IOHK | BLOG

GOODBYE MIKE AND SOME THOUGHTS ABOUT BITCOIN

JANUARY 15, 2016 CHARLES HOSKINSON 13 MIN READ

On Mike

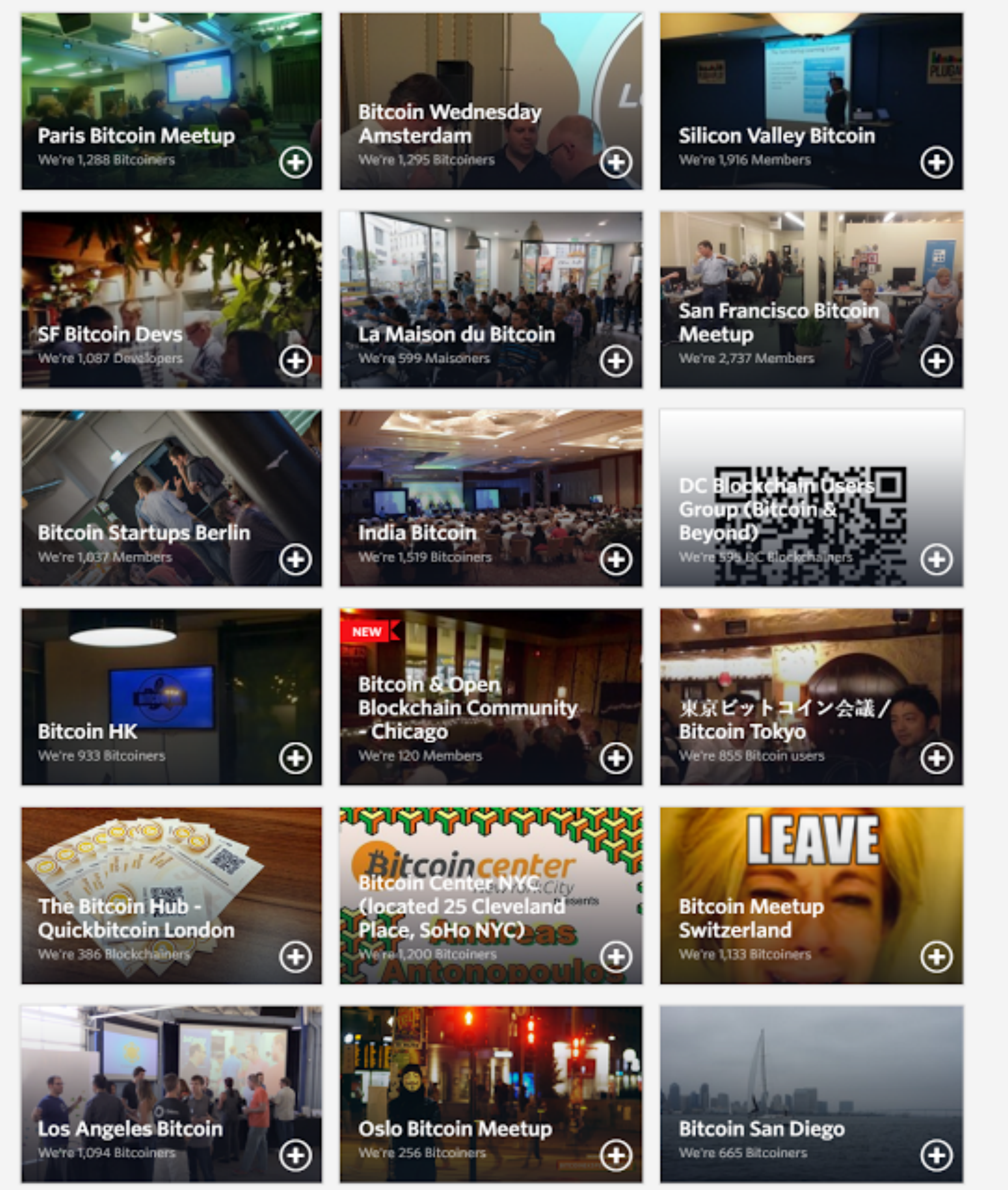
After reading Mike Hearn's farewell letter to the community, I've decided to finally draft my thoughts on the blocksize debate, but first a few things about Mike. Hearn, joined the Bitcoin community back in May of 2009 and has been an active contributor for as long as I can remember in some capacity or another. He's also an incredibly bright and creative person who brought a lot to this ecosystem in its earliest days.

The point of decentralized systems is never to reach ubiquitous consensus about truth. Settling upon a final truth is pyrrhic at best and almost certainly a sisyphean endeavor. The goal is to facilitate the free flow of ideas and provide an effective framework to actually test them with something at stake.

Mike was a voice for a certain philosophy and regardless of whether you feel that philosophy is correct, it is a terrible tragedy that our community descended into the murky swamps of censorship and personal attacks. I will miss Mike and want to extend a profound thank you for all he has done and good luck on future projects.

All this said about Mike's contributions and positive influence on the space, I would be remiss if I didn't comment on his core argument that the Bitcoin project has failed. It's not only wrong, but utterly offensive to the thousands who have contributed weekends, painful explanations about the nature of money to their friends at bars and the repeated scorn of having to endure the scams, exchange failures and regulatory misunderstandings.

Burt Wagner was arrested for legally selling bitcoin and had to spend his life savings to have the State of Colorado accept its own laws. He's still in the Bitcoin space. Many of the thousands affected by the collapse in MtGOX are still in the space. There are hundreds of meetup groups actively evangelizing, onboarding their local communities and coming up with creative solutions to various problems. A colleague of mine even paid for a recent meal at the Shard with Bitcoin thanks to the magic of Xapo (American beef is still better :)):



Paris Bitcoin Meetup
We're 1,288 Bitcoiners

Bitcoin Wednesday Amsterdam
We're 1,295 Bitcoiners

Silicon Valley Bitcoin
We're 1,916 Members

SF Bitcoin Devs
We're 1,087 Developers

La Maison du Bitcoin
We're 599 Maisoners

San Francisco Bitcoin Meetup
We're 2,737 Members

Bitcoin Startups Berlin
We're 1,037 Members

India Bitcoin
We're 1,519 Bitcoiners

DC Blockchain Users Group (Bitcoin & Beyond)
We're 595 DC Blockchainers

Bitcoin HK
We're 933 Bitcoiners

NEW
Bitcoin & Open Blockchain Community - Chicago
We're 120 Members

東京ビットコイン会議 / Bitcoin Tokyo
We're 855 Bitcoin users

The Bitcoin Hub - Quickbitcoin London
We're 386 Blockchainers

Bitcoin Center NYC (located 25 Cleveland Place, SoHo NYC)
We're 1,200 Bitcoiners

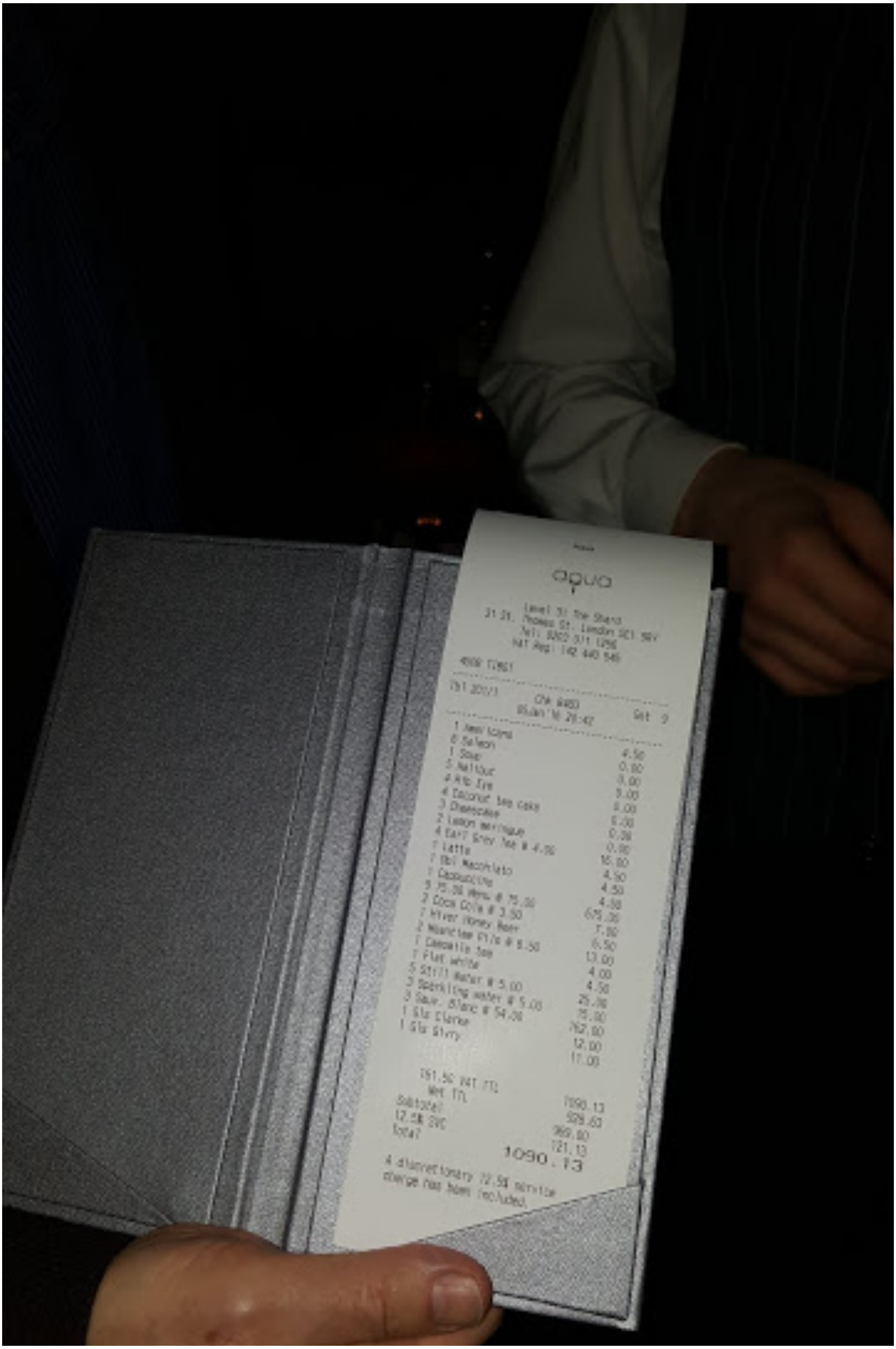
Bitcoin Meetup Switzerland
We're 1,133 Bitcoiners

Los Angeles Bitcoin
We're 1,094 Bitcoiners

Oslo Bitcoin Meetup
We're 256 Bitcoiners

Bitcoin San Diego
We're 665 Bitcoiners

Mike thinks we don't matter :(



```
                 Aqua

                 aqua

          Level 31 The Shard
  31 St. Thomas St. London SE1 9RY
         Tel: 0203 011 1256
        VAT Reg: 142 440 546
4008 Tim01
------------------------------------
Tbl 201/1
              Chk 6483
          05Jan'16 20:42        Gst 2
------------------------------------
1 Amer Iced
6 Salmon
1 Soup                          4.50
5 Halloumi                      0.00
4 Rib Eye                       0.00
4 Coconut tea cake              8.00
3 Cheesecake                    8.00
2 Lemon meringue                6.00
4 Earl Grey Tea @ 4.00          0.28
1 Latte                         0.00
1 Dbl Macchiato                16.00
1 Cappuccino                    4.50
9 75.00 Menu @ 75.00            4.50
2 Coca Cola @ 3.50              4.50
1 Hiver Honey Beer            675.00
2 [illegible] Pt/n @ 6.50       7.00
1 Camomile tea                  6.50
1 Flat white                   13.00
5 Still Water @ 5.00            4.00
3 Sparkling water @ 5.00        4.50
3 Sauv. Blanc @ 54.00          25.00
1 Gls Clarke                   15.00
1 Gls Stvry                   162.00
                               12.00
                               17.00

    151.50 VAT TTL
      Net TTL
Subtotal                     1090.13
12.5% SVC                     529.63
Total                         969.00
                              121.13
                  1090.13
A discretionary 12.5% service
charge has been included.
```

In Pounds; Paid in Bitcoin

Furthermore, the state of Bitcoin technology has never been better. One has to look no further than the Princeton bitcoin paper to see the amazing diversity of interesting problems being examined in academia and industry. A recent redditor posted a database of over 600 papers on Bitcoin or related to cryptocurrency technology. IC3 is a joint research group of two major US universities lead by some of the top cryptographers in the world and they have received a 3 million dollar NSF grant to study cryptocurrency technology. And yes those scaling bitcoin conferences were very productive and included a lot of wonderful industry support:

Mike thinks we don't matter :(

Bitcoin has hundreds of thousands of passionate people, over a billion dollars in VC money and the support of ideas from over a thousand altcoins running experiments including Bitshares and Ethereum. The fact that we are having a transaction crisis is a symptom of success not coming doom!

So Mike I'm terribly sorry that you lost the XT fight and it's definitely true that it wasn't a fair fight, but don't take your anger out on Bitcoin the experiment nor the Bitcoin community:

Darth Vader on Mike Hearn

Some Basics About Blocksize

Now on to blocksize, there is already a great deal of detailed content floating around the interwebs on the various issues thus I will quickly summarize the crux of the matter. Bitcoin blocks have an arbitrary size cap of X MBs and each transaction takes on average Y bytes. As the network grows, we will (and have) hit this cap and the result will be an overall reduction of performance, reliability and robustness of the Bitcoin network.

So how does one resolve this seemingly intractable problem? The naive and kicking the can down the road solution is simply to increase the blocksize from X to a new arbitrary amount- say X(1). If Bitcoin continues to grow, then we'd have the same debate all over again in a few months or perhaps years (see US Debt Ceiling Debates). This said, one could develop either an algorithm to scale blocksize via some set of network parameters or increase it at regular intervals similar to how coinbase awards are cut in half every four years.

One could also increase the rate of block production (referred to as the block interval). There have been several proposals to do this in a way that wouldn't increase the amount of stale blocks and Ethereum even implemented one called GHOST developed by Zohar and Sompolinsky. The basic concept is turn Bitcoin's blockchain into a directed acyclic graph from an append only linked list. This path is reasonable, but doesn't resolve the issue of data bloat (more on this later).

We could approach the problem from the other side by examining transactions. Again the most naive approach is to reduce the size of transactions from Y to something smaller say Y(1). Again this approach doesn't solve the fundamental problem that future growth will push blocks to their cap.

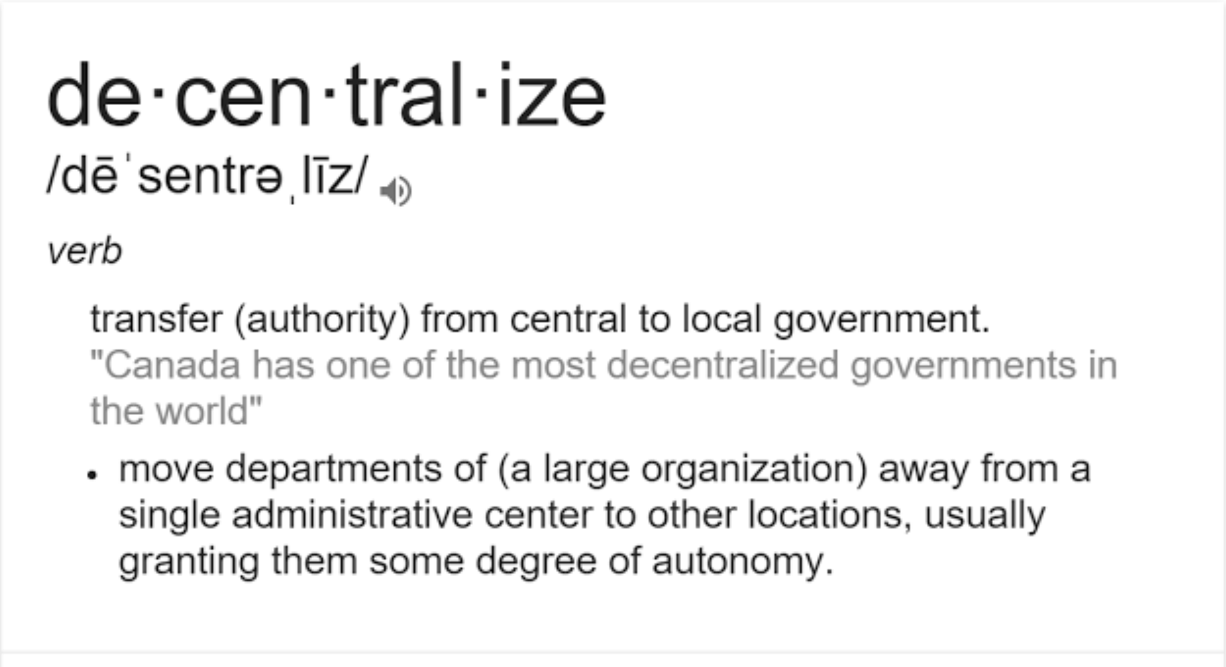
Along the same line of thought, one could create a mechanism to gradually retire transactions (called pruning) or reduce the amount stored on chain. There have been some interesting ideas proposed like segregated witnesses and Pieter Wuille has been a great mind in considering pruning. It's a nice efficiency improvement and something that could definitely help the network, but again doesn't solve the core issue of long term growth.

Finally, one could push transactions off-chain so they don't appear in the Bitcoin network at all or eventually in a reduced form. This idea is seen in efforts like the Bitcoin Lightning Network and the Sidechains project. It's the most politically friendly of all proposals as there are already many projects exploring how to facilitate the offchain infrastructure without necessarily requiring a fork of the Bitcoin protocol (or at least a dramatic hard fork). As a side note, It's probably not an accident that a large pool of the Bitcoin core developers happen to work for the company spearheading these approaches.

Blade Runner's take on Transaction Pruning and Off-Chain Solutions

Off-chain is compelling, but still has a lot of unresolved questions about trust models, security concerns, centralization issues (in certain cases) and also unpredictable privacy (for example, if transactions are moving to a new network, then the gatekeepers of that network could attach metadata to the transactions for KYC/AML and other such things). Furthermore, the practical question of why bother seems to be looming? We are going to solve the issues of Bitcoin by using federated or centralized actors?

I recall the argument to get merchants to adopt bitcoin is to use services like Bitpay, yet then we go back to the solution to asset volatility of our decentralized network is to connect all the merchants to a centralized service provider? The same applies for transaction scalability solutions for the Bitcoin network. Seek decentralization wherever possible!



de·cen·tral·ize

/dēˈsentrəˌlīz/

verb

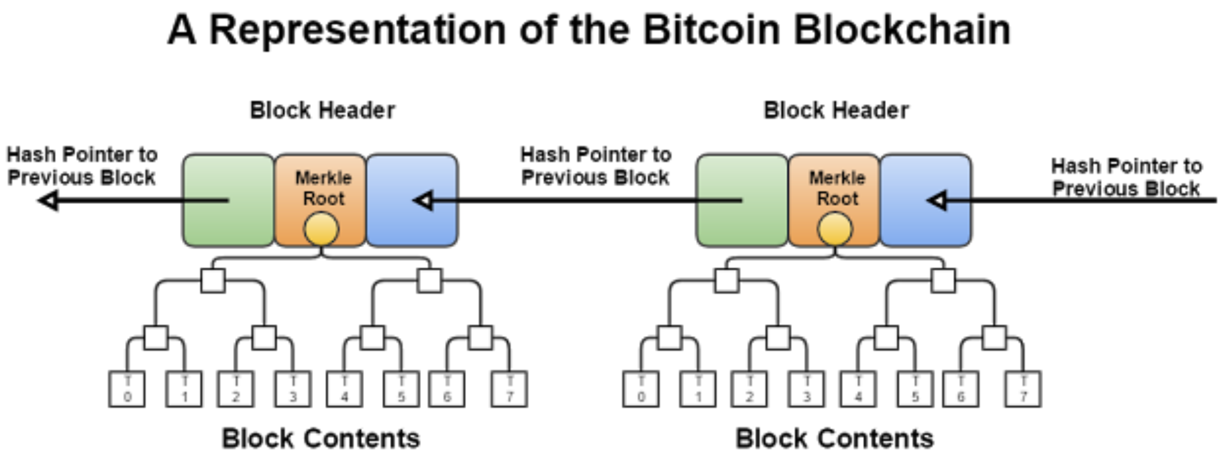
transfer (authority) from central to local government.

"Canada has one of the most decentralized governments in the world"

- move departments of (a large organization) away from a single administrative center to other locations, usually granting them some degree of autonomy.

What the Bitcoin movement is trying to do in a nutshell

Solutions in a Technological Context


A Representation of the Bitcoin Blockchain
Block Header
Block Header
Hash Pointer to Previous Block
Hash Pointer to Previous Block
Hash Pointer to Previous Block
Merkle Root
Merkle Root
T 0
T 1
T 2
T 3
T 4
T 5
T 6
T 7
Block Contents
Block Contents

I created this graphic on Gliffy. Gliffy is pretty Spiffy!

The diagram above presents a rough idea of what the Bitcoin blockchain actually looks like. There are two components: a block header and the block body storing the actual transactions.

All the parts are wired together with some form of crypto. The block body is connected to the header via a merkle tree data structure. The headers are wired together via hash pointers. And proof of work provides a mechanism for validating a given collection of blocks (the proposed blockchain) is the correct one via the notion of algorithmic weight (the proposed chain with the most work wins).

So we have been given a menu of options to change the core protocol to reflect the goal of more transactions. Increasing the blocksize makes the block contents heavier (larger merkle tree), but has no impact on the block header. It's an interesting question to consider the impact of larger blocks on block propagation times. I'd highly recommend this excellent paper studying propagation in general by Decker and Wattenhoffer.

Reducing the block interval will likely involve changing the structure from a single hash pointer to multiple hash pointers to different blocks, but no impact on the block contents. Inclusion of double spend transactions and longest chain selection rules are the topics of primary interest here. I'd recommend two papers to get a deeper understanding. First, Sergio Lerner's DAG-Coin proposal and then Lewenberg et all Inclusive Blockchain Protocols.

Pruning means that over time certain leaves in the merkle tree should be removed or perhaps even entire blocks replaced with different representations. It's also interesting to consider what other authenticated data structures could be put into the block headers to improve scalability or better facilitate pruning schemes without compromising trust. The Bitcoin wonderkid researcher Andrew Miller has done some foundational research with Katz and others.

And finally off-chain means that we are effectively wiring something more onto the block via the header or more likely in the block contents. The concept here is separation of concerns and layering. For example, rootstock is discussing how to do smart contracts via a sidechain of bitcoin. This area reduces the need for whole sets of transactions by simply having them done outside of the main Bitcoin blockchain in different domain. It also modularizes the set of things a client has to download.

The Hidden Demons Behind the Debate

The original design of Bitcoin was to have a completely decentralized network of equal actors with no barrier to entry for participation. Mining was done on ordinary CPUs (in fact Satoshi mined more than a million bitcoins using CPUs). Maintaining a full node wasn't a serious commitment. It was less taxing than running bittorrent with a few HD movies.

The separation of block headers from the block contents does suggest a path to heterogeneity via light nodes holding only the header collection; however, again this action isn't forced upon anyone.

Now enter 2016, Bitcoin is a very different animal. The Bitcoin blockchain has grown considerably. Mining is heavily centralized:

These Guys Own More than 51 Percent of the Mining Power

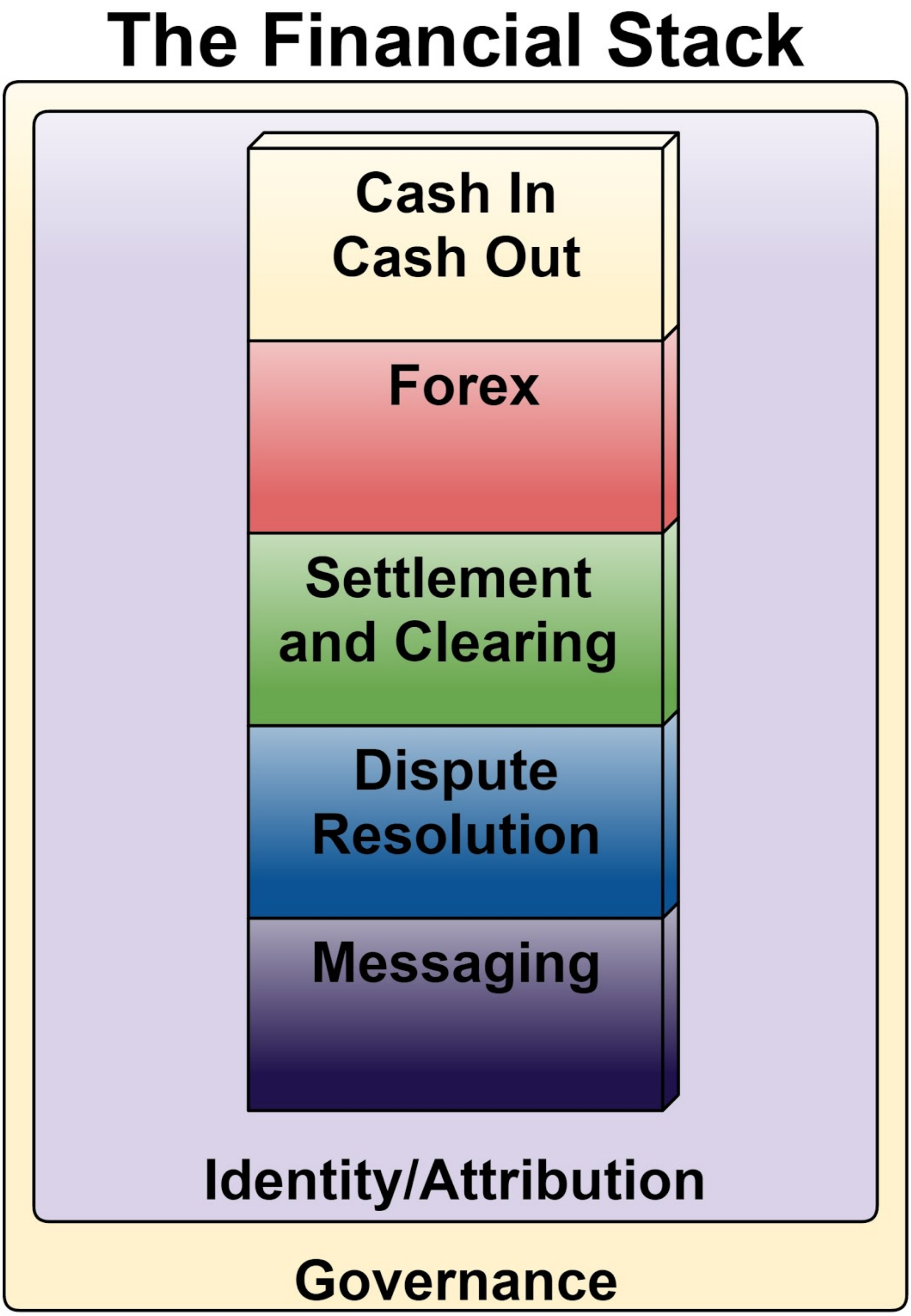
There are millions of dollars of value floating around every block. There are numerous, well-funded business interests and even a cabal of powerful bankers scheming in a sufficiently NWOish named group called R3CEV:

Totally not trying to co-opt the ecosystem!

Thus things have really changed over the past seven years beyond the humble beginnings of Hal and Satoshi trying to get the wallet to work in order to send a single transaction (It was block 170 BTW- a whole 10 bitcoins!).

I feel that this debate has exposed more than certain people's inability to work productively with each other or the need for a new set of reddit moderators. It has exposed that Bitcoin is basically at a philosophical impasse. There really isn't a clear direction for the Bitcoin ecosystem to take. Is it supposed to be the ultimate payment system with a super cool deflationary digital gold coin backing it? Is it a settlement layer for many systems to eventually clear upon? Is it the arbiter of digital truth providing a cryptographic beacon, notary services and a logical clock? Is it a system for decentralized governance?

Fair arguments can be made for any of these directions and there is a legion of good tech to sneak into the protocol to make Bitcoin better suited for these tasks. In general, Bitcoin could basically be the entire financial stack:



Bitcoin could be the whole stack

We simply cannot productively move forward until the meta-question of **what does bitcoin want to be when it grows up** is answered. There is no measuring stick to say ok this is good enough. For example, 3 transactions per second is absolutely fine if our goal is settlement of large contracts between multibillion dollar actors, but it's terrible if we are trying to replace VISA.

Should Bitcoin be blind and deaf to other systems and cryptocurrency or does it need to talk to them on a regular basis? Are we going to tokenize all assets like gold and USDs and trade them in a decentralized network? Or are we going to trade them on exchanges and move them between exchanges using some connection to the Bitcoin blockchain? If there is a dispute, then is arbitration connected to the data held on a blockchain?

Each of these questions and the hundreds more have a dramatic impact on what needs to go into a transaction, how of many per second we need to include in the Bitcoin blockchain and also the intended set of users. Let's be intellectually honest, have we answered them? Where do you even go to start that process? Who gets to decide?

In effect, we don't have a blocksize crisis, we have a governance and philosophy crisis. And the pain will continue until this crisis has been resolved either out of some cabal gaining control of the network or by a new mechanism to decide things in a decentralized manner (See DAOs).

My Proposal to Solve the Debate

Since everyone has a proposal, I might as well throw my hat into the ring. First, we need to solve the immediate crisis at hand. Let's take Kryder's Law of storage growth and combine it with Nielsen's law of bandwidth to produce a reasonable rate of block growth in regular intervals. The basic idea is that blocks will grow at a rate that scales with local storage and the rate of bandwidth increases of internet connections.

Second, adopt the plan devised at the scaling bitcoin conference. It's reasonable and doesn't require dramatic action. Segregated witnesses in particular are a very solid concept. Furthermore, scaling bitcoin should really be a bi-annual event moving forward- get people talking to each other on a regular basis.

Both of these actions will take the pain off of the network and give us some breathing room. We have to then move on to phase II, which is investing in some foundational technology to radically improve the entire network.

- Sidechains is a fundamentally sound and reasonable idea. It's a conversation about getting blockchains to talk to each other and move value without needing special actors. The project is also incredibly well funded and backed by some of the best people in the space. Sprinkle some soft fork on that shit. In the absence of soft forking, BTC-Relay is pretty cool.

- Reducing the block interval is a really good idea. Ethereum's implementation of GHOST serves as a great example of a path to do this and the researchers behind DAGs are solid people. Faster settlement with the same level of security as the slower interval is frankly good for us all.

- Change Bitcoin's consensus algorithm from proof of work to something else. Mining centralization is a problem. The original idea was that the network was to be secured by many different people not a small cabal of anonymous mining corporations floating around Asia. Furthermore, we have a lot of cool things that can be done with different consensus algorithms like voting and allowing for many assets to exist concurrently on the Bitcoin network in a scalable and mobile friendly way.

- Invest in Blockchain sharding. There is an interesting project by Professor Shirer that has some legs. The point here is that Bitcoin's data model is 1 byte requires N bytes of total storage with N being the set of full nodes. It's terribly wasteful. Increase the dataset from D to D(1) via erasure codes and then chop up the blockchain into reasonable sets of shards. We could have a many petabyte blockchain that is in 50 MB pieces. Changes to Bitcoin's consensus algorithm and fundamental data structures could dramatically help here.

- Develop more productive federation technology for service providers in the Bitcoin space to interact with the Bitcoin blockchain. The reality is that we'll still have a lot of services off-chain entirely for privacy, cost or performance reasons, but we shouldn't have to completely trust the people running those networks. Ideas like Pavel Kravchenko's Infraproject and Blockstream's Liquid are movements in the right direction as are concepts like proof of solvency.

- Create a mechanism to incentivize data relay on the Bitcoin network. As the network scales, there will be enormous amounts of data floating around and it needs to be economically optimized or else you'll have centralized hubs acting as relays to millions of dependent nodes. Eric Lombrozo has been a great voice of reason in this respect.

The final phase is to make Bitcoin a self-funding evolutionary system. There needs to be a DAO that integrates into the core protocol that provides a framework to discuss and implement BIPs as well as cover their associated costs of implementation.

Until the development of Bitcoin is free from outside corporate influences, it can't be discussed in an objective and fact based way, and the stakeholders of the system are able to decide instead of a cabal of well capitalized actors, we aren't going to gain the resilience of the crowd.

This phase is probably an innovation of the size and scale of Bitcoin itself and thus is unlikely to materialize immediately, but organically over a collection of hundreds of experiments. And like Bitcoin, it would fundamentally change the very nature of organizations, their mandate and the flow of funding.

Thanks for Reading!