FAMU-FSU
College of Engineering

Digital Cash, Bitcoin, and the Distributed Consensus Revolution

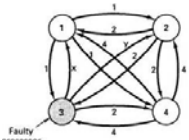
ECE Graduate Seminar
Tuesday, January 14th, 2014

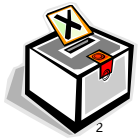
Dr. Michael Frank
Associate in Engineering
FAMU-FSU College of Engineering

v1.2

Abstract of Talk (Summarized)

- A classic CS problem for digital cash:
  - The "Double-Spending Problem"
- Essentially solved in 2009 by *Bitcoin*
  - A distributed, P2P digital currency protocol
  - Has grown rapidly, worth >$10B today
- But, the solution has other applications!
  - Bitcoin's distributed consensus mechanism addresses an even more general CS problem of "Byzantine Agreement" among distributed parties
    - Many applications: Name registration, electronic voting, digital fundraising/stakeholding, distributed autonomous corporations, digital law, *etc.*
      - A new organizing principle for civilization?





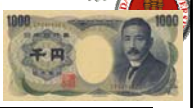
Talk Outline

- Distributed Digital Cash systems
  - Motivation
  - Some early history
  - Emergence of Bitcoin
- How Bitcoin works
  - Cryptographic tools used
  - Peer-to-peer protocol
- The Byzantine Agreement problem
  - Distributed Consensus as a general solution
  - Survey of (far-ranging!) applications

Some Motivations for Digital Cash

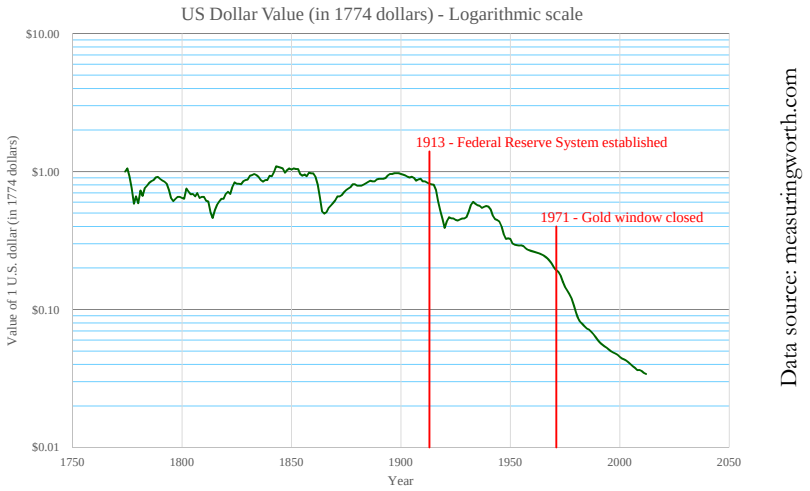
- Cash money (vs. *e.g.* checks/debit+credit cards/EFT) offers the following features:
  - Anonymously transferrable, hard to trace
  - Can be accepted with confidence, w. limited need to trust/consult a centralized authority
  - Transactions are irreversible
- Certain kinds of cash money (*e.g.*, gold coins) have the additional advantage that their supply is fairly well limited
  - Reliable as a long-term store of value
- Some ways digital cash > physical cash:
  - Instant long-distance transactions, encrypted storage, backup copies, (in some systems) nonrepudiability.

Fiat Currencies



- Almost all sovereign (gov't-issued) money today is what's known as *fiat* currency.
  - Not backed by gold or any other limited resource.
    - True in U.S. since "Nixon shock" in 1971.
  - Can be issued at will by government/central bank.
- The problem with this is that the money supply can increase without limit over time…
  - Long-term supply inflation → declining value
  - Fiat is not a good long-term store of value!

Example: History of U.S. Dollar Value, Based on Consumer Price Index



History of Digital Cash Research

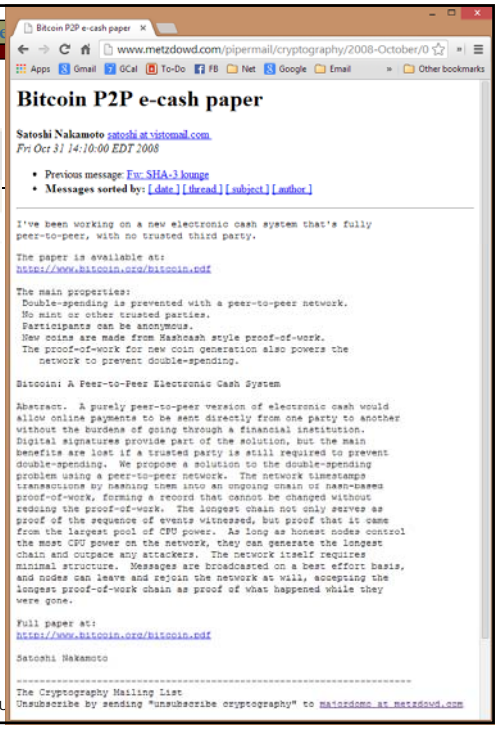
- Some notable prior efforts:
  - David Chaum's Ecash (seminal papers in 1982 & 1988)
    - Patented approach based on his "blind signatures" invention
    - Founded DigiCash co., Netherlands in 1990 to commercialize idea
      - Company went bankrupt in 1998! -- Lots of management problems
    - Depended on a trusted central clearinghouse for transactions
  - Adam Back's Hashcash (proposed in 1997)
    - Computationally expensive "stamps" to prevent email spamming
  - Wei Dai's B-money (proposed in 1998)
    - Incorporated Hashcash together with a distributed ledger
  - Hal Finney's Reusable Proofs-of-Work (RPOW)
    - Under development in period 2004-2009.
  - Nick Szabo's Bitgold (1998-2005)
    - Introduced chains of proofs-of-work (similar to Bitcoin)
    - Still vulnerable to Sybil attacks (a.k.a. sockpuppets)

Why Distributed Digital Cash ~~is~~ *used to be* difficult to achieve

- The classic "double-spending problem:"
  - What prevents me from sending (copies of) my digital cash to different parties, and thereby effectively spending it twice (or more times)?
    - If recipients have to check back with a central authority to determine whether the cash was spent yet, that tends to ruin the anonymity property of the cash.
      - Also, the central authority then becomes a single "point of failure" that needs to be trusted to do the right thing.
        - Chaum's Ecash scheme dealt with some of these problems, but not all.

Introduction of Bitcoin

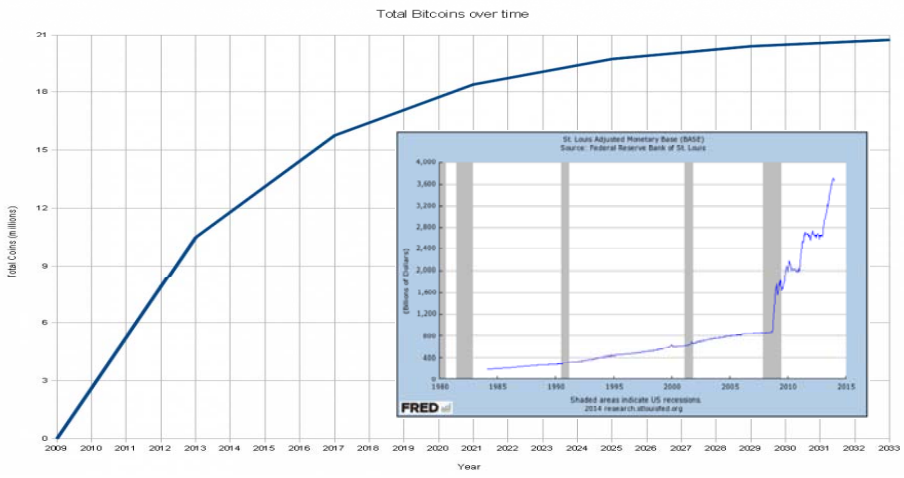
- Aug. 18, 2008:
  - **bitcoin.org** domain registered
- Oct. 31, 2008:
  - "Satoshi Nakamoto" <satoshi@vistomail.com> announces Bitcoin to the **cryptography@metzdowd.com** mailing list.
    - A lively discussion ensues!
- Jan. 3, 2009:
  - Satoshi releases first (0.1) public version of Bitcoin client source



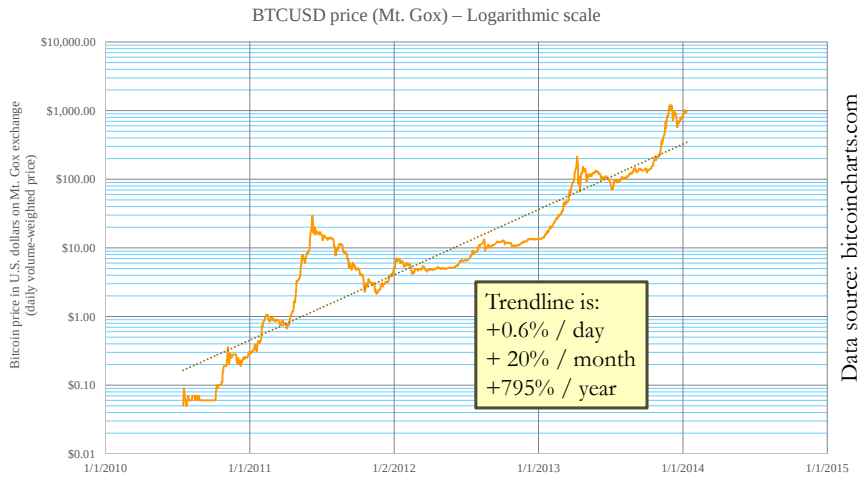
Some Properties of Bitcoin

- Anonymous (or at least, pseudonymous)
  - Yet, transactions are non-repudiable (unlike with cash)
- No centralized authority (instead: distributed network)
- Anyone can create new Bitcoins (by 'mining')
  - In this process, miners also perform the service of timestamping valid transactions
- But, total supply of Bitcoins is finite! (~21M)
  - New Bitcoins are produced at a rate that asymptotically approaches zero over many years
- Transactions are (almost always) irreversible
  - They get exponentially more difficult to reverse with age
- Double-spending is (very nearly) impossible

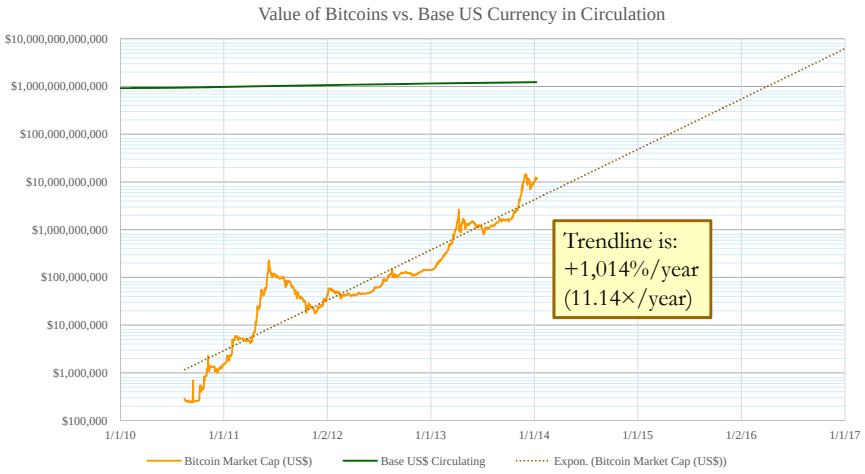
Bitcoin Supply Over Time (Inset: U.S. dollar supply over time)



Bitcoin Price Growth



Bitcoin Market Capitalization vs. Base U.S. currency in circulation



U.S. data source: Federal Reserve Bank of St. Louis
Bitcoin data source: blockchain.info

Market Cap Equation

- What does Bitcoin's price or market capitalization really mean, in terms of what is happening with the currency at the level of individual users?
- Some definitions:
  - P = Price of 1 bitcoin in (U.S. dollars, say).
  - Q = Quantity of bitcoins in circulation.
  - C = Market capitalization of Bitcoin (defined as $C = PQ$).
  - N = Number of users of Bitcoin
  - V = Average value (in dollars, say) that a user wishes to / feels confident keeping in Bitcoin form.
- Then, at market equilibrium, we can derive the following simple, fundamental equations concerning the market capitalization C and bitcoin price P:

$$V = \frac{C}{N} \therefore C = NV, P = \frac{NV}{Q}$$

  - Otherwise, average users will buy/sell bitcoins until equilibrium is reached.
- Q increases only gradually... Thus, exponentially increasing bitcoin price P or market capitalization C suggests corresponding exponential increase in the user base N, or user confidence (expressed as V), or some of both.

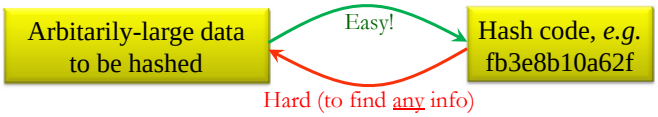
Some Merchants Accepting Bitcoin (Plus 10,000s of Others)

Some of the Key Ingredients of Bitcoin's Core Technology

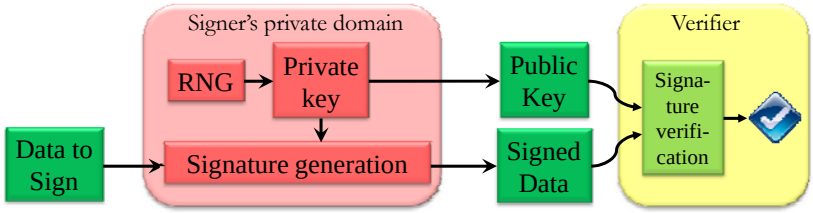
- Basic cryptographic primitives:
  - One-way cryptographic hash functions:
    - Specifically: SHA-256, RIPEMD-160
  - Public-key (asymmetric) digital signature systems:
    - Namely: Elliptic Curve Digital Signature Algorithm (ECDSA)
      - more specifically, using the secp256k1 curve
- Various higher-level functions built on those elements:
  - *E.g.*, Merkle hash trees, Hashcash proof-of-work, distributed timestamp service
- Other important aspects of Bitcoin:
  - Peer-to-Peer (P2P) networking – no central server!
    - *A lá* Bittorrent, gnutella, *etc.*
  - Open Source development process
    - https://github.com/bitcoin/bitcoin

Cryptographic Hashes & Public-Key Digital Signature Systems

- One-way cryptographic hash functions:



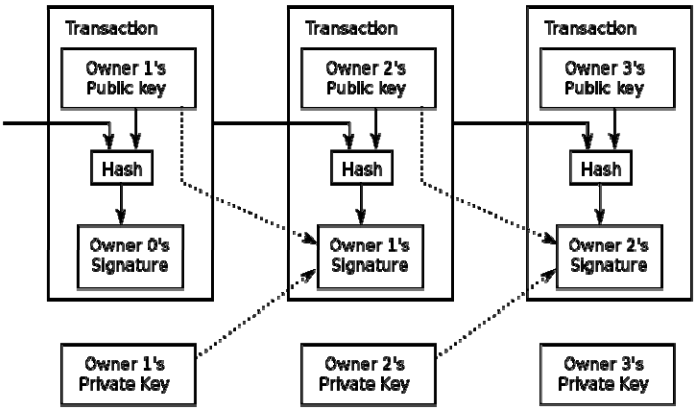
- Public-key digital signature systems:



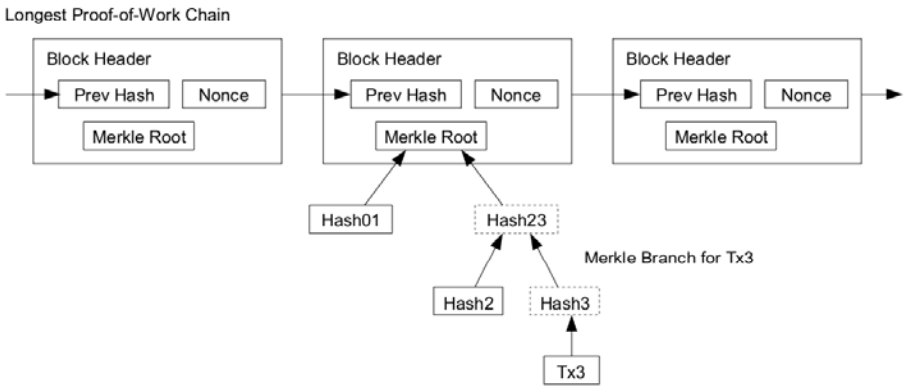
How Bitcoin Works (Basic Outline)

- Anonymous accounts are associated with ECSDA public keys, identified by public *addresses* (hashed from public key)
  - Each account has a current balance (denominated in bitcoins).
- In a typical Bitcoin *transaction*, the owner of some account(s) signs a transaction order,
  - Thereby deeding coins (received in previous transactions) from his accounts to a set of destination addresses.
- *Full nodes* (running the core Bitcoin client) keep track of the distributed account ledger called the *blockchain.*
  - Each block contains a set of newly confirmed transactions, a timestamp, and a *proof of work* (based on Hashcash).
    - The POW prevents new blocks from being created too quickly.
- *Miners* (running an extended client) create new blocks, and receive a predetermined reward (plus optional transaction fees).
  - Newly created blocks build on (link back to) previous ones.

Bitcoin Transaction – Basic Structure



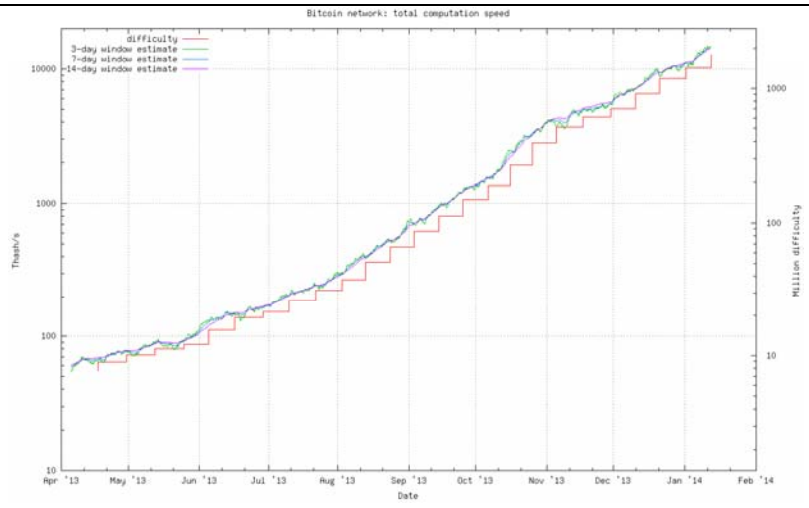
Bitcoin Blockchain – Basic Structure



Hashcash Proof-of-Work Function (as used in Bitcoin)

- Take the block header (including nonce), and hash it with: ***hash*=SHA256(SHA256(*header*))**
  - Compare resulting 256-bit number with the current *target*.
    - *target* = *maxtarget* / *difficulty* [*maxtarget* = $(2^{16}-1)2^{208}$]
    - If *hash* < *target*, you win the lottery! Else, try another nonce…
  - Bitcoin's difficulty is automatically adjusted every 2 wks.
    - Keeps average rate of mining fairly steady & on-schedule
    - Current Bitcoin target (as of 1/12/2014):
      - 0x00000000000000026666000000000000000000000000000000000000000000
    - Chances of winning the Bitcoin lottery (per attempt) are currently only 1 in ~7.7 quintillion!
      - Yet – the Bitcoin mining network is collectively so powerful that the lottery still gets won about once every 10 minutes on average!

Bitcoin Network – Aggregate Speed And POW Difficulty – Last 10 mo.

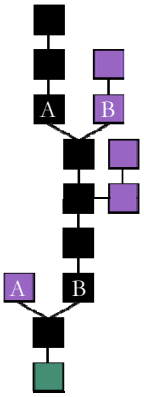


Bitcoin's Core Innovation

- Can view the main job of Bitcoin network as implementing a *distributed timestamping* function, which effectively *serializes* Bitcoin transactions
  - *I.e.*, puts them in a definite sequential order
- The reason to serialize transactions is to decide, in case someone tried to spend the same coins twice (or more), which of those attempts was *first*.
  - This effectively prevents double-spending!
    - 2nd (and later) attempts to spend the same coins are simply ignored
- Distributed timestamping is an example of *distributed consensus*.
  - A set of widely-separated entities arriving at unanimous (or near-unanimous) agreement on some decision(s).
- In Bitcoin, any dispute re: transaction order is automatically resolved via a very simple arbitration mechanism:
  - Whichever full node happens to find the proof-of-work solution first, is the one that gets to decide which of any conflicting transactions to accept!
- In other words, **computational power → decision-making authority**.
  - We'll talk more later about other applications of this principle…

Some more details of how distributed consensus is achieved

- Suppose two mining nodes (A and B) happen to announce a new block at about the same time – who wins in that case?
  - Some set of mining nodes will build on A's block, and some set will build on B's block.
    - However, one set of nodes will be faster than the other, and will produce new blocks faster.
  - **Important:** All nodes on the network are programmed to work on the longest chain!
    - Eventually one chain becomes clearly longer than the other, and as all nodes shift to work on that one, consensus is thereby achieved.



Importance of Distributed Consensus

- In Bitcoin, nodes achieve distributed consensus as to *one* decision: What is the sequence of valid transactions making up the Bitcoin blockchain?
  - However, the same protocol could be use to attain consensus about *anything* – so long as the decision made is included/encoded into the block data.
- A distributed consensus mechanism such as Bitcoin's can be used to solve the very general classic CS problem of *Byzantine agreement:*
  - How can *N* distributed notes reliably come to an agreement if communications between them could be arbitrarily interrupted/corrupted by attackers?

"Byzantine Generals" problem

- Generals must coordinate armies for attack
- Messages may be intercepted/forged
- Some generals could be turncoats!

Alternative Applications of Byzantine Agreement / Distributed Consensus

1. Distributed unique-name registration
   - *E.g.*, Namecoin, distributed replacement for DNS
2. Reliable P2P delivery of encrypted messages
   - *E.g.*, Bitmessage application
3. Distributed electronic markets (*e.g.* Ripple)
4. Secure electronic voting!
   - Record candidate selections in Txns/blocks
     - Mining pools function like political parties
   - Caveat: Not really "1-person/1-vote"
     - More like "1 Ghash/1 vote" or "1 BTC/1 vote"

Some Other Intriguing Applications

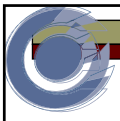
5. Issuing Stock w/o Underwriters or Banks
   - Just create a cryptocoin representing your shares
     - *E.g.*, Invictus Innovation Incorporated's *ProtoShares*
6. Digital Autonomous Corporations (III's idea)
   - Bitcoin can be viewed as the first example of these
   - A DAC reliably executes the "corporate charter" that's encoded in its open-source codebase
     - Its algorithm is the CEO, human ops are like employee-owners, and are paid in 'shares of stock' (the DAC's coin)
7. Secure pseudonymous digital identities
   - *E.g.*, III's Keyhotee proposal

Reinventing the fundamental organizing principles of human civilization?

- *E.g.* could we make a distributed-consensus-based legal system?
  - The system's "laws" are encoded into the open-source code-base of a blockchain network. Initial code-base = the system's constitution.
  - All participants in the system can (via messages embedded in transactions/blocks) propose changes to the law and "vote" on them.
    - Changes to the law are represented in the form of patches to the open-source codebase, in some pre-defined patch language.
  - As is runs, the node software *modifies itself* to automatically incorporate changes that have been previously proposed, voted on by the community, and then accepted by blockchain consensus.
- Our old-fashioned, flawed, fallible human systems for politics, law, and governance could become obsolete!
  - The new system is *incorruptible* – all changes to the law that occur are *by definition* legitimate, as per the original constitution and the automatically-arbitrated community consensus.

Top-10 Largest Cryptocurrencies (as of Jan. 11, 2014)

#	Name	Market Cap	Price	Total Supply	Volume (24h)	% Change (24h)	Market Cap Graph (7d)
1	Bitcoin	$ 11,110,509,414	$ 906.96	12,250,275 BTC	$ 42,867,619	+3.06 %	
2	Ripples	$ 2,378,493,110	$ 0.024	99,999,998,162 XRP*	$ 66,786	+3.17 %	
3	Litecoin	$ 658,435,367	$ 26.56	24,785,954 LTC	$ 21,352,713	+2.68 %	
4	Peercoin	$ 136,422,621	$ 6.48	21,037,407 PPC	$ 2,102,759	+8.88 %	
5	MasterCoin	$ 72,303,997	$ 128.39	563,162 MSC*	$ 87,059	-8.32 %	
6	Namecoin	$ 53,193,378	$ 6.87	7,737,492 NMC	$ 1,791,616	+0.49 %	
7	Nxt	$ 45,254,492	$ 0.045	999,997,986 NXT*	$ 70,448	+6.54 %	
8	Quark	$ 19,514,905	$ 0.079	247,206,233 QRK	$ 84,266	-4.61 %	
9	ProtoShares	$ 18,951,556	$ 14.44	1,312,651 PTS	$ 39,282	-6.60 %	
10	Megacoin	$ 17,756,755	$ 0.82	21,688,625 MEC	$ 12,213	-4.07 %	



Conclusion

- To say (as some have) that Bitcoin is "just another payment system" is like saying the Internet is "just another communication medium"
  - Rather, Bitcoin's core technology is a fundamentally new kind of *platform* which opens the door to a vast new space of applications, based on Bitcoin's revolutionary technological innovation of *distributed consensus.*
    - Similarly to how the Internet is a new platform, based on its revolutionary technological innovation of its *network stack* separating applications from low-level data-transport plumbing
- The Bitcoin community is growing exponentially (~10×/year) and its adoption, applications, and diverse spin-offs are flourishing.
  - I think, in Bitcoin, we are seeing the early stages of *the* most transformative revolution in technology & society of our time.