California Gathering 2016

# Transcription introduction

Some Bitcoin developers and miners gathered together during the end of the July to socialize and become better acquainted with each other. The following discussions were live transcribed by an untrained volunteer with attribution removed as per Chatham House rules. In bitcoin, discussions can move very quickly, which can cause an increase in errors, including semantic errors, when typing in real time. This text was not produced from an audio recording. Any errors are the fault of the transcriber. We hope that by sharing these notes with the broader community that a broader discussion can be cultivated and we can all get to better know our perspectives and each other.

PDF: http://diyhpl.us/~bryan/irc/bitcoin/cali2016.pdf

Text: http://diyhpl.us/wiki/transcripts/2016-july-bitcoin-developers-miners-meeting/cali2016/

# Some breakfast notes (2016-07-30)

((Some words from breakfast when I ran into some folks.))

Hashrate and price are dependent. Sounds like it. Hashrate is protection. Additional volume, you're decreasing the price. It seems that way.

With today's hashrate, compared to two years ago; because it's so high, ... well, to me, ethereum hashrate is also more elastic than bitcoin because you can mine it with GPU and you can rent GPUs from genisys mining, they have a datacenter for GPU mining, you can rent them by the day; you can rent GPUs from amazon, and so on. If it becomes 10x more profitable to mine, the hashrate can go woosh. But in bitcoin this is not the case because ASIC production takes longer.

Basic economy rules changed in ethereum all the time. You can never be sure what they will be on the next day. Solidity, for example. They should change it. PoW to PoS for ethereum. It's a bad idea. It's taking the roots of the economy and replacing it for different one.

If you buy a financial instrument, like a bond or something, where there is a definition of the financial asset, that's important. But now it’s whatever the Ethereum Foundation decides.

The ethereum policy is about the gas, so it can be cheap or expensive for smart contract one day. Gas price will be changed, so a contract could just stop working the next day.

You can be sure that a building could be running for 100 years. But if you are changing the rules in the contracts, you cannot rely on that. The people making the decisions in EF have a conflict of interest regarding TheDAO. I would say, in my opinion, rescuing TheDAO was bad for Ethereum. They were doing it because they were losing money.

Ethereum data blockchain size is growing exponentially. It is a big problem for them. A lot of garbage in there.

How would you convince people that you cannot trust that blockchain? And what about the people who feel disenfranchised about any blockchain at all? It's good for someone other than you to make a mistake, so that people can realize what the difference is. When you have a warning after that, it's no longer hypothetical.

In ethereum, there are not that many nodes. How could there be, you can look at how long it takes to sync as it continues to exponentially grow, it will at some point be impossible to sync. Also, each node won’t be able to run the smart contracts anyway, if it's growing too quickly.

.... (breakfast to venue transition) ....

Someone needs to make beanie babies with private keys embedded inside. How much is a bit? It's a millionth? Do we have enough chairs? 25 total chairs. Well there were supposed to be 25 people. Maybe we should start without the moderator. Maybe we should introduce ourselves. Oh there he is. Since we are all introduced, should we get started? Who would like to break the ground first? How about review of other conversations? Lessons from Ethereum. Like an example, it's a good example. Both good and bad examples. Better cooperation and communication in the future. Lots has happened to improve communication, it would be good to look at how that has improved things.

After this, it would be nice to talk about what developers are working on and interested. Miners as well. Maybe voice your concerns or something. It would be good to get to know each other. Maybe smaller groups. We are all facing each other. It makes it feel serious when we are sitting like this. Another good topic would be fungibility.

Lunch will be arriving at noon according to the person from the building. There are some food containers that are labeled behind us

Introductions

What are you guys working on? What have you previously done and what are you working on now?

I was working on a cloud mining platform, the only one that wasn't a ponzi. Before that, I was working on an exchange. I believe it is the only one where nobody went to prison [laughs]. At the moment I have been working on code for the wallet to work better and faster. Improving the wallet software. There is also an issue of initial block sync. It's more expensive to do an initial block sync, than keep up with the network. If you have a growing blockchain, then the time to sync is related to this. This was presented at the Scaling Bitcoin Montreal. It's an inherent property. It's the part where it takes forever the first time you run Bitcoin Core. Maybe in 5 years time, perhaps nobody would be able to download the blockchain. It takes a long time to validate that as well. It's not just the time to download it.

They have also been working on the same problems. They would like to exchange thoughts and experience on that.

Okay sounds good. Next person.

Analyzing bitcoin and how it works internally. I was searching for potential vulnerabilities in Bitcoin Core. At least, serious vulnerabilities. I also have an economics degree and I understand how Bitcoin functions on an economic level. This also applies to ethereum and similar altcoins. I understand the vectors of interest in blockchain and bitcoin from different roles like users and miners and how they impact each other.

Could you talk about what you are working on now?

We have been designing mining chips and thinking about the future. We are also working on and building marine shipping containers for bitcoin mining. Immersion cooling. It's not air cooled. It's approximately from 11 to 12 petahashes in one shipping container. Uses a half megawatt for power. Three's a big cable this thick for powering the container. You just need the power at your location. You could install it inside a data center. If you use immersion cooling, you can continue long life even with partial cracks and break-ups.

How do you get rid of the heat from the whole container? Are you pumping water in?

Also, what would you like out of this discussion?

Practically, I am in a strange position. I am working for a company. And it's also an inertial company. At the same time, I like the idea of bitcoin. I was searching for something similar for many years. I was thinking about electronic money and it's one way for most other things. I like bitcoin itself. Even if the company will die, I will still continue to work somewhere related to bitcoin. I like bitcoin and I would like to keep it up and running and help people understand why it is working.

Any concerns or issues that you would like to talk about? Ethereum and bitcoin economics.

I have been working on Bitcoin Core since summer 2011. I have been responsible for a lot of the code in Core and making it faster. I found several significant bugs. I am also the primary author of libsecp256k1. I have been working on segregated witness proposal. That is the main thing I am working on right now. Getting Bitcoin Core to version 0.13. And later a version with segwit included and activated on the network. In the near future, I would like to work on Schnorr signatures, signature aggregation, better scripting language as a successor to segwit making use of its versioning support, and various other ideas for improving things in the short term.

He is working on ATM machines, bitcoin wallet, and mining. And a hardware wallet. One of his interests is how to make mining in China more decentralized. Because the centralization of mining in China, there's more concentration. Developed at 10 nm. Decentralize the hashrate in the future.

I have been working on Bitcoin Core since 20xx. I have been maintaining a different version of Bitcoin Core called Bitcoin Knots. I have worked on getblocktemplate. I have been working on a hard-fork proposal but I don't know if it's going anywhere.

An open-source mining pool, .. he's working on a blockchain explorer, btc.com, and also an open-source mining pool. It's not part of Bitmain.

I started working on Bitcoin about two or three years ago. I work on NBitcoin. It's like bitcoinj but it's dot NET. I have also made a block explorer on bitcoin.ninja. My goal with my library is to help with some requests coming in from Core. I have been contributing to Bitcoin Core because as I want to stay close to the latest testing, I need to be able to understand this source code. So I started contributing to Core earlier this year. On bitcoin.ninja, it was the first block explorer that implemented segwit. Another user of NBitcoin is smartbit, a block explorer, a user-friendly block explorer which implemented segwit because they are using my library. I am working on fiat money on the blockchain by using colored coins protocol. My goal is to make it scalable, using payment channels and payment hubs. That's why I am interested in segwit and checksequenceverify.

I work for MIT DCI but I am given the freedom to work on whatever I want in Bitcoin. I started on the boring stuff. Like the build system and the release process and the more internal development processes. My goal and reason for getting involved was to get the development process more specialized where experts wouldn't have to know every single detail. At the moment Bitcoin Core is difficult because you have to know about more parts. I want some people to be able to be specialized areas in some areas but not others. One example is libbitcoinconsensus which we got going in 0.10 a while ago. It's a library that uses the same code as Bitcoin Core that lets you verify transactions. My goal and the goal of others -- increase modularization and libbitcoinconsensus functionality. Make it independently. I am working at the moment on the p2p functionality, getting it pushed on its own, to live separate, so that it's walled off from the rest of the code.

I do many different things in the Bitcoin space. I have many different jobs, you could say. A lot of it has common threads through it. I am usually thinking about 5 and 10 year time frames with this idea that Bitcoin exists with a careful balance of incentives and balance. Much of the work I do is trying to expand the space of opportunities that Bitcoin can be successful in. Make it work under more conditions, make it work under weaker assumptions, make it work in the presence of malicious actors, and work to expand the technology to expand to more applications. This overlaps with the work I do at Blockstream where we take Bitcoin tech to finance companies and convert them to Bitcoin tech and use the income from that to make more Bitcoin infrastructure tech investments. When I see an incentive problem, a political problem or something, I search for tech that improves that and take it to others to get the solution built.

Okay, thanks.

When I got into bitcoin, there weren't tools for securing bitcoin. I started to work on my own libraries to build my own applications. I built a wallet app which I could use to store my own coins securely. I began to contribute to Core and make the wallet. I realized it was hard to make contributions. It was because of the nature of the technology. I found the team to be amazing and really cool people. There was a lot of great collaboration. It was just hard to change things. After a while I figured out how to get into the process and start making contributions. Most recently I have worked on the segregated witness stuff. I began to get concerned about social attack vectors. There's cryptography but then there's social attack vectors. People began to be very hostile and negative. I noticed that this could be a very major weakness of the system where people could come and create polarizations. We have now seen this in a capitalized network. This is where I have been focusing now, trying to figure out how to prevent the social attack vectors, how to improve communication with the community and become stronger. Everything from the last few years has helped our immune system. We will be facing larger adversaries in the future. There will be adversaries with much larger resources to throw at us and I want to be prepared for that.

Okay, thanks.

I think that people don't see each other face-to-face might encourage some of the social media attack vectors.

Okay, my story is a little bit different. Most of my time is taken up on non Bitcoin software. I am a lead developer for a communications software and radio signal. That's my professional life. I have been in the security space for a few decades. I have been in Bitcoin since 2012. I come at this with a different perspective. Our non Bitcoin project has a much larger code base, much smaller user base and also it's not insanely politicized. It's interesting to compare how that open-source project compares to this one. I did one of the python reference implementations for bip32. My contributions have been fairly small in terms of direct code for the project. I do considerable work in the machine learning space, mostly related to radio signal processing. I am interested in applying these machine learning techniques to blockchain and network analysis for anomaly detection or analysis on fungibility or forensic type stuff. I am interested in applying the same machine learning techniques from radio signal processing to blockchain analysis.

It's a platform. It's not a wallet. It's a wallet platform. Also building a mining factory. Building both a mining factory and also a mining pool with about 70 petahash.

Okay, thank you.

I am probably most well known for CHECKSEQUENCEVERIFY which recently activated. I worked on that because I was interested in lightning network. We needed checksequenceverify and a malleability fix, which is segwit. Now that one is deployed and one is close, I have a research-interest in making lightning network happen. There is enough people working on lightning for payments. My interest in doing distributed exchanges, credit currencies, like IOUs instead of hard currency. Debt-based currencies on lightning network. I am doing research on new scripting language and tools. Either this would be an opcode extension, or perhaps entirely new languages, and the tooling infrastructure around so that you could write a smart contract and compile it into a script. Distributed exchanges, asset issuance, and the tooling to provide the smart contracts related to that. You could use the same software to setup other networks for tech such as credit-based money.

Lightning works across multiple networks. You could swap a US dollar for a yen. If you have lightning on litecoin and lightning on bitcoin, I could send a lightning payment on bitcoin that releases a lightning payment on litecoin. That's how you exchange. You can do automatic trade across the payments.

Oh that's interesting. Okay.

Also very interested in fixing fungibility. Finding ways to make payments more private and hide information that is currently being leaked on the blockchain. Maybe using crypto tools or better coinjoin or things like that.

Okay. ... coinjoin ...

Most of my work has been in doing fintech clients, like smart contracts. Figuring out how to build the systems they want to build, like on top of bitcoin, more modular and scalable. Like replacing ethereum with better bitcoin tech. On tech I do security review and peer review. Strong interest in how to scale this system. Block propagation incentives and better blockchain designs that scale better, like treechains. UTXO commitments.

Hi. I have read a lot of content. To start with, I have reviewed most if not all of the public bitcoin scaling proposals. I have also read all the emails to the bitcoin-dev mailing list. And I have read all of the forum posts in the R&D subforum on bitcointalk.org ((group laughter)). Wait, there's more, I'm not done yet ((more laughter)). And I have also read and memorized a good chunk of all the IRC chat logs, although this is an incomplete effort so far. I also organize lots of information in the form of bookmarks and links. I am somewhat of a "librarian", in that aspect. I would like to ask before we move on, who here contributed to segwit by show of hands? And who here contributed to peer review of segwit by show of hands? Thank you.

Anything else? Okay. Great.

Involvement in electronic cash protocols from 93-95. In ecash systems, it was completely fungible. However, those ecash systems were completely centralized and they were shut down. When I saw bitcoin I saw that it wouldn't be shutdown because of its decentralization, but its fungibility is terrible. For fungibility, bitcoin uses decentralization. Confidential transactions, which mixes with coinjoin well. Encrypted transactions. Sidechains as a way to make more complicated changes to bitcoin, so you can have different chains with different features. The previous electronic cash systems had something called blinding. I would pay them money, they would give me an electronic coin, but even you inside the bank would not be able to tell who I was. It has properties similar to zerocash in that it is very anonymous. The point for fungibility is, you know, say TheDAO hacker was using zerocash. You can't freeze the coins or take the coins, because you can't identify them. You can't see the coins move. It's completely unobservable.

Completely transparent?

Opaque, so you can't see it.

I think fungibility is the big problem for bitcoin. We have to improve the technical fungibility. Schnorr signatures can help. We also have to improve decentralization. Otherwise we will have a fungibility problem. At the moment I think we have a risk, that hasn't been attacked yet, but we're exposed. There was something in the news about somebody in Europe, someone bought something with bitcoin, it was in the news and I don't know if it was correct or not. Well the news agency retracted this. Well, anyway... it doesn't have to be true to be a problem anyway. Biggest black market is supported by US dollars. Nobody seems to remember that many guns are purchased with US dollars. So anyway I think that, most of the utility and value of bitcoin is because it's fungible, permissionless, decentralized, and if we let that fail then people will lose confidence and interest in bitcoin.

If we knew how to solve this technically, if we had a space-efficient secure protocol to do fungibility, we would do that right now. There are things that we know how to do, but some things we haven't figured out yet. We can't always immediately solve these problems through technical means.

To add to that, it appears that any approach that makes bitcoin scale better, makes it more private and fungibility. So if we don't broadcast as much information, it helps improve fungibility. Long-term changes can improve this. It basically means that you broadcast less data.

This is why we support and develop lightning network. There should be many additional layers to expand and provide more functionality. Lightning network might help fungibility. We probably can't use lightning for everything. It helps. Lightning can provide the capacity for payment channels, like hundreds of thousands of transactions per second in multiple directions. It's not just for bitcoin, it can be connected to all the altcoin chains and any coins that exist can be connected together into lightning network. We don't have a complete solution. But we have many things that help somewhat. We're trying to do things, but there's non-protocol things we could do -- like making sure the hashrate is in different countries, with more companies, with different control, anything we can do and maybe even positive news stories about bitcoin to balance the false negative stories. There are multiple dimensions and vectors through which we can work through issues.

I learned bitcoin in 2012. My training was computer science. I found an interesting project regarding how mining can make a decentralized system for currency. Since I learned bitcoin, I contribute a lot of ideas, especially in the consensus protocol. Since I did not have enough skills, I contributed ideas. In the Hong Kong conference at Scaling Bitcoin last year, I wanted to do more and learned segwit. I learned coding and began to contribute. Recently I am trying to propose new scripting systems like MAST and new opcodes that might be useful. I think the consensus protocol in Bitcoin is very unique. It's not like Linux. If you don't like a distribution of Linux, you make a fork yourself. We have hundreds of distributions of Linux and that's fine. But in Bitcoin, the bitcoin consensus protocol needs only one chain and one consensus otherwise we have problems like Ethereum is presently experiencing. That's why I am particularly interested in these topics.

Okay, thank you.

We are manufacturing Antminer S9. Most of our S9 customer are from Western countries especially the United States. In the next one or two weeks, we will announce another miner. We recently acquired a company. We will open-source most of btc.com to help bitcoin ecosystem. Bitcoin mining pool is functional on btc.com and that will also be open-source. In the future, many miners in many countries can deploy their mining pool easy based on this mining pool. The most important today on bitcoin fungibility is block size.

Do you guys have any questions?

I came into contact with Bitcoin in 2011. At that time my goal was simple. It would potentially be a good asset to keep. At that time, there was a lot of negative press about bitcoin in Chinese social media. So he was going out there to .. bitcoins.. like repetition, and he developed it in the public space vigorously along with some other people during that difficult era. He's the one who translate Satoshi's whitepaper into Chinese. He's also the one who presented Bitcoin to the Chinese media until the situation turned around in 2013.

In the late part of 2012, I started to get into the bitcoin mining aspect of bitcoin. I was trying to develop the technology and also trying to fathom the economy around that industry. At that time, I was trying to invest in the mining only and I bought shares in a mining company. I also invested my own money plus investor money to purchase mining machines. Unfortunately at that time, the vendor couldn't deliver. We suffered a great loss from that investment. That experience compares us to getting into the mining industry myself. I found my partners and we started to invest and start to develop mining machines by ourselves because of that bad experience we had.

Back in that time, the mining community has come to the viewpoint that if I can control all the mining hardware in my own hand, then I can benefit most from this control. But this is running against the principle of Bitcoin network. I actually vehemently against that philosophy. We also observe that over the years those mining companies that practiced that, have inevitably failed and floundered because of their bad choices and poor judgement.

In the future, we will continue to manufacture the mining machines. We will only keep a small percentage of the machines for ourselves. In later sessions, I would like to share that data with you to verify that.

For myself, I would really would like to see the .. of the bitcoin protocol because I have now invested so much financially and personally into developing this protocol since 2011. I stay up until 1am or 2am in the morning to debate or to talk with people on social media. I work late nights to make sure everything goes smoothly. Just to realize Satoshi's vision that Bitcoin is a decentralized system that cannot be controlled by a single organization or a single entity or anyone who wants to take control of that system. It should be a global reserve currency for the whole community to take advantage of.

Okay, thank you. For the latecomers, could you introduce yourselves and also talk about what your current interests are and what you're working on lately.

I think everyone knows me. I have been around in Bitcoin for years. Since mid 2011. So at least five years. He was in high school back then. Relay network. Educational efforts.

Oh, hi. I do work on lightning network. My intent is to help make bitcoin great again. Fedora. It is my hope that we can build a similarly strong community for bitcoin. Also community efforts on sidechains. He's very much one of our community building people at Blockstream.

I was working on Bitcoin in 2014. I had no understanding of the whitepaper when I first read it. I took some computer science classes and then realized it was pretty cool. I graduated from school in June. I am working on lightning network. I also do some work on btcd. I am also working on oblivious RAM.

Okay food is here let's get food then we can talk more.

# Lunch

food

What do you each want? Not in terms of technology, but in terms of roadmap for what you want to see in 5 to 10 years. What do people want to see? What's on their wishlist? Gold ran for 6,000 years or something, and maybe for bitcoin it will make sense in a few centuries. Let's worry about things that are within our reach in our own lifetimes at least, more achievable goals should be picked. Do they want to aim for market volatility? Lite clients?

Whether to bring up legal risk. Has a risk of this being considered a primary concern. If it was the only concern we had, we would find ways to route around it. There are technical reasons that we could discuss as well, of course.

## Oblivious RAM

Like a XOR linked list? I also have projects in encryption like ssh stuff. We have a paper we are submitting in like a few weeks. Computational private information work.

# About mining

Back from lunch.

So we would like to talk about the mining situation in China. Okay. So it's coming up, is it too dark? Can you guys see in the back? Oh we should turn off the lights. Okay who has control over the vapor machine?

Hi everyone. I would like to introduce about the miners. Before I came to this meeting, we discussed some concerns from the miners. I should like to share some data. First about Antpool. You can see that we have a full node that can generate a block, they are distributed across the land, in different locations around the world. Antpool is a single pool, but the nodes are distributed around the world. So we have some control over the propagation. We do not necessarily have the advantage over a small pool. We cannot synchronize to work together because the lightning still travels still spends time, we switch the job we send the jobs to the different miners around the world and that still takes time.

We operate globally and do not necessarily have the advantage over a small pool. Antpool's hashrate is about 14%. The other 86% is by other guys from our customers or other mining machines. Bitmain 2015 customers, by person. We can see that from the perspective of individuals we can see that 76% of customers come from outside of China. United States takes half of it. And Canada takes another part of it. Germany had the second largest area of sales. Right now it's Canada after US. 24% of the customers are from China. This is accounted by individual person. Another statistic is by units of machine. We can see that China takes the majority of it, that's about 74.8% of the mining machines goes to China, and about 25% goes to foreign customers. If we combine these two statistic together, the China customers are more likely to build larger farms.

Question, is this by nationality, or is it by shipping destination? It's by nationality by person buying. Are there Americans buying hardware and shipping it to China? No, it's by shipping address.

Chinese miners are more likely to buy on average more large customers. From our experience, it shows that it is typical that American customers buy only one or two units of machine that they put into their own home or basement. Lots of our Chinese customers are large farms like 1 or 2 megawatts. These are kind of small scale. The large customers are 10 or 20 megawatt.

Cost structure for mining farms in US and China. Why is this the way it is? We can see that the capital expenditure per megawatt in China is 50,000 and in America it is 300,000. Power cost lowest available, $/kwh in China is 0.04 and in America it is 0.02. Time to build, in months, in China is 1, and in America it is 3 to 6 months.

America has much lower power cost available near hydropower stations. America will require more time and more CPEX to have a mining farm. These are mostly infrastructure things. $50k/megawatt in China. It's like $300k/megawatt in America. The labor cost is much higher in America. All of the wiring needs to be by licensed individuals. They need to have licenses. If you decide to build a mining farm, in China you could do that in one month. In America, a bunch of that time is spent talking with firefighters, electric company, regulators, you need to show them the places, the designs, make sure they are okay with the designs, they need to check everything, and they need to change this change that and that's another safety law. It's a very slow process. In China, it's very fast. You can build things very quickly. Regulation is very loose. You have very little to deal with.

From a capital perspective and time perspective, mining farms in America are very expensive to build. The amount of time in America influences the decision of course. And the power cost in China is not as good as America because you have more hydropower stations. You have 2 cents or 1.5 cent or something. In Canada too, it's cheaper power. The low price is not available in China. It's about $0.04/megawatt according to our experience. In China, there's a oligopoly of .. from a legal perspective, if you are any of the power company need to sell electricity through the Greek company and they charge a lot of it. If you want to make deal with a power company directly, it's against the rules. You need to spend resources and energy and relationships and these things on trying to get the - to travel with them - so basically in China the lowest cost of power is not as good as in America. To summarize, in America, if you do a short-term business where you want to get your investment back very fast, it's not as good as China.

Difficulty is rising fast. We know the reason why China miners are more likely to launch many farms. I can summarize this as because in the past few years, the risk involved in a mining investment are high. Miners do not like the difficulty going very high very fast. We can see in the past few years, this is a good time in January 2015 where the mining difficulty was not moving. There was a big shot around January 2016. Miners also do not like the price of bitcoin going down. We can see since the ASICs came,... January 2013 ASICs were delivered around them. Friedcat started doing their own mining farm. So we can start that graph around that. January 2014 was a bad time as well for the market price for mining. Inside the miners community, .. losing a lot of money .. because of the crash of the bitcoin prices... and lowest corner, .. and highest is $1000 U.S. dollar.

What's the reason behind this? The market is not controlled by miners. The technology is improving very fast. 130/110nm was ready in 2002. 65/55nm was ready since 2006. 16/14nm only ready in 2015. Bitcoin experienced technology improvement journey of 13 year semiconductor technology in about 3 years.

name	process (nm)	sign off date	hashrate in GH/sec	efficiency in J/GH
BM1380	55nm	Sep 2013	2.8 @ 1.25V	1.643 @ 1.25V
BM1382	28nm	April 2014	14@0.70V	0.494 @ 0.70V
BM1384	28nm	Oct 2014	18 @ 0.75V	0.386@0.75V
BM1385	28nm	June 2015	30@0.66V	0.216@0.66V
BM1387	16nm	Dec 2015	80@0.4V	0.08@0.4V

So about 20x technology improvement. You need a war. The smaller the process node, the harder it is to improve. We improved the power efficiency of the semiconductor. You have a lower capex and OPEX when jumping to the lower resolution. Yes we're hitting a wall. You can have a lower power cost, but the cost to fabricate the wafer increased. Maybe you have to increase the cost to make a single transistor to improve your power efficiency. The mining technology improvement have somehow just uh well slow that pace. It's kind of good news actually to mining rig investors because older generation miners hate the new generation. So the new generation will now come at a slow pace compared to before.

In 2011, ... miner will have less risk than before. The improvement of mining technology will have to wait the improvement of semiconductor technology. Moore's law is hitting the wall. bitcoin price is expected to be more stable. As stable as the U.S. dollar against the Euro. It will have some up and down, but generally it is stable. People are more likely to accept it as a reserve currency or to put it inside their savings inside the bitcoin network. So this will be good news for bitcoin.

I think there's a potential that the mining will shift to Western because regulation, the legal system and the power cost, this kind of long-term if we consider things from another perspective, in America there's lots of advantage over China. Even in Europe, we can find lots of cheaper; and lots of stable ecosystem. From another perspective, mining will have an edge in the Western world. People are waiting to invest in mining. Bitcoin hashrate tends to be more decentralized or more widespread when there's a more even state. It depends on how the economic and how the market for Bitcoin mining evolves in the next few years.

We need more people to put their savings in the Bitcoin network. Thank you.

Q: You mentioned how much of Antpool's hashrate is bitmain? How much is the hashnest service? Do you know?

Hashnest does not have a physical hashrate. They are in the 14%. It's actually separated, the hashrate.

Q: You said something like 80% of the hardware is sold, and only 12% is kept by Bitmain? Is it that shipped hardware, or does Bitmain own it and operated by someone else?

Our own hosting, our own mining operation with our customers and so on. We discourage them from putting their mining rigs inside our mining farms.

Q: You had a picture of where your hashrate is on which of your nodes. I wanted to ask if you could speak to the infrastructure around that. Is that all owned and operated by you in China? Is it operated by other individuals who aren't necessarily able to censor transactions?

Most of the hashrate is from other individuals.

Q: No I mean the pool operation. Are you operating the pool in the US? The antpool servers?

They are under Bitmain's control. We rented servers from Amazon. Antpool servers will connect to the US antpool server. European customers connect to the European Antpool server.

Q: What about having other people run the Antpool servers?

Maybe.

Q: You would collect the revenue, but you would have separate people in separate regions have the keys to the servers so that one agency wouldn't be able to target.

Frankly I have never thought about this. From the beginning of the business, .. next generation of the mining pool and open-sourcing it and it will be easy for our customers to setup their own mining pools. They don't have to us a third-party pool like Antpool. They will be able to build their own mining pool.

From the development side, we want to make tools to make that much more easy. We have had some difficulty because consumer adoption of mining hardware has gone down. There does not seem to be as much interest in people deploying their own mining equipment. It's hard to develop software without interaction with users. We need the users so that we can build the software to make it easier to have users in the first place. Yeah, it sounds great, if there's anything that we can do to help, we would be happy to help with that effort.

I want to add a point here that we need Bitcoin community I think we need to have a welcome that is kind of mining farm thing. For example, in China actually, 3k half-megawatt each. About 10-20% are that scale. There will be thousands of these. We need some conferences to invite the power companies, miners, local governance, and try to promote the mining farm building services. Just building the mining houses, it's a real actual company. If we can do this in America, then if we were to have a long-term business plan, you could have an advantage to China. Mining pools are a centralizing factor, but as long as we start to open-source our infrastructure, I think it will become easier for others to build a mining pool.

The existing mining software, I get lots of complaints from some other open-source mining pool, it sucks. Yeah, agreed. It does. It's very difficult right now to setup the existing mining pool software. Only a small number of experts can figure it out. It needs to improve. Yeah. There's also some tech that we know how to build but haven't built yet, which would allow you to pool your income without pooling your transaction selection. P2pool is an example of this but not a good example. It's not a good pool. Never was. There is tech that could be developed here where users can pool their income but keep transaction selection decentralized. Multi-PPS? The mining pools have to join together to share their income. It also increases the performance of the network because, right now all the pools are buckling against the other ones, it's creating a lot of orphans. Because they have like Bitcoin protocol is not so efficient from the block propagation ... in the middle of 2014, to the middle of 2015, we are losing approximately over 10% of mining power for nothing because of the creation of orphan. They were not propagating because of internal software performance issues. We could also create a how-to for installing pools. Why do users not do it? There is no reason to install a pool if you only have a couple gigahashes. You should have at least like 20-30 petahashes to be really efficient. If you combine a lot of users, and if it doesn't hit the, then it negatively impacts bitcoin because many users are just following this simple "How to install a pool" and they might do that for a few terahashes, there will be less profit and very high risk and they cannot provide the sources. At the moment there are only a couple of people that can configure the mining pool. It's a bare quality for end user.

It creates a liability though for the system. Exactly. Yeah. I think we can fix this going forward. Combining the pools, I think it's the next logical step. Instead of battling one against the other one, it should be some next step in the software development. Then the old pools will work together without any point of failure and without weakness from attacks, and the pay-per-share and so on, will provide you just payout. It will be logical. I think it will maybe not .. maybe not this year, but it should definitely be created ideally before the next reward split, and then the fee will be more reasonably high.

Am I understanding you correctly that it's possible for pools to not be concerned about orphan loss in the future? It's a question about the efficiency. ASIC development growth, it's a question about improving the bitcoin network. Imagine you have a Visa datacenter with 100k transactions/sec. If you can optimize your data center and reduce the electricity consumption, it means the transactions are cheaper for end customer. Replacement of CPU power for GPU power, it's a next logical step. It's decreasing power consumption and it's also increasing the price of your transaction, and ASIC increasing the price more, and increasing ASIC efficiency decreases the price per transaction. Making it as much cheaper as possible. But the miner power also creates protection barrier for asset, for bitcoin or for any coin what you are using inside the blockchain. If hashrate is higher, it's very hard to attack the coin or asset inside the blockchain. Additionally, you can just note take in line the cost of the bitcoin, you can also lower the bitcoin with an additional cost, like with a smart contract, the share inside the bitcoin, so it's the price of a bitcoin plus the shares of the company. It's more high cost the asset. Hashrate should go up. We're definitely reaching technological limits for now.

Selling the containers, selling the warmers for homes, like warming for water or something. In Ukraine, our partners, we have already designed a miner that works like a heater for a house. It's just warming the water. It's consuming the same amount of electricity and creates warm water. The question is only, if you are using a very small cheap and you're distributing them, they become inefficient. There's no possibility to install right now just one gigahash in a diesel router. The efficiency of the one million chips, not in one single miner, but distributed across the world, will be less efficient because of the delay in communication.

Q: After the halving, the difficulty went down since then by a little bit. Do you have any insight into whether a disproportionate amount are shutting it off geographically?

75% of the mining rigs will be shutting down. Or 80% of the mining rig of last generation at 28 nm. It's still profitable to run it even in some high power cost areas. Recently I think the shutdown is related to specific issues and power companies. Mining rigs were having trouble with their power companies. This drop is unrelated to the halving.

I was surprised by the decline in hashrate. So it sounds like it's unrelated, a local supply issue. In China, hydropower is very cheap right now because it's summer. In october, when winter is coming, some mining farms have to be closed. The mining farms will be moved during those periods. Some people are stealing electricity. Bribery cost.

Q: You were talking about installations in homes. High nm were cheap to install and more efficient as a heating element. Perhaps you won't get high hashrate from that because they are less efficient as miners?

It's a different economical reason to install them. Instead of buying just a heater, which will cost you almost the same money, but doesn't provide any return, the mining agreement will provide you economic return. But it's not logical and not efficient. If you install miners into TV sets or something. .... yeah everyone in this room is still scratching their heads about that. Right. But for warming, warm air, warm water, then the miner is almost the same efficiency in terms of condition. Why is it not exactly? The .. of the device will be higher. If regular warmer for water, cost like $1, then the miner will be $2.50 and higher price. But right now the growup of the difficulty is so fast that if you buy it, you will not be able to get a return to cover the price, because of the growth in difficulty. When it reaches a maximum point like 10 nm or 9 nm chips, then it will be more linear and then the home users can buy it and they can be sure that in 2 or 3 months they will get their investment paid back, plus some benefits and some investment from bitcoin. The bitcoin price is lower than it should be right now, it will grow up, it should approximately happen when mixing the maximal point of the technology, so then price should go up and then over a k, and this create an interest in all the public to invest more in the bitcoin.

As soon as the development of bitcoin mining chip catches up with mainstream general purpose CPU, we will see a slowdown in growth and thus the chip lifetime will grow and this will make it viable for consumers to have them. I agree with this. It makes the investment less risky. Yes I agree. However, on the other side, I think that if the growth of technology itself slows down, I expect the profit margin of mining to go down as well so that you can plan ahead and do better analysis and probably the competition would be higher so the profit margins might go down. This will also depend on bitcoin exchange rate. For competitive mining sure, but for compliance mining perhaps it would be different. Cost of supply would get close to the cost of production, more efficient. The adoption of the bitcoin is growing over time. The price of the bitcoin will be also growing up. As result, this is increasing the profit and making the compensation. I think it's a dangerous assumption that the market price will go up or do anything in particular.

You sort of assume that mining hardware ends up at the same state of the art as general purpose CPU. I don't know whether that is the case. In particular, if you could build a mining chip that gives a completely wrong result of the time but is 2x as efficient, that would be awesome to have for mining but it's unacceptable for general purpose for CPU. I think that once the tech catches up, they might find that for mining ASICs, they will find that a different design is interesting for other purpose. Can we stop here so that we don't lose the audience.

When we think in terms of PoW security, if you want to attack the network, you can do many types of attacks. There are less expensive attacks to worry about. Some of them will be faster than ASIC fabrication. In the future if we have a lot of latent hashrate turned off, and if it's vulnerable, then we have a situation where someone can turn on the hashrate as a hashrate attack. This is particularly concerning when you have a lot of latent hashrate.

One other thing that we can talk about later is block withholding. It can be fixed with a soft-fork, actually.

# Future outlook of Bitcoin

One of the things that I hope to do here is to hear this from other people as well. I think we share common vision about what the future is for the bitcoin system and currency. Like all of us, I want to see the usage grow and see it penetrate every corner and aspect of the world. It will take time for this to happen. If everyone was to awake tomorrow and know that bitcoin will be the world reserve currency, there will probably be war. There will be fights over mining farms, even. It is good for all of us in the room that Bitcoin grows at a steady pace and that the world has a chance to adapt to this system and for ownership of bitcoin to be well-dispersed and very wide-spread so that everyone can participate in a system that is seen and received and is fair to everyone in the world. The technology that is possible in the protocols on the network, we're looking at things today that are much more powerful than we have already deployed. We know that many things are possible in the future that end users, if you think about the further out technology, like zero-knowledge proofs for synchronizing the blockchain. We know there are tech improvements that are possible, but it will take time to get to them. During that time, we need to advance the system, get more adoption, dive into more use cases, and keep track of the long-term advantages of bitcoin that make it valuable to everyone, that is permissionless, that it is open, worldwide, and to keep this at the forefront of the system. To get here, we might have to cooperate and work together harmoniously rather than in dire competition. There are many people outside in the wider world that don't use cryptocurrency-- that's the competition. We should be focusing our energies. We should be collaborating to make bitcoin successful there.

It's possible for interesting systems to become popular, but less important over time. There was an example. Everyone heard about paypal. It started as a bearer electronic cash system on palm pilot, a PDA before smartphones. People who were doing it thought that electronic bearer cash was very interesting. Paypal became centralized and had the same problems as banks. It became big and controlled by corporate interests. It became the thing it was trying to displace.

One potential outcome for bitcoin is for bitcoin exchanges to become banks or bought by banks or incorporated into banks. I am not accusing of anyone. It's just how human evolution happens in previous systems. They could become stock market listed, bought by banks, and the permissionless properties might be eroded. For some people, that would be uninteresting. But perhaps someone would try to work on an alternative because Bitcoin would have degraded in quality, just like paypal is being replaced in a few ways.

So we just have to avoid that failure, and maybe bitcoin in 5 years could have, I don't know, a nice positive outcome would be the same amount of distribution and value as gold or something.

Let’s say 10 years. Ok, maybe. You need aspirations.

I would also point out that in that kind of evolution to something more centralized, it would be easy for Bitcoin to change into something where mining is not needed. In ethereum, they intend to switch to something where PoW is no longer going to be required. In a centralized system, PoS is going to work. If you have a central authority that can decide between different systems, it will probably look like it works. If Ethereum switched to then, then why would you need all the environmentally wasteful work? Why not use the system that ethereum is using? It would be much less interesting even if you did switch. In that outcome, the miners wouldn't exist. It probably isn't going to happen in the next few years. I would much rather have a system that is interesting and secure.

It's easy to make centralized systems. The trend is probably going to go towards that if people don't care. The more centralized the system, the better it will seem to work. There's also the risk of boiling the frog. I think we have been boiled already.

Centralized systems are always going to exist. Paypal already exists. We should recognize that if we build a system that is getting closer to those alternatives, without providing major differentiation, then we could lose the competition because we wouldn't be providing something unique. Whereas if we make sure that we can maintain our core values, then we can continue precisely because we continue to provide something unique.

A wild Bobmon has appeared in the room. It's very important to capture this pokemon. We can't mention the name, of course. ((It was a pikachu, if we can relax the CHF rules.))

There is a transcript projected on the screen. Thank you. You're amazing. Really just the greatest person ever.

We have a list of topics on this side. Who would like to kick off this topic?

We don’t have to discuss this but we all go to different meetings, and perhaps from Scaling Bitcoin or elsewhere there might be some information that would be good to share.

# Lessons from the Ethereum hard-fork

There are talks from Scaling Bitcoin that we will add as links to the transcripts or email that around. If there is nothing to talk about regarding prior events and conferences, then we can talk about lessons we could gather from the Ethereum hard-fork. Who would like to start on that? Where to start? It's a broad topic. Who was surprised by this situation? Surprised by TheDAO situation? Surprised by the hard-fork? The fact that it had a bug? That people suggested a hard-fork for it? That the hard-fork went through? I was surprised that they did not have an improvement proposal for it. They just did a hard fork without writing it up. I would suggest that the DAO might not be that topical.

There are lessons there because we are also talking about different types of forks. There are forks, replays, things like that, The DAO might not be as relevant. There is the possibility or the fact that they are exploring new possible scripting languages for bitcoin. There have been arguments that if the DAO code had been more auditable or more provable, the specific recursive construction in the ethereum VM was reviewed and a warning was given regarding sandbox escapes and code that is hard to reason about. If I criticize everything, then I will be right about everything that fails... [Specific conversation about the tech failure in the ethereum script system] Cycling is risky, it was just ignored. People warned specifically about this.

I will provide a short summary about this. They are creating the technology in the way that they would like it to exist into the future.

If each morning you wake up and the rules are changed, then you are changing the game. They start to use the technology and there are a couple of points in the timelines.

First, it's a smart contract by itself. With Solidity, it is definitely not the choice. It should be improved. If it's changing anything in Solidity, it's changing all the rules in ethereum and changing all the rules inside the smart contracts in ethereum. If you're designing this smart contract today, it doesn't mean that tomorrow it will be able to work. If you change something in Solidity it might stop working and there is not continuous support of the same system.

A second point that should be marked is that it's changing proof-of-work to proof-of-stake. So first of all the issue about PoW is that it's created like a temporary and it's by design created by working on limited amount of time. The issue which PoW the more transaction you get, the more complex the hashes you construct, more memory for GPU cards, at the same moment there will not be enough memory for the GPU card to generate PoW. Once, we have already reached that limit. So the hashrate generation requiring for 2-3 GB of memory, then at one moment all of those GPU cards stop working and stop generating PoW. It was a software limitation.

You can update and continue proof of work.

Changing from proof of work to proof of stake changes the economics of the system, all the rules change and it will impact everything. The next point, the construction of ethereum, it's built for rolling out to getting the current point of a blockchain should possess all the smart contracts. And smart contracts using solidity, it's consuming a lot of CPU power. If you get a lot of smart contracts, if the blockchain would be bigger, you would not be able to download the blockchain and synchronize new nodes. It requires a lot of CPU power. And during the time, if smart contracts would be bigger, than a regular node would not be able to process all the smart contracts. At this point you should somehow also perform hard-fork, and split the network. Each point is practically creating the pandora's box. If it doesn't solve it, it's basically the death of ethereum. If you solve them, meaning the hard-fork, it's meaning change of rules of the whole system, and the user will be ....

All the users already decide to use ethereum, they will be impacted and lose trust at this point. As you go forward in time the more users you will lose. Ethereum is too young to brave this, .. They are not thinking about the users because they are testing the network as they go and modifying the rules.

And also rolling back the transactions if it's money is quite risky. Someone should decide. Is it fraud transaction or not? It's also changing a lot of rules and also impacting the users and creating a dissatisfaction for the users. Some users will not be satisfied.

I was surprised about the Ethereum process that there wasn’t a document. They have their own BIPs, and they didn’t use it.

They were trying to fix the problem as fast as possible.

Yes, but they still had time to go. It wasn’t last minute. They had some time.

A separate issue with this is that their response time to the issue seemed slow to me. I don't quite understand why. When there were network incidents in the Bitcoin network in the past, I think that the response time of the Bitcoin community was much faster. I saw basically no response from the Ethereum technical community other than telling exchanges to stop trading. For days after, funds were being drained out of The DAO and they had not given patches to the miners to block the transactions. Why didn't they reorg in the first hour? There were some simple things that they could have done. There were some things that they could have done well. I think they took wrong action. But they did take action. Credit where credit is due. Their hard-fork was bilateral, meaning that the new hard-fork chain would reject blocks created by Ethereum Classic, and Ethereum Classic would of course reject blocks from the new chain. The prior hard-fork proposals for bitcoin like 109, 101, 102, none of those were bilateral hard-forks. What this means is that if Ethereum Classic gets more total work than Ethereum, which to the market looks like it could possibly happen, it will not reorg. You will not have Ethereum Classic get more work and then the ethereum other chain gets erased. This is because of the bilateral fork. If they did a fork like the BIP 101 fork, and you had a situation where the classic chain got more work than the other chain, then it would have erased the chain history from the other one. Presumably they would have made a fork to erase the history and bring it back. It was probably easier for them to do it this way, but they did it well. The replay situation I think is quite interesting and has a parallel in Bitcoin. A year and a half ago, there was a discussion in the #bitcoin-dev chat channel when Gavin and Hearn were talking about their fork proposals. Some people began to discuss how to do replay prevention between forks of bitcoin. This made Gavin mad because he rejected the idea that another chain would exist at all after the fork. We had an extensive discussion about replay. I think we did that better than Ethereum because bitcoin has less replay risk, inherently. In bitcoin, we would not have as many replay problems if we had a fork like this. In addition to this, this was something we were thinking about when we started to think about hard-forks in Bitcoin.

Why is that?

The UTXO model would be why we would be better off. Ethereum has accounts, instead. So the anti-replay counter is more inherent. If you make a transaction you can spend them equally if they were in the same accounts. If bitcoin forked like ethereum did, there would be some replay. You could change things in the transaction format in the hard-fork, and other tricks to reduce the chance of replay. Ethereum developers knew about replay. They in fact apparently had a conversation with coinbase about replay before the hard-fork and their position was that there would not be two surviving chains so don't worry about replay. So I think the failure mode was a lack of sufficient paranoia, being overly confident, many things I think we do in Bitcoin we over-engineer a little bit but this over-engineering is for a good thing because we can't predict all the failure modes.

We cannot fix things in two seconds. It takes us some time.

But for example, replay is still not fixed in Ethereum world even though it is causing many problems. I am sure it will get fixed in some numbers of weeks or months. Replay could even be an attack against another chain, so some users might consider it a good thing. It's only a good thing if the other chain actually dies.

One point I would like to make, as an interesting thought experiment, is that it's important to make replay protection to allow prior transactions before the fork. There was discussion to change the transaction type to allow for prior transaction types. Particularly in bitcoin you need to do that. One challenge is that in bitcoin you might have locktime transactions that are pre-signed and we don't want to invalidate. Some Bitcoin ATM vendors have some timelocked coins and they can recover those in the event of the ATM being stolen, but they can't do this in another way.

So the interesting wrinkle in this is that if you have nlocktime transactions, if there is a hard-fork construction that allows for a new transaction type, and it allows priors, then the hard-fork transaction format would not be replayable. Well, there was a suggestion in that earlier discussion, to prevent replay without any need to change any transaction formats but it was somewhat complicated. Did it require nested or something like that? You would require miners to start producing 0-value TXouts that anyone could spend. And then transactions would pick those up and spend them. This is a lot of code. You don't have to require them, they could do this voluntarily. Well, it's complicated, it would work, and doesn't have those downsides. When we had those discussions and realized it was complicated, we realized how much work it would be. It's easy to do this as a soft-fork with for instance a signature hashing flag that says that there should be on the stack a previous block hash that is earlier than today minus 144 blocks which would be equivalent to that other proposal, with zero-value outputs. The challenge we had with that is that the only people who were interesting in solving that problem at the time were the people who were not interested in hard-fork arguments at the time. We talked through some of this, but Gavin was really angry that we were talking about that, he saw that as an effort to undermine a hard-fork, but it wasn't.

Seems like we have not translated in a while. They are reading this transcript, live. I would be curious to hear their perspectives on any of that discussion.

Whether the minority chain should be allowed to exist or not. We see that in Etherium Vitalk said that it is good with two-chains coexisting. But some of it might think that the minority chain should not exist at all.

I think a big problem you have with that attitude is that the moment you have any disagreement it does look like a 51% attack against a minority chain. At least with the obvious way to do it with a soft-fork. At worst, you could end up with legal problems.

Me personally, I would be dubious about participating in a forced fork like that. We should distinguish between should exist and should be prevented. It is bad in etherium that the other chain exists, but that doesn’t mean..... any particular action to prevent it, such action might not be valid.

Because our difficulty adjustment is relatively slow, if we were to say that a hard-fork would only happen after 99% miner support, assuming it was achieved by 99% miners supporting it rather than a forced soft-fork to get there, you would be in a situation where it would take a long time to adjust on the minority chain that it would not be usable over there.

The challenge with this point is that, in the case of ethereum, it's not just that they moved which was a problem too, the go-ethereum client would not synchronize a shorter chain even if it's the only one with valid blocks. Ethereum Classic had to blacklist the hard-fork block immediately. Ethereum Classic also forked at that point. It was a soft-fork, though. If you start a pre-fork Ethereum client, when only happened to connect to Classic nodes, it wouldn't know at all. It's a complex set of variables for that scenario. You can't count on retarget to [...] -- a minority side, under bitcoin rules, it's very difficult to do make trades because you're waiting such a long time. You're in a position where it's less likely than ethereum, for people to start making trades and creating a viable currency. One thing that we learned is that there's a large economic incentive for traders to encourage the splitting of assets. Poloniex alone in the first several hours after opening up ETC made $200k in trading fees. Traders have made money on the volatility, as well. If nothing else occurs, an incident like this is an opportunity for exchanges and traders to potentially make a lot of money. If they need to take some actions to make that outcome occur, thy might do so, even if the market cap of the currency goes down. Ethereum currency holders lost out on this, but the exchanges and traders made some money, although not universally. BTC-E and Coinbase are probably not doing so great, although others might have better outcomes so far. It might be easy to get into a situation where you can do an anti-replay mechanism. One exchange might be in a situation where they lose a ton of money if the fork has value. Who is responsible for the lack of care that led to this situation? Is it the exchange's faults who didn't protect from replay? Is it the developer's fault for not foreseeing this as a problem? In the U.S. legal system, the way to answer that is by court cases. I think that in this case, because it is designed mostly by ethereum team, it's not like open-source, they might have liability because I think legally ethereum more look like a commercial project because they are selling a piece like a commercial company. So technically for a lawyer, it's a commercial project (all open source is commercial). The specific economics around ethereum, like the pre-mine, maybe makes a stronger argument there.

I think we are learning as we go, but I have noticed that only the native English speakers are talking. I would encourage everyone if you want to say something, please jump in and make yourself heard. Or if you feel like people are going too quickly, ask them to pause and stop.

In such a fork, in bitcoin, if that happens, lots of bitcoin miners will start to protect the viability of the majority chain. They will volunteer to attack the minority chain.

So one of the interesting things in Ethereum is that immediately after the hard fork occurred they declared the other side the loser, but both sides did that.

I wouldn't go and assume that it would be easy to get away with 51% attacks against minority chains. And they might start taking legal action against anyone here. I would never do that with my name attached. Pretty good chance that I would end up in jail for that. We would all be liable to some extent.

Maybe if you mine an empty block, on that chain, then basically it has no value. Otherwise they will compete against each other long-term for value. If we just work together, to technically somehow make sure the minority chain cannot not exist. There were some proposals made that the minority chain could not exist, or that the minority has to have a hard-fork themselves, and that is fine.

Technically this is easy to do. This is called a forced fork. The problem is that there's a good chance, no matter how you did that, if there was someone in the minority who said "no, you're attacking us, you're preventing us from transacting" that could then result in legal action. It's such a grey action. We have no idea how courts would rule on this. Anyone with their names on this publicly, especially in western countries, . The other thing is that we do know how to increase capacity through soft-fork methods, so we should prefer that. But we are getting off-topic. Ok.

The bigger point that we need to be careful about is that in the Ethereum community, they argued that this is a safety mechanism in Ethereum, that if there's a disagreement about the rules, then life can go on and yes the economic effects of two competing chains are bad -- I agree about that although they don't all agree — that's a balancing protection in the system perhaps. If the majority of Ethereum miners want to do something bad, as some argued that they did, that the network can continue on without them. And it's a way for people to feel more comfortable with their Ethereum investments, and that if the worst happens, then they could at least stay on in a diluted split system. I don't know if it's possible, in bitcoin, to really make it so that the minority fork cannot happen in Bitcoin. Even if we could make it impossible, we would lose an argument for Bitcoin's long-term safety. We should be conservative in how we talk about and think about that. The fact that the miners are counterbalanced by the users enforcing the rules is an important part of Bitcoin's security model.

In addition to that, not just the long-term effects of how that affects the pseudo-political view of how the system works, any effort to try to create a situation where the minority or one particular chain cannot continue to exist, there will be many people that strongly hold that view and they will fight to make sure that chain can continue. I know there have been proposals to make it less likely that a minority chain can continue, I have not seen anything that makes it absolutely impossible to continue. If you attack a minority chain, then basically bitcoin is no longer permissionless. This also plays poorly with concerns about mining centralization. If the system is balanced, it's okay to say the other forces are balancing, but if you need permission from other miners to run another chain, then the centralization of mining is much more of a concern.

In the next few months, maybe a fork would be likely to happen, I just have 1% of hashrate maybe, I decide to fork away. I have only 1% of the hashrate, and I fork away. What would happen to that chain? It's hard to say. And do exchanges need to care about that? They can profit from that, independent of whether that 1% chain is technically secure. If some random person with 1% makes a fork, and an exchange doesn't know about it, and they didn't protect themselves against replay, do they have liability for any random person that makes their own fork? Should there be a standard mechanism for preventing replay in bitcoin hard-forks? Even if we don't want to do a hard-fork, we should recommend an anti-replay mechanism. The transactions should commit to a blockhash, which is dangerous to do with the most recent blockhash because then reorgs cause problems. But if it's a blockhash from 1 day ago, like 144 blocks, then it does close the time window for when a replay attack could happen, and the chances are that this wouldn't happen for situations that might show up in court. We should properly fix replay in bitcoin, so that if someone wanted to create a fork, then there wouldn't be a replay issue.

But couldn’t the purpose who is forking could chose not to use that mechanism? Well that’s on them. But it’s not on them. [cross-talk]

We can’t force people to be sensible. We could do some work to encourage them to be sensible. I think at a bare minimum on a cultural level, it's good to establish the precedence that exchanges in the event of a fork, have an obligation to give coins on the old fork back. This is more of a cultural norm, of course. One of the things we have to be mindful about, in the infrastructure of bitcoin, when we do things that change things on how bitcoin works, it imposes cost on all the users of bitcoin. And they have their own business concerns. If we impose too much cost on them too quickly, then they will respond in dumb ways like not listening to us, adopting strange altcoins, ignoring us, etc.

Can we let the miners talk a little bit?

I think the part of the blockchain created by multiple years, creating another one, split in a chain continuously leaving independently, create a lot of potential issues. We may be should take the point of view that if someone likes to alternative chain, they should just waste their fearless one blockchain, like new start for a blockchain. Like a new point. And then continue. It's more like splitting the result of the previous year, and in October's its lights and you could never prevent exchanges from playing on this split. You could never prevent the users, because you mostly rely on user belief of money, and on one side of the blockchain and they have the private keys. There are a lot of users. This should never happen. Most likely the current blockchain doesn’t fit into your requirements, and you would like to, just to create something.

Okay. Miners, could you talk a little bit about your perspective?

I don't think it's reasonable to assume that exchanges can give back the other coin. The thing with Ethereum Classic, it's an interesting scenario is that the thing they didn’t give back was the original coin. It wasn't like someone created something; someone created something new, they jumped to the new thing, and didn't give back the original asset. Some of the exchanges have given it back already, like on Poloniex. The ones that aren't giving it back, that's the situation they are in.

It’s like two copies of the lottery ticket, but the first to show the lottery ticket gets the prize.It's possible right now for coinbase to give it back. Even though they lost, they can buy it back. Let's say the price went back up, well then there's no way. They lost it because of replay in this case. If we're looking at what are the ultimate lessons from this to learn? What should be the standard of care from developers? Some exchanges profited from the volatility from this. Think about victims, though. Users, other exchanges, other businesses, TheDAO hacker, it's a tremendous amount of systems that you have to change very quickly if you're an exchange in a very fast moving and confusing situation, when you have a situation like this. I'm not even talking about legal responsibility. What about an ethical responsibility of the developers? What should be the future standard of care that we expect for cryptocurrency?

I would widen that from developers to infrastructure. Together, developers and miners are part of the infrastructure that make Bitcoin go, and to a lesser extent the exchanges and infrastructure providers. They are the ones that make the bitcoin currency usable, we have a duty of care to make the system stable and make sure it upholds its value. We have to make sure that nobody loses money.

For example, the client should avoid the cases where you're entering the wrong address and you're able to send the money for nothing, like destroying it. The point here is that Ethereum doesn't do that either.

Standard or duty of care, the community should learn from history like incidents like this. They should ask the question: are the developers moving too fast? Are there reasons for this change, and are those reasons good?

Many people would see TheDAO hack reversal as a social good. And that good could outweigh the potential harm. However, I would much rather see duty of care as much more important for Bitcoin. I would see this as an immutable ledger. It's a social good that outweighs these harms.

This reminds me of one of the announcements on the p2pfoundation site from Satoshi which was that the advantage of cryptography is that it gives you security that cannot be taken back no matter what no matter the reason. (See link for quote)

<http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>

It has clearly poisoned the other chain. A lot of the community has found it less interesting because it no longer lives up to what other people joined the community to do. That was not analyzed when people said "just return TheDAO coins". You cannot control the markets. A lot of users lost money in the Ethereum hard-fork. Some of them lost trust in blockchain technology, maybe forever.

Other aspects of duty of care could include the vigorousness of technical review, having a specification, promises made to users when a system is not ready. Clear communication to users.

Has ethereum scared users away from cryptocurrency in general? I think it has some, at least. Did we, the bitcoin community, do enough to warn people in advance of these events with ethereum? If we had done more, would it have scared away fewer people because "we told you so"? I don't know. I have kept my criticisms of ethereum relatively quiet, because I do not benefit from criticizing their efforts. If I say that ethereum has a bad design, then some people would say hooray, and the ethereum people would throw more rocks. There are enough people that are throwing rocks at me already anyway.

There has been a lot of schadenfreude in this community. Damages in ethereum hurt us all to a very significant level. But at the same time I could have warned people more. I think we are all guilty of this. When it pertains to legal risks, if they do things that could complicate things for us..... Also keep in mind that this situation is not over yet. It's a competitive solution it's like blaming one side and another one side. Only independent experts, independent technical experts who understand how blockchain works, might mark the potential risk for the technology. But from our side, it doesn't look like a ... even if we provide any indication, this could be interpreted by many sides, but neither person would be just blaming.

The hard thing is that experts don't exist. Asking someone to create like certification or qualification, ... it will also be harmful for there to be certification. This is a great risk in many industries. If cryptocurrency as a whole doesn't mature and behave responsibly, the result will be that either we fail entirely, or there will be regulatory pressure that creates enormous cost for all of us. We don't want that. In the past, I have reached out to competing cryptocurrencies and told them advice about how they might be screwing things up. Some have listened, others have not. There are places where as a whole cryptocurrency needs to get its act together so that we don't end up getting regulated in bad ways.

This kind of risk is a particularly bad one. We can't function in an environment where developers as a whole can't operate in the public. If we were in a position where we had to all be pseudonymous, anonymous like Satoshi and so on, and if developers would be politically and legally blamed for their actions, nothing would get done. Notice how outside the room it does not say "bitcoin meeting". FBI knows. I bet your plane ticket says.

We need to let the miners talk. Anyone else who hasn't been speaking?

I would actually say that regarding the eth hard fork that yes the situation is still ongoing, but even if completed the analysis should be going on for some time. We haven’t heard all the stories about how various companies were affected by the hard fork, but that doesn’t mean that they don’t exist. There should be a post-mortem.

If we wait long enough they will probably do another hard-fork anyway.

It's important to understand that all the confusion and losses and broken promises were entirely foreseeable. And many people had foreseen these problems. The whole Ethereum debacle is really bad for Bitcoin because it shows that some cryptocurrencies are not trustable. For the general public, it's hard for them to make the distinction at all. The public doesn't know the difference.

There's a question of product differentiation that arises here. I think the Ethereum split is an opportunity for bitcoin to be product-differentiated from ethereum. But I don't know what that product message is exactly. I don't want to say something like "bitcoin never has any hard-forks ever" because I can't make that happen anyway. How about "Bitcoin has a vigorous duty of care"?

Once we have AI and machines manufacturing mining rigs and setting up automated facilities, and AI writing code and we take out the human element, then bitcoin is really immutable. The ethereum mission statement was basically exactly that. Removing the human element. We could say that we're doing the same thing, and we are, script validation is law. If you redefine law, then that's meaningless. This is profound for me, because the ethereum website had the strongest language and it's still there. The ethereum website and ethereum README said ... it had the strongest statement that code is alw, and it's much stronger than anything on bitcoin.org, and it had a contract like code is law, and a lesson we should take from this is that saying these things doesn't make it true. And it doesn't even persuade public opinion, at least not enough to prevent a mess.

I don't know what it is that causes this expectation. Ultimately it is expectation of the community, if a community assumes that a hard-fork for whatever purposes are hard, then they are hard. If people assume they are not hard, then they are not difficult. In the case of ethereum, or TheDAO, there was an explicit language and an explicit contract that said the opposite. Compare it to the Bitcoin event where MtGox happened, where sort of the relative economic impact was the same. I cannot remember anyone even suggesting a similar approach. So clearly at the time in Bitcoin there was an expectation difference. Was there just one address to do to undo the MtGox problem? Well yes that was a difference. Would a hard-fork have been considered if there was a single address in the MtGox problem? Well there was a concern about MtGox destroying 3000 BTC because they sent it to a zero-length script. There was discussion much later on where some random person on IRC discussed a hard-fork to recover those 3000 BTC. It never got any traction.

It's a conflict of interest when there's some insiders that have a vested interest in the outcome of an event ... if you have a strong separation of concerns, where the different players are not crossing over, well we all have kind of a vested interest. It's different because of TheDAO. Ethereum Foundation has something like 20% of all ether. It gives them a lot of weight. With MtGox, if we reversed the MtGox stuff, I would have made a profit from the MtGox insolvency coins, but I never suggested that because it would be wrong to do.

A lot of the fintech stuff I have worked on, the data to do reversal simply does not exist in the public. Fungibility actually boosts immutability because if you can't target the coins to take back, then you can't even make a proposal to undo it. At minimum, it requires a lot of upfront effort to do that change. If I wanted to reverse a MtGox scenario, I would spend a couple months petition users to collect data about the MtGox scenario, and perhaps this would be stretched out even longer, which would be helpful for preventing a hard-fork.

Talking about what we can learn: The expectation regarding the ethereum hard-fork, we are talking about making it hard to do reversals in Bitcoin in such a case as if it was always the right thing. And it might not always be the case. But I think what could happen is that if you build a system where it is nearly impossible to reverse in case of a mistake being made, people are more diligent about what people do with their money. This is the outcome that you want. You want people to use the system in a way where the people are sufficiently diligent such that there is no demand for reversal in the first place. This could be done by education, for example.

If you want a reversible system, you could always build it on a second layer on top of the immutable layer. This is not technically hard. I don't think that people in the community realize this. There's a special element in TheDao where it was described as "perfectly safe" whereas nobody in the Bitcoin world described MtGox as "perfectly safe". TheDao was described as perfectly safe and if you didn't like it you could take out the coins. This is something we should be mindful about for future smart contract work.

Both TheDao and MtGox were both perceived as "too big to fail" to some extent. But yes MtGox failed.

I had an idea for a underhanded smart contract contest -- compete to come up with the best safe-looking script that actually steals money. This would help increase awareness regarding how difficult it is to create safe smart contracts. I stopped working on this because of TheDao hack because it would be in poor taste.

In Financial Crypto conference, there was a short talk about a particular script in Ethereum that was a provable pyramid scheme. It was not only a pyramid scheme, it was advertised as one, and it was also a provable pyramid scheme, and yet people still sent money to it. Yes, it's gambling. It's the ethereum investment thesis. Some people want to play that game. People like the redistribution of wealth game. It's a game. But there are probably many things that the bitcoin community could do to increase awareness of various risk, which might reduce the risk of thinking things like "the network needs to reverse to save theDao". "Of course it was full of bugs". It would have played out differently in the Ethereum world because of that. Well, with the exception of the Ethereum Foundation conflict of interest.

We saw the poll before the Ethereum Foundation hard-fork. There was 10-20% against it, but we see right now the market cap of ETC is about 20% of the market cap of the ETHF currency now. We can see this disagreement between two parties because one party say we should have "code is law" and the other party says "since this DAO hack is not acceptable and lots of people lose money, then we should save it because they are saying save it". It's a different opinion between two parties. That's why ETC can gain momentum. Right now, for Bitcoin, we're in a different situation. Increase the block size or not. Do people in Core still agree, 10-20%, is that still a significant?

There are a few points to make here. 20% of ethereum people voted for it and 80% voted against... it was only 5% that voted at all. It was 5% voted. And then 20% of the 5% was... so it's very unclear what the actual numbers would have been.

.....

With bitcoin, again, we can try to know. But keep in mind that people saw a hard-fork go horribly wrong. It went wrong in a way where a lot of people invested in Bitcoin would consider it going really wrong. Perhaps to Ethereum investors they might have other expectations. I don't think I could convince a lot of Bitcoiners to do a hard-fork, anymore, after this.

The outcome for Ethereum is no where near as bad as it would be for Bitcoin, which is actually used by people. Whereas Ethereum is not really used in any retail or p2p money transfer cross-border stuff right now. People are buying it on an exchange and then they put it into TheDAO or make test contracts that don't have real value. Whereas in Bitcoin there is real money to be lost by mistakes.

But arguing the other way, in Bitcoin there is more incentive to get the details right. Ethereum failed even the most basic due diligence in terms of even specifying what they were doing. In Bitcoin land, we wouldn't fail at that part. In Bitcoin, what we do matters a lot more than what they do in Ethereum today. But you have a point at least.

It's still difficult to get accurate views on any of these. I'm not sure we have any clever way to poll the community that Ethereum didn't try before the hard-fork. They spent a few days of polling, whereas in Bitcoin we would take many months or years to gather the election data. I don't think we have a clever way to poll the community.

Part of the problem is that opinions change, and they are often conditional, and it's hard to collect all the conditions of those opinions. If you start with one idea, then change it, other people might no longer find those opinions to be representative of their beliefs.

It's difficult to reason about dynamic systems that involve these non-linear incentive relationships and we just need to target stability. In the bitcoin community, we favor soft-forks because we can build safety mechanisms where it is less likely to result in two chains. We can do this with consensus building as well. I think that in a world where everyone wants a hard-fork to happen, and they all agree, then it's not a big deal. But it's a grey area between everyone and not everyone, and how do you determine this?

The act of the Ethereum Foundation releasing the hard-fork was partly the cause of the trouble. It seemed official that there was a vote and everything was decided. And then miners/pools piled on. And in some cases, miners voted against it, but their pool didn't want to be the one mining the minority chain, and ignored the user vote. That happened and it's not representative. That's the Buterin Effect.

The official air of it gave it more traction than it would have had organically. If you said here's another client at another area to download, if that was how it was done, then it may have taken months and months if ever for the fork to activate because not enough people would have cared. Pools were just looking at this out of control effect that just happens.

If that one pool didn't switch to the other fork, they would have made a lot of Ethereum Classic coins. This is not unique to this kind of situation. It's the same in almost every vote on anything, like elections in any major country. People are often heavily influenced by who they are told who will win. Exit polling, even, can have major effect on this. If someone is on an exit poll showing the other way, it could swing the other way.

The value of money is in consensus. So the Buterin Effect here is way stronger here than in other political systems. It makes sense to go with the majority because otherwise my money might not be worth very much. This could cause a big amplification effect. It looked for a while that the Ethereum Classic market price would go up, it would be more profitable to mine, some hashrate would join, the price would go up, then more hashrate would join, and at some point it reached some equilibrium where it would stop going up. The hashrate got to the point where ... there were these run-away effects. It's psychological. It's a psychological cause for price increase. It caused people to explore the supply-demand curve in a way that moved the price up. Some people were saying "oh it has 12% the hashrate, so why is it only 10% of the market cap therefore it is underpriced".

I thought it was interesting that there were probably a lot of miners that had no opinion either way, but they mined it because they could make profit. Yep, that's what happened. That's how it works. For a future possible split, it's something to consider.

There is a lot of profit to be made by stirring the pot and inciting people to go off and go on a different fork, or maybe incite people to do things that might not be in the best interest of the system. As infrastructure providers of bitcoin, we should be careful to avoid stirring the pot, and we should be clear to not put ourselves in a position where it is incredibly profitable to cause things to happen.

Pretty graph of hash rate and price of ETC / ETH:
<http://slacknation.github.io/medium/13/13.html>

… Social aspects are incredibly important to understand the possibility of having the social motivation for having a contentious hard fork in the first place. It’s interesting because it is Hobbesian. You can have different social constructs.

... and by avoiding that, you can create new social systems that are more fair, etc. And ethereum is trying to build a society where their justifications are related to social norms. How you go about, you have the political justification like a "majority" or "majority belief" that the coins should be taken back. And we need to be cognizant that throughout the history and future history of cryptocurrency, this is going to be a defining factor in terms of justification for doing this.

This idea of like, what's going to come next after that, we're already increasing the block size with segwit. That's the reality of it. With segwit, the block size increase that we're doing is a one-time thing. The underlying technical details of this is that we cannot repeat segwit again, although we get a boost from Schnorr signatures in the near future. The specific technique only works once. With hard-forks, you could attempt to do that indefinitely and create a new coin every single day. There could be a trade-off between decentralization and size from each day, and doing a hard-fork from that standpoint could be quite controversial depending on the social precedence. It's hard to avoid that level of social controversy if you're trying to do a block size increase hard-fork. Equally, just the notion that anyone could do a hard-fork at all, it would be controversial and it's tricky to make it less controversial.

To bring it back to ethereum, since ethereum classic has such a lower gas rate, could we get the gas rate raised up to infinity and test out a fully scaled up chain? That could be really interesting, because then we don't have to test bitcoin with transaction fees only. They didn't fork their testnet, in ethereum, they had a testnet but they didn't fork it first. Has ethereum forked their testnet?

They set up a continuous integration network called Hive to do testing. You have to do live network testing. You learn different things in different environments. None of them teach you things that you learn in the production network.

It's more of an opportunity for security researchers to say "aha! I broke your test network", you know instead of saying "aha! I broke your coin" which would be decidedly worse.

You can answer some economic questions with a test network. One of the things I wanted Gavin to do with his block size increase proposal, was to backdate the date of the fork sufficiently far back so that we could see whether anyone bothers to run test nodes. You would need a couple hundred gigs of hard drive space to even test this. He said, in private, "of course nobody would run it". But he didn't think that was important. He had a point: the fact that nobody would run testnet, with lots of 8 MB blocks, doesn't mean that nobody would run bitcoin with 8 MB blocks.

During the Ethereum hard-fork, exchanges make play more important role for the success of Ethereum Classic. After fork, we did mine a number of blocks on the old chain. Until we gave up and nobody gave us any ...... but ethereum classic gets succeed once major exchange supported the chain. If we fork bitcoin, I think it's a situation maybe similar.

By the way very interesting that the exchange price, it was based on bitcoin. The exchange rate is based on bitcoin price. So what currency to setup the price? Kraken pairs are all bitcoin based now.

I have talked with Ethereum developers about this. They are all getting paid in bitcoin. Their prices are denominated in bitcoin? The way that they get paid is by transferring bitcoin. They have USD denominated salaries, but it's paid in BTC.

Some of this ethereum activity has impacted bitcoin price. On the exchanges, everyone who made an investment in ethereum, ... the volume of fiat for ethereum is very small. People making the exchange for bitcoin and then from bitcoin for fiat for use then for euro. This is the reason why the bitcoin price is pressured all this time volume selling is higher. So the people just leaving ethereum, at least some of them [are driving down the price].

The suggestion that they gave up on mining ethereum classic, because it wasn't necessarily as tradeable, to me that begs the question is it the obligation of exchanges to always by default continue listing the pre-forked coin? Even with 99% of, ... Well, remember there's a lot of money to be made with listing all the things. But let's say you have a preference for one. At minimum, because you bought in, you should deliver.

Say you are a gold depository. And there's a new thing called lead. And you're switching to lead. Yeah you should switch to lead. But at minimum you should deliver the gold bars.

A better example are stock splits. It's more clear that you should give both parts back, after a stock split. It's property. As long as there are some blocks on the other chain, it's hard to argue in court of law that you could get away without delivering both coin properties.

They could have waited a month with some best effort to hold coins to see how things play out.

Have we beat this topic to death yet?

So one thing to say about ethereum, is that you can say that what ethereum did well is that they made lots of positive media and PR while things were failing in the background. They continued to taunt success, while everything was failing in the background. In bitcoin, we tend to say things like "I don't like the way that's going" and have our arguments in public. It might be good for bitcoin confidence if we were more positive, like let's say companies were working together to say joint positive marketing. That kind of PR and marketing, in the bitcoin world, has the ability to be self-fulfilling. With a little bit more, the ethereum side could have maybe avoided some of this, if they were better at this. At a technical level, we could be very upfront with each other.

You have to be careful about how far you go with this. You have to build trust with external communities. They have to know that when they are talking with you, they are getting the real deal. Previously at a geophysics startup, they like to bring the investors to the engineers who talk frankly about what's working and not working, because we're talking about a 12 year project with $150 billion poured into it. The investors want to hear that something real for the next year is happening, not that something that is being filtered. I think there is a balance.

You have to look at other industries where nobody would dream of letting engineers speak in public, which could backfire for those industries. It's not necessarily the way to go for some industries.

There will be a reception in 20 minutes. We can keep talking. We can eat and talk.

Maybe this kind of hard-fork is very difficult to be prevented from, this kind of cryptocurrency system. The idea of a currency is given by the consent of the people who have participated in the system. In a hard-fork there might be 3 groups of people. Two kinds might be, I will persist in A, and the other party will persist in B, and there will be some people who say both parties have won and now there's two coins. In that situation, the split of the community will be very hard to be prevented. Before the ethereum hard-fork, lots of people still have an illusion that okay maybe one is the genuine ethereum... actually that's a lie, it will not survive. But after the hard-fork we just see that there's actually no genuine chain. And the miners, to kill the minority chain, is it the right thing to do? Any other hard-fork is now more difficult as a result of the ethereum hard-fork.

Ethereum's hard-fork, for example, is very controversial. It's against their own advertisement that code is law. In bitcoin, increasing the block size is much less important rule, it's just a technical rule that was written by Satoshi in 2010. It's technical, but it's not related to the philosophy or the value of the system. I think this thing, makes maybe in the future any hard-fork will be contentious no matter what.

Can you explain why you don't think it's tied to value? Well, I think he meant moral value. Why do you think the block size change is not tied to moral value? If we did a hard-fork to unlimited bock size, I would quit and I would be done. The block size at a technical level determines the decentralization and whether people can participate running the nodes.

But perhaps we should look at this in terms of fungibility. If there was a hypothetical break in fungibility, then people would find bitcoin uninteresting and move on. Block size can break fungibility, and that's why it's controversial.

The fact that you're hard-forking for a block size change, obviously presupposes that you're hard-forking. But we have a soft-fork for block size increase. The fork itself, ... hard-fork from the point of view right now, in the future, any hard-fork will be contentious because people can always argue oh this fork I disagree with, and both sides persist.

Did you say soft-fork as well?

If we activate a soft-fork with 95% with hasrhate, and someone says, this soft-fork I don't agree with. They would have to hard-fork. Maybe some people don't accept a soft-fork.

There’s a common argument that with a soft-fork there is less opportunity for people to disagree. There is also no problem with disagreeing. You are free to. Let’s let it play out -- say that a soft-fork is blocked. 6% don’t run it. What happens? It doesn’t activate.

Then it just doesn't happen. Then say this situation persists, and there are people are angry and they want the additional capacity and features. Then I think that situation is similar to what happens if miners are blocking some kinds of transactions. Because they are effectively blocking the segwit transactions, which people cannot make without that change. So how would users respond if miners were blocking and censoring these transactions? How would the stakeholders respond? I don’t think we know.

There have been guesses that people have made about this in the past. Perhaps there would be a hard-fork or something. But we don't know.

This is not about disagreeing with soft-forks. The solution we have for this is fungibility. If transactions are not identifiable, then this problem goes away entirely. That's sort of an aside, though.

Going back to the other point though, maybe after Ethereum, all hard-forks are controversial perhaps. I hope that is not true. One thing that when hard-forks came up in Bitcoin, which I proposed, was that this block size stuff whether you like it or not, has controversy. There are changes that we could do that would be uncontroversial as possible, if we were going to talk about a hard-fork in bitcoin, then we should first get experience with a change that is purely technical. I think that block size is not a purely technical measure. Perhaps a change that everyone is capable of agreeing with, for a first hard-fork.

Because of this split in Ethereum, it sets a precedent for Bitcoin for the possible future of hard-forks. For bitcoin, a hard-fork there can only be two options. One side must accept multiple chains, multiple attacks from multiple vectors, or we just stay on the main chain and try to kill the forks and the minority chains. There can only be two possibilities. Either you accept that there will be multiples, or accept that you can attack.

Attacks could be stopped, because you change the PoW on the other chain until the attack is not successful. And botnets might have PoW to attack anyway on a new chain.

I have 10% in this direction and you -- American government says I like this direction. Companies can lead their own chains because of the hashing power they have. ... .

... price increase, and it may have more than 50% of hashrate, to become the main chain.

I don't think we want multiple chains. I think that would be bad for bitcoin.

His point is that you if you don't want multiple chains, you have to attack the other chains. No, this is untrue. There are ways to prevent those attacks.

In the past, people thought that a hard-fork is good because there is A and B. In a soft-fork, ... if something is not controversial, maybe it's better to use a soft-fork.

Hold on. I reject the premise that a hard-fork necessarily results in multiple chains. Many hard-forks would result in multiple chains. There are technical ways to prevent this. Anyone can make a new hard-fork. It's always a possibility, even if no change is made, like we could walk out of this room with 10 hard-forks of Bitcoin in the next 10 minutes.

I don't think that's the real spectrum of choices. Attacks will not be successful if people want another chain to accept, if you use technical means to prevent those attacks from being successful.

I think is unnecessarily pessimistic to assume that any hard-fork in the future will result in two chains or be contentious. It's hypothetically possible that a carefully-prepared plan with all stakeholders in agreement somehow over some sufficient period of time, over some time period to satisfy duty of care, to make some change that has no philosophical or economic effect, or very little, then those things shouldn't result in any more drama than what we could create without a triggering factor.

Do you think exchanges and traders profiting from it, would they create drama? But they can do that now.

It requires users to believe that, at any point, there would be some point, ... right?

.. because of the... anyone who wants to start a new coin business, they could control a certain position of the hashrate, you could fork off the current chain and perform a hard-fork to lead the chain in the other direction that you would like it to go. And there could be only two ways to deal with that, either we have to accept that fork or we have to suppress.

No, no we’ve been saying strongly that there are technical measures that can be taken to prevent there from being that choice between follow and attack.

PoW change. Ok stop, one possibility is that there is not a fork created. One proposal that was made, as a hard-fork change, would be to in every bitcoin block header, there is 32 bits of zeroes which are always zero because of the minimum difficulty in the field that contains the prior block hash. There was a proposal to hard-fork the system such that the values that have to be zero right now, could be any value. This would give you extra nonce space in the header, which would give you things like the asicboost optimization without having to use version space. It would also allow more efficient mining hardware. It would change nothing else about the operation of the system. If this was done, then I think it would just happen and there would not be multiple chains. However, the asicboost patents make this political, whereas earlier it would have not been political.

If someone has the economic motivation to create a fork, then the choice fundamentally is to allow the fork or you disallow the fork. That's true for altcoins as well, though. Effectively a hard-fork is an altcoin, but it's pre-distributed in the same way that bitcoin is distributed. This has existed in the past in bitcoin, like Clams. It's not a problem. I suspect that if you did a hard-fork like that one, with a reasonable amount of notice, and an ability to get strong indications from the stakeholders and coin holders and 1 bit in nsequence, if you saw that for 90% of the transactions for the past 12 months, then I could see yeah the old version of bitcoin might be traded, but you would be in a situation where the social consensus would be to mostly ignore it. I think that's much higher chance, in comparison to ethereum with short notice for dubious reasons.

We had the ... which did eventually fork off older nodes in March 2013, no fork was created in actuality, because it was in the software for many months beforehand, it was uncontroversial, there were announcements, there were fixes that you could apply to old clients. Occasionally there are old clients that fork off, and they try to get back on. So yeah....

As I said, even, I would not define that as a hard-fork. It is from a technical point of view that it was a hard-fork. There was no fork actually created. It was a hard-fork rule change, but not an actual hard-fork. I think usually when we say hard-fork, we mean rule change. We don't mean an actual fork. When people talk about hard-fork in a colloquial sense, they are referring to the other thing. Thus this is inherently impossible to talk about in a clear way.

I don't think that technically hashrate attacks, I don't think that's an option that makes sense. Plus the legal options. We accept that altcoins exist. It's no different. It is the same. Mastercoin.... Clams is a better example here.

In ethereum, Ethereum Classic says they are the real coin, and Ethereum Fork says they are the real coin. Using the word "altcoin" might be politically loaded, though. It's unfortunate.

I am sorry for using this word again, but I would say, then I would say that the reason why the ethereum community split in this way, ultimately goes to a violation of a duty of care. If they were adequately careful in how they approach all their decisions and promises, then they would have more universal support of the community in one direction or the other. I don't know, that is the fundamental issue. Well, if they had they done that sufficiently well, then they wouldn't have done a TheDAO bailout.

8 conversations at the same time. Need more cephalopod arms. More chains needed.

A failure of duty of care in this case for Ethereum was not being careful in engineering for the disaster to happen. There's more than that. They were tempted to violate their own principles. There was also a conflict of interest in that they were invested in TheDAO as well. The outcome could have been different without the conflict of interest with their TheDAO investments.

What he was saying was that people in this room are angels. Don't assume devils don't exist. You can't assume some actors will not fork to a minority chain to disrupt the market.

EVAs don't exist ????

Could you explain, he's making a point about game theory, or, I am not following. Yes, game theory.

I think there's a misunderstanding, I don't think anyone is saying that we think it's bad to attack and so attacks won't happen. I think the argument I was making was that attacks to suppress an altcoin won't be successful, because they can change their technical rules to suppress the attacks using security defense attacks. Political and market attacks might be much more successful. 51% attack an altcoin and they will adopt, they will change their PoW, they will make technical defenses.

I think it is important to emphasize that in the same way as bitcoin, altcoins can deploy technical defenses as well.

The history of this is that there was an altcoin that was killed because someone said it was dead. That's mostly what he did. He was also 90% of the hashrate on this. But he said it was dead and that stopped it.

I have to point out there was an example of an altcoin that was attacked by a 99% hashrate attack. It had like a 72 block time warping reorg. They made zero changes and survived for 2 years before changing the PoW. I think this was feathercoin.

There was another one where the developers attacked it. There is lots of obscure history here that is hard to document in a timely manner. Have you ever played a game called Illuminati? Let's bust out the board game and we can all play Illuminati the board game.

Short reception break soon or now.

# Mining software

(Back from break)

We could continue our discussion tomorrow, if we want to. Any closing remarks? What about problems with Bitcoin Core? I have never been a miner, so for miners, what has been the biggest problem? What are the issues that need to get fixed?

For people who are programming Bitcoin, we use the software, and sometimes we don't like a problem and work on it to fix it and make it better. Some developers are mining, but definitely not at the scale that the professional miners are doing. Who in here is mining? Who has ever mined? Who has setup Core in order to mine with some actual hardware? Do you include failing to do that? I just wanted to make a point that it may be surprising how few developers are setting up miners in the current environment. It fucking sucks. What could we do to make this better?

There was a period of time when development was actively ignoring mining considerations. It was sort of assumed that the mining industry was big commercially successful and that it could take care of itself. As a result, developer attention went to other areas. As a result now, I am not happy with the state of mining configuration in Bitcoin Core. But I am sure that issues, like pool operators and miners encounter, go beyond just configuration of mining, and usage of it is probably differing. I would love to hear about any issues.

For a miner, he can just setup a Core software instance, and then he can start mining. But one problem that cannot be resolved [that arises] is the orphan rate.

Hmm. Hm. Mm. Mmm. Okay. I see.

So there are mining farms. They want to setup mining pools. Because of the orphan rate, and the stability issues in the system, forced them to give up on that. So they have to join mining pools to mine blocks.

What stability issues? Besides being a pain in the ass?

bitcoind hang-up sometimes.

When were you doing this?

Maybe at least two years ago.

That may have been, for example, HTTP connection errors. RPC errors. So these have been fixed. We fixed that particular issue since then.

If you can improve it, one thing is, it's very hard to set or prioritize transactions and setup our own manual rules to select transactions. The transactions (rules?) do not persist if I restart bitcoind. Maybe a better way to customize the options here. I would like to see bitcoind connect to outside network with same time using Core network and also another network at the same time.

You can do that. Maybe there needs to be documentation about this.

If you set a proxy... ? It's -onion. It's not -proxy, it's called -onion. There are a bunch of different options. The behavior you want is possible, but we need better documentation to explain how. Better documentation would be helpful for you here.

It will use the normal network for normal connection, and use the tor proxy. To connect to tor nodes it will use tor, and for normal nodes it will use the normal network. I want to have my bitcoin nodes behind, only connect to some known trusted nodes.

He wants -connect combined with -onion. Ah, it doesn't do that right now, but it could be done. He wants to connect a local node, but then all other.... This make connection much more reliable. You still have a slow link, but it's a link.

((Developers mumble amongst themselves. Solution found. Can fix.))

The request to persist transactions... prioritization? Persist the mempool, and to persist prioritization, and a better prioritization API in general.

Also, it would be better to have more proxy settings which one could be a backup of another one. Our nodes have to be setup outside of China as a remote server. We have to setup two tor proxies to make them much more reliable. With only one proxy, if one fails, then everything fails.

Yes, I think we can do that. You need the ability to add proxies without restarting? Do you need the ability to add proxies without restarting? Well, we will send you an email and get your requirements. I think this should be no problem to do everything you just asked for.

This would make bitcoind much more reliable and as reliable as possible while keeping the IP secret.

When the networking library gets merged it would be good to have a tool that analyzes the network config to make sure we do not incorrectly connect to the incorrect networks.

In 0.13, there is compact blocks, which can help lower orphan rates somewhat. This has been deployed in FIBRE network for world-wide block broadcast and this can help reduce orphan rate. There will always be an orphan rate in the network by design, but we can make it very small. The problem we would like to solve is the one where you have to join a big pool to get out of orphaning. That's an example where big pools have an advantage due to their size. And better block propagation could reduce this advantage that big pools have. Larger blocks that take longer to propagate contribute to this problem, which is a problem for block size increase proposals.

This is part of a general project that we would like miners to be mining locally off of a local bitcoin instance. So they said they were trying to do that, but it didn't work for them. They were talking earlier that they want to open-source their pool software for this purpose. If you see any hang-ups to this, then we need to know about those bugs so that we can fix those. Some of the tor configuration things can be alleviated.

At the time of Satoshi, everyone was running their own bitcoin nodes on their desktop computers... but now only exchanges and major businesses, they run this software on their machines. Bitcoin Core is still basically designed for desktop.

Well, not really. I think most developers run Bitcoin Core instances without the GUI and this makes Wladimir sad often.

I think he means small devices?

You can have several Bitcoin Core configurations for different purposes. Like the default dbcache size. Number of connections. If the db cache size is too low, it's super slow. The default, until 0.13, has been 100 megabytes, and that's slow. It hasn't been larger because we expect people to not run it on desktops because desktops have lots of RAM, but to run it on VPS where RAM is more limited.

There are many things where if it was only running on desktops, we would have made changes and made it faster. But we haven't due to concern of running it on small VPS devices ((sorry, browser crashed while typing)).

This is a longer-term goal of Bitcoin Core to provide the basic consensus part, through libconsensus, so that it is easy for people to go and write full node packages which are completely compatible with the rest of bitcoin but also have different API and different feature sets and written in different languages. Well, we are in the weeds here. This is something we hope to work on as developers.

The C++ code is difficult to maintain and it's slow. It's an important goal for us to have, to have a consensus package that we have that could be used by any language, and could be used for any application they want to integrate that into. So maybe btcd could have different wallets on different networks and everything else. Well, particularly he was talking about mining policy, which I assume is the kind of development he is interested in.

I am working on libconsensus specifically because a customer asked me to. To have a node more easy to customize in C#, that's the same reason why we were talking about making libconsensus.

I think we only have 10 minutes left. If anyone would like to make some closing remarks, then we could wrap up today's discussions. We should also mention topics that we would like to talk about tomorrow specifically.

# Some topic ideas for Day 2

- - Fungibility
- - blockwitholding attack
- - soft-fork to prevent block withholding attack
- - soft-forks
- - maybe we should discuss latest innovations in block propagation
- - how to communicate better
- - Bitcoin Core communication issues regarding updates and progress
- - lightning network stuff
- - miner profitability regarding second layer solutions
- - block size, HK agreement, etc.
- - AsicBoost and patents (and soft-fork prevention??)
- - Patent pools, patents, defensive patent strategy
- - regulatory pressures on miners if any
- - regulatory pressures and legal considerations for developers
- - decentralized variance reduction
- - weak blocks
- - long-term mining profitability (like when a transaction fee might become higher than the default subsidy)
- - new APIs for bitcoind for wallets and blockchain services
- - overview of segwit and segwit security review (re: their question regarding how do we know it is secure)
- - the future of transaction fees, wallet fee estimation
- - mining policy rules and expression and loading that into Core
- - getblocktemplate upgrades
- - bip9 version bits stuff
- - weak blocks
- - replace-by-fee things

Google Bus tour will require you to sign your name on the sheet of paper. When is the tour? On Monday afternoon at 3:30pm.

Mempool synchronization. There was a request for historical mempool snapshots and that data to be made available. Maybe we will ask Chainalysis, do any of us know them?

# Day 2

For developers I would like to request coordination using IRC regarding allocation of talk time. We need explicit pauses and "catch up" time. Transcription has a slight delay and projection has an additional (internet) delay. Time must be given for reply.

Good morning. Does everyone have a wifi connection? Who does not have a wifi connection?

((going through list of topics enumerated on the previous day))

There might be topics that people are not aware of that developers are working on, things like segwit and other scaling items.

What about the miners? Would you like to start out with some topics? Anyone else?

Developers meet in public every week with each other on the internet. We talk regularly with each other. It would be better to have input from the miners regarding what they are interested in talking about.

What about requirements for bitcoin? We all want bitcoin to succeed. We have in mind things that we want. It would be good for users to be able to buy ASICs. We often don't talk about how that would be done. We would like more people to be able to use bitcoin, or for bitcoin transaction fees to be lower, but changing the format in a certain way is not a requirement. I think that if we could collect a list of requirements, that we would be surprised how much we might agree on those requirements. It would be a good exercise to go through.

What do you mean by buying ASICs?

You can go and buy a bitmain S9 on a website. I could put in a credit card, and some time later an S9 will arrive by mail. For example, there are not many manufacturers that sell ASICs in a form factor that work in a house. There used to be KNC, they don't exist anymore. These guys make shipping containers. KNC is out of the market.

The housing market is just for reputation.

It was like worse the implementation. Doesn't sell the miners because inside these dangerous high voltage and it's not possible to certify them in the EU or the US (for consumer use?). If you are making them smaller, then you are just using the type, and there's no reason to sell it. So you would be going for bankruptcy, you would not be able to make it. It was just maybe wrong decision on our side. It would be good to create the product without the certification and some specific requirements, they just solve the technical problem, but it doesn't pass the certification. And lately, it was just a question about survival. There is no time to split the team and there is the other percent. Right now this is some other problem with containers. But chips, there is the key I think, they will release and they will be available. I know about creating USB efficient stick, will not be so efficient for the functions.

Just the idea of a requirement is that many people should have ASICs.

What do you mean? You want to buy ASIC or you want to buy miners?

What I am saying is that it would be better if there were more manufacturers.

Maybe we should reformulate it. Mining hosting? Keeping the miner at home I think more far is will be more complicated task.

What I think he is trying to say is that for the long-term survival of the Bitcoin system, we think that it is important for participation in mining to be very widely distributed. And that's sort of a requirement. But how we get more mining more distributed is an open question.

In the future perhaps we will have better distribution of ASICs and mining among users.

Yesterday we saw a graph, for all the companies, for mining companies in 2015 from 10 companies there are 8 is ... so the .. because is grow very fast, the combination is very very high. So then it came to stagnation, so often, maybe we will see other players.

There is also Avalon 3, right? They got bought by somebody? I cannot talk about them I think.

The bigger thing that he was trying to ask about is that we all think about things that Bitcoin needs to achieve in the future. A requirement example is that Bitcoin mining is widely distributed. Another example requirement is that bitcoin should be easy to use. Perhaps another requirement would be "bitcoin fees should be under X threshold". It is often useful to think and ask about requirements, and not technical mechanisms, because there are often multiple technical mechanisms to achieve requirements. There is also often more agreement about requirements than there is agreement about mechanisms. So perhaps we should talk about requirements that we find interesting.

Mining data center not centralized, we already draw them up and tried to show how many miners is distributed by the .. of the map. I could also mark his data center because I did not have any information, they could release them up and it would be great PR because it would show that mining is not just some point, there are 60 persons located in China for example, and it's very distributed and the statistics can show, it's great PR.

Multiple locations does not distribute it. It's still under the same control of the same company or government.

No, even the data centers, what they were saying yesterday was that .. they cannot just make some attack so easily, they perform maintenance and just to combine all the power .. so I think it's technically very hard to organize like that. In our case, a huge part of, to investors. It's not our power. I think it's not just one or two investors, it's hundreds or thousands. It's even more than the number of Core developers all together.

Keep in mind that if the developers go away, nothing happens in Bitcoin Core development for a while. No, that's not correct. Well, it's not the same as mining issues where immediately bitcoin fails. I mean that nothing goes wrong if developers vanish. The software keeps working, for a while. Whereas if mining disappears, bitcoin breaks immediately.

If someone were to do a hidden modification someone wouldn’t discover it.

No, it’s not that easy. It's very difficult to get things to pass peer review. I would say that I am much more worried about, and in particularly because if something happens to the developers, there's a big pool of talent in the Crypto community. It will take a few months.

Let's just agree that both our concerns, that we want decentralization.

If we want bitcoin to be a success in 5 years, what characteristics do we think it has to have to be a success? Perhaps mining should be reasonably decentralized. We could say, it should support many users. It should have reasonable fees. Which of these do the miners agree with? What are they interested in? Do we see fungibility as a pretty existential interesting item? Maybe if you say mining, that might not be a requirement, the actual requirement is fungibility perhaps.

The main requirement for bitcoin mining is the low cost of electricity. A lot of those low power costs are located in remote regions. They are distributed around the world. That advantage by itself proves the decentralization model.

# Progress and organizations

I think we should try to short-term plan and long-term plan. We should try to improve our image to investors. We could also talk about the image presented to investors. All the internal battles and conflicts hurt that image. There is no centralized PR for developers. The developers are actually somewhat opposed to centralized PR. Nobody from venture investors, they say many times, they are not really technical. They are not following technical presentations. They would like to get some financial information about the status of the project. It does not yet exist. Maybe we should hire some people to represent Bitcoin community interest.

I recognize that someone mentioned the opinions on the decentralization effort. I would like to make two points. I think that the R&D in bitcoin is currently needs some improvement. I believe that it's a little slow in pace. We need to improve and accelerate the R&D effort in Bitcoin. The second point is that I would like to make is, could we have multiple versions of software and multiple parallel R&D teams getting involved in Bitcoin development to improve its R&D? For example, in Ethereum, the R&D efforts are very active and funded by Ethereum Foundation and we could learn from their examples and draw lessons from and also improve our own R&D effort.

What is Ethereum doing that we're not? Some concrete examples would be useful.

I would like to ask how many in your room has submitted more than 1000 lines of code into the Bitcoin repository in the last year.

Lines of Code is not a good measure for progress on development. It is difficult to measure what is progress. What about when people review source code? How do you measure that? What does it mean whether someone contributes by line versus time reviewing or designing? Code review can be much more useful than writing code.

Can we get a translation regarding what Ethereum Foundation has been doing that we have not regarding R&D? What is the perception here?

Okay, so. He thinks that because ... they have more versions of the software, and also the price of ethereum also proves that it has more activity in terms of R&D and system improvement.

His point is that there is correlation between price and ethereum's R&D activity.

Well, bitcoin's price is much higher.

Bitcoin's current rate of R&D is much higher than it has ever been. We could use statistics to show this if we would like.

I definitely agree that there are communication problems in the Bitcoin space. For example, talking about what is going on in development. Awareness in the public is not particularly good. We need help to fix this. The actual level of R&D activity is high. Since Bitcoin Core 0.12.1, which was just a few months ago, the diff size between the master branch and 0.12.1, is 184,000 lines of patch between them. So that's a considerable amount of development activity that is going on. This work includes major features, including features which are important to the mining ecosystem. Maybe we don't talk about these improvements often enough? Perhaps we do not speak clearly enough about these developments? We are often talking to other developers. From a development perspective, our focus is on development activity, making sure things are running smoothly, but we do not often communicate to drive the price for example. We would like to do more.

There is a fair amount of hostility in the Bitcoin ecosystem. This creatures pressure against the development community to speak about progress. Every time the developers speak, there is a hornet's nest of negative responses. We get a lot of negativity, even for talking about forward progress. This is very demoralizing. In development, our culture is often that we would prefer to do good work, and not necessarily promote our work or talk about it.

I counted the bitcoin repository lines of code. I only found 120,000 lines of C/C++ code including empty lines and header files. Where did you see 184,000 lines of change? Where did it come from?

It was a "diff" (the difference) between the older versions and new versions. It includes both additions and deletions. Between two versions, there are added lines and deleted lines. This adds up to 184,000 in total. Someone can work for 1 month on a new feature to replace an old feature. This can mean 1,000 lines of new code, and 20,000 lines of removed code. The line of code metric is not a good measure of R&D quality or progress. You can see this result yourself in git, we can show you how to measure this you just type `git diff v0.12.1` after `git checkout master` and you can see for yourself the differences between the master branch and v0.12.1.

```
git checkout https://github.com/bitcoin/bitcoin && cd bitcoin
git diff v0.12.1 | wc -l
```

... more details can be read on <http://bitcoincore.org/> (or <https://github.com/bitcoin/bitcoin/compare/v0.12.0...v0.13.0rc2>)

I would like to thank you for your efforts on R&D. You are the main development team in the Bitcoin space. I recognize that as you just mentioned there is a lot of negativity and attacks on Core developers. From the outsider perspective, this contributes to the image that we are not unified. We have divisions among ourselves because of this. This is in turn compromising the development of Bitcoin. At this point, I am not sure that the Core development team is going to improve their PR effort, or whether they will dig in and bury yourselves into the work and not try to improve your PR.

One clarifying remark is that some developers feel that they should not participate in PR (public relations).

It is very difficult in a project like this to get PR because one of the reasons is that, ... they have massive investment, they have money available to market themselves and Ethereum. In Bitcoin

Core, we do not have this funding. All of us work as volunteers. We do not have funding. We are not experts on marketing. We are not PR experts. Is there a way to improve this? The Bitcoin Foundation did not work very well. We are open to ideas. You have to understand that we are developers. We are not good at PR. We are not funded.

All of you are volunteers? Okay.

The claim that Bitcoin's creator has a premine is untrue. It should not be circulated. This claim is false. No, we did not say that. We were joking about something else. Oh, okay. Yes. In bitcoin there was no premine. In ethereum, they premined and funded their marketing and development. We don't have that in bitcoin.

My belief is that for such a large development effort, without financial resources, it's not feasible to move forward. The Bitcoin Foundation fell not because the model was wrong, but fell because of its poor management.

Because they got arrested. Only two of them.

Maybe the bitcoin community needs to rethink about how to fund the development effort. He proposes that maybe we can fund another foundation to provide financial resources to development efforts to make things easier for you guys, to make it feasible and sustainable in the long run.

.. and it should involve the major players in the bitcoin space in this foundation.

Bitcoin Core has a sponsorship program in place. We have worked a little bit on that. There is also an unfortunate barrier of entry regarding education for developers. One of my projects is using libconsensus such that people with less technical skills can make their own full node. That's what I'm trying to do right now. I hope that in the future there will be more work there.

Are you doing that full time or part time? Part time.

He believes that for the Bitcoin development effort, just rely on donations and sponsorship and also part-time work. Also, a couple of highly skilled developers is not enough. It's not sustainable in the long run.

An interesting question for the people in the room here, of the developers, who is working on bitcoin full time?

We definitely agree that there needs to be a more sustainable model. It cannot be just one approach. We need to do multiple things to make R&D sustainable. One problem that we have had in the past, which has made our PR efforts more withheld, is that we have had problems with initiatives to do public outreach. These initiatives have used our work to try to take control of Bitcoin. They have used our work to try to argue for their own authority over Bitcoin. This was the case with Bitcoin Foundation. This was a bad experience for many of us in Bitcoin Core. The Bitcoin Foundation failed and failed to be sustainable. But also, Bitcoin Foundation used its influence in ways that were harmful to long-term sustainability of bitcoin.

As someone who worked for Bitcoin Foundation, I did not like telling people that I was employed by BF. I went out of my way to avoid even mentioning it, as a developer. Even though I was free to work on code without being involved in the other stuff they were doing. They tried to express control over Bitcoin [like in a social way].

I don't mean to say that Bitcoin Foundation took bad actions. However, many outsiders perceived it to be in control of Bitcoin. That was a problem. As an example, Ethereum Foundation is perceived to be in control of Ethereum. This kind of control over Bitcoin must not exist. We need sustainability without control, and we need this without the perception of control too. The perception of control is also a major problem. By stating that Ethereum is forking, a statement made by Ethereum Foundation, they were able to silence people who had disagreements with that hard-fork plan, through social means. Also, see the related Buterin effect.

Okay. He feels that the reason why you feel that some initiative would try to take control of Bitcoin and through Bitcoin Core development. Why people blame you for that is because the interest being represented by Core is still narrow. (Something about narrow business interest?) The interest group you represent is still too narrow. The community is not being represented. I think he means that you are not representing the majority. What he is proposing is that we need to form another foundation that could engage most of the companies in Bitcoin industry so that they can all fund that foundation which in terms would fund you.

Some developers care less about earning money, which is why we do not [...].

The foundation may not be able to represent most of the industries in the Bitcoin space. Because those companies and industries might have their own private interest. They might be antagonistic to each other, like Coinbase versus Blockstream, so it may not be inclusive itself. It is hard to have one foundation that represent the majority of interests in the Bitcoin space because of the conflict of interest. How could you setup one organization that can....

It is not possible to have one organization that represents everybody.

We should do what is right; as a developer who does not own a company, I do not like the idea of companies controlling a foundation.

<https://bitcoincore.org/en/about/sponsorship/programme/>

We need to design a system where there is nobody in control. This is perhaps not best represented by the companies that exist today. Business interest is important, as well.

Let's separate the issues first. Let's not talk about the format of the organization or this foundation. Let's instead revisit what I just mentioned before. My points are that, first, for such a complex and large-scale development effort, you must have financial resources. Otherwise, you cannot be sustainable in the long-term. You must have full-time staff. You cannot be part-time. That is also not sustainable. We need to involve more people. We need more than a few smart developers. Based on these, we can talk about how we can form that foundation or some other entity. I just strongly disbelieve that this amorphous and loose organization can really sustain in the long run in terms of the complexity of the R&D effort.

I think we have to discuss whether such an organization is necessary. And then we can discuss how to run such an organization, as a later step.

My personal experience from the Linux industry and especially... I agree that we cannot rely on volunteers for sustained progress. The trouble here is that we have seen dangers of a single centralized organization. Since that time, it has been confusing to not have a single centralized organization. However, since that time, we have made more progress than in the past from contributions of a mix of contributing orgs, some private companies, some non-profit organizations, have worked together, such as the two developers working at MIT DCI. There are some chain engineers at ChainCode Labs, as another example. There are also some engineers at other companies. I have heard something about a Chinese company wanting to train an engineer to become a Core developer. (That has not been going so well). Oh, I see. Well, you have to continue that investment. It takes a while. I hear that a Japanese company now wants to begin the long-term investment to also train Core engineers.

And, there is no company that controls Linux. There are many companies that contribute engineers full-time to work on the upstream open-source development projects that Linux relies on. Linux Foundation is more of a coordinator. Linux Foundation does not control Linux.

Sure, I can explain. Linux has many companies. There are a number of other Linux vendors in addition to Red Hat. There is Intel, AMD, ARM, and many 100s of other companies in the Linux software ecosystem or in the system integration companies like IBM, HP, there are many of these companies all over the world and they all decided over time to devote full-time engineers to the upstream development projects of the Linux kernel project and the many other thousands of pieces of software that are used in the Linux stack.

There is really no one company in control of Linux. And Linux Foundation serves as a coordinating function for the Linux software development community. It is a little confusing there. To simplify how people understand Linux, it is sometimes described as the Linux Foundation making decisions -- but I think that the way that things actually work in Linux is that the Linux engineers make decisions based upon peer review. They won't let a large moneyed interest to override what they think is a sound, technical decision.

One thing I would add is that the Linux Foundation has helped other open-source industries to better coordinate. The Linux Foundation has offered to help as a neutral process facilitating function regarding Bitcoin. They theoretically do not have anyone inside that cares either way about Bitcoin. It is an option to ask them for help. However, I don't know if it is the right approach.

I think Linux is a good open-source example. Linux Foundation helps Linux to do PR and engineers focus on development direction. I think Bitcoin developing can take example from Linux. My first request, I want to modify my request. Where does such organization, many organization, whether it is necessary for Bitcoin.

Okay. I think Linux has set a good example. The Linux Foundation has, they work on the PR for Linux and the engineers are just setting the rules for the system development. Based on that, I would like to modify my first proposal. Can we learn from the Linux example and maybe we can follow the Linux example and setup one or multiple foundations for Bitcoin such as for Linux like Fedora, Redhat and each one has their own foundation. Is that true?

That is not exactly how it works.

I would like to add that, I personally see potential for process facilitation and communications as early roles that are easier to agree upon.

One thing to say perhaps is that there is a perception that there is no Bitcoin Foundation-like that is guiding bitcoin. However, there are many different organizations that are supporting, in limited capacities, different parts of Bitcoin. MIT DCI is paying for a number of developers to work on Core on a full-time basis. They are running classes. They have been organizing events that help to promote bitcoin. They are supporting only three developers, right? Yes, but there are others being supported by other organizations. Bitmain is currently paying for one of the current developers. Blockstream pays Pieter to work on Bitcoin full-time. Ciphrex pays Eric to work on Bitcoin Core. There are other organizations that are doing political lobbying (like Coin Center in the U.S. for political changes).

It is a fact, though, that from the point of talking about the technological work that we are doing, that the community is failing to communicate this adequately. We had this discussion earlier today about comparing to Ethereum. There was some laughter from the developer side earlier during that discussion when someone made a comparison to Ethereum. It was not meant to be insulting laughter. Rather, we feel that we do a lot of dev work compared to Ethereum. Since a few minutes ago, I looked at the data. I found that there were 3x more commits to Bitcoin Core over those to go-ethereum. (the numbers are 27 contributors to go-ethereum vs 96 to Core; and 1294 to core commits vs 490 to go-ethereum since january first) There was even more developers for Bitcoin Core not Ethereum in this case. We could be doing more work to communicate this more widely. There is more work to be done to communicate to the public about this. Perhaps there are some additional needs for organizational efforts around that? But we need to keep in mind that we have had very specific problems in the past with these organizational efforts, such as the earlier stories about Bitcoin Foundation that we have explained. [And despite the lack of funding, we are still more productive than Ethereum Foundation.]

If ethereum is written in Go, is it a higher-level language and do Go commits compare to C++ commits directly?

Can we take a break? Yes.

From my perspective, we try, we the development community, we are successful if you never hear about us. However, this is not always the most useful perspective. We agree. There could be some organizational efforts to promote Bitcoin technology could help a lot.

I am curious about the miners in the room, who mine Ethereum, how many different client implementations do you use? Just one.

Lunch will be setup outside this room. We will continue to have the meeting in here.

Apparently, Ethereum literally has more marketing employees than developers. There are literally more people working for Ethereum Foundation with the role of marketing, than there are employees that do development. This is surprising, but it also explains a lot. Bitcoin has 3x more engineers, has much more value, much more code, and has approximately zero marketing. There has been some improvement, perhaps.

Something else about marketing. So the discussion about setting up a new foundation. To me, it sounded like one of the intents would be to have some Bitcoin marketing. Maybe from companies. One of the problems in the Bitcoin ecosystem is that some companies are saying negative things about Bitcoin. They are anti-selling bitcoin. They are saying negative things about Bitcoin or negative things about each other. In Ethereum, they fight only in private. However, the marketing people still continue to say positive things in Ethereum, even while the hard-fork was failing. It was very positive marketing. We all want Bitcoin to succeed. How about a marketing alliance that advertises and says positive things to people who would buy Bitcoin or who would buy miners or buy services from everyone's companies? Why are we not doing this?

Why not a standardized foundation in that sense? If you are proposing a marketing alliance, why not use a foundation which could have a template format we could use? It's more expedient.

We are not good at marketing.

Those are such very different goals. To mix the two with one type of organization, is what we're afraid of. We do not want this to have perception of control over Bitcoin. This tends to create the perception of control, and controlling the narrative and the way that people start to look at it. The previous proposal for a marketing alliance very specifically did not include development.

No control, like a Linux Foundation?

What is needed is not so much control of development, but rather process facilitation between the stakeholders in the industry and community, such as for marketing purposes and advertising purposes. When I say process facilitation, it could be to better coordinate marketing, but it could also help to better coordinate --- a very common problem is that people are not talking to each other. There are very simple problems that for example, miners or exchanges could have solved, if they would have asked (requested) the developers for help. Historically, that request has not happened. This would be solved by process facilitation. [Regular, scheduled contact and communication.]

What does facilitation mean? One example of facilitation is regularly scheduled one-on-one meetings between industry members whoever they may be. Some stakeholders don't naturally communicate with other stakeholders, and perhaps having an intermediary or other coordinating roles could help. When you don't have this, all kinds of assumptions happen, often these assumptions are incorrect. For most developers communication is not a natural skill. Having others to fill this role and fill up calendars with scheduled meetings would be profoundly helpful. Having others to be available to work on these problems, to help assemble a big picture view, so to know who to connect to on a given issue. Developers are not naturally going to put those on their calendars without being requested. You cannot rely on volunteers for this sort of effort to be a sustained benefit to the ecosystem. Instead, there should be people who are paid to have these roles. So when I suggest an org that is only process facilitation and maybe also a marketing alliance, this is what I mean by "facilitation" and what I think about in general.

My question is, first I say that facilitation is an important role and to make it sustainable it has to be someone doing it full-time. Is there one or more people that everyone can agree could do this with neutrality because they do not work at any company?

There are companies in Bitcoin who are more effective at marketing. BTCC does some marketing. Blockchain.info did a promotional video. I think I have seen videos from other companies. Maybe the companies that are good at that, could form an alliance for marketing and persuade other companies to join. Probably those companies could get some help in providing technical progress reports that they could make. They could simplify the Bitcoin Core meeting notes. There was a release of a candidate for Bitcoin Core release yesterday, but it has not reached mass visibility, perhaps it has not even reached visibility to people in this room. This would be a good example of a task for such a marketing alliance to focus on.

Who here is subscribed to the Bitcoin Core mailing list?

Would it be helpful if we publish mailing list summaries periodically? We need a place to talk where it is in our language. But perhaps summaries could be more targeted to a general audience? Maybe a digest?

Your weekly release for developers, it's not for common people to read. It's not for non-technical people to read. That's why they hope you can make them more transparent.

We can definitely make communications more directed to a general audience. That feedback is very useful, so thank you for sharing that.

I wanted to share my perspective as a developer of an alternative client. One thing about "we need more bitcoin developers". It's actually an arduous process to get up to the level where a developer can contribute (not to bitcoin core, but to _bitcoin_). I have done this recently myself as a developer. In btcd, it's funded by a company called Company Zero, and we have much less developers than Bitcoin Core. The intersection of developers that know bitcoin and Go is smaller than C/C++. We have been working to catch up with Bitcoin Core with soft-forks, but btcd is behind at the moment on the soft-forks. I think bitcoin development is going quickly. We have been working on BIPS 68, 112, 113, 9, all the segwit BIPS. The CSV package (68/112/113) has pull requests outstanding. They are pending review (btcd is behind on BIP9/68/112/.. But has segwit in progress). We don't have enough reviewers. There are maybe 5 active developers for btcd. It's a different skillset. I think the btcd code base, and it’s sub-packages is itself a big investment in terms of bitcoin infrastructure, they are good libraries, and Lightning development is enabled by btcd and infrastructure investment there. Maybe btcd itself does not do enough marketing for itself. It's a little less known than Bitcoin Core in that respect. However, if people want to contribute, they could get into the development team.

I have been testing segwit for the past 4 or 5 months. We have tested on segnet, testnet, we have made lightning channels, One developer made the first lightning channels on both segnet and testnet. The pull requests (segwit, csv-package) themselves have not received as much review, but we’ve been testing it for the last six months or so. He made the big blocks on segnet and testnet to make sure that we could verify them properly. I'll slow down.

How big was the segnet big block? It was about 3.6 megabytes. We had a competition between ourselves. We wrote good spamming tools.

The other thing is that I think one thing that is needed amongst other development teams for Bitcoin is that collaboration is required. The recent segwit BIPs have helped with this. It's good to have multiple eyes reviewing the BIPs themselves. Us implementing the large changes, we found some things about segwit, and we gave feedback to the other developers. We made a transaction on segnet that had 19,000 inputs to test how well the sighash function works. Before that, it took about 29 seconds for Bitcoin Core to validate that. We implemented sighash mid-state caching in btcd and then it took 3 milliseconds or something. Core has a PR to implement hash caching also, and as a result of our testing has some great examples to benchmark against.

This was an example of how other implementations can help because btcd used a different approach to implementing the Bitcoin protocol. From this, we were able to see that they were compatible with segregated witness, and showed some corner cases. This was helpful and very useful. This work was good and we're thankful that they did this work on segregated witness.

Maybe I will make a couple of comments here. I think that, I am not against creating a separate team for developing the project. If we have multiple teams, then coordination between teams takes a lot of time and cost and resources. You cannot go to war with 10 battalions and no general to lead. Developing the product, you always should have a general architecture and a general engineer. In the Bitcoin network, it's more about the standard, it's a communication standard. You cannot create ten different software projects because they will not be able to communicate.

What good do you see coming from having multiple implementations?

From the perspective of the venture investors, it will be very complex to explain what you are doing and how you are doing it. If it would be a battle between Core and other implementations, it would decrease the trust in Bitcoin, decrease the market price of Bitcoin, and it does not help make R&D go faster. If someone thinks that they can make a new split from scratch, then they should name it something else like an altcoin. I think that it is much much better if we create a team like Lightning where we can inspire the bitcoin core team and then coordination between different teams will increase productivity overall. They can internally discuss the idea and agree, and if they all internally agree then it would be helpful and efficient and stable, then it can be merged back into Bitcoin. For Bitcoin Core, I think it would also be helpful to add more efficient developers and more leaders and support them in a more transparent way. Right now, even than some companies are paying for some developers. Okay. Right now that's not the issue, but there might be lately a lot of questions, it should be really transparent, like one central point, I don't know, one whatever you call it, it should be transparent and like a business you donate your money and this money supports developers [like the Bitcoin Core sponsorship program?]. That's it.

Thank you for the recap. Lunch is setup outside.

Development is somewhat hampered when you increase the number of implementations. Development can also be hampered by having multiple implementations. It takes more coordination and more effort to have developers reviewing multiple implementations of consensus-related software. It is enough work to do it in Bitcoin Core. If you are asking for multiple implementations, then this request is incompatible with having faster and more R&D because it divides our efforts, our time and attention, and weakens our ability to make R&D

progress. Ethereum Foundation might seem like a fast mover on R&D but that is perhaps due to the misperception generated by their marketing efforts. They have more marketing employees than developer employees. "Let's split your engineers on 3 different projects so that we go faster" is nonsensical because software engineering does not work like that. Perhaps we are not understanding what the other side is saying.

(Note that this was from lunch chit chat, the following was not discussed as a group.)

What do the miners see as the future of Bitcoin in the long term? What is their take on this? Yesterday there were two answers, but we would like to hear more from the miners.

Can we please also get an assessment from both sides regarding the level of misunderstanding that they think is continuing to occur here today? This would be valuable feedback.

Wallets should probably show the moving window average of number of zeroes appearing in blockhashes. This would be useful for improving knowledge about current difficulty. However, consumers might get concerned when that number does (or does not) change.

The short-term interest that some have regarding bitcoin market price would be to crank block size to infinity and pump the price. But what about the long-term interest in bitcoin? What is the long-term value of bitcoin? Why is bitcoin valuable in the first place? What is it about bitcoin that is different from other products? The concern that some developers have, regarding constructing an organization exclusively devoted to PR and marketing, is that control can unintentionally degrade the value of Bitcoin even if we each individually have good intentions going into such an effort, because of how contrary it is to the ethos of Bitcoin, decentralization and fungibility. Core developers don't have a way to design this type of organization, while preventing the negative outcomes that are obviously applicable, and for this reason we have not made a proposal for this type of organization.

# Block size and hard-forks

We had a good discussion in the morning on a number of topics. In the afternoon, the miners would like to shift the discussion to block size scaling.

I think that we can start by talking about the Hong Kong agreement. I know that it is not an agreement with Bitcoin Core. I know that Bitcoin Core cannot sign an agreement. I know that it was individuals that signed. We know that there is a disagreement even within Bitcoin Core whether to scale the block size, how much, how large, how to do it, whether to do it. Those individuals promised to propose a hard-fork proposal to the Core community for reviewing.

With everyone joining forces, it is good for marketing, it is good for the economy, but at this time we feel ... with the promise of those individuals ... several today are joining us here as well. I also recognize that we will have to spend resources for you guys maybe you have salaries and means lots of budget and... some... forum. I think it's kind of a promise. Maybe you are not representing Core, and we understand that. But from your personal promise, I think this is a promise that you guys need to fulfill. There might be some delay, but I think we should talk frankly to see what's going on here.

Keep in mind that we do have segwit, which is a block size increase. We need to go get segwit out and implemented. After that, the Hong Kong agreement what it was, was a change in how segwit's block size increase would be allocated.

Let's answer the question. Let me keep going.

I think that right now, I think the biggest concern is that Ethereum has shown that this is looking a lot more risky. When we met in New York, we talked a lot about how we would get consensus and show consensus. The miners were not in New York. I am not sure if people are aware about this.

Many of the HK agreement signers spent a week in NY. We did a lot of design work. We talked about how to properly construct a hard-fork. We talked about how we would do this in a way where we would not have the same risks that Ethereum has recently experienced. We talked about in HK how it is important for Bitcoin to remain unified and how it is important to the long-term value of Bitcoin. In HK, and in NY, there's no desire to do anything that would be controversial. We would need consensus around any kind of hard-fork that would happen. It would have to be incredibly non-controversial. While it's certainly the case that a lot of that research and many of those discussions should be made more broadly available, there's certainly a lot of concern now that even from people outside this room that it would be very difficult to get that level of consensus around a hard-fork. While proposing a hard-fork is one thing, which I think should still happen, or at least proposing some details about how a hard-fork should look, which I think should still happen, as of the last week I do not think we would be able to get the kind of consensus we need, such as from Bitpay and their investors, who saw what happened with Ethereum Classic, to get the level of consensus required for Bitcoin Core or for Bitcoin to have a hard-fork that does not result in a significant loss of value.

I think it's worth mentioning too that, a majority of, we were heavily disagreeing in NY amongst ourselves even in the New York office how something might be deployed. Much of that was due to talk of signaling. Since then, we have talked about several assumptions. One assumption that someone originally proposed was that "nobody would follow a minority chain" or "nobody would attack another chain". There were discussions about those different scenarios. It has been enlightening in the last few weeks to see that some of those things are in fact very possible and are more concerning than we thought before. It's something that requires thought. It provides a new data point. It requires some new analysis I think.

I wanted to point out that hard-forks are very disruptive to markets. They are disruptive to merchants, to markets, to entire ecosystems. We have to take this into account. Unless there is an overwhelmingly strongly justified reason to do a hard-fork, then the costs outweigh the benefits. We have been looking at ways to solve these problems in Bitcoin without having a hard-fork. This has been a huge focus of our engineering work over the last several years. We have been working on ways to make everyone happy in the ecosystem [although we are not maximizing happiness].

Also, yes I have been writing code for the hard-fork. It's not ready at the moment but I do want you to know that I have been honoring that commitment and have been writing code towards that.

<https://github.com/luke-jr/bips/blob/bip-mmhf/bip-mmhf.mediawiki>

<https://github.com/luke-jr/bitcoin/compare/bc94b87...luke-jr:hardfork2016>

Regardless of whether we have reached a broad consensus on a hard-fork, based on the recent Ethereum hard-fork experience, a Bitcoin hard-fork would inevitably take place. At some point in the future, it's bound to happen. Based on the ethereum hard-fork and experience, they believe that the hard-fork for splitting Bitcoin is inevitably bound to happen.

Only if we try to make it happen. Already happened with Clams, right? A controversial, disharmonious hard-fork does not need to happen.

This divergence in opinion is kind of hard-wired into human nature, even amongst this small group we have divergence in opinion not to mention the broader community. Because of this divergence of opinion, it's going to split the public into like two or more multiple user groups and opinion camps and ideology of how bitcoin should be implemented. Some may belong to Core and some may not have a development team. That might be hard-wired into human nature and politics.

Okay. Even though there may not be such a development team at this point, because people are driven by interest and this drive might compel or invite another development team to jump in and do this kind of work.

To offset this trend, it's necessary for us to increase the user base. And if we treat Bitcoin as a reserve currency, then the possibility for it to split is high. But if we treat it as a payment network, then people are unwilling to let it split because you would increase the usability.

When you say payment network, what does that mean in 5 years or 10 years?

If we treat bitcoin as a payment method, then we have to support new tech development such as LIghtning Network and a bigger block size to support that functionality. Based on this logic, all of our effort is to defend ourselves against such a hard-fork effort that may occur in the future. In order to defend a potential hard-fork in the future, we need to provide some kind of forum or unified basis so that different voices in the Bitcoin community can have a platform to communicate with each other and resolve their differences and reach consensus and to protect ourselves against such a malicious hard-fork in the future.

It’s not that easy to get everyone together to communicate and discuss.

It’s not that it’s hard, it’s that you did not do it. (Scaling Bitcoin conferences?)

I agree. I think we need to work to make sure that Bitcoin is both a system for payments and a reserve currency. As a system for payments alone, payments do not have sticky long-term value. You (the customer) buy coins to pay, then you pay to purchase some item, then you (the merchant) sell coins. This does not result in long-term preservation of value. Also, to be a good payment network, Bitcoin must have tech like lightning because no reasonable amount of block size would make Bitcoin large enough to scale to the payment needs of the world (like 1 million transactions/second). We must preserve the long-term value of Bitcoin while growing the user base. We need to find as a way as a community of Bitcoin users to come to strong agreements in order to defend against malicious hard-forks that would damage Bitcoin's long-term value.

The first link is the BIP draft. The second link is some of the code to implement that BIP. This is related to the hard-fork commitment.

I would like to apologize to you, and to the developers, for undermining their efforts to produce this material for you regarding their commitments. I did so because their efforts in New York came right after some public comments about blocking segwit regarding a hard-fork. In that environment, I felt very uncomfortable about hard-fork proposals slowing the scaling of bitcoin through segwit. I regret the climate that my comments created. I am sorry for that and for my comments.

I think I need to clarify this. Segwit block also come from the ... that the HK agreement would not be respected. It's a very bad spiral that we have got into, in terms of bad communication. Maybe both parties don't want to do something under pressure. Maybe both parties don't want to be threatening.

One problem I did have was that a lot of people in the Bitcoin community told me that they would never want to hard-fork. So despite my agreement with you, I had others telling me they were concerned about a closed door meeting. I was hearing that a lot.

After the HK agreement, both parties were unhappy. The big blockers want really big blocks. 2 MB would never make them happy. They were not happy. And it was a bad agreement for them.

And for those who want to control block size growth, they .... and I think at the meeting we both agreed that we should try to convince other people that this is kind of a best compromise.

There are a lot of people that don't want a hard-fork at all. It's a hard-fork. Everyone has to agree to a hard-fork. It's difficult.

Do people not want it? Or rather, do they not want it now? People have said "oh, they never want a hard-fork".

Oh, that's not true [of my beliefs] at all. The negative discussion about hard-forks makes future hard-forks harder. That frightens me. The system will need hard-forks in the future. But they need to be harmonious hard-forks. People fighting against hard-forks makes this less likely. I think that we will need hard-forks in the future. I hope there will be hard-forks in the future.

The HK agreement did not happen the way I would have liked, but it happened anyway. It would be better to have a better way to come to agreement about how hard-forks happen. It would be good to have lots of community voices coming together. Hopefully we can set a precedent regarding what is the right way to do a hard-fork.

One observation here is that it sounds like we could have avoided much drama. When I heard about the "let's block segwit" statement, if I had reached out to you directly and clarified in private, it sounds like this could have avoided problems and improved Bitcoin's public image. I think there are many opportunities for us as the Bitcoin industry to try to settle our disputes one-on-one. This may improve Bitcoin's public image as well and be more productive for all of us.

Maybe someone could describe the, like the MMHF hard-fork. And someone else had some BIPs about that. What are in these BIPs? What is the structure?

I think a lot of the opposition I was getting was regarding a closed door agreement. They wanted it to be something that develops organically.

I think that if I can expand on that, there is a political challenge where if someone external to Bitcoin tries to enforce a hard-fork on bitcoin, then it must be rejected for bitcoin's long-term survival. When we are talking about designing a hard-fork, we must make it clear to the community that the desire for the hard-fork is organic from the Bitcoin space. I think that what he found was that the structure of the HK agreement undermined that understanding. Perhaps that could be overcome by getting more support for it, but still it is something to keep in mind for how we handle harmonious hard-forks in the future.

I think that people believe that communication should be open. Nobody noticed that BIP draft. There was no place to publish things like that. There was no blog post about it, or a tweeted link or something, to the draft. Anyway, please describe what it does.

I had summarized some of the ideas we had discussed in Zurich. I think we first need to know, it seems like there's some discrepancy even between a few people, regarding the ... maybe he could explain his BIP draft.

If you scroll down to the specification section; well basically, don't read the document. What features does it have in it? Pretty much most of it is making the hard-fork safe. How does it make it safe? The simplest possible hard-fork would be one where old nodes continue on the old chain and not follow the hard-fork. If people did not upgrade, then the nodes would get stuck and the chain would be vulnerable to attack in the worst case. So what you are saying is that one of the concerns you discussed in New York was that un-upgraded systems would be vulnerable to hashrate spinning up and mining fake confirmations where people don't know about the fork, like automated withdrawal systems would be compromised unfortunately. So your hard-fork proposal is one where they are still mining on the original chain from the perspective of un upgraded original nodes. The way this is designed, the old nodes will see the old chain as empty blocks. They will follow that block and they will not be left vulnerable to fake confirmation attacks. This is done by defining the serialization of these headers separately from the hash algorithm of the block hash. So the block hash is then calculated with a more complex algorithm than currently. Have you implemented this in source code? Yes, partially. The p2p stuff will at the moment not talk to the old nodes, this needs to be fixed, which is similar in segwit. It has comparable complexity to the segwit change.

I think it's important to clarify that this is a difference from the Ethereum hard-fork. In that hard-fork, if you ran an old client, in comparison this one will not allow transactions to be confirmed. The old nodes are forced to make a decision, do they want to do the hard-fork or do they want to do a different soft-fork to prevent the hard-fork? They are not left vulnerable. They must make a decision one way or another.

You could say that this proposal is not much of a fork. It is blocking transactions. There must be a fork to block the transactions. Anyway, this is the main design principle. There are other interesting elements in the design of this. The new header structure gives more nonce space to the miners that they could use in ASICs without having to do the whole merkle tree for the transactions in the ASICs. So it would lower the communication cost to mining devices. However, it does not put the extra nonce space in the compression run. It's asicboost [extranonce?] nonce. It repurposes 3 of the version bytes to nonce space as well. You have version bytes in the new header. This also gives, this proposal also gives nonce space in the version field. It's basically enabling asicboost. It's an interesting discussion that we should have separately in another venue. Does it have other interesting features?

It fixes the timestamp overflow issue by cleanly overflowing. It's using 32 bits to represent a 64-bit timestamp. It makes a long-term improvement for timestamp handling, because we want bitcoin to last many thousands of years. Part of bitcoin's value is that it's forever. If we can fix the time/clock issues, then we might as well fix that.

Another thing that the proposal does is that it's designed for merge mining natively. So namecoin won't need to have whole bitcoin transaction bogging down every block of theirs. Merge mining is more efficient, which we could also use for side chains. Version bits have been expanded to have separate bits for more hard-forks in the future, so that we don't need to repeat the complexity of this R&D so that it can simplify the idea of a soft-hard fork. Anything else? He's looking at his BIP draft.

It redefines the merkle tree algorithm to fix the duplicate transaction issue that we worked around. It fixes a bunch of technical minutia and it's hygienic, it cleans things up, it reduces technical debt. Obviously we need to .. for the old blocks. Also it improves things for SPV nodes and lightweight clients.

What were the problems with this proposal?

Well (laughter), I think the tricky thing with this is that because it's a firm fork.... No, let's translate. I would say that the tricky thing with this is that because it's a firm fork, ... a firm fork being, that it is a soft-fork that forces everyone else off the network (those who do not upgrade). If you try to do that with 50/50 approval, then politically it looks like it's an attack against the minority. From a technical level, it means that miners can do this by veto. The problem is that we want to avoid political ugliness. Do people understand a firm fork? It's combining a soft-fork and hard-fork. There is zero possibility of two coins afterwards. By default, it would not be two coins. If I am running a bitcoin node and I do nothing during the hard-fork, then I am guaranteed to be forced off the network. Then I have to take action to either accept or decline the hard-fork. This is coercive. However, if we got solid indication that we got consent from the bitcoin community, then it would not raise major issues.

A lot of what I talked about in New York and previously, was how do we see whether coin holders have approved this? Are they going to use this new chain? Are we going to not end up with Ethereum and Ethereum Classic situation? Or are we going to end up with a unified bitcoin? I think it's important that we find a good way to have coin holders to show that yes we actually approve of this. We can actually use coin voting as a way to argue that the whole economy has approved of this. We can otherwise set a precedent where miners can push through changes without consent, which calls into question the value proposition of Bitcoin. So that is why coin readiness signalling methods would be useful to avoid having the value proposition violated so directly.

It's not necessarily that the whole community is going to vote on this. How are we going to look at those results? What would it mean if some voted but not others?

If you have a wallet and you did not upgrade, then you are at risk. It's easy for that wallet to end up on a chain other than the one you suspected. We must respect people's rights to not go with this consensus. It would be dangerous for us to try to question the consensus they want to go with. Who is in control here? Is it users? Or is it the group of bitcoin miners? It could infringe on the value proposition of this being a currency with a stable meaning.

He believes that in this case, if those wallets refuse to upgrade, then they would be taken off the network.

It's only if they neglect to upgrade, then they would be left off the network. If they choose not to take the hard-fork, which they must do actively, then they can continue on the chain without the hard-fork. They must do something to accept it, or to reject it, but there is no "default" behavior.

The existing chain will have blocks, but with zero transactions.

So his proposal is that, people who are using the current software, their software stops working. New software is released, and then if you install it, it defaults to the chain with the most hashrate. And there is a button that would say "no I want the other chain" .... no, there would be no default. You must choose A or B. It's a user interface question. So who is the origin chain? Nobody would be the origin chain. And if we are doing our job right, hopefully nobody would choose reject, because otherwise we failed our community by choosing something without consensus.

Ethereum's voting turn-out was so low (5.5%), and the people who voted were probably very invested in TheDAO. It's possible that they had hashrate majority, but not most of the users.

Can I give a bigger picture here? If it was designed such that the greater hashrate could decide that this would be a powerful weapon to befuddle bitcoin in the future, the people would look at bitcoin and say "oh the government just needs to buy a bunch of hashrate and rewrite the rules at whim". We need to be able to respond to that and say no, lots of hashrate can attack the network, but no they cannot rewrite the rules at whim. So this BIP design still supports the existence of the original chain, however through non-technical means we should make sure that perhaps nobody wants that original chain to exist. "Hashrate deciding" is a long-term threat to Bitcoin's value and fungibility. It's each person that must decide for themselves. Nobody should decide for them.

In this fork, I think the economic or market cap, ... we want everyone to make their own decision to join the hard-fork. But yes, market cap would matter. Importantly the things that were mentioned on security earlier is that we need to build public process to make sure that everyone knows that this has nearly unanimous support and then it would be very easy. If there is doubt, then there is opportunity to trade on the doubt and make a political stink about this.

Their point yesterday was that people would try to do that. Well, we can minimize that. A very clear signal that there is no doubt, would be to show that a significant percentage of UTXOs or something in the last year, that yes they agree, through some coin signalling method. That's what coin signalling can show. It can show that people who use the chain and own coins that they agree with this.

You should explain that proposal. Have they heard it?

I know that ethereum with their hard-fork did a limited version of coin signalling. They used their coins to say "yes I agree/disagree with this change". The concept is simple. If you own some BTC, then you should have a voice and you should be able to say I own BTC and I would be willing to use this new definition of what BTC is, and I am not going to oppose it. Wallets would have a button for which way do you want to go. Some BTC might be in cold storage, etc. It should be about coins that are spent over the last year, not about old cold wallet coins stored a long time ago.

Before the hard-fork, there should be a new version of the wallet where you could signal with your coins, whether you like the proposal or not. If that is reasonably high through this measurement, ... we would work with all wallet vendors, exchanges, hosted wallets, everything would be using this coin signalling mechanism. The point is not to trigger the hard-fork. The point is to build political consensus so that any adversarial fork created from this has the least chance of surviving.

Coin signalling is very easily gameable by malicious entities. The method is to purchase some BTC and then signal in a way that does not represent the wishes of the community.

There would be public outreach, coin voting, and using every means at the community's disposal to make sure that everyone is on the same page and such that the harmonious hard-fork would be as clean as possible. Ethereum should not be the point of reference, it should be testnet4. Yes, just a second, I am almost done making testnet4.

He actually believes that what has been proposed here is something that makes the hard-fork easier. You almost make the hard-fork a not-so-hard-fork. That is why he believes that you may have opened up some other issues.

Yes.

If we are comfortable with this approach, then in time we would be inclined to perform more and more hard-forks in the future if we are getting more comfortable with it. Because it would not be as difficult to execute any more, based on your method. So this might open up a pandora's box for more hard-forks in the future which might alter the immutability principles of the Bitcoin blockchain. Although I believe that we need a hard-fork eventually, but we have to do it in a way that we should not set bad precedent for the future. We must do it with precaution to minimize such jeopardy and pitfalls in the future.

The proposal does not change that the hard-fork needs consensus. This is still a requirement.

Many people in the development community share these concerns, and this is part of why there was not much published after the meeting in New York as well.

When this idea was originally thought of, it got termed an "evil fork". That was the term. Precisely because if you have 95% hashrate then you can perform any type of change you want. But if we had a simple hard-fork, which means that the miners are kinda threatening the community. What if it is not accepted by the market or the users? So in that sense it is threatening. But miners want to kill the old chain.

We don't agree. Part of the proposal makes it easy to make it the side rejecting the fork to fire the miners. It has a switch to ignore all the blocks produced on the "evil fork" chain side. There has been effort to make sure that the miners don't control it. There is a risk, I agree it. It has that risk, but he was saying that when you upgrade, you have to make a choice. There is no default choice. If "A" is the high hashrate and "B" will make a checkpoint or change the PoW or something, but it would be implemented and ready for that eventuality. Let's say that we don't know what the users want, even after coin signalling. Perhaps the old chain doesn't exist, maybe it does, but we make it possible for it to exist anyway, without making it a default.

Is it possible to switch to PoW and to a PoW+PoS so it is a mixed system? A mixed system is much more difficult to attack?

Research does not support that.

If someone proposes an evil fork, then perhaps there are attacks on the old system. [.....] .... that mechanism could be used to coordinate that fork away.

My main point was that the mechanism of people signalling their support for a hard-fork, with their coins and UTXOs, could be used to also change the PoW function. If miners want to go against the economic majority, then the users can show support for a PoW switch and continue on, and leave the miners behind. I hope this will never happen. But it makes it easier to do so. I have bobchain and it's the best thing ever. Because this thing could happen, I think it incentivizes people to cooperate.

There is a research question in there. Could these hybrid systems be used? All of the PoW+PoS hybrid proposals in the past were very obviously broken. They opened up new serious attack vectors, for each attack vector they reviewed. Perhaps in the future someone will come up with a strong hybrid. I look forward to the research, but we don't know a way like that.

Using coin signalling to start a new chain could in theory work, but we don't know how to both of them at the same time. We know how to say at this point start this new thing, and it's PoW. But not about both things at the same time in the same change.

It gets into a lot of complexity. All of the hybrid altcoins end up doing checkpointing with a central point of control. It's interesting to note that.

[Short break.]

# Long-term goals for Bitcoin and fungibility

So what about some long-term success goals for Bitcoin? What are the things we hope to achieve over the next 5 or 10 years?

We have to remain secure. We need efficient ASICs. I argue that we need fungibility. It's one of the important distinguishing properties of bitcoin, that it is permissionless and global.

We need competitive fees. They can't be too high because they might prevent use cases. We need lightning and Bitcoin on-chain. We want, presumably, many users. We want everyone to benefit from this technology and for everyone to own bitcoin.

We need long-term confidence for this to function as a store of value. We need people to be confident that these properties will survive. We need to also survive regulation risk. There are less regulatory risks than compared to years ago, but there are still some.

I would say that positive marketing, like the marketing discussion earlier, could help these things. We could attract new users. We could explain the benefits to any users. We could figure out what people like. If we had positive marketing, it could help confidence. A nice positive bitcoin business ecosystem could help regulators feel more comfortable and help reduce regulatory risk on our industry.

If we look at this at a high-level, it helps developers figure out what to work in the short-term. We care about fungibility, therefore we work on new protocols to create fungibility in various methods. Maybe we try to make mining sufficiently decentralized to achieve fungibility in practice. And perhaps we are careful [Chrome crashed].

I am suggesting that it is useful to have a framework for discussions. For people who are making ASICs or doing payment processing; if they all agree that over the next 5 to 10 years these are the objectives, then great. I think that sometimes we get stuck in a mode where we don't think about these long-term objectives. What do the miners think about this? It's like me going to the ASIC manufacturers and saying we need 10 nm tech. But maybe 14 nm is better. How would I know? I should let them inform us. If we agree on the high level details, then we can let people who specialize on the details do what they are good at, including people who are good at development, or people who are good at marketing especially regarding why people should buy bitcoin.

Perhaps miners feel that there are long-term priorities that are different; perhaps for bitcoin transactions you would pay more because it is a permissionless system. Perhaps you would pay more for this transaction because other systems would block those transactions. In an ideal world, perhaps transaction fees would be low. Yes, externally, competitive. They can't be punitive of course, only those who would be extremely

What is their vision for what we need or want in 5 years?

Fungibility is a relatively new term to us. I think the decentralized money is-- money should be decentralized. Specifically, that's something I agree with. Fungibility is a new word to this community. What does it mean? I think it will create lots of disagreement in this term. We want a united network. Store of value. Maybe we need to keep the principle as simple as possible. If it is too complicated, it needs to be in a single term that everyone can understand, and not something that will create lots of disagreement.

What is fungibility? It is a big word. We can give some examples of things that are not fungible. Paypal has a bad reputation because they suddenly one day stop accounts, even though you had done nothing wrong. And then you have to argue with them for 6 months to get your money back. That is not fungible.

Fungibility technically is the ability that every coin has the same value as every other coin. Specifically, the example about paypal, is that someone as someone that receives money as a paypal user, if you fear that paypal will revert or block the transaction, or freeze the account or undo your ownership of your own money. So fungibility, in bitcoin, translates to the inability to censor transactions. This relates to privacy and decentralization. Maybe fungibility is too high level of a term to describe what we want here.

I can give an example. Let's say that some people give me 1 BTC. It should not matter which person gave me the 1 BTC to pay you. They should all be 1 BTC. That's what fungibility means. There is no "dirty coins". There is no blacklisting.

If coins are not the same value as each other, then they would be worthless.

Paper cash does not have this problem. They have serial numbers, but the serial numbers on the dollar bills are not used. It's not your fault. If somebody gives you some money that they have obtained in a crime (or ethnic crime), in most places you are not in trouble for spending that.

To be clear, this is not necessarily about crime. It could also be for funny examples. Let's say that if you have 25 BTC that are freshly mined in a block, then they should not be any different from any other 25 BTC. What are you talking about? You mean 12.5 BTC. No, 3.125 BTC, look to the future my friend (where testnet is).

Another related concept to fungibility is that Bitcoin is permissionless. You don't need to ask for permission to sign up. You don't need permission to send a payment to a person. There are things that reduce fungibility. There are some companies that are trying to analyze the blockchain to claim some coins are worse than others because of their association with people and payments and transactions. That is very bad for bitcoin. We should make sure that people do not have to be involved with a government or bank in order to send a transaction. It should be cash-like.

Maybe a remark here. I think that point number 4 on the board, that many users. I think it should be higher on your list of examples. I think the second point, fungibility, should be... in that place.. More people using it, more people know about the technology, it's immediately create bigger fungibility. A very good example is what I saw was happened in just a couple months in the Ukraine is that they just include in monk an option to send you can keep bitcoin on the account and you can buy them on light the bunk it. And people stop to buy it even just to try, and they create huge volume in just one single month. And right now they create a lot of ... and I am receiving just a lot of email in one small country. They have been creating 10 different events. And people start reading about the technology and start trying that. And what bitcoin is still missing is missing the good documentation, and good representation by someone. So the users should be indicated, and to indicate the users you should get some lectures for reading and talking about bitcoin, marketing materials for explaining bitcoin, and so on. So many users, depends on documentation, and from lecturing, from books, from mentioning in the news, in multiple ways.

Among this group, only I am running an exchange other than the person that had to leave a moment ago. I have first hand experience with regulators. Regulation in China is big but … in the U.S. it might be even worse, the pressure of regulation is heavy. A lot of those exchanges, have problems with coins getting frozen, because of association with money laundering. If bitcoin becomes fungible, I am afraid that you would be even more subject to regulators.

He feels that the regulation pressure in China, is big, but the regulation in the United States is even more. There are even more regulations here in the U.S..

Bitcoin today in practice is fungible. You can trace it, but it doesn't matter which BTC I give you. It's still a BTC.

For example, in my exchange, there are some frozen funds by the government because of money laundering suspicions. We hired experts that analyzed the blockchain to trace the source and movements of those coins through the blockchain to prove that you know we have no relation and that we're unrelated to the money laundering activity. So that is why we need to know the traceability of bitcoin in the blockchain.

I think bitcoin might not be comparable to cash for this because in bitcoin you have, you can track the source by anyone and in cash it's very hard to trace the source.

That is exactly what fungibility is about. It's about making bitcoin more like cash.

Yes it's like cash, but it's not...

The bitcoin whitepaper calls it "p2p electronic cash". We think it needs to be more cash-like.

Maybe like cash, but anyone can trace where it is coming from.

Yes, but not reliably.

Yes, but we are talking about long-term goals.

What I heard is that, what I understood, so please correct me if I was wrong, if Bitcoin becomes more fungible then regulators will be more burdensome to you because they would not be able to track Bitcoin. I think it's the reverse. If Bitcoin becomes fungible, then regulators will not go to you because they will not be able to extract information.

I don’t know how the U.S. police do but because law enforcement in China work, even though you cannot provide the source information or the source of fund information to them, that would make them even more suspicious of the outcome and the source of the funds. This might make them take action to freeze funds. This is why he thinks fungibility in Bitcoin could create even more regulatory pressure for the exchanges in China.

If the coins are fungible, then they cannot be frozen. By technical means, regulation cannot be...

You do not enforce the regulations in the protocol itself. The enforcement would happen at higher levels. You could audit businesses, without modifying the fungibility of bitcoin itself. [The AML/KYC happens at the business level, not on the blockchain.]

Bitcoin in many ways behaves like cash. On this particular issue, the characteristics of bitcoin, because if you want to make the protocol and make bitcoin even more fungible on the protocol-level, I believe it's just a wish. You may not be able to make it happen. It's because you know, there's a difference between coins on the blockchain. Some coins are dirty. Some coins are clean. That's just how they are. You can't erase this difference. You can't make them the same.

We can erase these differences.

Let me put another angle on this. The other part of fungibility is that, even if you could trace the origin of coins. There should be an expectation in Bitcoin that if I create a transaction and I pay a competitive fee, the coins should go through. So the transaction should happen regardless of whether governments want to lock that transaction and prevent it from happening. In ChainAnchor they wanted to go and block transactions that did not have correct AML/KYC. To some in the Bitcoin community, this is more concerning than fungibility itself. Even if you could trace the origin of the coin, then at the very least you could not prevent the transaction from happening. So you could still trace the origin of the coins, but the transaction would never be stoppable.

Gold is legal and is highly fungible. If there is tainted gold, and tainted serial numbers, you can still melt the metals down into liquid and get untainted gold. So we can do the same with bitcoin.

In a system with good fungibility, regulatory compliance can be achieved even greater than it is today. If payment protocols between exchanges allowed for the sharing of identifying information on that other network, that would improve regulatory compliance. If the system is not fungible, then we have international uncertainty created by different policy in different jurisdiction which creates uncertainty about coin value. It is perfectly technically possible to make coins that are absolutely always equal with equal origins. There are competitors like zerocash (zcash) that do this as their competitive basis. If bitcoin is poor at this, then it is not as good at digital gold and not as good as a store of value and we could see bitcoin out-competed by those competitors.

The fungibility aspect is a huge competitive advantage of Bitcoin versus the existing financial system including Visa, Paypal and Mastercard. The greatest advantage that Bitcoin has is that it eliminates counterparty risk. It can eliminate counterparty risk with legal risk. You do not need to underwrite your counterparty's legal standing. The moment that they deliver your bitcoin, you have the good. The underwriting in today's financial system has a significant cost.

Maybe explain underwriting? Well, it's the idea of taking responsibility. If I take a bitcoin from you, it's not up to me to determine if you are complying with the laws of some other jurisdiction. Underwriting means you are not responsible for the liability of the other party (the counterparty).

The point is that it's cash. If I pay you bitcoin, you own the bitcoin. It doesn't matter where it comes from. There are technical ways to make the origins indistinguishable (the same and equal).

People talk about chargebacks. It goes deeper than Visa chargebacks. The interesting thing about this is that when you are dealing with transactions worth millions and billions of dollars, they are not concerned about chargebacks, they are concerned about solvency of the counterparty. That’s why we have title insurance. With money itself, there is a lot of underwriting necessary similar to title insurance. When you remove that need, when you make bitcoin fully fungible, that's a huge advantage that bitcoin has over all other monetary systems.

This is also very important when we think about automated payments. Machine to machine transactions. And smart contracts. Because smart contract or a machine can't evaluate the counterparty risk or AML counterparty risk in a transaction; they can only look at the transaction. The only way to make a machine automatically do this, is to make the system more permissioned and trying to eject "bad" users from the system which would harm the permissionless of bitcoin. So, we the developers in the community think that being cash like is a very important competitive advantage of Bitcoin which supports other competitive advantages like smart contracts, machine-to-machine transactions, and that if we want bitcoin to grow in the world then we need to protect this advantage and find ways to further it. If we don't do this, then Bitcoin might be supplanted in the market by alternatives (like zcash, monero, etc.) which do.

Legally or technically?

If legally, then this might not be universal across the countries.

You make it work technically so that the legal choice becomes irrelevant. You don't need to make that kind of decision then.

If you are trying to make this technologically fungible, then you have to a serious change to how bitcoin works?

So there are ways with no protocol changes to achieve much better fungibility in Bitcoin. For example, this is done with lightning network. Some technology, like coinjoin, is built into bitcoin from day one. One of the things this results in is that someone who is engaged in criminal activity can already get pretty good privacy in the system. They can mine in order to get fresh coins. They can use coinjoins. They can swap their coins with other users. So the criminal actors already have fungibility enough for them. So the remaining question is what about the non-criminals? What fungibility do they have? What risk are we placing on users in our system?

Criminal users do not need as much fungibility as you might think. They need money laundering. The irony is that they are trying to make dirty money look clean. They actually want a paper trail. Criminal users want a paper trail. That's the weird paradox here. They do not want an invisible trail.

Most of the people doing coinjoin, you think, why they do that? I think most of them because they are probably not very clean, so they use coinjoin, ...

Criminals make false transactions that make them look like real transactions like "I sold a car" or "I sold a t-shirt".

I have been running my joinmarket coinjoin client the whole time on my laptop for this whole event. Why should I want to use a system that has poor privacy? I would rather use monero or zcash. Why would I want money that I cannot use to pay my obligations or to buy goods and services? You have competition from centralized users (which often have good privacy), and decentralized things which offer better privacy than bitcoin.

I received payments for moderating a forum online. Some of the coins from those payments came from totally lawful gambling sites, and the coins went to the forum, and then the forum paid me. And I deposited to Coinbase, and then Coinbase took weeks of arguing with me to get it fixed. It was not Coinbase's fault. They exist in a regulatory environment where they are forced to act in a certain way. The United States is very negative about lawful gambling services from other countries. Coinbase had to do this because they live under the jurisdiction of U.S. law. It's unfortunate because it's an application that U.S. law hates, even though I was paid for something completely unrelated to gamble. I never gamble. This is an example of getting hurt by a lack of fungibility in Bitcoin.

I think that responsibility should be applied to the user, and not to punish the entire system or the exchanges for the behavior of bad actors. Fungibility protects the innocent. Fungibility is about protecting the innocent. The criminals want to money launder, and they want public records.

I will tell you a true story. Some user a few months ago deposited 1000 BTC to an exchange. They believe the coin comes from a darknet coin mixing service. So he seized the money and asked the user for their photo ID and their AML document. After receiving the document, what did you... Did you release the coins? Yes.

Wouldn't you like a system where you can't even tell whether it's from a darknet market in its history?

Well they might be required by the police to do this.

I have an interesting experience where my employer is a regulated as a commodities trading platform, … the interesting thing is that even if bitcoin is completely fungible the regulators are completely okay with that. The thing is that the regulators require us to perform AML and KYC regardless of the fungibility of the underlying coins. So if the coins are all equal with equal origins that are indistinguishable, the regulators are okay with this. We are still obligated to investigate who our customers are, but the actual network-level blockchain sources are completely unimportant.

..... once it's in your wallet, it's moving around hand-to-hand cash in an economy, and in an exchange it's more like a bank account where you are transferring it to someone else and someone. .... cash on hand is more fungible than cash in a bank account.

We were talking about fungibility, AML and KYC for exchanges. Could you share some experiences from your exchange about that?

If there is a problem, then the police and government will come in and want to find out where the coins went.

The assertion was that fungibility is a desirable long-term goal or property. We are trying to talk about long-term characteristics that are interesting to all of us as a group.

It's hard to say I think. If you have fungibility, then it is what it is. It could be the argument that, if everything is the same, then there is nothing you could do. You can't really say it's good or bad right now, but right now the regulators do ask for where the coins go or where they were from. If it's not to a known address, then there's nothing you could do about it anyway.

Confidential transactions? Could we have updates?

As some people here know, there are a number of technologies for improving confidentiality and privacy in bitcoin. Coinjoin is one of these R&D efforts. Coinjoin has a limitation, which is that the coinjoin does not hide the values of the amounts being moved. Commercially, the amounts can be valuable information. The difference in values from before and after a coinjoin can be used to dis-entangle the coinjoin and find out the information. There is a R&D effort for signature aggregation which can increase blockchain capacity by 30%. It will also let you save fees by using coinjoin, it's a side-effect of aggregation.

About a year ago, there was a publication for confidential transactions. It exists in various sidechain systems now. CT (confidential transactions) makes the values or amounts of the bitcoin transactions completely private. We have been working on making this more efficient. Unfortunately the previous construction of CT added size. We have since then made it 20% faster. We have made it natively support colored coins and assets, and making them private, which is perhaps important for other systems more than it is important for bitcoin. We have also more recently come up with better ways to combine it with coinjoin that make it easier to deploy. We have been working on improving that technology. One of the great things about CT technology is that it only has a constant factor cost of scaling. If you were to apply confidential transactions to the bitcoin network, there would be an additional size to those bitcoin transactions that use CT would be higher, but that would be the only downside. The ring signatures in monero and the zcash tech have worse long-term scaling characteristics, CT is better in this aspect. I hope that this confidentiality work will benefit bitcoin in the near future, and if not bitcoin then at least sidechains.

You could say that you can separate the fungibility in an exchange, is different from the fungibility of a coin in your pocket. This is the same for physical cash and bitcoin. There are a lot of people who really love fungibility. They would be very sad if bitcoin became less fungible. If you were to talk about for many of the bitcoin holders, and asked them, if you lost a feature of bitcoin, would it upset you or would you stop using bitcoin? If it lost fungibility, many people would get upset. It's something that many people are passionate. That's why you hear all this excitement about new tech, decentralization as important, because decentralization is the current mechanism that bitcoin is using to have fungibility. It's the assurance that someone will eventually process your transaction. If one miner has a government that says don't process this transaction, then someone with a few terahashes in their garage in another country will still be able to take that transaction because of decentralization. So you need some reasonable level of decentralization to guarantee that all transactions will get processed.

Lot of stuff. But government and police may not share the same view. If we change the current fungibility technically, governments may change their attitude toward bitcoin.

Properties of good money: <http://contrarianinvestorsjournal.com/?p=391>

He thinks there are more people doing bank transactions than people using bitcoin. So does bitcoin really need fungibility? He believes that maybe we should focus more on the underlying technology to make bitcoin processing, like lightning network and making the infrastructure more robust.

Keep in mind that if you don't need fungibility in a system, then you do not need mining. You can use banks. You don't need infrastructure. We have a severe risk of competition from highly centralized efficient system.

We need ... very easy to ... .. banks and governments... still... maybe we need a fungibility, but maybe we can make this fungibility in another layer of this network, like sidechains maybe, and make it into the mining network, but on the main chain we should make the protocol as simple as possible.

I want to make more of a point there. If the main chain is fungible in the sense that you can do a transaction and it will always be mined, then you can make layers on top to make it more fungible. You can do coinjoin and lightning as second layers. The protocol does not have to be complex. If someone wants to make bitcoin less fungible, then I am not able to just go to you and say here's a list of addresses to blacklist. I think right now it's not a good story for now. When we look at the hashrate graphs on blockchain.info, it's not a true story, but it hurts investor confidence. We need to assure them that they will be able to spend their money. At the exchange level the privacy might not be good, but they need to be able to move money around.

Machine-to-machine transactions and smart contracts, it might be difficult to make alternative protocols reliable if bitcoin is not sufficiently fungible. Automated decisions made by wallets will not be able to respect the non-fungibility of a coin, which is an invisible property, which makes all of these bitcoin systems less usable. However, I agree that we should move complexity to other layers and keep the base layers simple.

My impression is that we are more in agreement than it seems.

A point there is that in bitcoin, even with no change to the system, fungibility changes over time. Originally in bitcoin wallet software, a new address was used for every transaction. Back when bitcoin started, there were no companies like Chainalysis or Elliptic that connected to every node in the network and monitor everything. Sometimes tech has to adapt to the world, in the same way that the block size has to change to adapt to the world.

Like a VPN, you run it on top. I think we are in agreement on this. I agree. It's not a magic bullet. In a bad world where bitcoin was very unfungible, then lightning and sidechains might not even be possible, or they might be unreliable. You cannot build a fungible system on top of one that is non-fungible. It's not possible. It's effectively impossible. Anything built on top of it cannot be fungible.

If you want to break those privacy properties, you break the underlying layer. This is not a detail. This is important. Building something "strong" on top of something "weak" is silly. We should make the base bitcoin layer as strong as possible. This sounds like a detail, but it's not a detail.

His point is that he still has to wait to see until after the exchange has used this fungibility functionality, then they will know the actual effect on their operations and systems. They think it is too premature to talk about its actual effect. So let's not spend too much time on this. Let's move on to something else.

Let's take a 5 or 10 minute break and then we can continue.

# Hard-forks

What topics do the miners consider important that have not been discussed?

Please have a seat so that we can continue and wrap up. Long day, lot of information, exhausted. We still have a few more topics to touch before we wrap up the meeting. Let's go with the miners first. Who would like to start?

Under the existing situation, the ... of Ethereum... have already given us an example of a hard-fork. Bitcoin could have a similar situation in the near future. How should we solve this problem? In the long-term, we should promote the use cases of bitcoin. In the short-term, we should build a wider, broader consensus. We need to form a platform to communicate and talk. It should include Core developers, miners, Bitcoin companies, bitcoin exchanges, and other users. Based on all the lessons we have learned from the other coins and their histories, we should give up the fighting and conflict. We should pay our attention to communication and cooperation. We should build such a platform.

Another topic we would like to talk about is that right now it's July 31st and it's the last day of the HK agreement. We think that individuals should give an explanation to the community.

How should we make that communication platform? What explanation should we give to the community? The miners need to give kind of an explanation or somehow to the community as well. We have those pressures as well.

Personally I am happy to see work on that.

If someone was to post about the status of this, to draw attention to the documents and code that he has written, would this be the communication you are looking for about the agreement?

I believe that would help a lot. Okay, I can do that. One thing that I wanted to ask about that, on that subject, because of the people opposed to the hard-fork from the agreement, and because of the people who are saying deadline time is up time is up all the time, maybe we should remove the pressure, and I will continue to work on a hard-fork anyway?

We should research this. He doesn't want to be working under pressure. There are many open problems still. It's better to do this without the auspices of pressure.

Okay a better communication would be, how would you like to do this work? I think it's important that people do not continue to perceive that work as a closed door Hong Kong agreement to do a hard-fork. The hard-fork itself must be designed organically and normally.

So perhaps a question would be, on a personal level, would you want to work on a hard-fork proposal? Yes I am going to do that, but if there's an agreement, then the community perceives that negatively.

So maybe present about the deliverable, and now it is better for the larger community to collaborate on it. So further collaboration and work would be open collaboration and work. Would that be agreeable and good?

You can make a proposal to the wider community. The proposal might not be completely finished, it could be a draft, it's obviously something that requires further work, it's the proposal so far. The HK agreement said after segwit, too.

It is much better to admit that the time is delayed. It's not a problem. We can just say frankly, it's delayed. For lots of engineering reasons; ethereum stuff, we have lessons learned; segwit is delayed, etc. Are we okay with saying this? It's not just him, it's everyone.

It is not fair that the attention has shifted to him. It's not all on you. We want everyone to be aware of this. If this work going forward is seen as a forced outcome of a closed room agreement, then it will be opposed on that basis alone. I think this work is good and useful, but we have to remove the specter of "this is a forced change on the network". We need to collaborate to improve that. We can say that the process is delayed, segwit caused delay, complexity of this caused delays, and that's fine, but we need this to go from an "HK agreement" proposal to being a community proposal. I am saying this for the sake of the proposal. Without this, it cannot get widespread public support.

May I ask a question. Why is he the one working on this but it was never communicated. Why wasn't it shared? Why did we not hear about this work? Why did you not hear about this work?

I can't stop them from working on things. He published about it on the bitcoin-dev mailing list. I think we all just are very bad at communication. So within the developer community, some of us were not aware either. None of us were eager to talk about this when it sounded like this was going to be used to block segwit.

My belief that is what has been proposed, that we try to and turn this HK agreement into a community-based consensus work, is somewhat hard to do and impractical in his belief. There could be another way to realize that. We could do it through a foundation that we were proposing earlier. It could be the consensus for a new foundation to try to realize that.

I think that if you tried to do that through a new foundation, it would lead a lot of backlash against that hard-fork plan and organization.

You would have to get people to accept and embrace the foundation. That would take time.

We could explore the possibility of doing that. We can be open to working with other efforts.

It would be extremely challenging to do it that way.

We should talk more about it.

At the bare minimum, the best suitability for a foundation is things like marketing efforts, not hard-forks.

Regardless of which plan we are trying to adopt, we cannot, it's not reasonable to expect 100% consensus. So the question is to what extent we want to reach consensus. How much effort would we like to put into engaging the community to get there?

When you said you wanted to use the HK agreement to make it a community proposal for a hard-fork, you meant the development community? Or do you mean everyone?

I mean everyone. The point is that politically, the Bitcoin ecosystem should not accept imposed rule-changes on the network. And so, a hard-fork that comes out of a closed-door meeting sounds like an imposed rule change on the network. There are many people who will principally reject this, reflexively. I want there to be collaboration. Most people will ignore it. But I want there to be collaboration so that we can say this is a product of the Bitcoin community. It cannot be a closed-door agreement.

This was Luke's post on the mailing list:
<https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-February/012389.html>

At this point, it would be a little bit difficult or challenging to reframe the HK agreement to a broader community-based effort. Trying to reframe the HK agreement to an open community agreement would be difficult. The simplest way is to, we just based on the HK agreement, then we try to pull people into that and then gain consensus on that. That would be the simplest way.

My understanding of the plan in February was that we would make something, we would then propose it to people, and then hope they would like it. We would hope the community would reach consensus on it, and we would ask them to discuss it and build on it and so on. So I think that's good, to me personally.

In order to make bitcoin grow sustainably in the future, it's important for us to build a platform here as I mentioned before. We need communication. We need to resolve differences. We need to bridge gaps so that we don't have those situations again. A lot of us in this room did not even know about that work. We should all try to prevent that from happening in the future, and a platform could facilitate that.

We should work to improve communication.

Tomorrow we don't go to Stanfordland until 11. Perhaps tomorrow we could talk about how miners can get into better communication with Core and how Core can have better communication. Yeah we could spend a few hours on this tomorrow morning. We have breakfast at 9am tomorrow again.

My point is that now the market cap for Bitcoin is almost over $10 billion USD. It is big. Driven by private interest and technological interest, there will be a lot of ... that will be popping up one after another. And a lot of Core developers here, you are many of you are the most influential figures in the Bitcoin community. So the sooner you form such an organization, the better off you become to protect yourself from those potential competitors in the future. So, don't mess up.

We could post on the medium blog and link to his code and proposal and write a few things. Maybe, I think, it's himself who should tell the community. He can sign his name on the blog post. The update should be provided in the same location. We just need some channel to announce it to the public for mass media and so on.

I think it would be good to post it on the bitcoin-dev mailing list.

He should also mention the other contributions from the others contributors. "In the future we need to move forward and have better communication". Does that sound good?

We need to be careful to not make this sound like bitcoin is talking about hard-forking immediately after Ethereum Foundation's blunders.

We have refreshments in the back.

Breakfast and meeting starts at 9am tomorrow morning. We can talk for an hour or two, then we will head out to Standfordland.

# Day 3

We don't have a lot of time in the morning for discussion. We have a hard stop for discussion in the morning. In the morning, we will have a wrap-up discussion. We will leave for Stanford and we can share rides. I have already sent the parking email and we can all park at the same location and walk over to the building.

# Block withholding attacks

I had a brief chat with a developer during the Hong Kong Scaling Bitcoin event. I think a miner and I share the opinion that it is quite a challenge for any pool operators to ... I think most of the developers haven't recognized how risky this could be. I would like to hear more from you about this.

From my side, I am not familiar with mining. The attack is when one of your participants finds something with PoW and it does not broadcast it to the pool? Okay.

And this is particularly acute for pay-per-share pools because they continue to get effectively the same return until the pool goes bankrupt.

We think there have been real attacks against ghash.io and we also think it's the main reason why they had such bad luck for long time. And also, there was one more possibility. If one pool suffers from this kind of attack, then they may launch the same attack against another pool if they think the other pool was launching that attack against them. And also, if this happens, maybe many people just attack each other with this withholding attack, and it's quite dangerous for the whole industry. It’s like a death spiral.

https://petertodd.org/2016/block-publication-incentives-for-miners

I don't think you need to talk about death spiral, block withholding is important anyway. One of the challenges with fixing this is that there's no fix that we know about that doesn't also kill p2pool or kill a totally decentralized pool as a viable option. Several years ago, this was much more of an issue than it is now, because it seems that p2pool has died its own death independently of this attack. There are several ways to fix block withholding this. The mining pool could retain some secret which it gives out only after you return the block to it. And then this is made part of the Bitcoin consensus rules. The most straightforward way to deploy this would require a hard-fork. Unfortunately this hard-fork would be incompatible with the safe hard-fork method that was discussed yesterday. There might be some ways to fix that and improve that.

There is a quasi soft-fork way to fix block withholding attacks. Unfortunately it's kind of ugly. I am not sure if it's a path we want to go down, although it's easier to deploy. The basic idea in all of these fixes is that you can make it so that the hasher can tell if it has a valid share or not, but it can't tell if it has a valid block. So it emits the share, and only with the secret data can it do the final check to see if it has a valid block. How CPU costly is checking? It's .. same as validating a share.

As far as I know, there are no way to detect all the possibilities that signal to the attacker. There are also some .. that the detector can detect from...

One of the things that fixes block withholding helps with is this issue of "accidental block withholding". Because there is not enough nonce space in the blockheader, mining software has become sophisticated with reaching into the bitcoin block and mucking around with the internals of the block. This has made it easy for authors of mining software and device firmware authors to mess up their handling of mining, such that they correctly return shares (because if they didn't do this then they would notice immediately) but they don't correctly return blocks. There have been a couple of cases where this has occurred. One reason for this is that stratum encodes the difficulty as a floating point number in JSON or JSON-like format, which has made it easy for people to mess up type handling and do dumb things. There are some cases which I am confident were accidents. But from a pool's perspective, it's even worse than a malicious withholding. At least a malicious withholder will at least be strategic, so it's kind of worse if it's not even a malicious event. I think it is fair to say that I would like to fix it. When we talked about fixing block withholding several years ago, with the mining community back then, there was relatively little interest in fixing it. Part of the reason for that lack of interest was that, at the time, there were no pay-per-share pools. Many of the existing pool operators (at that time) that they did not have to worry much about withholding and that the attackers would only be harming the attacker's selves. Since then, the pooling climate has changed. Some people have published an analysis that particularly with the existence of Very Large Pools there are ways to strategically mine that profit, er, that profit from withholding rather than merely being destructive with withholding.

In terms of choosing payout mechanisms, like pay-per-share, pay-per-last-share, all these different things, is this user driven? Do people want X or Y method? How do pools decide on this? What has been the recent demand or drive behind this?

You said it's mostly pay per share?

F2pool and antpool and BW are pay-per-share. Is that mostly driven from the pool who says this is easier and better for us?

Only users want this. If you use PPS, maybe the mining pool doesn't care about operate. Users do not like the fluctuation of the income. That's most of the reason why there are pools.

That's the reason pools exist in the first place.

We were the first major mining pool in China to do PPS. You can see everyone else copied their FAQ from us.

It was surprising to me to see the migration back to PPS because there was a period early on in Bitcoin's life, where PPS was used, and it was attacked and then people stopped using it. I was surprised to see pools transferring back to that. I understand, though, the user concerns. One of the biggest block withholding attacks we knew about with PPS was that BtcGuild lost 1400 bitcoin at least due to block withholding. It seemed like it was inadvertent

…. ((lost connection to google doc, briefly commandeered another laptop))

Could you fix this in a soft-fork?

There is a soft-fork way to fix this. It’s a little bit ugly. It’s not a pure soft-fork. What you basically do is you can imagine the normal way to fix withholding is to change how, it’s a hard-fork that changes how someone decides whether a block is valid or not. It changes the definition of a passing block. The way you do this with a soft-fork is you impose a new rule, the original rule and a new rule. The new rule starts with zero difficulty and you ramp it up slowly over time. IT narrows th… it lowers the network hashrate by a small fraction of a percent. You ramp it up over time to the point where it actually has enough bits of entropy to effectively stop withholding. It has the soft-fork like advantage that it cannot encourage a network split over it. But in every other way it has disadvantages.

So don’t fixes to block withholding inherently make selfish mining worse? Because the defense against selfish mining is that the miner can broadcast the block, and now they can’t do that.

In practice, no they don’t. One of the potential answers to selfish mining is that you can imagine a pool that is mining that is not announcing the new blocks. One of the way to avoid this is to have the hashers leak the blocks that the pool solves. With stratum, this is not possible. With GBT mining, it’s possible to do that.

Is that block withholding? Or is that share withholding?

No, that’s selfish mining. If you imagine a pool with a lot of hashrate, more than 1/3rd. If a pool finds a block and instead of announcing a block, perhaps they keep the block for themselves and… after retargeting and so on. And really there’s no interaction here with block withholding. … so the solution to selfish mining cannot work with stratum. I don’t know if pooled selfish mining is a major concern, because it would be very detectable. All the miners would see that the blocks aren’t being announced, and at that point action could be taken.

Do mining pools keep statistics on the luck of different users? It’s not like you can do a whole lot.

Yes, but it’s, they do that, but it’s not useful. Particularly… you can’t kick them off, it’s not actionable. An attacker would spread themselves across many low hashrate accounts.

Basically, if they are actively trying to hide from you, the only remedy is to close access to the pool, only friends and family. Which is not helpful to the idea of pooling.

We should publish a proposal (or two) on fixing block withholding. I would be happy to work on this. In the next 30 to 60 days, I will put out some kind of proposal on this.

# Concluding discussions

We only have 30 minutes left. Who would like to give a summary talk? We don’t have a lot of time. So could you keep it short and simple?

Maybe we could close by having a discussion about how to, there was some discussion about communication platforms and where we come together and how we stay current with each other.

I think we have had very good discussions this weekend. I hope we have improved our relationships greatly. I would like to talk about how we could continue to do that going forward, how we can continue to have open collaboration.

My suggestion would be, not reddit.

I believe that because of the market cap of Bitcoin is continuing to grow, I think that Bitcoin enterprise and companies are the engines behind the market cap growth. They are the ones most incentivized to protect Bitcoin and its ecosystem. I am proposing for this platform or organization, that the Bitcoin companies and enterprises, whether miners or exchanges or application developers, they are the major participants in this platform. To start out with, as the first step, we can first setup some kind of social circle as the first step. It’s kind of like a consortium. We can connect through email and wechat or skype. There are all kinds of mediums and technology available for us to setup this circle so that we can start communication channels first. So the participants should be the major players in the Bitcoin industry and they have to pay a certain fee to join this social circle. So it’s semi-public, but it’s not free. On the Core side, they can send some representative to represent Core development and to join this social circle. And then we try to within this circle, we try to work together and with coordination and try to establish some kind of foundation-like entity. I know you guys hate the idea of a foundation. For a lack of word, I am using the word foundation as a reference. So this social circle is monitored by its chairman and its secretary, to host the communication between different parties and companies within that circle. So that is the proposal as the first step towards building this communication platform.

What do you guys think?

Sounds reasonable. I guess nothing seriously wrong with that. I have heard some conversations where people said let’s create that. Nothing has happened so far.

Who would like to take the initiative and someone has to drive it.

Maybe using the Bitcoin roundtable as the name of the org.

They can organize everything on the legal level. How it will be more efficient to open it. And then we can just decide.. Or how they choose the Chairman, some leaders, etc. And who will it be? So any suggestions from the Core developer side about this proposal?

The pay-for-access component of it may have bad optics to the public when it's presented that way. Participation in any group has cost, regardless. There are a lot of cost that people have incurred to come here to this meeting. We should be cautious in how this organization is setup and presented, to avoid bad image.

Maybe it's not paid, maybe it's sponsorship.

I think that there is, it's useful to have a pay component to provide a neutral access control mechanism. The argument would be that "if the pay level is too high, then that access control mechanism is not particularly neutral". I think this can be worked through and solved. I think it's a potential source of issues that should be considered.

This circle is trying to protect the commercial interests of the Bitcoin companies and industry. I believe that bitcoin in the long run is driven by those enterprises and companies.

They are in the initial stage of bitcoin development. It's still a hacker culture. It's informal. Casual. It's relaxed. But now, at this point, in its history, he believes that it should become more formal and formally structured, driven by commercial interest. So there could be a transition from a hacker culture to...

I think that there may be a mistaken belief that these are incompatible cultures. I think that if you look at all the protocols of the internet, then you will see that almost all of them are developed in the context of IETF, like the HTTP protocols. Most of the attendees at the IETF meetings are working for some of the largest tech companies in the world like Google, Microsoft and Cisco. They participate in an open environment, talking about technology. There is no fee to participate in IETF. Individual meetings themselves have conference fees, but the mailing lists are open. This environment is the one in which the Internet is developed. I agree that bitcoin as it grows needs to become more formal and professional. However, there are many forms that this can take. It definitely needs to be heavily driven by commercial players, not volunteerism. However, this does not necessarily mean that you have a hierarchical system of authority where an elected body is in charge of Bitcoin or something like that. An example of this is how the Internet is organized.

It's worth pointing out that we are all here. Well, all of us here are here. This meetup was able to be arranged, without that central organization. It was not a top-down meeting.

This idea of "hacker culture" is actually not really what the IETF and these kinds of process organizations... I think this is actually just the outcome of professional development in a situation where you cannot impose on other people. I think this is what the Internet protocol saw as well. There are professionals developing these technologies. They are not in a situation where they can impose.

Decentralized professional development, which happens to look hackery, because the hacker behavior is decentralized, but not necessarily professional. So it is kind of similar.

He believes that this hybrid model is a good idea. He also believes that they can co-exist in a healthy and organic way. He was thinking that maybe there could be two payment and donation structures so that we can collect and solicit fundings for this forum. Maybe some industry companies can pay a fee to join this circle or some others can just donate or sponsor this entity.

They would pay a fee to join. For those who pay a fee, they would have a voting right. For those who donate, they do not have a voting right. And the opinion or voice coming out from this organization or circle, they only represent themselves, and they do not represent the entire Bitcoin community because there are other organizations or other groups within that community. So that's his idea.

So..... like, one thing I want to say, ... let's discuss more, we're not going to solve all of this in 5 minutes.

So... the one thing to think about is that today, bitcoin is small and friendly. We know each other. We know those companies. Relatively small. Wait a few years. You haven't seen "more" my friend. So the point is that, if you look at HTTP, now there are very big powerful companies involved like Microsoft. And they want to control HTTP. And IBM wants to control it separately. Bitcoin is finance. When we think about setting up an organization, we're thinking about ourselves. But in 5 year time, that will include Goldman Sachs and Microsoft. And they each send 20 brilliantly manipulative people and they will bribe politicians and spread mayhem and chaos. We the Bitcoin world will lose control of this organization. Goldman Sachs will create 40 subsidiaries, they will each pay the X membership fee, and then they will now have the entire vote of the organization. So we need to be mindful of this sort of situation. The Internet IETF things for example have evolved to allow for technical development to proceed in a way that promotes good technical outcomes that are good for users even though some of the engineers work for Big Evil Corps like Microsoft.

Are they independent even though they are working for big companies?

Somewhat. That's the objective, anyway, with IETF. Oh really?

This discussion is critical and important. There have been many good ideas expressed. We can't solve everything here right now. There's too much to discuss. We should not have the expectation of solving everything here.

We have three minutes. We have to find a place to park, then we have to walk. Stanford is down the street but it will take 30 minutes to get there. The Stanford campus is huge. I sent the parking instructions. That's the closest to the building, so please check your email.

His point is that it doesn't matter that in the future some kind of bigger company like Goldman Sachs trying to take over. It's inevitable that some company will try to take control of the organization. At that point, we just have to move on and form another entity and another group. It's not going to be the only social circle in the Bitcoin ecosystem. There could be many of these. It's not going to be that they take over one and then they get to takeover Bitcoin. They can try whatever they want to take Bitcoin over. We can always change our tactics. We can move to other mediums.

As long as the organization doesn't give the impression it has control over the protocol.

They will try to setup a circle. They are asking you whether to do it at this point. They don't know if you are willing to join an organization.

hey are offering a proposal that we can form this together at this point.

I think we are interested in any and all opportunities to collaborate.

We will try to setup a commercial circle. We hope that the Core developers will join.

In the afternoon, we can come back after we visit Stanford. We have an hour gap and we can come back here. I have reserved the conference room for the whole day. We can still come back here. Googleplex is not very far from here. It takes 30min to get there or less. We can still come back.

# Dan Boneh discussion

<http://diyhpl.us/wiki/transcripts/2016-july-bitcoin-developers-miners-meeting/dan-boneh/>

# Google Tech Talk

<http://diyhpl.us/wiki/transcripts/2016-july-bitcoin-developers-miners-meeting/jihan-wu-google-tech-talk/>

# Other session

Miners have some other events later this evening. Perhaps as a group we should think about any closing summaries?

What do we want to say to any journalists that ask? I think it is important to present this as some people gathering together who have been in the space for a long time, who have had trouble in the past with communication. By seeing people face to face, and talking about things, it helps us discuss.

A comment I made before, a story to take to a journalist later, that bitcoin is a global decentralized system and it works just fine as long as we do our own thing. But it works better if we collaborate. With this weekend, we were able to get to know each other better, we were able to understand many of the things we had in common. We were able to open more lines of communication. We were able to improve our friendships and these things in general are good for bitcoin.

In Zurich, we did a full transcript, but we also published a summary of the meeting, in the following format:
<https://bitcoincore.org/en/meetings/2016/05/20/>
.. if we do the same for our gathering, it would be much shorter than the above example.

We published the Zurich summary first, and the full transcript was published weeks later. In Zurich, it took about two weeks I think to go over the whole thing.

# Event Summary

Over the last few days, some Bitcoin developers and miners got together for a social gathering to improve communication, friendship, and to do some California sightseeing. We talked about where bitcoin is and where bitcoin is going. We learned a lot from each other. We also visited Stanford to attend a cryptography talk to learn more about potential improvements for Bitcoin, as well as the Google campus to give a presentation and talk about Bitcoin. We had many informal discussions amongst ourselves about topics such as mining decentralization, evolution of the Bitcoin protocol, safety improvements and progress for both soft- and hard-forks, as well as improving communication and cooperation across the Bitcoin ecosystem such as new venues to work together in unison. We think that Bitcoin's strength comes from the consensus of its participants. Many of us plan to attend Scaling Bitcoin 3 in Milan, Italy and everyone would like to continue with gatherings like these and others in the future with all parts of the Bitcoin ecosystem. We hope to be releasing notes in the near future for parts of the community that were not attending.

在过去几天里，一些比特币开发人员和比特币矿工们在一起进行了社交聚会来增进友谊，改善沟通，以及共同进行了一些观光交流活动。我们谈论了比特币的现在情况以及未来的发展。我们互相之间学到了很多。我们在斯坦福大学还参加了一个密码学的讲座，学到了比特币将来一些可能的改进。然后我们又去了谷歌总部在那里做了一个比特币的演讲和讨论。我们还有很多非正式的讨论，关于矿业去中心化，比特币协议演变，软分叉与硬分叉的安全性的提高和进度，以及改进比特币生态系统里的沟通与合作，比如通过新的渠道来共同行动。我们认为比特币的强处来源于所有所有参与者的共识。我们其中许多人有计划参加在意大利米兰的2016 Scaling Bitcoin 。我们每一个人都希望在未来和比特币生态系统的所有组成部分继续进行这样的聚会。对于那些没有能够参加这次聚会的社区组成部分，我们会在近期公布我们的谈话记录。