Cryptocurrency Challenges: Proof-of-Work (PoW) and Proof-of-Stake (PoS)

Bebo White

SLAC National Accelerator Laboratory/
Stanford University

bebo@slac.stanford.edu

Some caveats

- I am
  - a technologist and know very little about economics and finance
  - fascinated by the technological and mathematical underpinnings of cryptocurrencies and blockchain
  - primarily focussed on Bitcoin and Ethereum
  - convinced that there can be great social benefit from the technology
  - never going to try and convince anyone to purchase cryptocurrencies
  - always open to brainstorming and discussion
  - ….an owner of cryptocurrency

Bitcoin/cryptocurrency

- is not science fiction
- is not a computer science fantasy
- is not strictly the domain of criminals and hackers
- is a global empowering tool for 21st century society OR
- "Bitcoin and blockchain are a flawed solution to a problem that does not exist" (Izabella Kaminska, FT Alphaville)
- it frightens some or threatens the status quo

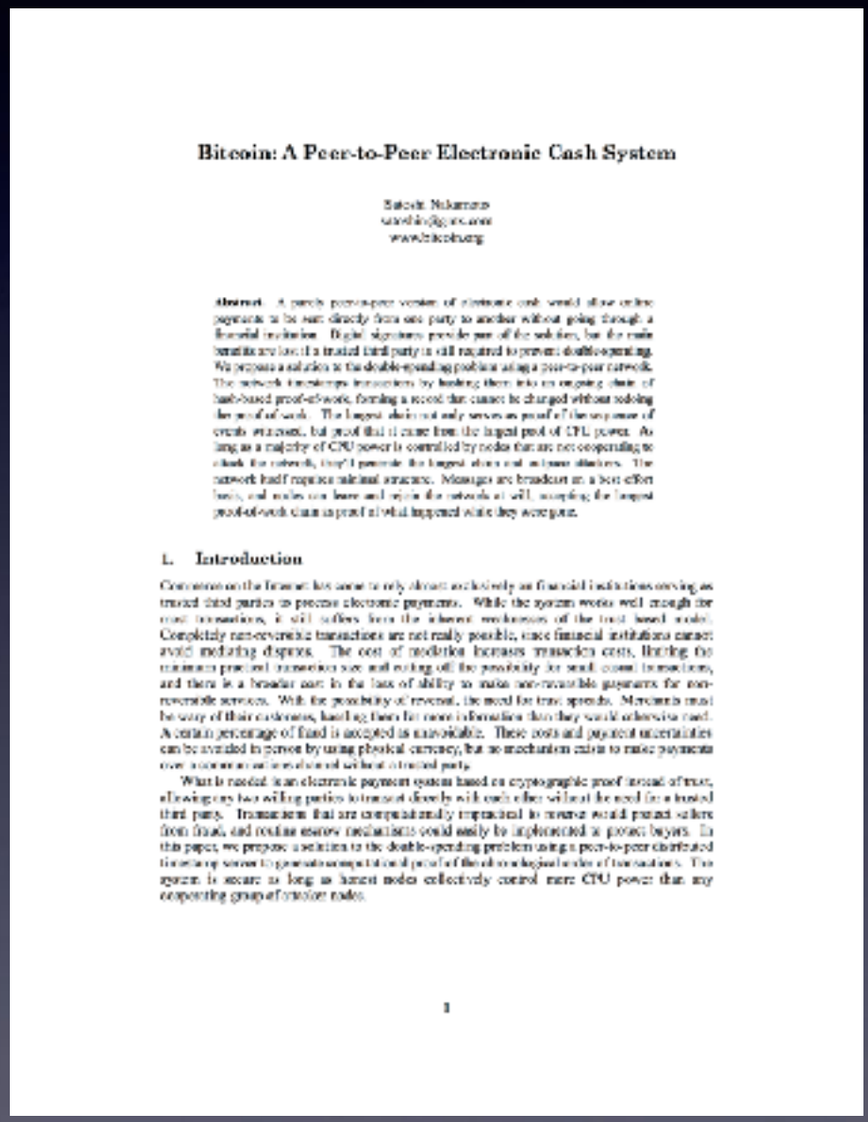
STU, April 2018

A little history (B-money, Wei Dai, 1998)

- "a person creates new B-money units in proportion to the effort spent in solving a previously unsolved computational problem"
- "it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual. The number of monetary units created is equal to the cost of the computing effort in terms of a standard basket of commodities. For example, if a problem takes 100 hours to solve on the computer that solves it most economically, and it takes 3 standard baskets to purchase 100 hours of computing time on that computer on the open market, then upon broadcast of the solution to that problem everyone credits the broadcaster's account by 3 units." (Dai, 1998)
- Bitcoin was apparently designed independently of the B-money scheme

In 2008 there came a white paper that

- defined a protocol for generating, validating, and exchanging cybercurrency
- was implemented in publicly available, open source software
- described a technology platform that goes far beyond its original purpose (the blockchain)
- was released on the Cypherpunks mailing list - not in traditional research channels
- was consistent with *The Crypto Anarchist Manifesto*



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 the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. 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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. 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. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

STU, April 2018

Satoshi outlined a way

- "The network is robust in its unstructured simplicity. Nodes work all at once with little coordination"
- a distributed, peer-to-peer network of payments ledgers (non-centralized)
    - impossible (?) to forge/modify - based on rigorous technology and techniques
    - doesn't allow double-spending and provides proof-of-payment (non-repudiation)
    - supported by "the power of the crowd"
- not based on dollars, euros, pounds, etc., but a currency "for the digital age" - bank-free, government-free, empowering

Disintermediation

- third parties are no longer needed to
  - establish identity or prove creditworthiness
  - distribute media
  - mediate communication between parties
  - mediate transfers of value

"Bitcoin is at the same stage as the Internet in 1992-1993. At that time it took UNIX command-line skills to send e-mail; no way near for mainstream adoption"
-Andreas Antonopoulos

What is Bitcoin really?

- no physical object, not even a character string
- “a chain of digitally signed transaction records leading from the original owner to the current holder” - similar to a chain of land deeds
- it’s permanent - can’t be lost, but can be inaccessible
- the transaction records contain
  - hashes that are difficult to find AND
  - virtual/anonymous owner IDs (addresses)
- there is NO bitcoin registry, NO centralization
- Bitcoin blockchains are broadcast globally; anyone can verify them; they encompass all the past and the present transactions

How Bitcoin works (addresses)

- Bitcoin software generates bitcoin addresses of 25-44 characters for users - a public and private key pair
- sample address: 1BBsbEq8Q29JpQr4jygjPof7F7uphqyUCQ
- the address is actually an elliptic curve public key; a 44 character key is as secure as a 7000-bit RSA key
- to send/spend bitcoins, user specifies a receiving address and amount
- to receive bitcoins, provide the sender your public address
- addresses are not registered to users; a user can have a different address for every transaction

You really don’t have to remember that long address…

- just your public key, not your private key
- can be stored in your cryptocurrency wallet on your phone or computer
- used when you receive BTC e.g., get paid, at a BTC ATM
- need to know the recipients when you make payment

5 other key cryptocurrency issues

- micropayments - difficult with fiat currency
- inflation - safeguards in the algorithm
- mining - which you will likely not do (but makes news)
- volatility - speculation? investment? certainly makes news
- forks/clones - other cryptocurrencies - why? FinTech

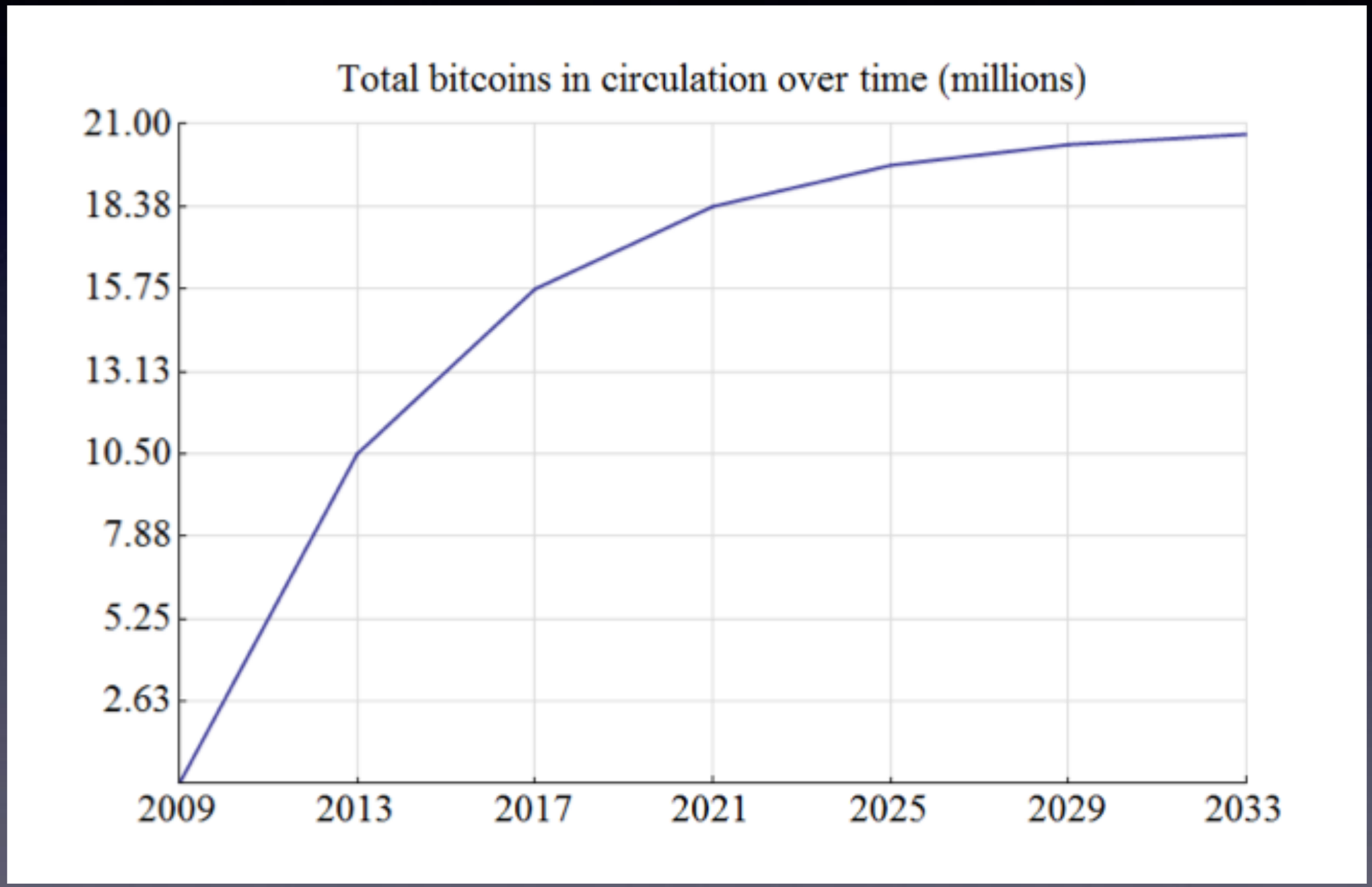
Micropayments

- basically (?) free - largely impossible now
- strong implications for IP, royalties, etc,
- 1 satoshi (sat) = .000000001 BTC (one hundred millionth)
- to put in perspective, for 1 sat = 1¢, 1 BTC = $1,000,000

Supply of bitcoins (no inflation)

- maximum number of bitcoins (ever) = $21*10^6$
- maximum number of satoshis = $2.1*10^{15}$
- amount of $US in the world = 10^{12}
- as value of BTC increases, most transactions are likely to be in satoshis

Controlled bitcoin inflation



What is Bitcoin mining?

- the process by which transactions are verified, added to the blockchain, and also the means by which new bitcoin are released
- the process involves collecting recent transactions into blocks and trying to solve a computationally difficult puzzle
- solution is verified by mining community and the solver adds a block to the blockchain and collects a reward (in fresh new BTC)

(Ref: Investopedia)

Why is mining so difficult?

- because of bitcoin's "public" structure, it needs a defense against malicious attacks
- uses PoW to make it computationally difficult to add a block
- has created a cost (equipment + operation) of mining and therefore a need for incentivization

A short review of Bitcoin architecture

STU, April 2018

Bitcoin nodes (1/4)

- *Full nodes* (Bitcoin core/reference node/full client)
  - stores the entire history of transactions
  - manages wallets
  - initiates transactions directly
  - receives blocks from the network, validates them, and then links to blockchain (i.e., updates its copy continuously and extends)
  - tracks the movement of funds incrementally, transaction by transaction, determining unspent value

Bitcoin nodes (2/4)

- *Lightweight nodes*
  - verify transactions using a simplified payment verification procedure
  - rely on full nodes to access a full copy of transactions
  - dependent on third parties for full transaction validation
  - follow the consensus of the majority of mining power
  - possibly vulnerable to attack

Bitcoin nodes (3/4)

- *Mining nodes*
  - compete to create new blocks by solving the *proof-of-work* algorithm
    - collect pending transactions into a new block and compete to confirm/validate
  - earn/create new btc when they confirm a new block before other mining nodes
  - reception of a new block from the network signals the end of one round and the beginning of a new round

Mining pools

- a pooling of resources by miners who share their processing power over a network
- they split the reward equally according to the amount of work contributed
- a “share” is awarded to members of the pool who present a valid partial PoW
- makes mining more accessible to larger audiences

Bitcoin nodes (4/4)

- *Web clients*
  - less capability than lightweight clients
  - rely completely on the third-party servers, including storing users' wallet
  - potentially vulnerable

Common functions of all nodes

- a *routing* function to discover peers and route traffic to them
- a *verification* function to
  - verify new transactions and propagate unconfirmed transactions throughout the Bitcoin network
  - verify new blocks and assemble those that meet the criteria to the blockchain
- a *selection* function among contending chains to choose the one with the most cumulative difficulty as demonstrated through the POW (longest chain) - consensus
- a *wallet* function to create private keys and addresses

Full node services

- *transmitting* new transactions, after verification, from users to miners
- *broadcasting* new blocks from miners, after verification, to the rest of the network
- *filtering* transactions and blocks on behalf of lightweight nodes
- *answering* requests for assistance from new full nodes to construct their own copies of the complete blockchain
- *supplying* missing blocks to any node that goes offline for any period of time

Block structure of Bitcoin

Field	Description	Size in octets/bytes
Block size	Number of the following octets until the end of the block	4
Block header	5 fields	80
Transaction counter	Number of transactions in the block	1-9
Transactions	The list of transactions in sequential order	Variable

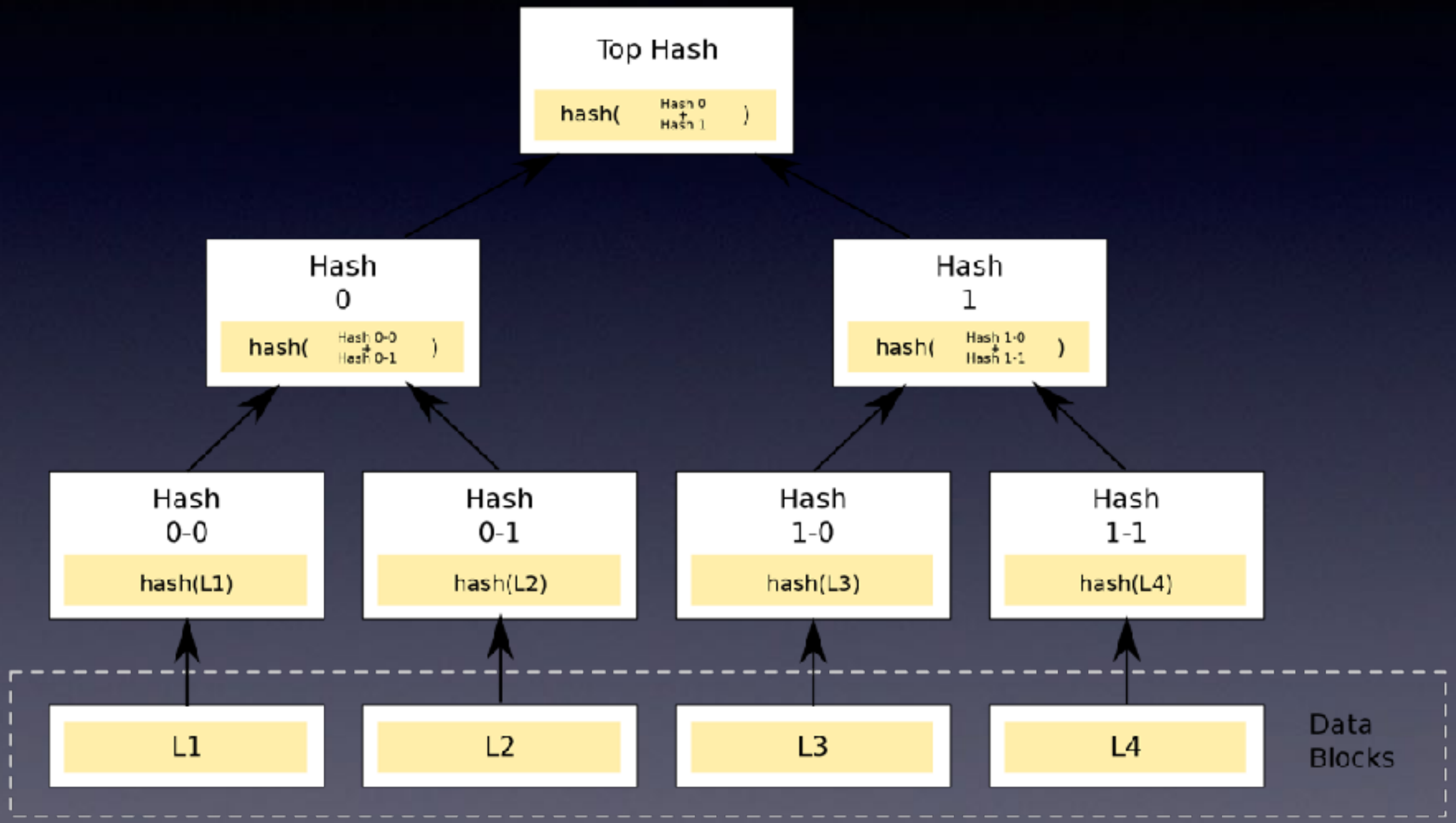
Structure of the Bitcoin block header

Description of the block	Size in octets/bytes
Software version	4
Hash of the preceding block	32
Merkle root of the transactions in the block	32
Time stamp	4
Difficulty target T	4

What's the Merkle root?

- a summary of all transactions in a block
- serves as a "signature" for the block
- is calculated as follows:
  - arrange transactions as a binary tree
  - recursively at each level concatenate the transaction hashes in pairs until there is only one hash

Merkle Trees



Difficulty

- the mining difficulty changes every 2016 blocks, which are found approximately every two weeks
- it is adjusted based upon how efficient miners were over the period of the previous 2016 blocks
- maintains an average rate of block production of 6 blocks per hour
- next_difficulty = (previous_difficulty*2016*10 minutes)/(time to mine last 2016 blocks)

What is Consensus Algorithm?

- also known as
  - consensus protocol
  - consensus mechanism
- algorithm to reach agreement among the network (blockchain) nodes
- all nodes should be able to agree about changes in the distributed ledger (blockchain) and current state
- examples include Proof-of-Work (PoW) , Proof-of-Stake (PoS) and others

Consensus Algorithm Requirements

- fault-tolerance
  - some nodes will be unavailable when the ledger (blockchain) is modified
  - consensus should be reached by part of the nodes (e.g., majority)
- attack-resistance
  - some nodes will intentionally misbehave
  - honest nodes should win in the consensus process
  - everyone on the network can verify a new block's correctness
  - untenable resources should be required for a successful attack

A Proof-of-Work (PoW) - what's behind mining?

- a piece of data that
- is difficult to produce
- is easy for others to verify

Proof-of-work algorithm (1/2)

"ask the sender of a message to execute a computation with a parameterizable difficulty before transmitting the message while the intended recipient(s) could verify the computation easily" (Dwork, Naor, Back)

problem: find a nonce such that given a nonce length of 32 bits

SHA-256[SHA-256(previous block header)||nonce|| transaction 1||…||transaction n] < difficulty target T

Proof-of-work algorithm (2/2)

- this POW approach solves two problems
  - it provides an algorithm for an emerging consensus by allowing full nodes in the network to agree collectively on the status of the blockchain
  - it solves the problem of deciding how to develop this consensus while simultaneously preventing attacks
- done by avoiding explicit elections and registrations and with an economic barrier (the weight of the contribution from any node to the consensus process is directly proportional to the computing power that the node brings to the network) - ***is this a problem?***

Environmental/energy impact is definitely a current "show-stopper" IMHO

STU, April 2018

Asia & Pacific

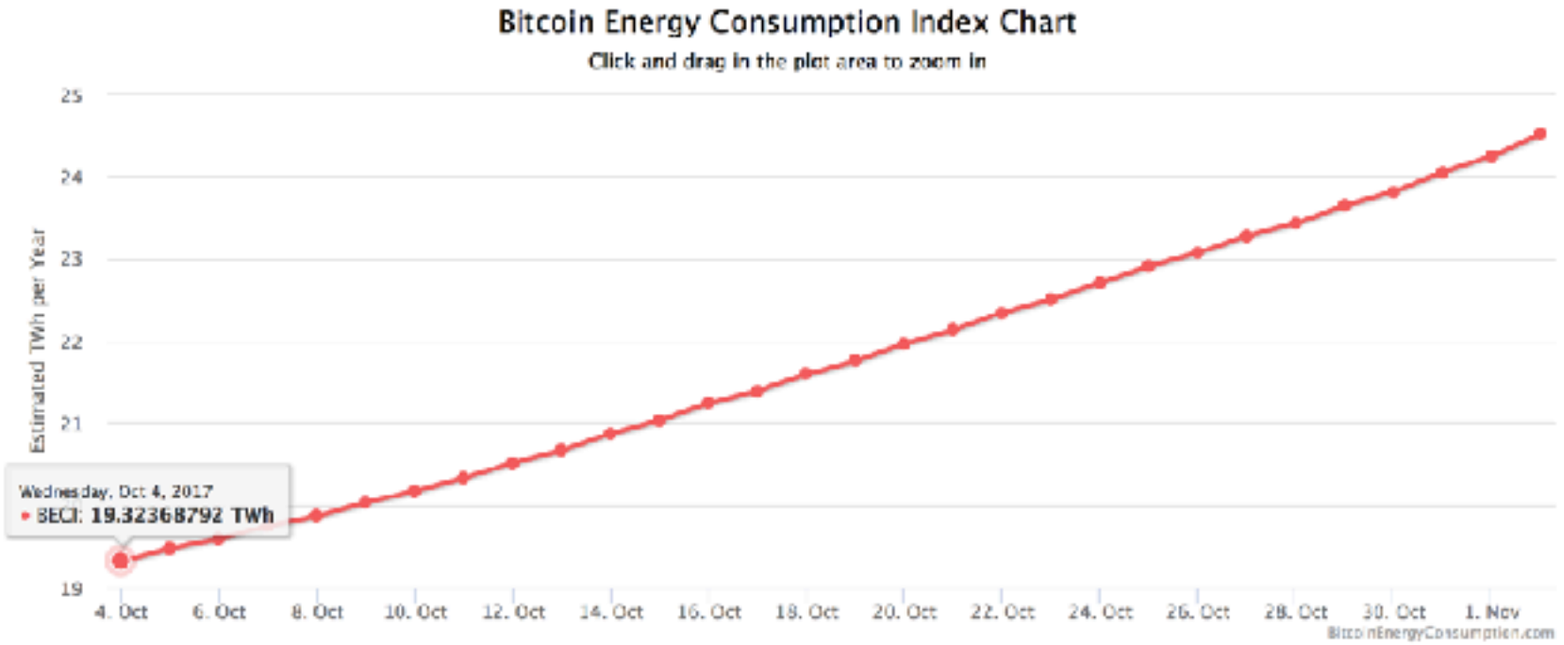
The bizarre world of bitcoin 'mining' finds a new home in Tibet

By Simon Denyer September 12

Set in remote mountains on the edge of the Tibetan Plateau, the bitcoin "mine" is strategically placed next to a hydroelectric power plant. (Paul Hanly/For The Washington Post)

STU, April 2018

Bitcoin Energy Consumption Index



Key Network Statistics

Description	Value
Bitcoin's current estimated annual electricity consumption* (TWh)	24.52
Annualized global mining revenues	55,841,159.218
Annualized estimated global mining costs	$1,225,751,400
Country closest to Bitcoin in terms of electricity consumption	Nigeria
Estimated electricity used over the previous day (KWh)	67,164,460
Implied Watts per GH/s	0.224
Total Network Hashrate in PH/s (1,000,000 GH/s)	12,476
Electricity consumed per transaction (KWh)	222.00
Number of U.S. households that could be powered by Bitcoin	2,269,910
Number of U.S. households powered for 1 day by the electricity consumed for a single transaction	7.51
Bitcoin's electricity consumption as a percentage of the world's electricity consumption	0.12%

https://digiconomist.net/bitcoin-energy-consumption

STU, April 2018

Yes, there are definite issues that should not be ignored, but

- Assumes current technology and computational (mining/consensus) models
- Supporting technologies e.g., energy, must (and will) also evolve

SEP 22, 2016 @ 12:32 PM 19,963

We Could Power The Entire World By Harnessing Solar Energy From 1% Of The Sahara

Crescent Dunes Solar Energy Project

From Wikipedia, the free encyclopedia

The **Crescent Dunes Solar Energy Project** is a 110 megawatt (MW) net[3] solar thermal power project with 1.1 gigawatt-hours of energy storage,[1] located near Tonopah, about 190 miles (310 km) northwest of Las Vegas.[4][5] It is the first utility-scale concentrating solar power (CSP) plant with a central receiver tower and advanced molten salt energy storage technology from SolarReserve. The project, developed by SolarReserve and owned by Tonopah Solar Energy, LLC, was anticipated to cost less than $1 billion.[6] EPC Contractor was ACS Cobra, which carried out the engineering design, procured the equipment and materials necessary, and then constructed and delivered the facility to Tonopah Solar Energy. Planned energy output was 500 MW·h.[7]

PoW Problems

- requires non-trivial computational resources
- is energy intensive
- has potential environmental impact
- 51% attack - attackers holding more than 50% of the power could potentially reverse-back transactions (double-spend) or deny service
- hashing algorithm types for PoW consensus
- transaction speed - mean wait time
- transaction throughput - transactions per second (tps)

There are definite issues with cryptocurrencies (1/2)

- mining often requires huge use of computational resources and therefore has an appreciable environmental impact
- miners are ‘a new center of power’ - if five (estimated) mining pools control the creation of blocks, how is that de-centralized?

There are definite issues with cryptocurrencies (2/2)

- transaction times compared to Visa, etc. - related to PoW and consensus times
- a major target of government, bank, and financial institution examination - result can be regulation
- is it possible to make mining and consensus less compute-intensive?

The current cycle of bitcoin mining

A thought experiment (1/2)

- suppose bitcoin or another cryptocurrency becomes a dominant form of payment
- miners would start with some initial holding of cryptocurrency, use it to purchase mining equipment and electricity, consume these resources, and in the process, acquire new cryptocurrency in the form of mining rewards
- this process continually uses more and more energy and raw materials

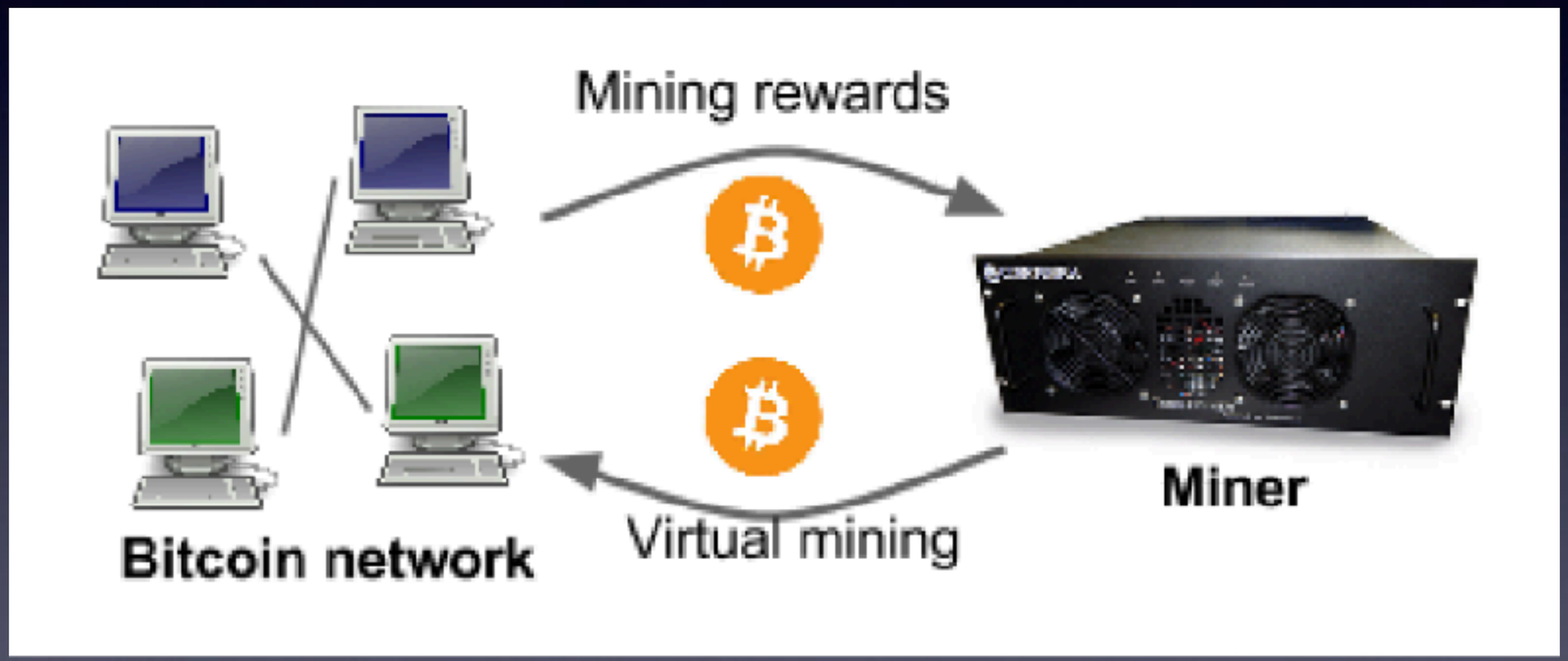
A thought experiment (2/2)

- once mining hardware becomes a commodity and electricity is a commodity (it generally already is), no miner would have a significant advantage over any other miner in terms of how efficiently they convert their initial cryptocurrency holdings into mining rewards
- barring minor variations in efficiency, whoever invests the most into mining will receive the most rewards

Question

- what would happen if the step of spending money on power and equipment was removed?
  - this step is primarily used to prove who has invested the most into mining
- why not simply allocate mining “power” directly to all currency holders in proportion to how much currency they actually own?

The “virtual mining” cycle



- remember that the original idea behind the mining process was to enable a consensus (voting) method for maintaining the integrity of the ledger (blockchain)

- miners with more computing resources have more votes…threatens decentralization

- instead, suppose votes were based on how much currency the miner has?

  - stakeholders

  - those who have "a vested interest" in the success of the currency - not just speculators

Advantages of "virtual mining"

- reduces environmental impact
- may reduce the trend towards centralization; since no mining hardware is included, all miners are able to mine just as "efficiently" as all others
- miners have an incentive to operate to benefit the entire system since it benefits them
- this is "Proof-of-Stake (PoS)"

Proof-of-Stake (PoS)

- designed to reduce resource wasting
- designed to increase network security
- the creator of the next block in the ledger (blockchain) is chosen by
  - combinations of random selection and cryptocurrency holding
  - difficulty of consensus algorithm is based upon amount and age of cryptocurrency holdings
- theoretically, a “monopolist” (holder of the most cryptocurrency)
  - could double-spend or deny/filter another transaction
  - executing “a monopoly attack” is much more expensive than in PoW
- great area of research IMHO

Implementing “virtual mining” : Peercoin

- uses a hybrid PoW/PoS algorithm in which a miner’s stake is defined by “coin-age”
- starts with PoW to mine initial amounts of cryptocurrency then switches to PoS relying on the amount of stake
- began an important discussion about solutions for PoW problems and sustainability
- requires additional research

Summary and conclusions

- Cybercurrency
  - is a creative and innovative application of established, robust technologies
  - has begun to evolve and spawn/fork exciting new variations
  - more widespread adoption is potentially hampered by serious issues both technological and non-technological
  - will continue to raise non-trivial issues surrounding adoption and regulation
  - defines a rich area for innovative research
  - requires a new wave of SMEs and developers

I encourage you to get onboard - your ideas are needed!

STU, April 2018

The Distinguished Speakers Program is made possible by

Association for Computing Machinery

Advancing Computing as a Science & Profession

For additional information, please visit http://dsp.acm.org/

About ACM

ACM, the Association for Computing Machinery is the world's largest educational and scientific computing society, uniting educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges.

ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence.

ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

With over 100,000 members from over 100 countries, ACM works to advance computing as a science and a profession. www.acm.org

Thank You!
Questions? Comments?

bebo@slac.stanford.edu

STU, April 2018