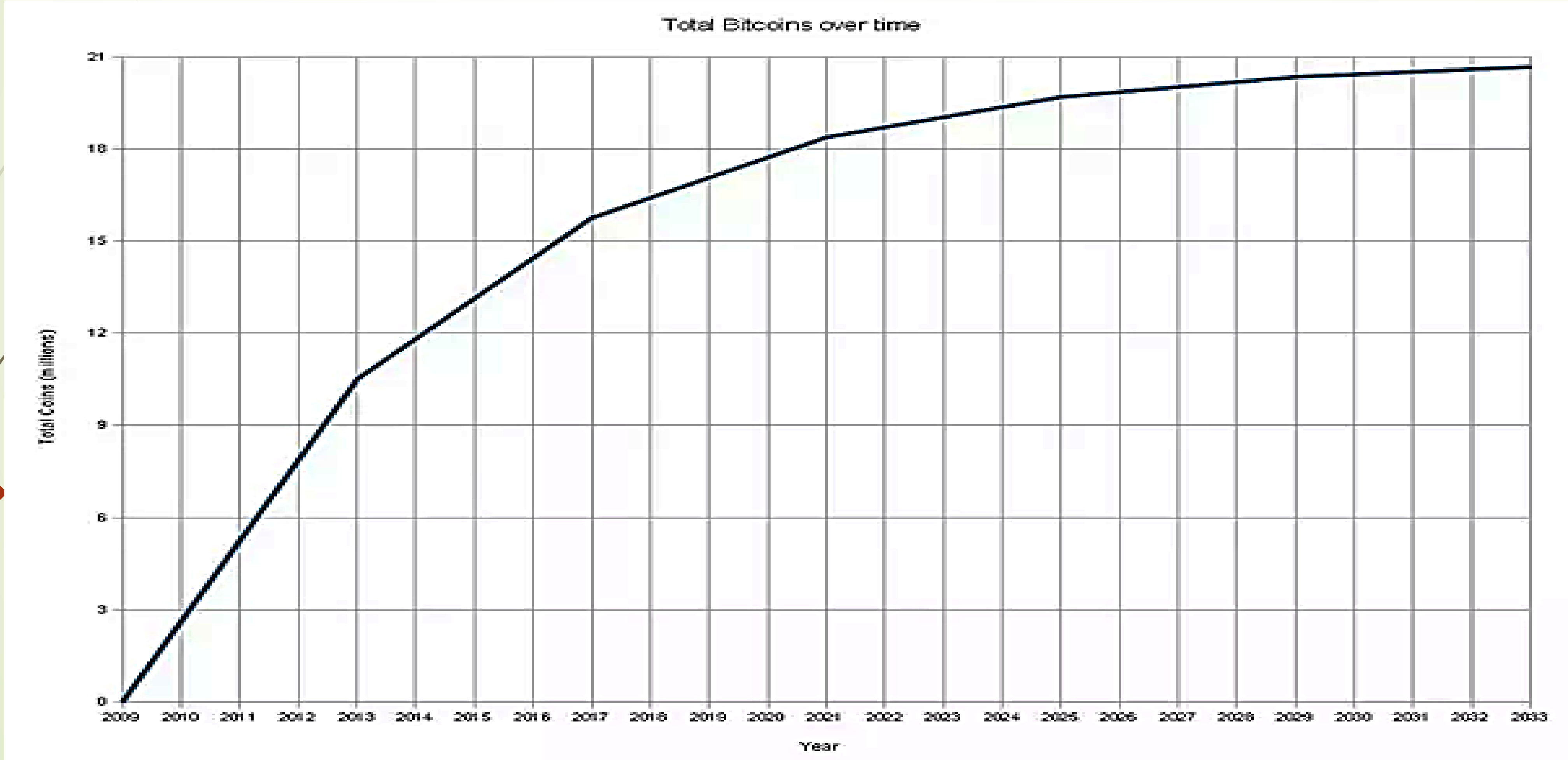
Some Design Parameter:

Coin Issuance:

- *Coinbase Transaction* - To claim block reward
- New Bitcoin introduced into circulation
- Block Reward halves after every **210,000** blocks mined (around 4 years)
- Issuance rate decreases with time
- Practically feasible **deflationary currency**
- Total circulation will asymptotically reach **21 million around year 2140**
- Bitcoin mining reward at present is **12.50 BTC**

Trustnet

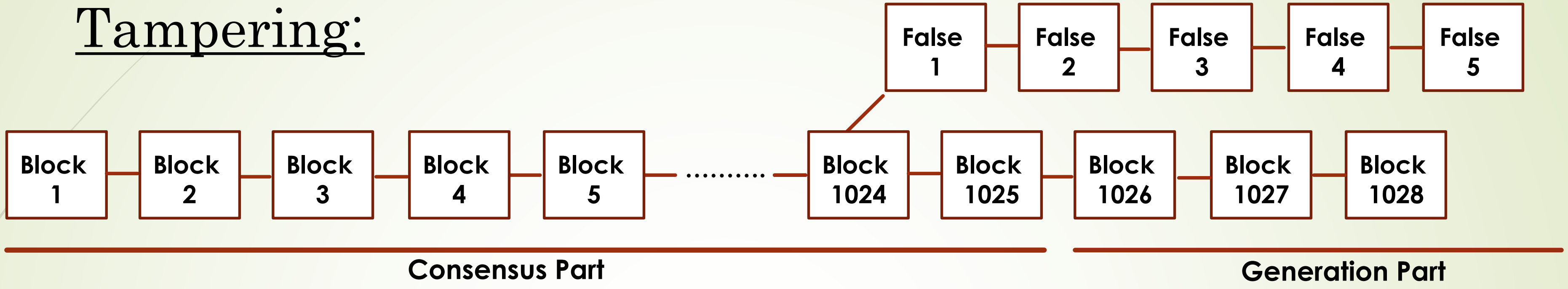
Some Design Parameter:



Source : *Bitcoin and Crypto currency technology*, Arvind et.al

TRUSTNET

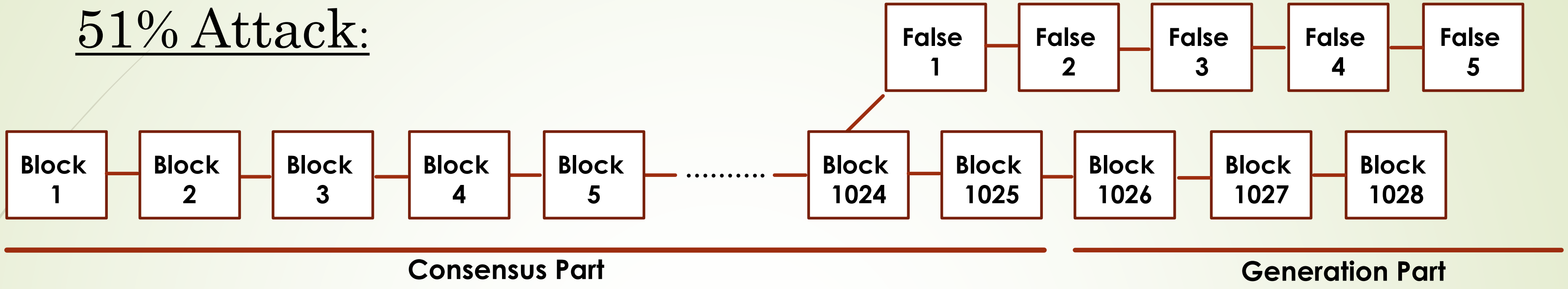
Tampering:



- Change propagates to present block
- To successfully tamper **n**th block :
  a) Recalculate all the nonce (from **n** to present)
  b) Perform faster than rest of network
- Difficulty increases linearly with depth.
- Security increases exponentially with **n**.
- Bitcoin - 6 block confirmation

Trustnet

<u>51% Attack:</u>



- 51% miner can outrun remaining 49%
- Can successfully win consensus
- This results into a Hard Fork
- Entire chain gets divided in two parts along with all network elements

Crypto Anarchy Movement

Crypto Anarchism:

- Use of mathematics to solve politics
- Crypto Anarchist manifesto – Timothy C. May, September 1992, Silicon Valley.

Cypher-Punk Movement:

- Movement of active cryptographic development
- Research Peaked in mid 90s
- A Cypherpunk's Manifesto – Eric Hughes, March 1993.

"Cypherpunks write code"

Nature as Anarchist

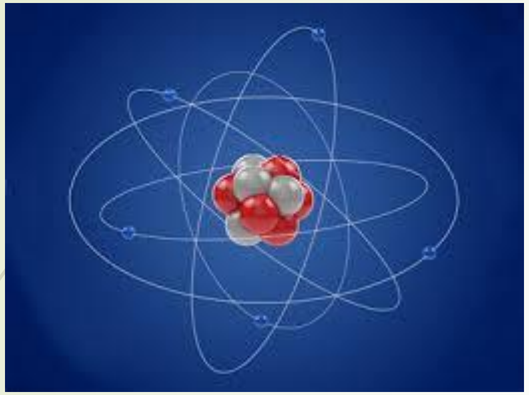
Anarchy:

- Greek Origin
- “A state of absence of governments”
- “To have Rules without Rulers”
- “Order from apparent Chaos”

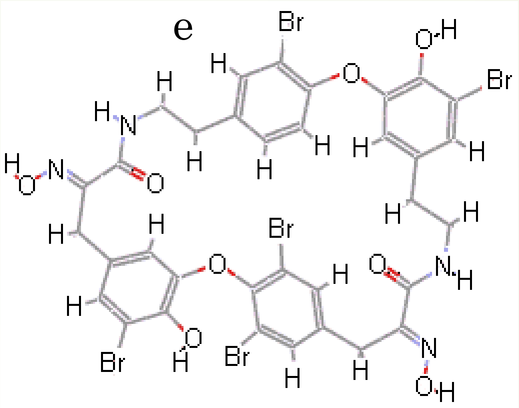
Mother nature is inherently anarchic

Nature as Anarchist

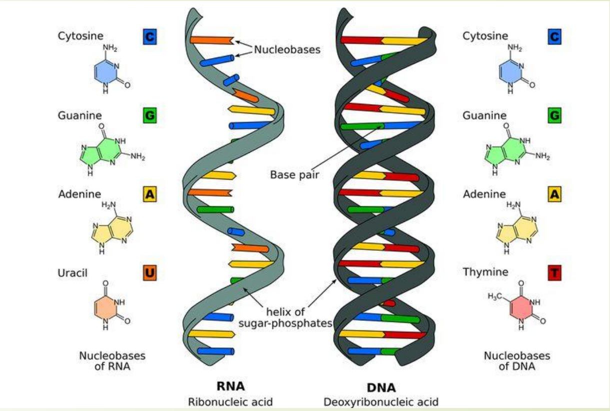
Atom



Molecule

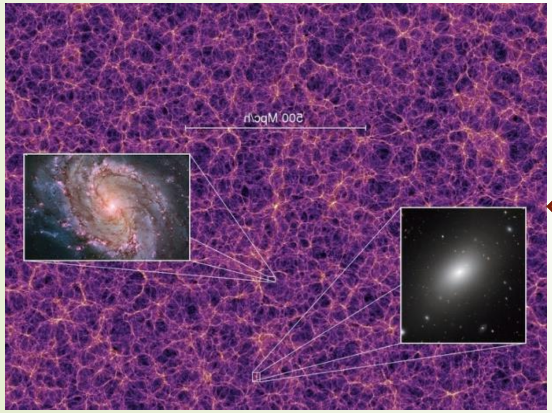


DNA



Single Cell

Multicell Higher Order



Grand Filamentary Structure

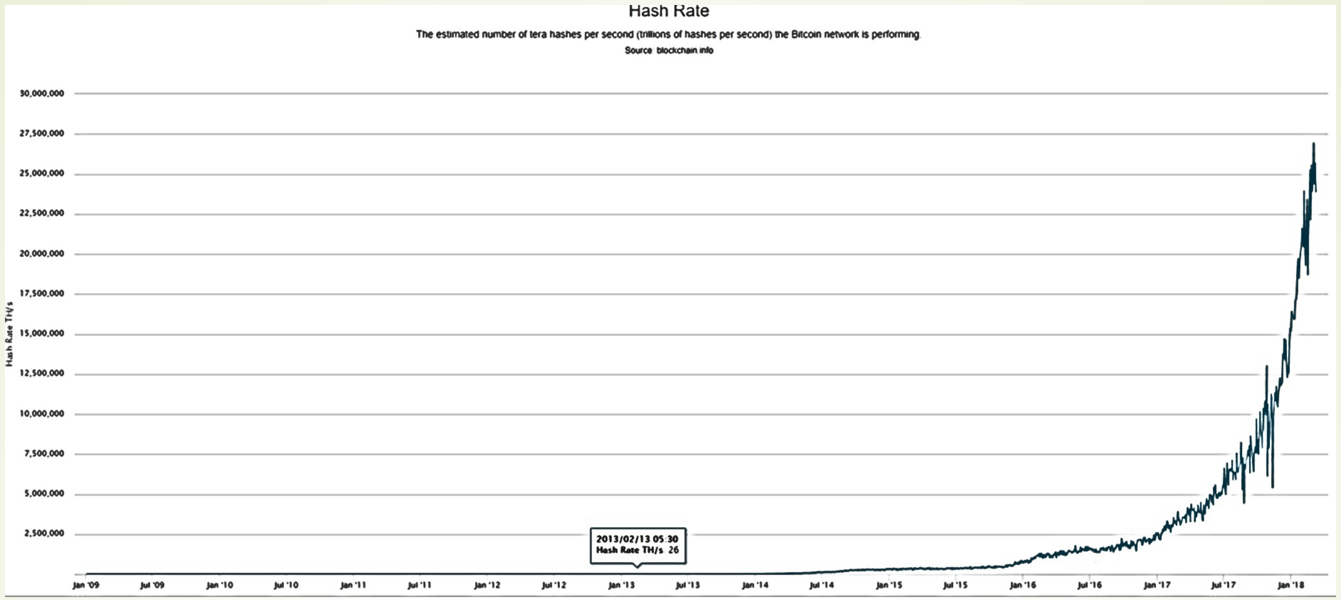
Bitcoin and Anarchy

- Network effect seeded into an algorithm
- Robust, reliable, security algorithm that simulates anarchy
- Technological, Economic, Political and Social instrument

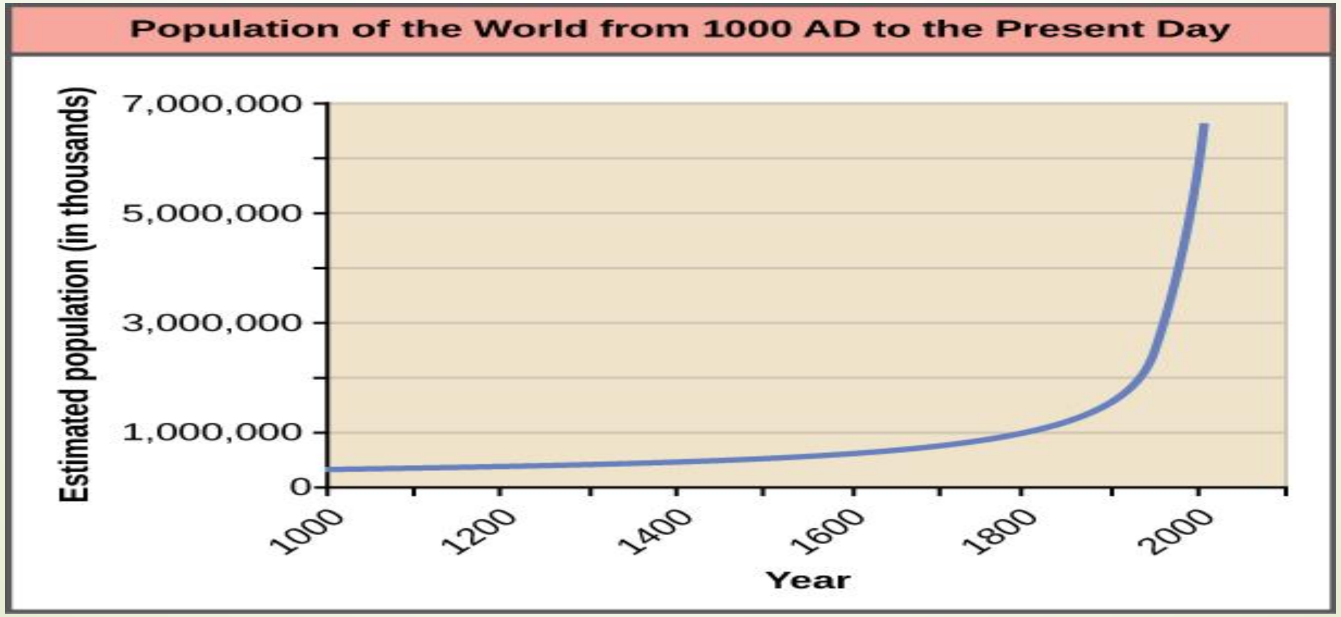
"The biggest misunderstanding people have with Bitcoin is, they think its about money."

- Andreas M. Antonopoulos (2017)

Bitcoin and Anarchy



Source : https://blockchain.info/



Source : https://courses.lumenlearning.com/biology2xmaster/chapter/human-population-growth/

Bitcoin and Anarchy

References/further study:

- *Bitcoin and Crypto Currency Technology*, Arvind et.al, Princeton University press.
- *Mastering Bitcoin*, Andreas M Antonopoulous, Github.
- *Internet of Money*, Vol I & II, Andreas M Antonopoulous, Github.

Resourceful Websites:

- http://nakamotoinstitute.org/
- https://bitcoin.org/en/
- https://en.bitcoin.it/wiki/Main_Page

“Study hard what interests you the most in the most undisciplined, irreverent and original manner possible.”

- Richard P. Feynman

THANK YOU