Title: The Blocksize War

Subtitle:

Author: Jonathan Bier

Contents:

1. First Strike 1
2. March To War 16
3. Scaling I - Montreal 40
4. Scaling II - Hong Kong SO
5. SegWit 59
6. Lightning Network 66
7. Bitcoin Classic 71
8. Hong Kong Roundtable
9. Faketoshi ୨୨
10. The DAO 106
11. Scaling III - Milan 1188
12. Bitcoin Unlimited 122
13. Exchanges 134
14. ASICBoost
15. Dragons’ Den 148
16. 151 Litecoin
17. User-Activated Softfork 157
18. New York Agreement 172
19. Bitcoin Cash 187
20. SegWit2x 197
21. Victory 214

Chapters

Introduction

* It was Saturdays August 15, 2015, to November 2017.
* A chronology of the significant events. This
* Conflict and includes coverage, from by and behind the scenes, during some of the most acute phases of players from both sides during the war, exploring their motivations, strategy and thought processes as the exhausting -campaign progressed and developed
* Appreciate the level of intensity with which the battle fought and how hostile each side eventually became towards the other.
* Difficult to appreciate it now, but Bitcoin came reasonably close to a catastrophic failure.
* Two sides are labeled “big bloc! Small blockers”, al -though in reality this is an oversimplification the groups were not homogenous.

## First Strike 1

* Mike Hearn and Gavin Andresen, had
  + Thrown their support behind a new, incompatible version of Bitcoin XT.
  + To increase this limit to 8 MB and the double it every two years until 2036, when the limit would be around 8000 MB.
* Proponents of the increase argued that higher capacity was needed to ensure Bitcoin could scale up and become a cheap global payments system,
* Blocksize would shatter and only the ecosystem
* T four somewhat interrelated issues :
  + The level of blockspace available in each Bitco in block
    - Capacity available in the blocks, or consistently fia 1l ocks.
  + How to modify the rules of the Bitcoin protocol]
    - Hould be more robust a only change in exceptional circumstances, with broad support from all interested parties.
  + The significance of the nodes of ordinary users:
  + Time preferences
* There was almost universal agreement in the community that the 1 MB limit was too small. However, there was consensus on what it should be or how to change it.
  + August 2015 when the client was officially released they encouraged people to run it, therefore this is when we mark formal commencement of hostilities.
* Chosen activation
  + A flag day and a miner signaling threshold
    - 750 blocks flagged support, in any 1,00-block rolling window, the upgrade would activate.
      * Two week grace period before the rule came effect and the blocksize finally increased.
* Extremely controversial
  + Primarily because it was an incompatible upgrade to the network.
* Running a Bitcoin node that validates all the rules would be required upgrade their software.
  + Small block world view, this could cause Bitcoin to split into two different coins.
    - Hardfork
      * Can essentially change Bitcoinin any way, from
        + Supply capabove 21 million, to taking away any coins any holder and giving it to anyone else. Many
      * This characteristic is what made the network esilient; it meant nobody could take away their coins and ensured the supply cap of 21 million was robust. This was
        + Example of the slippery slope fallacy, and a red herring.
      * An open system, it was not possible to conceal this disagreement from the public any longer
  + Letter of support published by some of the largest and m Ost gnificant companies in the industry:
    - Listening, researching and testing. We believe that work is complete, and it time to communicate our view in a clear and transparent manner.
    - It is imperative that we plan success by raising the maximum block size.
    - BIPI0] and 8MB blocks ar supported by a majority of the and we feel it is time for th industry to unite behind this proposal,
    - ¢ letter was signed by the CEOs of BitPay, Blockchain. Info, Circle, {ncminer, itBit, Bitnet, Xapo and BitGo. These were not only some the largest companies in the space, but many of them were also funded and had considerable venture backing.
* Gavin may have been driven by Jisego.
  + »opportunity for Gavinto show developers who opposed him that they barely mattered, that companies in the space did not even know who they were
  + Just under two years after the network launched, in december 2010, Satoshi left the project.
  + Gavin explains how, in his mind, he took over as leader of the project:
  + Satoshi started stepping back as leader of project and pushing me as the leader of the project
    - Control of software repository, of course, does not mean control over Bitcoin, Bitcoin users can run any software they like, from an repository like. This
      * Misconception has lingered on fury ears.
    - Is key to understanding Gavin’s role in the community at the time is his personality. In his public posts and at events, he came across as patient, thoughtful, calm pragmatic.
      * Gavin spoke, people listened; he sounded reasonable and took time to explain things.
        + 1n stark contrast some of the other developers, who were sometimes regarded as intolerant of those with weaker levels of technical knowledge, preferred to remain behind the scenes.
      * Level of influence over the technical community because of who he was, not a handover of power.
  + Bitcoin faut or
  + Co-founded the Bitcoin Foundation in 2012
  + First paid Bitcoin developer.
  + ‘Main guy.
    - Conservative, moderate and a driver of consensus.
    - Mike Hearn,
      * A lot of work on Bitcoin), a Java library for working the bitcoin protocol, which made the mobile wallets at the time possible, It
  + Bitcoin subreddit, /r/bitcoin. The
    - Accelerated the vitriolic nature of thee argument. In
      * Larger block message was clear and simple
        + Arguments against this were, typically, highly complex somewhat confusing.

1 MB Just seemed like low number and

Moderation on these forums intensified. This moderation appeared to only rile up some of the larger blockers even more: in their view, the moderation policy, or as they saw it censorship, was preventing Bitcoin from scaling.

* + - BitcoinTalk and /r/bitcoin were both controlled by the same person, with the username Theymos.
      * Controlled by the same person, Michael Marquardt
        + Early pioneer in the space, managing bitcoin.it Theymos had been
        + blockexplorer.com, was eventually overtaken by blockchain.info

Appeared to mostly sympathize with the smaller graphics.

Widespread agreement across community before hardforks

* + - * + On August 17, 2015, two days after the official launch of Bitcoin XT, August 17, 2015, two days after the official launch r/Bitcoin exists to serve Bitcoin. XT will, Bitcoin and create a separate Bitcoin and create a a separate network/currency. Therefore, it and services that support

Allow only submissions related to XT. In that case, the definition of “Bitcoin” will have changed. It doesn’t make sense to support two incompatible networks/currencies - ‘s only one Bitcoin, and r/Bitcoin serves only Bitcoin,

* + - * + Ido not want these people to make threads breaking the rules, demanding change, asking for upvotes, personal attacks against personal attacks against derators, etc. Without some real argument, you’re not going to convince wasting your time and ours.
    - Rules for the Bitcoin subreddit were reasonably clear: since new rules for the Bitcoin subreddit WU y since change, and would therefore result in a new coin, promotion of the change, and would therefore result in a and was an incompatible software was banned on the subreddit.
      * The Bitcoin Reddit was the main discussion forum in the community, and lobbying for the main discussion forum in the community, and lobbying for the change they desired on this forum was exactly how they envisioned such a change would take place.
        + Anti-censorship arguments began to gain momentum and proved to be quite compelling.
        + If one couldn’t campaign for a change due to a lack of consensus, then how would we ever reach consensus? It was a catch-22 situation!
* One should consider who many of the Bitcoiners were, at least the ones engaged enough to follow this debate. They were typically anarcho-capitalists or libertarians, who strongly supported free speech. It
  + Bitcoiners typically felt their voice ignored when expressing opposition to these policies, or deemed irrelevant. This is why many became Bitcoiners in the first place; they that this time it’s our money, not theirs! This time our voice will count! Their frustration and level of anger at having their voices enced in Bitcoin was therefore huge.
  + Large blockers gradually moved over to an alternative Bitcoin subreddit, /r/btc. And forums such as Bitco.in.
    - Became far less healthy and confirmation bias became problem.
    - Causes polarization.
      * People become more and more embedded in their views and have limited exposure the opposing arguments.
      * People on either side of a conflict cars barely believe anybody could legitimately hold an opposing view.
        + Assumed to be either stupid, corrupt or to have some nefarious agenda.
  + Theymos’s moderation policy post again, it becomes apparent that it contains many nuances, which were not widely apparent at the time. In many ways he was shown to be correct
* Paths to choose from:
  + Create a new alternative coin
    - Does not require widespread agreement
  + Lobby for consensus prior to advocating that anyone runs new client.
* Lot of these nuances were not appreciated or known.
  + Large blockers took more of a muddled path, unsure if they wanted greement from everyone or not.
* In these early stages of the conflict, it seemed clear that the large blockers were winning the war and making progress.
  + Many thought Bitcoin XT blocksize proposal might be too aggressive, with espect to locking in increases in the blocksize to 8,000 MB over the 20 years on a fixed schedule.
    - The space was notorious for rapid and unpredictable change?
    - A necessary step to get the debate going and act as a catalyst to encourage a counter proposal.
      * Perhaps this was the first of many of the critical blunders from the large blocker camp. Does one really try to win a war by losing the first battle?

## March To War 16

* The surface the system did not appear to have much value or potential. To be interested in the space, one had to have an imagination.
  + Had to see many steps ahead
  + Layer upon layer of assumptions with regards to how Bitcoin Building layer
  + Many in the community actually had different, conflicting assumptions with respect to how Bitcoin worked,
  + Disagreements were bubbling to the surface
  + Price had also appreciated significantly, some In the community became overconfident, ev - even a little arrogant.
    - May have based this investment on certain assumptions and a particular vision. They cou
      * Surely the assumptions made in 2011 influence one’s psychology.
      * Somewhat flawed and biased logic.
* When Bitcoin was released, there was no block size limit
  + Perhaps more than 32 MB, would have broken the system. T
  + On July 15, 2010, Satoshi added the following line of code to the software repository:
    - Static const unsigned int
    - MAX BLOCK SIZE= 1000000;^5
      * Sofware containing this upgrade was then released on July 19, 2010.
      * Not come into force until September 7, 2010, at block height 79,400 (,400 blocks since Bitcoin was launched).
        + Type of upgrade was called a softfork,

Adding or lowering the limit tightens the rules.

Increasing the limit would relax the rules and is therefore known as a hardfork.

* softfork/hardfork terminology was not known at the time, and was only used as of April 2012.6
* Satoshi never provided a clear reason for the block size limit at the time.
* Jeff Garzik, proposed removing it and increasing the limit.
  + He considered it important from a marketing and narrative perspective. Ju
  + Just 15 minutes later, Theymos replied, stating that: “Applying this patch will make you incompatible with other Bitcoin clients
  + Satoshi then chimed into the conversation: +1 theymos. Don’t use this patch, it’ll make you incompatible with the network, to your own detriment. We can phase in a change later if we get closer to needing Bunun
    - Only introduced the limit temporary measure and was already providing instructions on how to increase it, with a clear plan in place.
* Next quote from Satoshi widely cited by the large blockers is even earlier, November 2008, before Bitcoin had even launched,
  + being able to handle as transactions as Visa, 100 million per day.
    - If the network were to get that big, it network were to get that big, it would take several years, and by then, ending 2 HD movies over the Internet would probably not seem like a big deal
    - That Satoshi was making these comments under the assumption that Simplified Payment Verification (SPV) technology exists.
      * Therefore, in normal circumstances, not required to verify all the transactions. This technology has not Yet required to verify all the transactions.
* The very first reply to Satoshi when he announced Bitcoin was from very first reply to Satoshi when he announced Bitcoin was from somebody called James A Donald, who was already expressing
* When Satoshi referred to a competing client as a “menace to the network” and mentioned how the core design of Bitcoin was “set in stone”, in a discussion with Gavin in June 2010:
  + For the rest of its lifetime. Support every possible transaction type I every possible transaction type l could think of. The problem was, each required special suPport code and thing required special support code and whether it was used or not
  + Have been an explosion of special cases. The suition was script, which parties can describe their transaction as a parties can describe their transaction as a **predicate t**hat the node network evaluates.
    - The nodes only need to understand the The nodes only need to understand the transaction to the extent of} evaluating
      * Is it true or fales?
* Bitcoin catches on in a big way, these are things ‘ll want to explore in the future, but they all had to be designed at the beginning to make sure they would be possible later.
  + I don’t believe a second, compatible implementation of Bitcoin will ever be a good idea. So much of the design depends on all nodes getting exactly identical results in lockstep
* The debate appears to get almost religious, both sides poring over every Satoshi quote looking for comments or interpretations supporting their cause.
  + A lot has changed since then.
  + Probably know much more about Bitcoin than Satoshi back then, due the experience of seeing the network in action.
  + Bitcoin is not a religion and Satoshi is not a prophet,
    - Perhaps these characteristics contributed somewhat to Bitcoin’s success.
* On the Bitcoin XT was published, an email was sent from one Satoshi’s email addresses ([Satoshi@vistomail.com](mailto:Satoshi@vistomail.com)), articulating the blocker side of the argument, including a claim that he changed his mind about scaling:
  + Had hoped the debate would resolve and that a fork proposal would achieve widespread consensus.
  + I 3111 designed it in such a way as to make future modifications to the consensus rules difficult without near unanimous agreement.
  + Bitcoin competitive monetary system while also preserving its security properties is not a trivial problem, and we should take more time to come up with a robust solution. 1 suspect we need a better incentive for to run nodes instead of relying solely on altruism.
  + Bitcoin was meant to be both technically and socially robust. This present situation has been very disappointing to watch 11 probable that either this message is genuine or the account was hacked.
    - Since Satoshi’s other email account ([Satoshi@gmx.com](mailto:Satoshi@gmx.com)) was hacked when somebody was able reset the password
* Bitcoin Talк user “Vandroiу” posed a question: he essentially asked how miners would be incentivised when the block subsidy ran out
  + Marginal cost of including a transaction is near zero and, in a competitive environment, price equals marginal cost
    - “Fee death spiral problem
    - half the people thought this was a problem and half did not.
  + The block size limit would prevent fees falling too low, as users would have to bid against would prevent fees falling too low,
  + 2013, Mike appeared to recognise the fee death spiral as P legitimate problem, but proposed “assurance contracts” is as a potential solution, rather than a blocksize limit.
  + Issue was a argued that it was necessary for blocksize limit to remain small, such that users could validate all transactions and keep Bitcoin decentralised,
    - ‘Ignoring anyone trying to change the software you use,
    - “Replace by fee” allows users to replace a Bitcoin transaction (before it is onfirmed in the blockchain), a new transaction bY spending the same transaction input again, onlY with a higher fee.
      * Miners adopting this RBF policy would choose to include the higher fee transaction.
      * Not adopting this and instead using the first seen safe (FSS) principal, wo uld include the transaction they saw first.
      * Crucial distinction should be
      * Blocksize limit is a part of the Bitcoin protocol, while RBF is only a miner policy.
* Arguments over RBF seemed to have very similar inflection arguments over RBF
  + Focused on the long term;
  + User experience, making the system more resilient;
  + Prioritised growth, sustainability;
  + Business-focused, while small blockers were more scientific and theoretical,
* Gavin mphasised to me that 1 MB was ridiculously small, and that many pages were larger than that.
  + Technology was about exponential growth
  + Moore’s law Bitcoin would have much larger blocks, into the gigabytes, ventually Bitcoin would have mucn larger blocks
  + Was willing to compromise
* Mike was even asking if Gavin could boot the other developers out of the main Bitcoin Core repository on GitHub and take full control of the Bitcoin Bitcoin
  + How and when Gavin would do this, what specific action he would take, was unclear to me at the time.
  + May 4, 2015, Gavin published a blog entitled “Time to roll out bigger blocks”
  + Bitcoin-QT, however the name Bitcoin Core was adopted in February 2013 suggestion from Mike Hearn
    - Gavin had previously handed the ownership of the Bitcoin repository on GitHub to Wladimir, to enable Gavin to focus more on the research
      * Small blockers typically contended that Wladimir had no real power, and that owning the repository was only a janitorial role. 1
        + The Bitcoin rules are not determined by changes to software repository; they are determined bY the clients which users are already running.

Nobody was forced to upgrade.

* On May 29, 2015, Gavin gave the strongest hint Yet of what he planned to do: that he may switch his support over to Bitcoin XT and throw his weight behind the alternative incompatible Bitcoin protocol.
  + Implement a big increase now thar grows over time so we never have to go through all this rancor and debate again.
  + Prove to any doubters they’d better start supporting bigger blocks or they’ll be left behind, and to give them a chance to upgrade before
    - Ultimate authority for determining consensus is what code the majority of merchants and exchanges miners are running 22
    - BIP 103 - from Wladimir Van Der Laan and a developer called Gregory Maxwell for their suggestions23, indicating
    - Large blockers did react positively to BIP 103 at all.
      * Increase as so small that it was more of an insult than progress.
      * If both sides wanted the opposite, then could compromise really achieved?
* Full blocks would not be some kind of crisis; if anything, they were a success.
  + Some kind of paradox: “Nobody goes there anymore… it’s too crowded.”
* It was considered vital to always have a surplus of transactions which didn’t get in the blocks and were sitting there waiting to be included; that ways miners always an incentive to build blocks.
  + Anyone could store anything they liked in the blockchain, for instance their music collection or encrypted documents.
    - Demand for cheap, highly. Replicated storage was essentially unbounded, they argued.
* Decisions are made through agreement between Mike and Gavin, with Mike the final call if a serious dispute were to arise 25
  + This was all a power grab bY Mike. Who was Mike to make the final call”

## Scaling I - Montreal 40

* September 12 and 13, 2015, there was a “Scaling Bitcoin 2015 Phase 1”
  + Billed as an attempt to help resolve the conflict
  + Thought that, with face-toface discussions, people might have a stronger chance of appreciating other’s point of view. Who could argue against that?
  + Each side of the debate would be there,
* Gregory Maxwell (on the small blocker side).
  + Understanding of most of the various fields of study Bitcoin touched, and mining incentives,
  + In 2014, Gregory co-founded Blockstream,
    - Appeared to consist entirely of small blockers with a business model which depended on Bitcoin fees becoming high, as Blockstream offered potential solutions
      * Large blockers, did not, or more precisely, sho uld not, exist. Blockstream was therefore hated by the large blockers,
      * Cause and effect the wrong way around.
        + Staff appeared to have joined the company because of pre-existing view they had about scaling, rather than having come that view after joining Blockstream.
        + Nobody at Blockstream was being deliberately malicious; any failure in cognitive reasoning was likely subconscious. The same can be said of Gavin and the large blockers.
* Bitcoin development process as highly complex and scientific, with many challenging technical trade-offs. He did not welcome the involvement of what he considered the uninformed masses in the decision-making process, likening them to “beer cup spectators
  + Guy standing on the sidelines with a beer cup hat, saying “No problem guys: lets remove the breaks 1” and the crowd goes wild: Finally someone who cares about speed 27
    - Nickname “One Meg Greg
* considered explaining myself to my colleagues at the office and asking for more time off. After all, it was an investment company and this trip could be classified as investment research.
  + Many people in the company were also highly knowledgeable monetary history. Indeed, during my first week at the company,
  + I chose the path of an intense two-day trip to Canada, rather than the more relaxed schedule of an official business trip.
    - Ruffer would purchase around US$700 million of Bitcoin for its clients (around 2.5 percent of client
    - ‘Could prove to be a monumental moment for the ecosystem, especially in the UK.
* Debate between Gavin and Adam Back. \
  + Person referenced in the main text of the Bitcoin whitepaper for his Hashcash concept in 1997. And
  + Adam was the president of Blockstream.
    - Appeared to take a more moderate stance than Gavin, offering his support for the idea of increasing the blocksize limit to 2 then 4 MB and then &amp; MB, with two-year time gaps between the changes (BIP 248).
    - Satoshi had said nodes could be operated in data centers processing many transactions. Adam argued back that mining was more centralized than under Satoshi’s time.
      * Balance had shifted: users running nodes to validate the rules and keep the network decentralized was now important than it was before. It
        + When Satoshi was active in the space, there was no real distinction between validating nodes and mining nodes.
* Genuinely appear to be a good mix of people
  + Emphasis on the scientific method
  + Main organiser pindar Wong, a former ICANN Board member
    - Expertise in internet governance,
* Stood out the most to me: one by Peter Rizun on blocksize economics, and another from Jeff Garzik on various blocksize limit proposals.
  + Economic theory
    - Fee market death spiral argument did not apply as, without a blocksize limit, one could have a functioning transaction fee market.
      * Non-zero inflation was an assumption in his theory:
      * Regarded the blocksize limit as a production quota, which is an impediment to a free market, which claimed would determine transaction fees in a more efficient manner.
      * Showed pie charts on screen illustrating that two percent of
        + 15 percent by August 30, 2015. Peter then predicted this production quota would fail.
        + Bitcoin will break down dams erected by special interest groups attempting to block the stream of transactions. Comment attracted considerable laughter in the

Sensitive small blockers that this was trolling, and violating the collaborative spirit &gt;f the conference.

* + Jeff Garzik’s talk entitled “Issues Impacting Block Size Proposals”. Jeff
    - Another earl &gt;” Bitcoin developer, who had proposed removing the blocksize limit a
    - Trying to position himself as someone capable of bridging the gap between both sides.
    - Never appeared to support Bitcoin XT.
    - Keen on making some sort of decision, sooner rather than later, a
      * Fidelity problem. Fidelity is one of many Street companies looking at doing some Bitcoin experiments and they like many others say that if they switch on the switch on their Beta program, they max out Bitcoin’s capacity.
        + Project a non starter, from the get go, as
* Lessons they learnt from disputes related to cryptographic protocols, such as contentious decisions on how to select a hash protocols
  + Need for dialogue and patience.
  + Concept of “rough consensus” which involves judging the “sense of the group”.
    - ‘Dominance” is not to be determined on the basis of volume or persistence, but a more general sense of agreement.)
    - % of the working group does qualify as “rough consensus” and is better than rough. It
* Gavin’s turn to speak.
  + Decision needs to be made and someone, or some process, needs to in place to make that final decision. The
    - Nobody knew who or how this final decision would be made. What he said was reasonable, however I sensed he was becoming more frustrated and losing patience.
    - Mike Hearn had chosen. Not bother process, when
* Persona in the flesh; he seemed calm, curious, polite, houghtful and open-minded, a very different Gregory than one would expected.
  + Gavin and Gregory sat near each other and started lking. This is what many attendees had hoped to see: the
  + Both parties seemed uncomfortable, especially Gregory. His preferred discussion format was clearly web forums, where the conversation was open to everyone to view.
* The scientific merit format was certainly how many small &gt;lockers wanted the space to evolve.
  + Large blockers seemed to favour a more business-like approach; they did not regard Bitcoin as sorne theoretical science project,
    - Accused the conference organizers of making issue too complicated and using the event as a stalling tactic, to time. They cynically renamed the Scaling Bitcoin conference series as “Stalling Bitcoin”.

## Scaling II - Hong Kong

* Phase two phase two of the Scaling conte
  + To find an apartment vity anu nad a battlegrounds in this conflict and, if one wanted to witness this unfold, it was certainly a good place to be.
  + Cyberport, a business park Ka-Shing.
  + Conspiracy theories bY some of the most extreme large blockers.
  + Horizon Ventures, Li Ka-Shing’s VC firm, had invested in Blockstream and therefore this association with Cyberport was cited
    - Plot to cripple Bitcoin and keep the evidence of an
    - AXA was Henri de Castries, chairman of the steering group for the Bilderberg meeting, a closed-door gathering of the world’s financial and political elites, which provided perfect material for conspiracy
* Livelier and more intense
* Tensions were significantly higher. It
* Less productive and less useful than Montreal
* Mood was very optimistic: the overwhelming majority of people were large blockers who expected the issue to be resolved in a few months, few months,
  + Arguments in favour of small blocks were being gradually defeated
* Mosh technical. A key difference between Montreal and this conference was the presence of the miners.
  + China was regarded as having around 65 . percent of the global hashrate at the time.
  + Most of the miners indicated a preference for Bjp 100, rather than BIP 101. This is perhaps no surprise, as BIP 100 gave more discretionary power to the miners.
  + Wang Chung, the operator of one of the larger mining pools, F2Pool, said that miners are the only party that could vote and therefore miners would decide. Bitcoinis a proof-of-work system, he argued, and there is no mechanism for anyone else to vote. However, he went on to say that an 8 MB blocksize limit was too large, as it would take too long to sync a node, which he said would be a disaster.
  + Most miners seemed to agree that they were in control of the network -
    - Smaller blockers did not believe the miners had decision-making power over the Bitcoin protocol,
    - Proof of work was there to solve the double spending problem, they contended; miners merely decide on order of transactions. However, most miners believed this | decision was theirs;
  + Most work concept that controlled Bitcoin E governance, in
  + A way, each side was correct, bice
    - If Bitcoin XT reached the 1S percent threshold and then everyone upgraded to the larger block
    - 1f users refused to upgrade,
      * Miners would not be in control. The trouble here is that most people assumed that other users would behave the same as themselves, without considering that they may act differently:
  + Another discussion with miners, in a round table-type discussion,
    - Lost in translation, as the translator The message had supposedly been lost in translation, as the translator wanted to try and ɲip resolve the situation
      * Rather than make the conversation difficult and confrontational.
      * Miners had said that theY have real businesses, they invested real money and they produce the blocks, giving them real power over the network, while the developers had no such influence.
* Introduce Roger Ver to the
  + Backing companies such as Blockchain.info, Bitpay and Kraken.
  + Instrumental in driving adoption
  + Earned the nickname “Bitcoin Jesus”.
  + interested in the practical and business slut vi Bitcu, prior to the blocksize war, he had little interest in the technical or computer science aspects of the system.
  + Well known in the Bitcoin community for ensuring users the solvency of the MtGox exchange in July 2013,
    - This damaged Roger’s reputation to some extent, however people in space have short memories and there are always waves of new joiners.
  + Owner of the alternative Bitcoin subreddit, /r/btc
    - Forthright libertarian views, he was very strongly opposed censorship
* Jeff Garzik spoke again at the conference a
  + Essentially four pathways forward: BIP 101, his BIP 100 idea, a simple one-off increase to 2 (BIP 102), or doing nothing. After his speech, he was asked how
  + Transparency and discussion are the transparency and discussion are the: private visits to various people, deals, private visits to various people, in public. That’s the open-source way
  + State a proposal and if the audience agreed, they would clap:
    - Simple increase to 2 MB, there was a large amount of applause across the venue.
    - Appeared as if the consensus view at the conference was that going beyond 2 MB was too risky for
  + Jonathan Toomim, presented technical arguments as to why 2 MB was safe
    - Most miners seemed to agree with this logic.
* Bitcoiners do not like being told what to do, they
  + People feel like they own Bitcoin and they want to be in control. Bitcoin XT was thrust on them from above, with no effort to make the users feel like they are in control, like it was their decision.
  + Most wanted Gavin to listen to their advice and try to | increase the blocksize limit again with a more collaborative approach,
    - Just wouldn’t do this, as he did not believe it was the users’ choice.
* If w cannot resolve this dispute now, when only a few hundred people really care about it, what hope does Bitcoin really have? I
  + Immense pressure which would be exerted on Bitcoin by major economic and political players Bitcoin grows. It
* I began to realize that the rules of the network had to be robust.
  + It had to be really difficult to change the rules, otherwise it would not stand up to the pressure from the main financial establishment, which would surely emerge as the value of the system increased.
* The status quo had to be defined somehow.
  + Had to be dynamics in place to ensure the status quo succeed, there had to be dynamics in place to ensure the status quo would survive and prevail.
* Churchill: “Democracy is the worst form of government, except for all the others.”

## SegWit 59

* Pieter Wuille gave a talk on something called Segregated Witness (SegWit). SegWit is a way of increasing the Bitcoin blocksize, without the new client being incompatible (i.e. it was a softfork rather than a hardfork
  + New transaction format, where the signature would not need to be included in the old block, which still had a 1 MB limit.
  + 1 MB blocksize limit was removed and replaced by a 4 million unit “weight limit”. The weight limit was defined as four times the amount of non-signature data in bytes plus the amount of segregated signature data, in bytes. This
* Luke Dashjr had figured out a hack, which made SegWit possible as a compatible (softfork)
  + Regarded as one of the most extreme small blockers and was another hate figure in the large block community,
  + Strong technical understanding of Bitcoin and his apparent had a very strong technical understanding of Bitcoin, and his app
* Seemed like a brilliant win-win proposal. The network could get to 2 MB blocks, yet we avoided the problem of the upgrade being incompatible. In
  + Perspective of old wallets, the new style transactions would be perspective of old w
  + However, the wallet would still see the transaction and recognise it as valid once it was included in the
  + Transaction capacity could potentially increase faster than with a simple blocksize limit increase
    - Hardfork, because we would not need to wait for everyone to upgrade
* Solid win for Bitcoin,
  + Brilliant tactical move,
  + So good there were no valid arguments against it.
  + Large blockers would have been stopped in their tracks with their campaign for a hardfork, and tal time would have been bought. I
    - Thought they had been outmanoeuvred by what they considered to be an ingenious proposal.
* Proposal removed the limit and replaced it with something else, thereby negating the argument. However,
  + SegWit was exceptionally complicated and almost nobody understood it
  + It had a deeply cryptic and confusing name, which sounded highly suspicious to the large blockers
  + Additional stalling mechanism, to stop larger blocks.
  + Without really understanding SegWit, they opposed it.
* Misconceptions and misunderstandings
  + SegWit is not a “real” blocksize limit increase, it only compresses transactions (it
    - Upgraded nodes do see blocks larger than 1 MB
  + Chain of digital signatures, which SegWit removes thereby breaking the chain and creating a security risk;
  + If a miner does not upgrade for SegWit and produces a block, this block will be rejected bY the upgraded clients.
    - Risk of a chain-split
  + Unable to send funds to a user who has not upgraded:
  + Upgrade could be reversed, and then coins inside SegWit outputs could be stolen by anyone
* Most people didn’t really understand the basics of Bitcoin transactions in the first place.
* Even Jeff Garzik didn’t seem to understand it. He thought there would be “two buckets” for fee bidding: one related to the old 1 MB limit, and one related to the new
  + Extremely difficult proposal to fully appreciate and understand,
  + Simply not possible to communicate this to
  + In order to get the benefits of SegWit and the increased blockspace, user wallets had to upgrade to support the new increased blockspac
* Also fixed a number of bugs, namely third party transaction malleability and the non-linear scaling of sighash operations.
  + Ability to change the transaction ID of a Bitcoin transaction before it gets confirmed in the blockchain,
  + Necessary for a layer-two transaction network called lightning.
* The non-linear scaling of sighash operations means that, as the number of inputs in a transaction increase, the number of hashing operations required to validate the transaction increases quadratically
  + Attackers could create transactions which took so long to verify that the network could grind to a halt. This issue was actually one of the main reasons cited by small blockers for opposing blocksize limit increases
  + Computer many hours
  + Fixing this issue was a prerequisite to a blocksize limit increase.
  + Derided the large blockers for complacency in overlooking this weakness and lacking an adversarial mindset.
  + Believe Bitcoin was almost indestructible or antifragile, as
  + Hard work and caution from the development team, but that wasn’t
* Problem, again, was the complexity; most Bitcoin users had no idea about these problems and did not care about them.
  + More than just engineering and computer science. It is also a social system, a live payment system, an economic system, and a financial system.
* Not until November 2016 when SegWit was was finally released in Bitcoin Core,
  + , a tightening of the protocol rules
  + An activation methodology
    - If 95 percent of blocks signalled support in a 2,016-block difficulty adjustment window, the softfork would then activate, after another two-week grace period. If, after 12 months, the activation had not occurred, the upgrade would be aborted.
* To the large blockers, this activation methodology was inappropriate.
  + You never get 95 percent agreement on anything, they argued. This
  + Any small coalition of miners, small coalition oft
  + Large blockers tended to see miner flags as a vote, a decision-making process.
  + Smaller blockers saw the flags as a signalling mechanism or safety feature.
    - To ensure a safe transition to the new rules. It was not considered a political voting process.
* Last three Bitcoin softforks had all activated using this same 95 percent threshold: BIP 66 (restricting signatures to DER encoding) in July 2015; BIP 65 (Check Lock Time Verify) in December 2015; and BIP 68, BIP 112 and BIP 113, three
  + Previous soft fits had not progressed perfectly
  + Of BIP 66 in July 2015 caused a chain-split for a few blocks, as miners appeared to fail to upgrade for the softfork, despite flagging that they had upgraded.
  + Considerable uncertainty as .

## Lightning Network 66

* SegWit provided the option for users to create transactions that couldn’t be altered by malicious third parties
  + (third party transaction malleability).
    - Without this fix, lightning would have been too complicated to implement.
* From Joseph Poon and Thaddeus Dryja in February 2015.
  + Idea appears to have originated from Satoshi 43
  + リツ used to open payment channels
  + Network of channels.
* Architecture made much more sense for a high capacity and cheap global payments system.
  + “Broadcast to everyone’
  + All participants are then required to process this transaction to see if it’s a payment to them.
    - Inefficient, especially for small payments.
  + Needed as a base layer of a monetary
    - Improvement in efficiency and uses a more logical payment-network structure
    - Directly to the payment recipient, more of a peer-to-peer architecture.
    - Bitcoin’s proof-of-work mechanism, is therefore used as a dispute resolution service.
* 2015 had been a period of huge success. In 2015, Expedia, Overstock, TigerDirect, Newegg, Dell, Rakuten and Microsoft had all started allowing customers to pay with Bitcoin in
  + Using on-chain transactions.
  + Many of these merchants did stop accepting Bitcoin and the large blockers were proven largely correct. The phrase “don’t let the perfect be the enemy of the good” comes to mind
* To the smaller blockers, Bitcoin was not a business, nor a payment system taking on VISA, Paypal and Mastercard.
  + Main priority, which was a robust and new form of money.
* Not just a difference of opinion: to the small blockers, their priority was a smart strategic move, while the large blocker priority was naive.
  + If Bitcoin gains traction, these payment services can simply lower fees and speed up transaction times
  + Reason these centralised payment systems had not done this was a lack of competition and some admin-related legal issues, which could be overcome.
  + Contrast, becoming a new form of money, capable of unblockable electronic transactions, was something the traditional financial establishment would be unable to compete with, This
    - Disagreement about time preferences.
    - Not therefore a choice between a payment network and robust monetary system, with large blockers
    - The fast and cheap payments network idea would not result in a model with a sustainable competitive advantage.
    - The only way to effectively have both: they argued, was with a layer-two solution such as lightning.
* This of course led locked inside of lightning channels were subject to credit risk
  + Sufficient liquidity to facilitate payments.
  + Can scale effectively into a cheap, reliable payment network.
  + Required the receiver of the chain Bitcoin payments, for instance it required Transaction to be online and interact with the sender, something on
  + Ensure they have sufficient liquidity, and prevent theft from their channels.
* In the long term these issues would eventually be hidden away from the user and third-party services or
* Complex, technically elegant, but impractical solutions. Small blockers were said to lack business acumen and could not see that a simpler solution to these issues was required.
  + To date, large blockers have been shown to be mostly correct,
  + Merchant adoption of Bitcoin at the end of 2015 appears to have been more significant than lightning adoption today.

## Bitcoin Classic 71

* Waves of distributed denial of service (DDoS) attacks on Bitcoin XT
  + Anonymous small blockers appeared to defend the action on BitcoinTalk, referring to it as a “counter attack”.
  + Attack did bring to light, however, was the importance of a large, distributed and robust P2P network, something Bitcoin XT had not developed at this point.
  + It was never known who was behind these attacks, although rumours did circulate several months later of a Botnet operator who was paid anonymously
  + A rare example of a tactical blunder from the small block camp, assuming of course this was a about persuading people to join one’s chosen side, and
* 2016, Brian Armstrong, the CEO of Coinbase a blog in support of larger blocks.
  + Luckily, bitcoin has a built in upgrade mechanism with an elegant design. If a majority of bitcoin miners “vote” for a particular upgrade then by definition this is the new version of bitcoin.
  + Whatever chain had the most hashpower behind i
  + Bitcoin nodes did enforce certain rules; a block had to comply with these rules or it would be ignored,
  + If miners just change the rules like that, it would cause a split in the chain and result in anew coin. The coin following the original rules would continue to be Bitcoin.
  + All user wallets, even though they don’t enforce all the protocol rules, still enforce some of the rules.
* Different light wallets enforce different subsets of the rules.
  + Required strong clarity with respect to what was a network rule and what was not, to ensure there was always little doubt as to which was the longest valid blockchain.
* What happens if the miners create new inflation above the 21 million supply limit and gave these coins to themselves;
  + If miners did that, all nodes and wallets would regard that chain as invalid, 1
  + Is defined as the most work chain, whether their nodes were following it or not. If a user wanted to be part of Bitcoin, they may need to download and install new node software to make sure they followed the most work chain, whether it breached some rules or not.
* The extremists on both sides appeared convinced that they were correct, however they were both being closed-minded.
  + Assumed people would behave just like.them
  + Different people had different ideas and visions and would therefore behave differently. The larger blocker visions appeared to rely on almost everyone agreeing with them, while the small blocker vision appeared to require any significant minority to agree with them. From
* Opposed a blocksize limit increase, as it would make the cost of running a node too high, which could reduce the full node count and cause centralisation.
  + Not enough ! relay nodes.
  + Communication would therefore be centralised around a few large hubs.
* End users would be able to run Bitcoin clients which fully validated all the protocol rules, which could undermine the decentralisation of the enforcement of the protocol rules. The large blockers never seemed to even understand this concern and
  + Sides were talking at each other, rather than building up an understanding of the others’ point of view.
* A 51 percent mining attack could steal user funds,
  + All miners can do in a 51 percent attack is double spend transactions where they have a valid signature for two conflicting transactions.
* Last sentence in Bitcoin’s whitepaper, which read as follows:
  + Vote with their CPU power, expressing their acceptance of valid
  + Often circulated However, it is not clear that Satoshi shared this vision at all. Indeed, the whitepaper also states:
    - Consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such creating value out of thin air or taking money that never belonged to the attacker.
    - An invalid transaction as payment, and
* Satoshi makes clear that nodes do enforce certain rules.
  + The whitepaper in context: it was primarily about a potential solution to the double spend problem.
  + Running nodes to enforce the rules was not the key innovation of the system; proof. Of-work mining was.
    - Order of transactions.
* Fundamentally different visions as to how Bitcoin worked
  + Give miners free rein with respect to the blocksize,
  + Confusion in the space
    - Large blockers often claiming the majority of the hashrate was able to do almost anything, without adding any hashrate was
    - The idea users would download a new client to follow a longer chain that stole coins from some users and gave it to the miners made little sense. If
  + Argument about the most work chain defining Bitcoin as they thought it helped their cause.
* deleted) expressing support for Bitcoin XT.Almost immediately afte that, Coinbase was removed as a recommended wallet on the Bitcoin.org website.
  + One of the main information sources on Bitcoin and the website was originally set up by Satoshi
  + Infuriated larger blockers, who believed it was childish and divisive.
    - Proclaimed that Coinbase had effectively announced its intention to proclaimed that Coinbase had
    - Strengthen the resolve of the larger blockers and further divide
    - In the same blogpost, Brian included a screenshot
      * Indicated that the top three mining pools all opposed Bitcoin XT.
* On January 14, 2016 there was another seminal moment in the
  + 2016 Mike Hearn, frustrated by lack of progress ragequit
    - W hen parts of the community are viciously turning on the people that have introduced millions of users to the currency, You know things have got really crazy.
    - Appeared to have caused a 10 percent collapse in
    - A couple of days after Jihan Wu tweeted the following:
      * Racist and unfair opinion against China bitcoiners. Explaining why he could not get enough support 49
* Jihan
  + co-CEO and co-founder of Bitmain,
  + Clearly angry at Mike’s ragequit, however the criticism is somewhat ironic as Jihan would soon establish himself as the leading player in the large block camp
    - Blamed the lack of support for XT on Chinese loyalty to the oppressive status quo and drew parallels to the widespread support of ppressive status quo and drew
    - Post also explains why 8 MB was originally chosen the limit for Bitcoin XT; eight is a lucky number in China.
      * Community all the time. So this choice wasn’t based on any kind of scientific analysis.
      * Embarrassment, but nonetheless, we compromised and did it.
      * Miners changed their tune. They announced they would never run anything except Core, period, end of story
        + Thus compromising further was pointless
* Large blockers needed a new cause to rally around. Called Bitcoin Classic.sı
  + Simple, one-off jump to a 2 MB limit,
  + Gavin would be the lead developer, rather than Mike. Jeff Garzik now also supported the proposal and was listed on
    - Classic appeared to have a better chanc o succss than XT, with its much more moderate approach
    - A precedent had been set, a campaign to remove a Bitcoin consensus rule had just failed
      * Were trying the same thing again.
      * Jonathan Toomim had argued at Scaling Hong Kong that 2 MB was a safe limit, and he was an advocate of Bitcoin Classic. Small blockers nicknamed the coin “ToomimCoin”,
  + Released on February 10, 2016
    - Activation methodology was almost identical to
    - No effort to obtain widespread consensus before encouraging users to run the client
      * Large blockers did not want to do this, N
      * Lack of trust,
      * Aggressive behaviour from the small blockers.
      * Therefore kept the 75 percent miner activation
        + Flag in the Block header was considered a safety . signa ling mechanism, indicating that everyone was ready to upgrade.
        + The upgrade itself is not meant to be controversial or voted on.

In April 2012, the P2SH softfork activated with a 55 percent threshold

Miners who had not upgraded produced invalid blocks for several

Considered a problem and therefore a new 95 percent threshold was selected, which has been

* 1 do not think small blockers opposed miner votes in order to gauge their opinion. However, there is a distinction between gauging the opinion of miners and flags in the block header which activate changes to the consensus rules
  + Critical part of network security and combining activation with miner voting over proposals was dangerous and inappropriate.
  + A subset of the activated and the network split, the larger block nodes would consider smaller block chain as valid, while the smaller block nodes would consider the larger block chain as invalid.
    - Means is that, if the smaller block chain ever took the proof-of-work lead, the larger block chain could vanish from existence, known as a wipeout. Thi
  + Contentious split, this asymmetry created an advantage for the small
    - Create the opportunity or financial speculators to back the coin on the smaller block is an short the coin on the larger
    - The activation methodology could. Require that the first block at the activation point was greater than
* Was told this wasn’t an issue, since support for the larger block side was overwhelming
  + He said that it’s best to keep this issue quiet, better to not interrupt an enemy while they are making a major mistake, h
    - Lesson was eventually learnt
* Another self-imposed disadvantage, the 75 percent rolling activation windows.
  + Meaning that if 750 blocks flagged support for Classic in any consecutive 1,000 block period, it would activate
    - Means that, at the time the first large block was produced, approximately 25 percent of the miners would still be mining the smaller block chain. H
* Almost guaranteed to cause a chaotic split.
  + Regardless of numbers on either side, the likelY outcome was a victory for the smaller blockers.
  + Gavin was not concerned by this since, in his view, support for larger blocks was overwhelming.
    - It seemed like his frustration with the situation had clouded his judgement to some extent, and he was losing his patience.
    - Had Gavin fixed this, the same people would have just moved on to additional problems with Classic they had identified
    - The situation had clouded his judgement to some extent, and he was losing his patience.
    - Had Gavin fixed this, the same people would have just moved on to additional problems with Classic they had identified.
* Classic was growing in popularity Almost all the Silicon Valley-backed venture companies in San Francisco, , such as Coinbase, backed Classic.
  + Larger blockers had the momentum
    - However, the number of blocks actually flagging support for Bitcoin Classic was fairly low, and not many users appeared to be running Classic nodes,
* February 2016, a Satoshi Roundtable. Continued until 2020
  + Brian Armstrong blog post
    - The biggest risk bitcoin right now is, ironically, one of the things that has helped it the most in the past: the bitcoin core developers.
    - Poor communication skills or alack of maturity
    - Perfect solution exists they seem ok with inaction, even if that puts bitcoin at risk.
    - Need to form a new team to work
      * Welcoming of new developers to the community. Willing to make reasonable trade offs, and a team that will help the protocol continue to scale. You’ll be
* Small blockers, this war not about competing teams; it was about competing network
  + Bitcoin Classic wasn’t even really a competing team at all. It was largely the same code as Bitcoin Core, with a few parameters changed. There were already competing teams, with a different codebase to Bitcoin Core, that implemented Bitcoin. These other Bitcoin clients were written in different languages, for : nstance Libbitcoin or BTCD. The failure to appreciate the distinction between competing coins and competing teams was a pivotal mistake
    - The large blockers wanted larger blocks, but didn’t understand how Bitcoin work or how to conduct a hardfork,
* Larger block side were in a stronger position than had ever been, while the smaller blockers still had some tricks up their sleeves. Bitcoin felt on the brink of a catastrophic failure.

## Hong Kong Roundtable

## Faketoshi ୨୨

## The DAO 106

## Scaling III - Milan 1188

## Bitcoin Unlimited 122

## Exchanges 134

* In the year or so that the war had been raging, the industrial landscape of the cryptocurrency ecosystem had changed considerably.
  + Had changed considerably. Significant change was une emeiB
  + US-based companies backed by Silicon Valley, such as Coinbase, were staunch large blockers, the opinions of these newer players was largely undecided.
  + Without much prior baggage in this war, these exchanges were more pragmatic and appeared to be these exchanges

## ASICBoost

* Despite the denial, Bitmain did appear to admit to using what was presumably covert ASICBoost on the testnet and therefore it was probably implemented in their hardware.
  + Claim that they owned the ASICBoost patent in China and could egally use it if they wanted to, before going on to defend echnology as a legitimate mining optimisation. A
  + More effective munication policy would have been a simple, clear denial, rather defending ASICBoost in the hypothetical scenario that Bitmain defendin
    - Even if Bitmain was not currently using covert ASICBoost, the potentially intended to and therefore the spirit of Gregory “ potentially intended to and therefore the spirit of Gregory’s opposition to SegWit. It may have been all about the money.
    - Pollit, “if the restate Bitmain’s position in the blocksize war, that they would not run SegWit as the conditions of the Hong Kong agreement had not un SegW course, to the small blockers, it was never intended to a quid pro quo.
  + Extension blocks were originally proposed by SegWit co-author Johnson Lau in 2013, however the idea was largely abandoned as the experience of sending coins from the extension block to the main chain was not seamless. In contrast, with SegWit, where this process straightforward.
* Appeared to be important to them was that idea was not developed by Bitcoin Core. At this point, developing this idea was not developed by Bitcoin Core. At this point, ucz significant issue to the larger blockers, not a blocksize lim.it increase itself.
* The ASICBoost nato considered a significant threat to Bitcoin. Exclusive rights to use the technology and then dominate the mining industry due to the advantage the technology could provide.
* Industry due to the advantage neip patent for quite a high price and then, in March 2018, placed the patent into a defensive patent pool,
  + Then, in March 2018, p such that the patent could used except to defend against other patents
  + 2018, blocks on the Bitcoin blockchain started indicating the use of overt ASICboost.
    - Overt ASICBoost is far simpler and more ASICboost. 112 Overt ASICBoost 1S Iai Sump and more efficient than the covert
    - - As for the patent, was never clear exactly who purchased the patent, nor could one it was never clear exactly who purchased the patent, nor could one put the patent into the defensive patent pledge.
  + ASICBoost accusation appeared to have a very little impact in the larger blocker community In general, they did not understand the accusation and dismissed it as more Bitcoin Core propaganda and lies.
    - Little impact on persuading more eople to join the small block camp,
      * . However, it certainly did and have a very significant view impact in hardening the views of many

## Dragons’ Den 148

## 151 Litecoin

## User-Activated Softfork 157

## New York Agreement 172

## Bitcoin Cash 187

## SegWit2x 197

## Victory 214