November 15, 2016

Bitcoin Quarterly Update Call

As organized by **Needham & Company**

PRESENTERS

Wences Casares
Founder & CEO, Xapo

Dr. Adam Back
CEO, Blockstream

Jerry Brito
Executive Director, Coin Center

Spencer Bogart
Equity Analyst, Needham & Company

OTHER PARTICIPANTS

Chris Burniske
Ark Investment Management

Tuur Demeester
Adamant Research

Roger Ver
Bitcoin.com

Wayne Vaughan
Tierion

PREPARED REMARKS SECTION

Spencer Bogart
Equity Analyst, Needham & Company

Hello everyone. And thank you for joining us today for the Bitcoin Quarterly Update Call. I'm Spencer Bogart and I'm part of the Internet Equity Research Team here at Needham & Company where I lead the firm's coverage of Bitcoin.

Before we go underway, I want to make a couple of quick disclaimers. The first is that I personally own and invest in Bitcoin and you should assume that the other participants on the call do as well. The other disclaimer and reminder is that Bitcoin is a decentralized network. By design, no single person, company, or group of people can control Bitcoin or say what will happen to the protocol. And that includes the participants of this call, Dr. Back, Blockstream, and the loosely defined group of developers known as Bitcoin Core. The participants on this call do not represent Bitcoin in any official capacity, whatsoever, because again, by design, this official capacity does not exist. We're pulling together various industry stakeholders to provide an update from their perspective on what's happening in the ecosystem and to gather their various outlooks and concerns. The people included on this call represent a small set of perspectives relative to the wide range of opinions and perspectives throughout the broader Bitcoin community.

OK. I think that about covers it, so moving from the disclaimers.

It's exciting time in the world of Bitcoin. And I'm thrilled to be joined on today's call by three experts with deep domain experience in their respective corners of the Bitcoin world.

For today's call, we have Wences Casares, the Founder and CEO of Xapo, to provide his perspective on Bitcoin adoption. We also have Dr. Adam Back, one of the world's foremost Bitcoin technologists and CEO of Blockstream to provide his perspective and outlook as a technical expert. And lastly, we have

Jerry Brito, Executive Director of Coin Center, to provide his perspective and outlook on Bitcoin from a regulatory and legal standpoint. Thank you gentlemen for offering to share your perspective with us today.

For the call today, we'll first run through prepared remarks from each of our three experts who will offer their perspective on what's changing in their respective corners of the Bitcoin world. And then we will open up the call to audience Q&A.

As a reminder, today's call is not a Bitcoin 101 discussion about what Bitcoin is or how it works. Instead, given the caliber of participants on the call, we're going to jump straight to the cutting edge. In particular, I've asked each of our participants to focus their commentary on the delta, on what's changing out there, and their outlook for the months ahead.

Before I turn the call over to each of our participants, I want to briefly provide some high level color on what's happening in Bitcoin and how Needham is thinking about Bitcoin as an asset.

We think Bitcoin has utility both as a digital gold and as a payments channel.

As a digital gold we find that Bitcoin is valuable in part due to its known and finite supply, its divisibility, its portability, and its value as a liquid, speculative investment in a nascent technology.

As a payments channel, we're most optimistic about Bitcoin's adoption and growth in the areas where Bitcoin's relative advantages are greatest. In particular, as a payments channel, we think the prospects for Bitcoin adoption and usage are greatest for cross-border transactions and in markets with poor access to traditional financial services, which includes emerging markets.

In their invite to attend this call, listeners also received a link to our most recent Bitcoin research report where we provided detailed and comprehensive analysis and outlook for Bitcoin. Within that report, we highlighted items that our primary audience of institutional investors might be particularly interested in from a portfolio management perspective such as Bitcoin's evolving volatility, liquidity and correlation.

The skinny of it is that Bitcoin's volatility has fallen substantially and now resembles that of a small cap security.

Similarly, liquidity has also improved significantly. When we evaluate Bitcoin's liquidity, we restrict our analysis to the top five Bitcoin to US dollar exchanges and consequently exclude the tremendous trading volumes in China that are difficult for our typical audience to access. Even with those restrictions, we find that Bitcoin's average daily trading volume resembles that of the average security in the S&P mid-cap 400.

Lastly, and perhaps most encouraging to portfolio managers is Bitcoin's low correlation to major asset classes. It is truly remarkable that Bitcoin seems to trade in a world on to its own and doesn't have any significant statistical correlation to any asset that we've examined.

Even more exciting is that we've recently seen the code release known as segregated witness or segwit, which I understand is among the most significant factions of code in Bitcoin's history. On a high level, segwit is exciting in that if it's activated, it effectively scales Bitcoin by approximately 75 percent, it eases the process for further scaling improvements, it fixes a known transaction malleability bug, and it eases the path for robust second layer networks both on top of Bitcoin.

All in all, there's a lot of exciting things happening. And I think now is an appropriate time to address some of the commentary I've heard about Bitcoin's progress. Sometimes we hear what we believe to be unsubstantiated claims that Bitcoin has "stagnated" either in terms of adoption or development or both. I want to make it very clear that this goes against every piece of evidence we look at, all of which show very impressive growth.

In particular, a specific complaint that we've heard is that transaction fees are rising. Not only do we not see rising transaction fees as concerning, we're actually encouraged by the overall trend. It's dumbfounding when we hear rising transaction fees cited as evidence that Bitcoin is in some way failing. Ask any investor what they think about a situation where a product or service sees increasing amounts of demand as the price for using that product or service rises. This is the type of "problem" that we all hope for, especially considering that these rising transaction fees directly contribute to the security of the Bitcoin network which further increases its appeal. So that's our take.

Meanwhile, in terms or price, Bitcoin is up more than 60 percent year-to-date, more than 100 percent over the past year, and more than 200 percent over the past 18 months. All of that begin to backdrop as we've seen transaction volume increased more than 140 percent over the past year while the network's hash rate has increased more than 200 percent.

Despite all the success, we think Bitcoin is just barely getting started and there's a long way to go.

So we put out a price target for Bitcoin of 655 in March. Then in September, we had to raise our target to 848 due to faster than expected adoption, improving fundamentals, and a really compelling outlook.

Indeed, we think the short to intermediate term horizon is among the most encouraging that Bitcoin has ever seen.

And with that, I'd now like to introduce Wences Casares who will be providing his perspective and outlook on Bitcoin adoption.

For those who don't know Wences, he's the Founder and CEO of Xapo, which offers one of the most popular Bitcoin wallets, as well as a vaulting service that stores Bitcoin in underground vaults around the world, and also offers a Bitcoin debit card. Aside from being Founder and CEO of Xapo, Wences was officially added to PayPal's Board of Directors in January of this year. All of this is not to mention the several successful companies that he has put, including lemon.com which was acquired by LifeLock, and Patagon, which was acquired by Banco Santander. Originally from Argentina, Wences is no stranger to extreme currency volatility and inflation, which is part of the personal experience that led him down the radical of Bitcoin.

Wences, thank you for joining us today. Please take it away.

Wences Casares
Founder & CEO, Xapo

Thank you for having me Spencer.

Just for a framework, most of the things I will be commenting on come from the perspective of what we see from Xapo. We're one of the largest custodian of Bitcoins in the world. Today we are processing a little over 10 percent of the daily transactions of Bitcoin and we have customers in almost 200 countries.

We see a lot of different behaviors in our own customers. But I would say that broadly speaking, we could separate that behavior in two.

Number one, in the developed world, we see a small number of customers with a large number of coins that do not move very much and they're not being used for payments. It's a very speculative use. It's, I think, what you refer to as Bitcoin as digital gold.

We have many accounts that have well over $10 million worth of Bitcoin in one account. In every one of those cases, when we talk to our customers, you know, we see that for them it represents a very small part of their savings or their portfolio that rarely is more than 1 percent of their portfolio.

And they – the way they're looking at it is some sort of insurance, but most of them are looking it as a very symmetrical bet in which the worst that can happen is that they can lose 1 percent of their portfolio, and the best case scenario, over several years, this can go multiplied 2000x or more to half a million dollars or a million dollars to Bitcoin. And most of them are your high net worth individuals, family offices, and some institutions like hedge funds. That's where we see the bulk of our activity in the developed world.

In the developing world, it's very different. We have most of our customers there, even though they represent a small percentage of the coin, most of our customers and most of our daily transactions are in emerging markets.

And their number one use case there that we see are people who have a smartphone and don't have a credit card, and they have cash that they're ready to spend, that they want to spend digitally. And because they don't have a credit card, they are turning the cash into digital money, Bitcoin, to spend it digitally.

That was somewhat of a surprise. Going into this, we thought that countries that have weak currencies or currencies that are being devalued were going to be the places where Bitcoin was going to be used the most, mostly because that's what I – that was my experience growing up in Argentina.

And we have seen usage of Bitcoin in countries where the currency is being devalued quite a lot. We saw that last year in Russia. And we've seen that this year in Egypt, in Nigeria, in Venezuela.

But it's being used by people who are fairly sophisticated tech users, fairly sophisticated financially. And all in all does not move – they're much smaller numbers both in number of users and number of transactions and volume than the broader use case of people who are looking for ways to turn cash into something digital.

In general, we were seeing Bitcoin more or less double in transactions, daily number of transactions, dollar volume of transactions and number of users every six months up until January of this year. In January of this year, we first were reaching consistently $200 million being moved using the Bitcoin network daily. I was forecasting that sometime in 2017 or early 2018 Bitcoin was going to be larger than PayPal which is processing $800 million a day.

But since January, when we began to have more and more fuller blocks and the transaction fees began to go up, we have kept growing by a much more linear fashion, not exponential, until – the way we were growing them until January. And I think we are all, like you said, very excited about segregated witness

and as part of the solution to full blocks and to transaction costs, which can return to exponential growth again, hopefully.

We, today see, on average, we are processing about 30,000 Bitcoin transactions a day as a company. And we are doing another 500,000 transactions that are not on the blockchain but on us that we process off the blockchain. That number has skyrocketed since January for the same reason. And we would expect it to come down. I would expect to do more and more of those half a million transactions a day on the blockchain as the transaction costs come down.

That's all I have.

Spencer Bogart
Equity Analyst, Needham & Company

So Wences, I've got just a couple of quick questions here before we turn to our next guest. So maybe we can start with talking about capital flight. So we often hear rumors that Bitcoin is used for capital flight, typically in countries such as China. And we at Needham, we're actually a little bit skeptical that this could be true to any significant extent because there was something on the order of $500 billion of capital flights in China in 2015.

And if we think about $500 billion, if any significant percentage whatsoever was using Bitcoin, the price would necessarily be significantly higher. But that doesn't mean it's not happening at all, nor does it mean that there's no potential for Bitcoin to be used for these purposes. But I'm wondering, from what you see, has Bitcoin been useful for capital flight?

Wences Casares
Founder & CEO, Xapo

I think that your interpretation is absolutely correct. What we see is that it is being used but not to a degree that explains most of the flows in any particular country.

So if you go to China today, to Venezuela, and Nigeria, and a number of countries, of course, we can show you everyday a number of customers that are using Bitcoin to convert local currency and transfer it abroad. But it's not a material number. It's not defining. It's not a mainstream use at all. Not that we can see it yet.

Spencer Bogart
Equity Analyst, Needham & Company

And to dive in a little bit to your comments, kind of about how you think maybe adoption has been stagnated a little bit due to fuller blocks. And I'm curious if you can kind of parse this out for us a little bit of how much you think this impact this from confirmation delays from full blocks, versus transaction fees, or is two difficult to separate because the two just kind of go hand-in-hand?

Wences Casares
Founder & CEO, Xapo

I think it's mostly transactional fees, you know. I mean, in something that should have a marginal cost of zero for moving value from one account to another. It has a marginal cost of zero.

When you increase the cost of that artificially, people react rationally and they use it less. And I think – imagine if you had an email system where you have to pay for each email versus one where you don't pay for it, it's quite clear which one will win.

I'm not – I am not – I am very, very, very optimistic about Bitcoin. I always tell people that there is at least a 20 percent chance that Bitcoin fails. And I say that because I believe that's true. And I say that for people to be cautious in what they decide to invest in Bitcoin. But I truly believe that there's a higher than 50 percent chance that Bitcoin is worth over a million dollars one day.

So I'll tell you that, just so you know, I am clearly optimistic. I do think that we have a lot of things to work out. And I think that finding a way for Bitcoin to be able to do a much higher number of transactions at much lower cost is an important part of the things that we have to work out. And I'm confident that we will work them out. And it's not confidence in that something will come out of the blue but confidence in the things that I'm seeing happening in the ecosystem right now.

Spencer Bogart
Equity Analyst, Needham & Company

And I'm wondering if maybe you could help us kind of reconcile the idea that maybe people who are using Bitcoin don't have that many other options, some of which need censorship-free transactions. And so – I mean, at current rates, maybe the typical transaction fee is around 10 cents, which is perhaps up from – I don't actually have the number in front of me right now, maybe 4 or 5 cents at the beginning of the year.

Do you think that it's somewhere between that 4 to 5 cents and the 10 cents that we see today that it really crosses the threshold that makes it economically prohibitive for a lot of people in emerging markets?

Wences Casares
Founder & CEO, Xapo

I think that when you are designing a system it's a very bad idea to do either one of these two things.

One it's a very bad idea to think that people have no alternative to your system. It will lead to bad design decisions.

And number two, it's a bad idea to think and design optimized for the long tail of people who are willing to pay the most for your system. Because there are some very specific reasons why some people may not care about those fees but they're usually a very small part of the market.

And so, if you just – these numbers are public. You can just look at what the transaction fees have been and how that has had an effect in the number of dollars and transactions move with Bitcoin. So I'm not – I'm trying to be objective and trying to – we've seen it in our own service, we see it in the blockchain, and I think that a lot of us are working to resolve that.

Spencer Bogart
Equity Analyst, Needham & Company

And maybe we could talk a little bit about geographic adoption. So I mean, you've been operating for a few years in many countries. Maybe you could fill us in a little bit on what countries you operate in and where you see kind of the greatest adoption? And then most interestingly, why you think that is? Why is there better, greater adoption of Bitcoin in some country than others?

Wences Casares
Founder & CEO, Xapo

Our number one market is India, number two market is China, then Indonesia, Brazil, Bangladesh, Pakistan, Nigeria, and Russia. Those are our top markets.

And to give you a sense, we've seen – we've seen a 10-fold increase of activity in Venezuela in the last couple of months because of the currency depreciation which has been quite dramatic. But it still doesn't move a needle in our overall dashboard.

Even though we've seen a 10-fold increase in Venezuela, it's an irrelevant percentage of the daily transaction, daily number of users. The same thing is true when we've seen the same increase in the past in Nigeria, Egypt. And it was meaningful when it happened in Russia because it was already a significant country to begin with.

And in all of those large markets, when we interview our customers, and we see why they are using us, and there's – the vast majority of them do not have an interest or understanding of Bitcoin per se.

This is something they found to be able to turn the cash that they have – there's something – they have a phone, they have a smartphone, and this is the first time -- through that smartphone, it's the first time they have access to the internet. They want to spend on something digitally. And they have a cash that they want to spend but the phone will not take their cash. So they don't have a credit card, and they are using Bitcoin as a way to turn that cash into something that they can have on their phones and spend.

There is a lot of friction into that they have go through to turn that cash into Bitcoin. And once they have that cash into Bitcoin, even using us, there's still a lot of friction to spend anything what they want.

So I think that there's a lot of things that we can do to facilitate that. But it's remarkable that despite all of the friction it's our number one use case, at least for us as a company.

Spencer Bogart
Equity Analyst, Needham & Company

That totally makes sense. And you know, it makes sense seeing kind of a 10-fold increase out of Venezuela, but maybe coming off such a low base.

But that leads me to a question about India, you mentioned that's your number one market. Just last week, right, we had the President--or Prime Minister Modi announcing the ban of certain large bills.

And supposedly, there's been a bit of an increase in interest in Bitcoin as a result of that. Is that something that you've seen on the ground?

Wences Casares
Founder & CEO, Xapo

We think so, but it's very new. We don't have – for now, it's more anecdotal. But we would like to see more confirmation of that in the numbers.

Spencer Bogart
Equity Analyst, Needham & Company

And then maybe one last question here, Wences, before we turn over to Adam Back. You know, you were a very early adopter that played a big role in getting some large investors involved with Bitcoin. And I'm curious among kind of that investor base, how does the appetite for Bitcoin today compare to a few years ago when you began evangelizing Bitcoin?

Wences Casares
Founder & CEO, Xapo

This is just – I wouldn't extrapolate too much from what I see. I think – I honestly think that is not reflective of what may be happening in the market.

I remember early on bringing large investors into Bitcoin and it having a big impact in the price especially. But what I've seen since then is that the rate at which the capital comes to Bitcoin is fairly linear and that may change with big moving price. But what I've seen for the last two years or I think lower two years is that, the capital coming to Bitcoin is coming in a fairly linear, not exponential – not exponential manner.

Most of the people who come to Bitcoin is very good in behavior where we –I haven't seen a single Bitcoin investor get rid of all of their Bitcoin. And I've seen a small percentage of them sell part of their position, some of them as much as half of their position. But I haven't seen any of these large investors get rid of their position entirely.

Spencer Bogart
Equity Analyst, Needham & Company

Interesting. Thanks for that Wences.

So I'd now like to introduce our next participant, Dr. Adam Back, who will be offering his perspective and outlook from the standpoint of a Bitcoin technologist. Dr. Back is among the world's foremost Bitcoin technologists and has been working on Bitcoin like e-cash protocols since 1995. He's an applied cryptographer, inventor of the Hashcash proof-of-work and decentralized mining that is used in Bitcoin. He is also one of the very few citations or references that Satoshi Nakamoto made in the original Bitcoin whitepaper. Dr. Back is also the CEO of Blockstream, which is working to leverage Sidechains, Lightning

Networks, and other second-layer solutions to extend Bitcoin's capabilities and improve financial systems.

Dr. Back, thank you for being with us today. Please take it away.

Dr. Adam Back
CEO, Blockstream

Thank you.

So I think it's been an exciting year for protocol developments in Bitcoin. We have CLTV, and -- so it's a relative lock time, and CSV, also activated earlier in the year.

And we're now almost in the class of segregated witness going into a period where miners will be able to start signaling for it on the 18th. So that could be active at least around the end of the year or early January.

Segregated witness is an on-chain scaling technology and provides a number of features primarily fixing a long-standing design defect of a bug around so-called transaction malleability. And this affects Lightning, which is a layer two technology. So it's one of the problematic areas for Lightning. And it's also necessary to fix this for a number of multi-signature wallets and some old contracts.

Segregated witness also brings a number of other interesting improvements, a size increase to the block, switching to weight accounting, so the scale both the old Bitcoin relies on the memory footprints of the unspent transactions and the change to weight accounting and segregated witness leads to a more efficient use of memory and therefore more scalability in the future.

So that should bring scalability up, once adopted, to approximately twice the current transaction throughputs. It's also a soft fork so it's backwards compatible which makes a smoother transition to add new software to the network.

It also brings a signature on the value. So surprisingly Bitcoin doesn't sign the value of the transaction but relies on the receiver to validate. They value all the inputs and add them up. So that has presented sort of a challenge for hardware wallets in that it can be quite computationally heavy if somebody sends a transaction with many small coins in it to validate a coin.

And this simple change greatly improves that and allows much lower footprint, cheaper rents, different interfaces even because there's much less that needs to get into hardware wallets which is useful secondarily.

The amount of scalability coming from segregated witness depends on the ratio of types of transactions, different types of transactions of different sizes.

The last and valuable part of segregated witness is that it simplifies soft fork upgrades to the protocol, and it comes to a number of follow-on protocol improvements, namely short signatures, to better form of signature, very similar, and witness seems to create assumptions essentially as DSA, but allowing more compact signatures particularly for multi-signatures, two of two and two of three as used by many wallet services.

So that can allow a further scale even within the same bandwidth utilization on the network, going up 20 to 50 percent further.

And that's by combining signatures across the inputs of the sender and further scales can be achieved by combining the inputs across multiple users using coinjoin. This feature is starting to be available in some wallets, which will improve fungibility, privacy and stuff like that. I'll touch on that in a moment.

So all of that is to say that I think in regards to the on-chain scaling topic, we should see in stages, 2x increase, leading to 3 and even 4x, all within the immediate features and follow-on features that can be soft forked in a relatively straightforward way from there.

Together with segregated witness, there are also some important changes to optimize the network to avoid issues with increasing the trend, the bandwidth utilization for nodes. So there's compact blocks which was the one intended for technology to use network compression to approximately half the bandwidth use in transmitting what data, FIBRE which is very low latency, UDP-based protocol for relaying blocks and transactions to miners, which is also important for scalability.

The miner latency is one of the main problematic areas of scalability. So we should see more improvements from that area in the future.

I mentioned fungibility, so I think it depends on the uses obviously. But Wences touched on this. It's one of the attractive things about Bitcoin. is that it's very permissionless, cash-like, payment hubs, strong finality. And since permissionless systems that we see uses in maybe gray markets, international transfers, capital flight was mentioned, but I think that's not a huge factor in the scale of global footprint in that area.

So in any case, fungibility is a very important factor for Bitcoin. And there are also some changes in 0.13.1 which brings segregated witness to improve fungibility, particularly privacy and transaction origination is improved there.

So now on to layer two, or Lightning, so I think this is where we can see some really large improvements in scalability. So we can get a certain distance by increasing the on-chain scalability but it's still a broadcast mechanism and has some security trade-offs with scalability now.

In the layer two and Lightning side protocols, it's no longer a broadcast mechanism but the payments are sent, routed much like fetching a web page from the web service in that other people that are not in the path of the transaction would not see the payments. So that improves privacy obviously as a side effect, but greatly improves scalability.

And each transaction in the Lightning Networks – and there has been confusion that Lightning has somehow competes it with Bitcoin or is different than Bitcoin, but actually it's using Bitcoin as a kind of arbitration mechanism, an automated arbitration mechanism. And each Lightning transaction is a valid signed Bitcoin transaction that could be sent to the Bitcoin network at any time to close out a channel if one of the parties in the room wants to stop responding for an extended period of time, or go out of business, or something like that.

So it really does provide almost exactly the same security model as Bitcoin, with a slight difference in terms of monitoring for hostile channel closes but that can be outsourced securely. So that helps.

Segregated witness is an important factor to bring an efficient Lightning protocol to the markets. It is possible without segregated witness. But segregated witness makes it more efficient in keeping the channels alive for longer, so resulting in less on-chain demand for transaction space.

Final point, as there was a Scaling Bitcoin Conference in Milan just recently, and on the back of that there were some developer meet-ups. One of those topics was reviewing segregated witness leading up to the release and also another world's meeting between the lightning developers. There are now five or six different companies working on that. So they spent the time working on compatibilities.

So at least speaking for Blockstream's Lightning implementation, we currently observe 0.5, 0.6 will be coming shortly and will be intra-operable with the other implementations. And the following version would be a kind of more in a direction of live beta. So things will be warming up going into next year for actual live Lightning payments if everything is going to plan.

And the last topic, and about extensibility of the core point network, the concept of sidechains is an interesting way to extend Bitcoin in a permissionless way, so that anybody can pick up a Bitcoin, could (inaudible), add features, and so forth, and experiment with different features for different use cases or different scalability trade-offs and so forth.

So in Blockstream, we've been using the sidechains extensibility mechanism to add support for other types of assets, add confidentiality features. We have something called confidential transactions which hides the value of the transaction traded from the network but still allows miners to validate the transaction set is correct and adds up.

At this point, three companies are working on sidechains, and a big scale come from ourselves. There is also Rootstock. I'm using it to bring flexible, small contracting, and (hard language) fixed time prediction market. And there was also a sidechain technology meet-up on the same meeting in Milan recently.

And so there are a number of concrete proposals to bring forth peer-to-peer sidechain mechanisms that will be a new soft fork mechanism for Bitcoin off to segregated witness that will be reusable across any different types of extensibility.

There are sidechains running today that using a federated model. And with the introduction of P2P model, we would expect to be able to have hybrids and (fields) for sidechains to allow people to experiment.

So more advanced cryptographic protocols from academia and electronic cash and prediction markets, more contract experiments, many things that would be potentially too high-risk to do today in Bitcoin can be made available to use in communities on sidechains.

So that's it for my comments. So over to you.

Spencer Bogart
Equity Analyst, Needham & Company

And Adam, maybe very quickly here before we turn it over to Jerry. You know, maybe we could talk a little bit about mining concentration and Moore's Law.

So arguably Bitcoin's most important and defining feature is decentralization. But over the past few years, we've seen centralization in at least one respect, mining. And there's a lot of factors that contribute to this, such as the cost of electricity, the cost of cooling, length of supply chains, et cetera.

But my question for you Dr. Back is, is this centralization of mining that we've seen to date at all concerning to you? And how do you see the trend going forward?

Dr. Adam Back
CEO, Blockstream

So it is concerning. I mean it has built up to worse levels in the past than it is at this moment but it's still multi-central – more centralized than what would be desirable.

I do think there is some technology trends now in ASIC production which may lead to more decentralization, particularly the – sort of the usable life span of the miner has increased as the technology has approached Moore's law and cutting-edge processes. In the first few years there's a rapid ramp-up through previous generations of ASIC technology, and so going through 65 nanometer, 40, 28, now into 16.

And as it's caught up, the rate of process change obviously has slowed down now. And so we expect a longer shelf life on the hardware, and that enables people to make longer investment cycles. And I think that should potentially allow more people to access hardware.

There are also some protocol, mining protocol possible improvements, so I touched on the FIBRE network which improves latency. So one of the centralizing factors that causes miners to clamp together as it were, and use so-called SPV mining, and pools as the latency concerns increase if they are slow in obtaining information that blocks can be offered or outpaced by the rest of the network.

And that tends to be a centralizing tactic. So the FIBRE network brings the latency constraints so that it's not really so much of an advantage to take the centralizing approach any longer. You know, so that's my take there.

There is also one more factor on mining protocols. So many people use pools because it's – you know, it's a very large hashrate, and so you get low latency. And so long frequencies between winning blocks and high variance. And such that there is a variance, they use that.

But there are some artificial centralizing aspects of the current mining protocols. So there is scope to improve that. And I hope to see that also being worked on going into next year whereby a miner who is using a pool to use that variance would be empowered to choose their own transactions to put in the block. So that could reduce some of the centralization which exists purely as a result of protocol inefficiencies.

Spencer Bogart
Equity Analyst, Needham & Company

And shifting pace here just a little bit, I'm not sure than anybody can say for sure, but I'm curious on kind of your thoughts about how you think a contentious hard fork would play out if we were to see one in Bitcoin.

As in, how long do you think two reasonably sized chains, let's just say that each of them were, say, at least 20 percent of the original, how long do you think those could survive? And how would it affect people using Bitcoin as a payment system or as a store value?

Dr. Adam Back
CEO, Blockstream

Yes. I mean, I think most Bitcoin-invested people are not keen on that prospect arising. But I think the experience from, what happened with Ethereum and the Ethereum Classic fork showed, demonstrated that the – there was an expected market dynamic which is, even though a fork maybe 20 percent, if it's a little bit more profitable to mine, hashrate will switch to that chain.

And then there seems to be, with Ethereum and Ethereum Classic, actually a kind of pair of graphs going above and below each other. And so hashrate increased and the price increased and people would switch hashrate between the two chains. And there are certainly tools available in the old coin market that automatically switched the hashrate dynamically to be most profitable.

So there was some evidence that people who, you know, were slightly aligned with one chain would switch chains because it's more profitable, and many more switched to mine Ethereum just as a way to sell it and buy Bitcoin.

So I think that dynamic could exist in Bitcoin. There is one factor that intends to make that less likely, which is the difficultly adjustment mechanism in Bitcoin is much more damp and conservative than Ethereum's. We hash very quickly. So it would be more difficult.

Nevertheless, I think it's preferable that we have Bitcoin funds all the way to stay with one coin or one chain, at least for confidence reasons and predictability about the network characteristics. And I think things could get (inaudible) if that kind of things happens as difficulty moved around.

Spencer Bogart
Equity Analyst, Needham & Company

Right. Very interesting. Thank you Dr. Back for sharing your thoughts.

I'd now like to introduce Jerry Brito. Jerry is the Executive Director of Coin Center, a non-profit research and advocacy center that is focused on public policy issues facing Bitcoin. Jerry has testified several times before federal and state legislators and is regularly engaged in the policy dialog. Prior to Coin Center, Jerry directed the Technology Policy Program at the Mercatus Center as George Mason University and served as adjunct professor of law at George Mason University. His research has focused on technology and internet policy, copyright, and the regulatory process. Jerry is truly at the forefront of the policy and regulatory issues that are facing Bitcoin.

Jerry, thanks for joining us today. Take it away.

Jerry Brito
Executive Director, Coin Center

Thank you Spencer.

So first let me just say a little bit about what Coin Center is. We, you know, as you're mentioning, we're an independent non-profit based in Washington DC, and we're focused on the public policy issues that affect cryptocurrencies and open blockchain networks like Bitcoin.

Essentially, we exist to educate policy makers and the media about these technologies, what they are, how they work, why they're important, and what type of law applies to them. We develop policy research where there are gaps in the law that need new policy thinking. And we advocate, we advocate for solutions to help regulators and policy makers meet their ends while preserving the freedom to innovate using these technologies.

We're not a trade association. We don't represent anybody, any particular company, any particular technology. We're more akin to the electronic frontier foundation, what they're trying to do for the internet, is what we're trying to do for open blockchain networks. And that is to make sure that these open unknown resources remain free and open.

Bitcoin's regulatory outlook in the US, and I'll focus on the US, which is where we're based and where we concentrate our attention. The regulatory outlook there is pretty stable at the moment.

Anti-money laundering rules are clear enough. Same goes for tax rules. The treasury department, through FinCEN and the IRS, has issued guidance in each of these. And at this point, it's pretty clear to most operators in the space how to comply with these rules. It doesn't mean that they can't be improved or further clarified but at the moment that's kind of stable.

Also, law enforcement generally feels that they have a handle on illicit uses, and that they have tools to investigate and prosecute illicit uses. So that's also an area where, I think attention is pretty stable.

Our biggest challenges right now is, again, is addressing area, sort of gray areas where the technology has outpaced the law, and you know, thus creating sort of gaps in the law that lead to uncertainty. And the biggest area for that right now is in consumer protection.

Our number one priority is state money transmission licensing, which is how consumer protection is addressed for non-bank firms that take custody of consumer funds.

So if you are a Bitcoin company today, there is a strong possibility that you will be a money transmitter. And as a result, you're going to have to get a license in every state in which you have customers, which if you are an internet company, of course, means every state.

And the problem there is that these laws that you have to comply with, that you have to get a license through, are inconsistent. They are unclear and they are burdensome. So if you need to get a license, it's a very costly and burdensome undertaking.

More importantly, I would say, it's the fact that these laws are unclear. Many of these laws never contemplated cryptocurrencies. These laws were written in an era where they refer two things like wire transfers and faxes, never contemplated the technology into some laws, really.

Even if you wanted to comply, you would go ask the regulator, "I'd like to apply for license." And they would say, "Oh, come back because we don't know what to do with you."

And of course in the meantime you are operating without license, which is not just illegal at the states but it's also potentially a federal felony. So that creates uncertainty.

And it's uncertainty not just for those firms who need licenses but for persons who are creating technology who may not be subject to licensing but they just can't tell by looking at the law.

We have worked with the state bank supervisors and they issued a policy statement last year where they sort of said – and by the way, this is the association of all the different state regulators. And they said, "One thing where we can agree on is, what is the policy that these laws are meant to effectuate?"

And that policy is to consumer protection, right? The policy here is to make sure that if you are a firm or a person that is taking custody or control of consumer funds, and you're not a bank because banks are regulated by a different set of laws. If you are a firm and you are taking custody or control of consumer funds, then you are putting yourself in a position of trust. And you are presenting at risk to consumers. And so as a result, there are certain steps we want you to take. We want you to get a license. We want you get a background check. We want to post a bond, et cetera. And that's fine.

What this means also if you are not taking custody of consumer funds, or you're not taking control of consumer funds, then you're not putting yourself in a position of trust, you're not presenting a risk, and therefore you do not need a license. So that is essentially the policy.

And so now our goal is to update to the existing money transmission laws to effectuate that policy for cryptocurrency. And so as a result, we've been engaged state by state intervening where different states are, either creating new licenses for cryptocurrency operators or amending their existing licenses to include these.

And our goal there is, number one, to make sure that is the firm is the custodian, right? It's taking control of consumer funds. So if you're a Xapo for example, that you're – that the law is clear, that hopefully it is consistent as much as possible with all other state laws, and that it is simple to comply with.

That is an uphill battle but there has been some progress. Most recently in Washington State, the law has been – there's a proposed law that will be pretty clear and pretty reasonable and rational. Other places like California, it's been more difficult to get agreement on a rational and reasonable law.

So we're engaged state by state. And it's sort of a mixed bag there. Obviously that state by state approach does not scale. It's important to engage. And where there's a law being considered to, you know, engage and try to get a good outcome, but it's not an approach of scale.

So we've involved, as well with the Uniform Law Commission, which is a body of academics and legal practitioners that create model laws where states are taking sort of desperate approaches to a topic that ULC develop a model act to try to unify – uniform the law among the states. The uniform commercial code, of course, is probably their most successful model act.

And there, we're very happy to say that there is now a draft model act which passed the sort of the meeting of the full body of the ULC this past summer. It will – it is subject to a little bit more revision over the next few months. And it will be read and hopefully adopted at the final, at the next meeting of the full ULC this coming summer.

It's a long process. But this law is – the model act is very good. It adopts a definition of control, like it makes it very clear that if you're not taking custody or control of the funds, you do not need to get a license.

Now it's very important because you have different firms, different individuals, different developers, academics, practitioners, users who are using the Bitcoin network but are never taking funds or conducting certain activities with a set of funds but reading something like the New York BitLicense, you can't tell quite clearly if they are covered or not.

And so this would be miners. This would be nodes on the lightning network. This would be providers of the sidechain. These should clearly be exempted from the law. And so the ULC model act does that clearly. And so we're hoping that different states, as they are looking to update their laws, will look to the ULC and adopt that.

Now again, that doesn't scale perfectly either because it's not clear the states are going to adopt the model ULC act once it's finally proposed.

So ideally, what we'd like to see, of course, is federal preemption where the US Congress would listen. We use the commerce clause for a reason, it is to ensure interstate commerce and having 50 desperate laws surely is across purposes with that. So let's just get rid of the state by state regulation and have one federal rule.

Of course that is sort of politically infeasible. It's not likely the reelected Congress will do something like that. Number one, just because not much is coming up in Congress these days, but also because there would be very strong opposition from the states to that. So it's not really something that's feasible.

Luckily, we have been given a bit of a gift by the Office of the Comptroller of the Currency earlier this year. The OCC is a federal bank regulator. And under pressure from a lot of innovators, fintech companies, investors, Congress, the OCC sort of came to a conclusion and they issued a whitepaper where they said, they called it their innovation whitepaper.

And they said, the "United States is falling behind in financial innovation, especially in financial technology innovation. And a large part of the blame for that rest squarely with us, the OCC," which was amazing to see somebody seem to cope so clearly.

And they said, "You know, we've been too conservative about what kinds of business models we approve for chartering. It's – we want to make sure that we are not the bottleneck to innovation."

And again, this is in large part driven by FinTech interest, in particular, marketplace lenders. But it definitely covers companies like Bitcoin or cryptocurrency space.

And they set about taking comments for ways that they can improve their processes. And one idea that has emerged and we proposed is the idea of a National FinTech Charter.

What the National FinTech Charter would be is a very purpose-specific bank charter that a firm could apply for that says, "You know, banking has three main functions. It has deposit taking, it has lending, and it has access to the payment or check payment."

Well a National Fintech Charter is we proposed that, we would say, we don't need deposit taking because we're not interested in taking deposits of dollars. It's not lending, because we're not interested

in any lending. All we need is a FinTech charter, a banking charter, that allows one to have access to the payment system. So that if you're Xapo for example, if you want to send dollars to Xapo, you can directly send dollars to ACH and they can give you Bitcoin to your account.

And the beautiful thing about that, apart from solving some of the issues that Bitcoin companies have acquiring banking partners, more importantly with us, is if you acquire a federal charter, you are good to go in all 50 states and you don't need to worry about state money transmission licensing.

So I'm happy to say that this is an idea that the OCC has seems to be running with. They have begun a preceding that, we just filed our comments in yesterday where they are looking at abating their receivership laws which allows them to have a way to unroll bankrupt non-bank firms. So that means they're setting stage to create this National Fintech Charter, which is very good news.

Now notice that that is great for those firms that are custodian, that do take control of consumer funds, because they can get a national charter and they're good to go on all 50 states. It does nothing to alleviate the uncertainty of state money transmission law for all those firms that are not custodian, never take custody of consumer funds but yet are today in a gray area.

So for those we have proposed a National Federal Safe Harbor for Non-Custodial Uses of Cryptocurrency. And that would have to be an act of Congress. And it would be a law that's in Congress – of course, it would preemption, but it would be pretty limited during modest preemption where Congress would say, you know, state regulators are doing a fantastic job protecting consumers through money transmission law.

There is, however, this one set of activity that today is unclear whether if it's under money transmission or not. But it is very important that it does not fit. And so we're going to say to you, money transmitters – sorry, state regulators, you may not require a license from anyone who is engaging in this kind of activity. And you would have to carefully define what that activity was and then completely exempt those.

This is difficult, but we think ultimately possible. And we're happy to say that there is now a Congressional Blockchain Caucus that was formed last month. And there – which now has about seven members. And we're hoping that working through that caucus we might be able to introduce some limited legislation like that.

So that's sort of our main focus right now. It's clarifying that morass of state regulation, really of consumer protection. There are other areas that we're working on at the Securities and Exchange Commission making sure that as we inevitably have an enforcement action against the cryptocurrency that only the specific cryptocurrency may be seen as a security but not cryptocurrencies generally.

There are also alive sort of issues at the Federal Elections Commission. They are looking at how campaigns impacts may exempt cryptocurrency. Of course, there are ETFs also being considered by the SEC that would be Bitcoin ETFs. And there are some esoteric issues related to the Commodities Exchange Act at the CFTC. And I'm happy to answer specific questions about those.

But I think I'll stop there.

Spencer Bogart
Equity Analyst, Needham & Company

That's a great overview and update on kind of what's happening on the regulatory and policy front.

I have just one quick question I want to squeeze in before I open up the call line to Q&A here. And it's about Bitcoin as money. So Jerry, is Bitcoin money? Why does it matter if Bitcoin is considered money or not by regulators? And if I'm a fan of Bitcoin, and I want minimal regulations, or at least I don't want Bitcoin to be strangled by regulations, should I hope that the government consider it money or not?

Jerry Brito
Executive Director, Coin Center

It depends on the regulation and the law that you're facing.

So it's interesting, it's not just Bitcoin money. If people have to ask me, what is Bitcoin? And they will say, "Well look, the IRS says that Bitcoin is property. It's not money." And the SEC has said that – well they haven't but they probably will say that cryptocurrency could be a security. And the CFTC has said it's a commodity like gold. And these things seem to be in contradiction with each other and isn't that a problem for Bitcoin?

And the answer is no. Different regulators, for their own purposes, for their own act, laws that they are enforcing, can define Bitcoin as one thing or another, and that does not create a conflict. It's not inconsistent with each other. So the fact that Bitcoin is not universally seen as money is not a problem.

That said, you know, for example, if you are – if you have been caught doing some money laundering, and the statute that you are being prosecuted on requires that there will be money, well then you really want to make sure, you want to hope that the judge does not consider Bitcoin money, and they're considered something else, and then you're free to go. And we've seen cases go either way.

If you are paying taxes, well, if the IRS considers Bitcoin money, then any trades you make will be subject to your marginal tax rate but you will have de minimis exemption. If they don't consider it money, they consider it property, well then you're subject to capital gains tax, but you don't have an exemption. So it depends on what – how you want this to come out.

So I guess, it's sort of like a lawerly way of answering your question, which is, it's a very contact-specific about whether you would want Bitcoin to be called money or not. But the fact that there isn't a universal legal definition of Bitcoin as money does not hurt its prospect or what it does.

Spencer Bogart
Equity Analyst, Needham & Company

Very interesting. And I have a few follow-up questions for you and some of the other participants on the call. But I want to make sure that we have time for some people in the audience.

So operator, I think now is the good time to open up the call to audience Q&A.

And as a reminder, we have a few participants on the call. So it would be helpful, in asking your question, if you could identify to whom it is addressed.

Operator?

Operator
Thank you.

At this time, in order to ask a question, just simply press star then the number one on your telephone keypad. Again, to ask a question, just press star then the number one on your telephone keypad. We'll pause for just a moment to compile the Q&A roster.

Your first question comes from the line of Wayne Vaughan from Tierion. Please ask your question.

Wayne Vaughan
Tierion

Hi everyone.

My question is around – much of the hype around Bitcoin and blockchain right now is around the non-financial use cases for Bitcoin, of which I'm very skeptical about. Specifically, there's been a lot of talk about Bitcoin being a 1.0 protocol that can do a limited number of things, and Ethereum being a 2.0 protocol that can do all of the things—even blockchain all the things with Ethereum.

And I'm wondering the reaction of the panel to the current hype cycle and the prospect of these other technologies and how they're positioning themselves vis-à-vis Bitcoin?

Wences Casares
Founder & CEO, Xapo

This is Wences.

Right now, given – I am optimistic about the long-term impact of blockchain. And the Bitcoin blockchain is the only blockchain that matters today from a hashing power point-of-view, but short term, pessimistic. Given how much hype there is, it's impossible for blockchain to deliver on those expectations in the short term. So they're short to me, in terms -- I'm short blockchain, long Bitcoin.

And in regards, even though in the long term I think that a blockchain will be transformational technology.

And the way I think about Ethereum and others is the way you would think of computer about the beginning of the internet and others. You know, you saw a protocol like this, a TCP/IP that move information from anywhere to anywhere in real time and for free without censorship, and then someone showed you a computer and said, "Oh my God, this has more functionality."

Yes, it has more functionality but it has a lot more restrictions too which is much more close, much more proprietary, it has more attack vectors. And I think why would – why would anyone create a new blockchain when we already have the Bitcoin blockchain that has so much more hashing power and therefore is so much harder to censor.

I think thanks to what Adam is doing at Blockstream and other companies like Rootstock that are doing on top of that, we are more likely to see all of that functionality get developed on top of the Bitcoin blockchain and not on other blockchains.

Dr. Adam Back
CEO, Blockstream

Yes, I agree. I mean I'm not a fan of, personally, app coin as a model or old coins. And you know, it seems to me the switching cost is just too – if somebody does develop an interesting new technology to test it in the sidechain and integrate it into Bitcoin into longer term.

And I saw recently somebody had graphed all coins against the coins closer every years and it didn't look good for anything other than Bitcoin on the long term.

Operator

Your next question comes from the line of Chris Burniske from ARK Investment Management. Please ask your question.

Chris Burniske
Ark Investment Management

Hi. Thanks for the call you guys. This is a great format. And I think it's a good way to get the idea of Bitcoin out to the masses, especially in the capital markets.

So my first question is for Dr. Back. And it relates to the long-term security model of Bitcoin. So a paper came out recently about Bitcoin without block rewards which we will eventually have. And so I'd love any perspective on what Dr. Back's thoughts are in terms of a stable and secure Bitcoin without block rewards. And if it wouldn't be secure, what the feeling is around potentially making Bitcoin a slightly inflationary currency.

Dr. Adam Back
CEO, Blockstream

Yes. I'll start with the last comment first. I think that's one of the hard and fastest rules in Bitcoin, the 21 million issuance cap on Bitcoin.

And so – but on the former question about the recent paper, I think that paper was lacking some information about Bitcoin protocol details. So the – a number of the wallets, including the (inaudible) reference wallets, or the use of time lock for each transaction with the issue.

So the transaction (estimates) to the network are not valid unless they're in the following block and over the last block that they've seen. So that seems to encourage miners to move forward because the transactions that are available are not possible to integrate if you try to sort of (snipe) the fees in the current block just to complete your block.

The general topic of fees taking over for security seems to be progressing. Although, you know, there is a balance between scale and security. It's the fees are maybe a little bit of a high right now before segregated witness goes in. But it does impose both flat fees can rise for both securities as things done at the moment.

And there are other differences against – so another type of concern is that you might see lows in transactions and fees. For example, on weekends, there will be a gap in interest or there will be a set of transactions from especially high fees and the people will be incentivized to get block rewards and so on.

And there have been a number of proposals that attempt to combat these kinds of issues, including some fee averaging. And another more, obviously a simple one is for miners to pay, to voluntarily pay some of the fees forward because – and if they hold all the fees for the current transaction set, and all the people are incentivized to take them away from them, they were there to offer, I would say, you know, one-third of the fees forward to the next miner and to keep doing that.

So it would be interesting for the academic participants in Bitcoin to analyze some of the game theory around things like that. And that's something – it's certainly something that could be introduced in wallets or, you know, it doesn't necessarily even need protocols, of course, and all those things.

Chris Burniske
Ark Investment Management
Excellent. Thank you.

And then a quick follow-up for whoever would most like to answer it, you know, there is a network effect around users, but I'm sure as some of you know, also a network effect around developers. And so I'm curious about any trends you all are seeing with regards to developers, and any future initiatives to bring more developers into the Bitcoin ecosystem?

Thanks for the time today, you guys.

Dr. Adam Back
CEO, Blockstream

Maybe I can say a couple of things about the developer trends.

So I think that the business in the long tail was maybe a dozen, extremely (inaudible), something like a hundred, in terms of statistics, of people who gathered on that. And that has remained relatively constant at the time, actually.

But there have been initiatives to improve (reading) materials and Chain Code Labs, which is based in New York, to code developers or the founders of a company. And so they held a Bitcoin developer residency program. And one of the core developers of Blockstream, Matt Corallo, participated in the training exercise there. And a number of people participated. And I hope that helps people get started in Bitcoin.

I think another factor that has sometimes added confusion is that Bitcoin Core is not really an organization. It's not a part of 1C3. It's just, you know, a group of people who are interested to contribute to the protocol for and competing proposals for different technologies that will be presented, and ultimately what's considered to be the best will be adopted and move forward. So it's certainly open for anybody to participate. It's just quite complicated.

So you could also maybe draw analogy with Linux. And it might be a little bit like the long-term stable number of external developers. Linux and the guys that work in that space is -- like I said, it's something that is complicated. It's very mission-critical, high assurance, and has a relatively steep learning curve. So it takes a very experienced and expert programmer with knowledge for a range of areas to really become a top contributor in it. But there is progress in adding developers.

Operator

Your next question comes from the line of Tuur Demeester from Adamant Research. Please ask your question.

Tuur Demeester
Adamant Research

Hi. Thanks for the call. This has been really, really interesting.

I had a question, I think, for Wences and/or Adam about security risks with regards to cold and hot storage in Bitcoin. And in particular, from the institutional perspective, because, like recently, the CME group has launched two Bitcoin indices, and there is speculation that we might be seeing those like legally sound Bitcoin futures contracts. Jerry touched on the expectation of Bitcoin ETFs coming out.

And so, you know, in the light of institutional investors potentially becoming more active in the Bitcoin market soon, do you have any worries about things like fraction or reserve schemes popping up? Or inferior cold storage practices or insufficient insurance coverage, or about other risks that may not be fully appreciated by, you know, institutional investors that maybe are new to this space? Thanks.

Wences Casares
Founder & CEO, Xapo

Today we already do custody for the large majority of institutional investors and institutional products that are offering Bitcoin on the frontend. And the only way we can do that is because we hold more than 93 percent of the coins we're having custody in deep cold storage, in facilities that are never exposed to the internet because we believe that anything that is exposed to the internet, no matter their precautions, can eventually be hacked.

Dr. Adam Back
CEO, Blockstream

There are also interesting proposals. I mean, Gun Sirer and the group at Cornell Connell proposed, wrote a paper describing something called the Bitcoin Vaults which would sort of provide a two-stage method to move coins from storage. So I guess it will be something like the coin is hot but the users are keeping notice of its being on-vault and has a period in which they can contest on it.

So that's maybe a little bit more flexible to vaulting situation. But the best practice at the moment is the cold storage that Wences described. I think the – but I do find the hardware wallet methods, there are a number of them in market now, offer extremely good security.

Tuur Demeester
Adamant Research

So does that mean that both of you feel pretty confident that there's like an influx of, you know, say there's a big rally in Bitcoin and there's an influx of a lot of money that security-wise, and maybe legally also, things are set up pretty well for the moment to cope with that?

Dr. Adam Back
CEO, Blockstream

Yes. So I mean the cold storage is, you know, impenetrable that stands the physical security of the vaults which I'm sure are top-notch and geographically distributed and split in multiple parts, and so forth, in the larger vaulting solutions like Xapo.

For – another way to approach things has been the so-called multi-sig. So a form of shared custody where the vault has one key and the user has another key, and the user can keep that key in a hardware wallet.

So that t improves the picture even further by dissipating the risks. Even if they both were subject to equivalent of a bank heist or something, the funds couldn't be accessed because the users would also need to sign off on the transaction.

So remember this little flexibility because the equivalent of a banking mandate can be programmed as experimental. And time locking is also one of the interesting feature, perhaps similar in takes sense to time-lock vaults but -- in the physical world. But with Bitcoin, you can, for example, lock the Bitcoins so it can't be spent for six months or something like that. So that can offer flexibility in custody as well.

So in Blockstream, we require them a wallet called GreenAddress, which is increased service for the time lock. Normally, in multi-sig – two signatures, one from the user, one from the servicer required and it can provide two-factor integration with that.

There's also a time out, so let's say after a month, the user can spend the coins on their own. So that protects the user from any failing in the vault. And there are a number of solutions similar to that. Xapo and others may have some.

Spencer Bogart
Equity Analyst, Needham & Company

Wences, did you have something you wanted to add there?

Wences Casares
Founder & CEO, Xapo

No. We use the combination of what Dr. Back was explaining.

We have vaults that are completely offline, and in bankers that are deep underground, in multiple continents. And we use multi-signature, so three of five keys are required. And each key is in a different

location, in a different continent. So basically to break into – to move those coins, you would need to physically break into three of these bankers simultaneously which is very hard to do for many reasons.

And we do not offer the capability of our customers holding a private key because basically our customers are outsourcing that solution, or letting us handle that problem for them. If we give our customers, we have to decide whether that key is always required. If that key is always required, that becomes the weakest link if they lose their key. We don't control what happens to that key. And if that key is not always required, we are in the same situation as we were before. We give them that control.

So that's why we operate this way. And we keep about 3 percent of our coins in hot storage to – which are readily available for the movement of funds of our customers. And what we do is we self-insure by having separately a number of coins on our own balance sheet that is a multiple of that 3 percent. So if we were ever hacked in that cold/hot storage full of coins, we could replace them from our balance sheet.

Operator

Your next question comes from the line of Roger Ver from Bitcoin.com. Please ask your question.

Roger Ver
Bitcoin.com

First, thank you guys all so much for your efforts in this space. I have a question for Wences who has probably more business experience than anybody on this call.

Earlier, you touched on the importance of not assuming that the people have other options, and not to assume that people aren't (pricing) into the things. I was hoping you can elaborate on those two points a little bit more specifically from your perspective with Xapo and serving people over the world. I'd love to hear more of your thoughts on that please.

Wences Casares
Founder & CEO, Xapo

I think that Bitcoin has a network effect that are more nuance and then people realize at first glance. You know, the email system has an incredible network effect. But basically it's one dimension and the network effect of the email system is basically how many people are using.

Bitcoin has that dimension, has network effect around how many people are using it. And depending on how you count, Bitcoin has between 10 to 15 million users, and it's adding around 30,000 new users a week. Those 30,000 new users that Bitcoin adds every week are more than all of the other cryptocurrencies have ever added combined. That is super, super strong network effect.

And that's why – but Bitcoin also has very strong network in other dimensions. If you look at the hashing power, it's maybe the least obvious one and maybe the most important. Another one is the flow and the value of – not only of the outstanding Bitcoin but the daily flow of the numbers of transactions in the exchanges someone on this call already mentioned, the network effects with developers.

And a non-trivial one is that any coin that comes out has to decide what's the outstanding value of the currency when it's released. And if their outstanding value is very small, people tend to wait until they gets adopted so it's a chicken-and-egg kind of problem. That's why Bitcoin was 50 percent of the cryptocurrency volume about two years ago. And it's 96 percent of the cryptocurrency volume today. It has super strong network effect.

I think the bad side of this is we made them to think that people do not have an alternative, or we end up deciding for people in the long tail who are willing, who are very price-insensitive. We see that very clearly, today, the vast majority of our customers are people who have a smartphone and do not have a credit card and they are very price-sensitive.

And just like Bitcoin, saw a strong deceleration of user growth and transaction growth starting in January, when the transaction fee is starting going up, we saw it on our own system with the number of users adopting Bitcoin for the first time and with the number of transactions that we process everyday.

There is no reason why Bitcoin cannot process an unlimited number of transactions. Eventually, you know, I think that we may all agree that that's the case. And there maybe disagreements how quickly we can do that. But to create an artificial limit and an artificial expense on something that has basically a marginal cost of zero could be one of the ways in which Bitcoin dies.

I am very, very optimistic about Bitcoin. But I still think that they are waiting which Bitcoin can fail. And I think that that's one of the ways which you could say.

Roger Ver
Bitcoin.com

A lot of the technical community don't seem to share or understand those same concerns. Any thoughts on how we can bridge that misunderstanding between the business side and the technical side?

Dr. Adam Back
CEO, Blockstream

Yes. So I don't think there's really any misunderstanding. It's just that from the – you know, it's a question of balance. So I touched on my segment that there is a trade-off between security, which means for Bitcoin the censor-resistant, cash-like finality. And Bitcoin, it shapes those through decentralization.

And so, you know, as Wences said that ultimately Bitcoin should be able to scale indefinitely. And there is definitely a possibility. You know, let's run the theoretical example that different coin starts using the same technology, just a couple of Bitcoin that will also run into this security trade-off.

So the question then becomes, what do people buy Bitcoin for? Do they buy it because it's cheaper than PayPal? Or do they buy it because it's censor-resistant, permissionless and global? So we don't know the answer to that, and different people in the ecosystem have different views.

And my personal view is that permissionless and censor-resistance is quite interesting, since you know, we already do have PayPal, and if users are just trying to make PayPal like small-value transactions, they may not be worried about censor-resistance, and we are then directly competing against PayPal.

So you know, that could be another direction for Bitcoin, will be to push down the fees that PayPal and credit cards charge. But ultimately those people can reduce their margins. They have a lower cost technology than Bitcoin. Bitcoin has some complexity in network- or associated with it being decentralized and gold-like.

So I think, you know, it's not for us, anybody, to pre-judge which direction this can take. We should just try to improve the technology on front switches, of what's been happening basically. So as I said in my segment, really this last year has been the best so far in terms of innovations for Bitcoin.

It's malleability fixed finally, on-chain scaling, improved hardware wallet support led to coming online looking into next year, and progress on the sidechains to allow even more permissionless innovation, so that, you know, when somebody wants to try something experimental to do with scale or other features, they would have everything in their balance to do that.

So I think things are looking bright. And also with the short-term scale coming onboard, we should think it to see some uptake if that is holding back adoption.

Wences Casares
Founder & CEO, Xapo

Roger, I derive optimism from the fact that if we ask different people in the Bitcoin ecosystem, what we should do in – where Bitcoin should be in three months, in 18 months, and in three years, the gap of disagreement vanishes the longer the term horizon, right?

We – there's a lot of disagreement in what we should be doing over the next 12 months. But I think most of us agree on where Bitcoin should be in three years. And so how cautiously we should get there, and Dr. Back is being most cautious for good reason, and some of us that are running business, which we could move faster, but I think we all have Bitcoin best interest at heart and just a different perspective on how aggressively we should go on the same direction.

Dr. Adam Back
CEO, Blockstream

You know, I think that's fair. So you know, I mean, I think it's ultimately – there is some balance in there. There are some sorts of things even before segregated witness. I know it's interesting Wences that you are doing some off-chain transactions which can make sense in some cold storage situations between different hosted wallets for example, so the revenues there, also the payment channels are simple form of lightning.

We're expecting lightning going into next year. And I think that's where it really gets interesting that we should be able to run both the Bitcoin as a micropayment which can scale much lower than credit cards, say, go to places that credit cards and PayPal can't go on a cost basis, for example, per kilobytes streaming fees or all kinds of very, very low transaction fees, below 1 cent.

That scale will be possible, also the retail payments model, so we'll see how that works out. But at the moment, it's looking quite promising. And I certainly hope that people impressively adopt that

technology, and you know, work with the technical community to optimize what we already have as well.

We've seen number of improvements in wallets and efficiency of on-chain usage into last year as people have started to see fees that were non-zero basically.

But you know, ultimately it's the fees are still very low, at least for the digital gold and investment side of things. We recently did a $200,000 transaction for 4 or 5 cents, and (possibly receiving it at the cost of that) compared to what trends in your state, as well internationally.

So I think maybe Lightning is attractive for the very low-end sub-cent micro-transactions, and maybe even for the sort of retail payments use case. I was imagining myself with a wallet, with Lightning support, maybe I would put into the wallet the same amount of cash I will carry around and put that into the control of Lightning, let's say a thousand dollars, and then investment grade of money in the main Bitcoin network, something like that might make sense.

Roger Ver
Bitcoin.com

Thank you guys both

Dr. Adam Back
CEO, Blockstream

Thank you

Spencer Bogart
Equity Analyst, Needham & Company

Thank you all for joining us today. And a big thank you to our participants for sharing their perspective and insight and for all our participants for joining the discussion.

It's an exciting time for Bitcoin and we look forward to continuing this discussion on upcoming calls.

In the meantime, if you have any questions, feel free to reach out to me. My email address is sbogart@needhamco.com.

Thanks again and have a great day.

Operator

Ladies and gentlemen, that does conclude our conference for today. Thank you for participating. You may all disconnect.