The Solari Report

May 4, 2017

Bitcoin 101 with Sarah Wiesner

Bitcoin 101
with
Sarah Wiesner

May 4, 2017

C. Austin Fitts: Ladies and gentlemen, it's a pleasure to welcome a very special person to The Solari Report Sarah Wiesner, who is on the team at Bitcoin Embassy in Tel Aviv and is coming to us from Israel.

I've been corresponding with her for almost two years now. Of all the people I correspond with on Bitcoin, she is far and away the most intelligent, the most informative, the most interesting, and particularly the most coherent.

Finally, I said to her about a month ago, "Sarah, you have to come on and explain bitcoin. Our subscribers are extremely intelligent, and they vary from knowing nothing about bitcoin to being avid bitcoin users. So we need somebody who can handle that entire gamut," which I'm confident she can.

So, Sarah, thank you very much and it's a pleasure to have you join me on The Solari Report. We have a great deal to go over, but I know that you are extremely knowledgeable and well-prepared for this. It's really a pleasure to have you.

Sarah Wiesner: Thank you for having me on and it's a pleasure to be on The Solari Report.

C. Austin Fitts: Tell us a little about Sarah and the Bitcoin Embassy in Tel Aviv and how you got involved in bitcoin and why you got involved in it.

Sarah Wiesner: When I was in my early 20s, I was trying to understand what was going on in the world and about money. Then I discovered the idea of anarchism and decentralizing. I realized that was the right way to go.

So later, a friend introduced me to bitcoin. I didn't really understand how it worked, but I understood that it was a stateless currency. I knew a little about cryptography, so I thought, "It works. I'm going to buy some."

Later, I learned more about how it actually works, and I was very impressed and fascinated by that. So this is what happens to most of the bitcoin enthusiasts: One day, it just clicks for them, and they say, "Oh my God! I can't believe it!"

They somewhat fall down a rabbit hole learning about it and that's what brought me to the Bitcoin Embassy.

The Bitcoin Embassy was opened about three years ago in Tel Aviv. It used to be an architect's office, until he realized that bitcoin needed a place where people could in fact speak face to face about bitcoin.

So he opened this place, and I'm here right now. We have a bitcoin ATM here, and people can come in and buy bitcoin for cash, and we will explain about it. We have events and movies and meet-ups. Basically, we have an open space, and try to run it in an open source worldview so we don't have to have a manager. It's a very free and friendly place.

C. Austin Fitts: There are embassies around the world, right?

Sarah Wiesner: I think there are about ten different ones and each one is independent. There is no CEO of bitcoins, so anyone can open a bitcoin embassy.

C. Austin Fitts: You need to tell us a bit more about Sarah; you skipped over that part.

Sarah Wiesner: I was born in the United States in Boston, and my parents moved to Israel when I was five. I grew up with computers and that was part of my life. So then I went through the army and to science camp at the university and dropped out. Then I became interested in bitcoin, and now I'm working in the bitcoin space.

C. Austin Fitts: I would say that you are making a concerted effort to understand the economics and markets and how the world works. That I know.

So let's dive into bitcoin. First of all, what is it, and how does it work? Take us through it.

Sarah Wiesner: Maybe we can start with how it works, which is the hardest thing to explain, but I'll do my best.

The first thing that you need to know is something called a Public Key encryption. It replicates the encryption. You take a random number and out of it, is created a Public Key and a Private Key. The Public Key is something that you publish to the world, and the Private Key is to be kept secret.

Let's say I want to send a message and want to prove it's me. You know what my Public Key is; so then I can take a message and do an operation over it with my Private Key. I'm not exposing my Private Key, but I'm sending you the other number. Then you can take that number, and check and prove that it's from the person who has the Private Key that corresponds with the Public one.

Basically, it's a mathematical way to prove identity. No one except the holder of the Private Key can 'sign' – which is called a digital signature – a message that corresponds with the Public Key if you're not the same person holding the secret key.

C. Austin Fitts: Right, and that Private Key can be created offline, but you may have to communicate it online and can store it offline.

Sarah Wiesner: Right. The best practice is to create it on a computer that is offline, and maybe even prevent it online. Then you could destroy the computer afterwards or take any other security measure.

Later, we will discuss how to secure the bitcoins, but that is the first thing that you need to know about it.

Basically, the bitcoin is a ledger database. A database is full of bitcoin transactions. With the bitcoin transaction there is a Public Key, and there are a number of bitcoins that are associated with it. Also, there is a signature from that Private Key. There is another public address where the bitcoins are being sent. So the sender signs this transaction, and there is no way to fake it. There is no conventional computer that can crack this or reverse it and it's very, very high security. So that explains the bitcoin database.

The question is where are the bitcoins coming from? The other problem is: How does everyone agree what the database is?

For the solution for both of those questions you need to know one more thing. I sent a graphic description of the hashing and the public encryption. There is an item called a 'hash function'. A hash function is when you take a message and put it through the hash function and get a string or a number of a certain length. The thing about the hash function is that you can't predict what the string is going to be. You can't predict what number your message is going to create.

The only way to do it is to try it, and then you take the result and can show that it came from that message.

C. Austin Fitts: Where does the hash function get created, Sarah? Let's say that I'm on my computer, and may be interacting with the bitcoin database that is somewhere else, initially or shared. Where does the hash function get created?

Sarah Wiesner: The hash function gets created on the computers of the people who are adding the new blocks of data to the network, and they are called the 'miners'.

C. Austin Fitts: So the miners create the hash function?

Sarah Wiesner: Right. He takes the last ten minutes of new transactions and hashes them. So every block of information has a little identifier number in the hash. You can't create the hash before you have the data. They add to every new block the hash of the previous block. This creates a coherence in time because you can't get the hash before you have the information, so every piece of information has the hash of the previous block of information. So it creates a chain called a block chain. That is similar to a mathematical proof of what came before what.

C. Austin Fitts: Right.

Sarah Wiesner: So now we have two parts of the bitcoin, and there is one more part. How do you keep the security of who owns the bitcoin of the public encryption? You have the timeline with the hashes, and the last thing is: How the bitcoins are created, and how everyone agrees on the same database.

The miner gets to write the new block and there is a space to put in a Public Key to which he will receive a newly minted bitcoin. Obviously it's not for free. Basically. what is happening is the bitcoin program is like running a lottery every ten minutes.

Everyone who wants to be a miner takes the new block of transactions and they hash them. There's a little space in this block of information where you change a few numbers. It's called the nons and it's like a pervert – it's the same spelling.

C. Austin Fitts: Nons?

Sarah Wiesner: So with every block of information of the transactions, you can also change a few numbers that have no significance. When you change them, you get a slightly different hash. So the bitcoin program tells them that you have to keep trying to change the numbers – trial and error – until you get a hash with certain attributes.

For example, it starts with 000 and then whatever, and the only way to do that is trial and error. You can know your statistical chance of finding it and if you run the computer long enough, you will find the right hash.

Every ten minutes, one of the computers finds the hash, and that gives them the right to write the new block and receive the newly minted coin and add it to the block chain. Everyone looks at the hash, and can say, "Oh, yes. He ran the computer and did the work. So he is the one who deserves to add the new block."

This is also called 'proof of work' because it means that you ran many computers and used a lot of electricity trying to find this hash. That's how bitcoin decides how to create the database.

The rules in the bitcoin system is that the real database is the longest chain of transactions, which means that it is the chain that had the most work done on it. So the miner has an economic incentive to add his block to the top because he wants his newly minted coin transaction to be in the network. He wants to get his money back for the computer's electricity and that is the trick that is supposed to keep the system going.

C. Austin Fitts: How many miners are there worldwide?

Sarah Wiesner: The only thing you can look at is the amount of hashing power because the more computers, the faster you can find the hash. The bitcoin program checks how fast they're finding these hashes, and it's supposed to be ten minutes. Every time it gets too fast, it gives it a more difficult hash to find.

The hashing power has doubled or maybe even more in the last year. It's essentially, strong computing power, a few orders of magnitude greater than all global computers. It's the biggest computer in the world.

C. Austin Fitts: Really? So the bitcoin mining operation is that powerful?

Sarah Wiesner: Yes. It's insane because it's like a license to print money, even though it does cost a lot of money to make these operations. Apparently, it's very professional to have a large mining farm.

C. Austin Fitts: My understanding is that there is a law of diminishing returns. In other words, there is a real limitation on the amount of bitcoins that can be created over time because the mining operations and debasement get harder and harder to do.

Can you explain how the limitation works?

Sarah Wiesner: Every four years the amount of bitcoins that are created in every block goes down by half. So it started at 50 and went to 25. Now it's 12.5, and it's going to go to zero. When it gets to zero, the idea is that the miners will make money only from the transaction fees.

C. Austin Fitts: Right. Let me jump in. Can you explain the difference between a miner and an exchange?

Sarah Wiesner: Definitely. Bitcoin doesn't know anything about the exchanges. The exchanges are used to exchange what bitcoinners like to call fiat money – government-sanctioned money – with bitcoins. So it's a place where you can send money and they will send you bitcoins, or you can put in your bitcoins and send in your Private Key, and they're holding it.

You can go on these sites and trade bitcoins. There are a couple of big ones.

The miners are an inherent part of the network. They don't know about anything except the bitcoins. They don't know what the bitcoin price is. It's computers making sure that the system is coherent and safe.

C. Austin Fitts: Do you have any estimate of how many exchanges there are globally?

Sarah Wiesner: I think there are quite a few, but I would say that there are only about ten big ones. The best way to watch them is on a great site called the www.TradingWalk.com. It lists the price of every major exchange.

C. Austin Fitts: One of my favorite bitcoin pieces of information from you is the cartoon that you posted near the water cooler at the Bitcoin Embassy. Why don't you explain that?

Sarah Wiesner: "Never bitcoin in the exchange." In 2013 there was one major exchange in Japan run by a teenager. It used to be a car trading site and it was very unsafe and got hacked. Many people lost their money there and so we try to remind people of that.

Exchanges are centralized. It's the honey pot for any hacker in the entire world. They want to hack a bitcoin exchange, and they keep getting hacked. The biggest bitcoin exchange, Bitfinex, got hacked last year. They gave everyone a haircut on their bitcoins.

C. Austin Fitts: So the best practice is to keep it in a 'wallet'. Explain to me what a 'wallet' is and how I keep a bitcoin in my wallet and not on an exchange.

Sarah Wiesner: There are a few different kinds of bitcoin wallets. One of them is a program you download and there are various types of them. It's either on your computer or your cell phone.

That program generates a Private Key, and you use it to store your bitcoins and to send them or receive them. Because your Private Key is stored inside the program, it's very important to back it up. All these apps have the option of backing up your Key. It tells you to write down twelve words on a piece of paper, so if you lose your phone or if your computer breaks, you can use those words and rejuvenate your account.

C. Austin Fitts: Right. So the idea is that if they steal your phone, they can't hack it and steal your bitcoins out of your wallet because you have the Private Key.

Sarah Wiesner: If you put a password on it.

C. Austin Fitts: Right.

Sarah Wiesner: It's very problematic. If you are storing large sums of money, it's recommended that you do it in a paper wallet or in a hardware wallet. A paper wallet means that you create the Private Key as much offline and in as secure a way as possible. There are guides for that online, but the best way is to find someone who is an expert in this and do it for you, or learn about this in depth.

You create the Private Key offline, store it offline, and then you can send money to the Public Key, and it never even touches the internet. That is the most secure way to store bitcoins.

A hardware wallet is a little piece of hardware, and it can hold a Private Key. It is also considered a more secure way.

C. Austin Fitts: So it's like a stick?

Sarah Wiesner: Yes.

C. Austin Fitts: Before we go on to price and volume, is there anything else you would like to say about how it works?

Sarah Wiesner: An important point about the bitcoins system is that, essentially, it's a program. If you want to join the network, you have to use the network's rules. That's primarily how it runs.

Also, another important fact is that it's been around for eight years, and it hasn't been hacked yet. It's considered possibly unhackable.

C. Austin Fitts: When we talk about Catherine's deep aversion to cryptocurrencies, we'll discuss that. I'll challenge that a bit more.

It's fair to say that there is much enthusiasm everywhere in the financial system for block chain because it's extremely secure, and it's decentralized – which creates a resiliency we don't see in the financial system.

We've been at this for eight years, and one of the reasons people are so excited about bitcoin is the price has been volatile, but the price has really continued to rise. Talk a little about price and volume and who has been joining the market, how deep and liquid the market is, and then a bit about regulations.

Sarah Wiesner: The bitcoin started in 2009. It wasn't actually traded until 2010 and was worth very, very little.

Towards the end of 2010 and in 2011 it started picking up a bit, and it reached parity with the dollar. At some point it went up to $3 and crashed back to $1, and then it kept going up. In 2013, Cypress had a 'bail-in' that spiked the bitcoin price to around $250 or $300. It crashed back down to about $100. Then after a few months it had a big run-up, as many people remember. It went up to about $1,250 and then it kept coming down until 2015. It somewhat stabilized at $250 and afterwards, started rising again.

The bitcoin rose and rose and stabilized at $400. Towards the halving, which was when the bitcoin creation went down in half; it spiked at $750 and kept rising. Now we're hovering around $1,200.

C. Austin Fitts: It would be very interesting to figure out if you have a currency that is essentially impossible to debase significantly; it would be interesting to estimate how much of the increase in the price is coming from inflation versus new adopters coming into the market.

Sarah Wiesner: More bitcoins are being created, and I think that the fact that since production went down in half, the miners' revenue is cut in half. So they could sell bitcoins for a higher price and that's considered possibly one of the reasons the price was pushed up.

Also, I think the bitcoin is becoming more understood and recognized. I think the block chain hype also helped. Over the last year, for the first time I've seen investment professionals from the old school financial world talking seriously about bitcoin. I think that's where the speculators have been coming in.

C. Austin Fitts: Right.

Sarah Wiesner: I also think that CryptoLocker ransomware is creating much money coming into bitcoin.

C. Austin Fitts: Let's talk about who's who. You sent me a lovely description of the early adapters and who has actually been using bitcoin. So let's go through them. Start with ransomware because I was particularly intrigued by your description of the ransomware business.

Sarah Wiesner: It's really something! Ransomware is basically a standard computer virus. Usually people get it from opening a file they shouldn't have in their email. It takes over a computer, it encrypts your files, and it tells you very politely that you need to pay bitcoins to get your information back.

Sometimes they could take over a system or an office or factory and ask for a ransom. Of course, they are asking for a ransom in bitcoins because it's pseudo anonymous, and it goes straight through the internet.

That was a big deal over the last year or so because a lot of criminals have been catching onto this and using it. I think it also pressures people to have more computer security. As you mentioned, a computer is completely insecure and has to be dealt with and this brings it into the light.

C. Austin Fitts: You sent me a link of a famous example of a hotel in Austria that was using electronic door keys and was hit with a ransomware attack and has now upgraded to good old-fashioned physical keys. I thought that was intriguing.

Sarah Wiesner: It's very important to back up your information.

C. Austin Fitts: So ransomware last year was $1 billion, and ransomware was paid in bitcoin.

Sarah Wiesner: I read that estimate, and it sounds believable to me.

C. Austin Fitts: That is remarkable.

Sarah Wiesner: The standard ransomware is four bitcoins, which is about $5,000. We had many people coming into the Bitcoin Embassy and paying these sums. There were also bigger ransomwares. I heard of some asking for millions of bitcoins from hospitals. The companies don't want to disclose the fact that they're giving ransoms, but somewhat surprisingly they always want to pay their ransom. They just want to get their computers back and it may even be tax-deductible because it's not much of their operations, so they pay it.

That is a lot of money, but it could be that much.

C. Austin Fitts: Another one you mentioned was the black market activity. Explain the darknet and how bitcoin could be used on the darknet.

Sarah Wiesner: The darknet is usually an internet browser called TOR. It routes your IP through many different computers. Supposedly, you can't tell where the user is coming from, and where the internet is coming from. So it gives somewhat of anonymity and a site to cache it off.

The bitcoin is very good for the darknet because you don't need to identify yourself and no one can stop it.

One of the first uses for bitcoin was a site called The Silk Road. It was essentially an eBay for drugs and other black market goods. I surfed the site today, which is called AlphaBay.

I saw that there were 300,000 drug listings on it. I think it's an improvement because there is quality-controlled feedback. Also, you can order kits to check that the drugs are clean.

In my opinion, it takes drugs off the streets. Also, hackers can sell each other information and, basically, anything that hackers want to trade is done through bitcoin.

C. Austin Fitts: The use I see the most of – and I'm not suggesting that it's the biggest use – is investment by people who are completely disgusted with the traditional systems and want their money in something that they perceive to be grounded in a decentralized network.

Sarah Wiesner: Definitely. The bitcoin development grew out of cypherpunk mailing lists. Cypherpunks are fundamentally people who believe that the only way to keep people's freedom is to encrypt their information and they caught on at the end of the 1980's.

They realized what was going to happen, and started developing all these open-source tools to help people encrypt their information independently. They actually developed PGP, which is a very popular Public Key encryption system that people use, and therefore bitcoin was published. It's developed in that same kind of mindset – an open mailing list where anyone can contribute to it and there is no formal structure governing it.

Many people who joined bitcoin are people who were, beforehand, activists and monetary chains and anti-central banks.

C. Austin Fitts: Clearly, one of the defining characteristics of bitcoin is that ultimately it can't be debased. After an initial creation and growth, it becomes impossible to debase, let alone debase radically. For somebody looking for a currency investment, it's not a big liquid market compared to the large sovereign currencies yet. That makes it very appealing, especially in a world where you are very worried about inflation.

Sarah Wiesner: The volume is currently between $100 and $150 million traded every day. It went up a great deal in the last year.

Also, another nice thing about bitcoin – which is also a problem – is you're the one holding the Private Key. You can't have a bail-in unless it's on the exchange.

C. Austin Fitts: Right. Again, best practices are not to keep it on the exchange.

Talk a little more about the community. It's very interesting. With new financial innovations, it's usually the illegal or dark functions that get it going. So where you see big, important financial developments, a lot of times it's the dark money that is the early adapter that helps build the infrastructure; so that is pretty typical.

Sarah Wiesner: I'm happy to hear that from you.

C. Austin Fitts: The pirates are always the innovators.

Sarah Wiesner: I don't think it's the history. The history of bitcoin is really the idealist site for punk anarchist decentralized people.

C. Austin Fitts: Right. I didn't mean that it was the history of bitcoin; I meant that it was the history of financial innovation. So the innovators are always trying to get away from the traditional system, and it could be because they want freedom, or it could be because they want to avoid taxes, or it could be many different reasons. That's the way it goes.

Needless to say, if you look at the community of people involved in bitcoins – moving beyond the dark functions – you have a complete world of different folks who are very, very interested in decentralization and moving away from traditional systems. So there is a real community and culture growing up.

Sarah Wiesner: Yes, it's really great. I think it's one of those things that keeps people involved in bitcoins. It's like-minded people, and we try to create a community atmosphere. We have parties and had a block halving party and all kinds of things.

C. Austin Fitts: I saw the pictures.

Sarah Wiesner: Maybe I'll send you a link to the video where we were smashing concrete blocks to symbolize the block halving.

It brings in a lot of alternative culture, cyberpunk, and all the kind of counterculture coming off the internet. It's really part of what is happening in bitcoin; it brings in those kinds of people.

C. Austin Fitts: My perception is that you have a great deal of people who want to be free, believe in freedom, and it's attractive to be with them and be around them.

So let's talk a little about regulations. We have seen efforts by the various central banks and the banking regulators to understand bitcoin and consider what they want to do in terms of regulations. So what can you tell us about regulations?

Sarah Wiesner: It's unclear. Countries started putting different labels on bitcoin. They consider it a commodity, and every state makes its own regulations. I don't understand regulations very well, but in New York they adopted all these regulations that basically killed bitcoin there because every transaction needs to know the name of the person. It's called KYC (Know Your Customer) and it's a central problem for bitcoin.

I think in California they're starting to write the regulations. In Israel they're trying to make this horrible law to tax it from both directions. In Europe they're a little nicer to bitcoin but I don't know if they've declared that it's a currency. In Germany you don't get taxed if you keep your bitcoins long enough.

I think they're putting all sorts of labels on it, but there is no regulation being enforced. It's not being taxed yet, but this is something that is probably going to happen in the next few years.

The biggest American exchange is called Coinbase, and they were asked by the IRS to give them all the records of all the users a few months ago, and we don't know what is happening with that yet.

C. Austin Fitts: If Coinbase is asked by the IRS for all the users and they have the record of the transactions but they don't have the Private Keys…

Sarah Wiesner: They have a record of the transactions. When you pull your bitcoins off the exchange, you send it to a new wallet. Then you hold the Private Keys when you get the bitcoin off the exchange.

C. Austin Fitts: But Coinbase wouldn't necessarily have your name, would they?

Sarah Wiesner: I think that with Coinbase you have to prove your identity. Most exchanges will ask you for some kind of identification.

C. Austin Fitts: So Coinbase does know their name – or at least the name they gave.

Sarah Wiesner: Yes. If people don't want to give their name, they make you do it through local bitcoin or a cash deal with someone face-to-face. There are a few other ways of doing that. There is a decentralized exchange, and a few other ways but the easiest way is giving your name.

C. Austin Fitts: So let's look at the difference. The way bitcoin is brought with me is through clients who say, "Should I keep my money in the bank, or should I keep my money in bitcoin?"

If they leave it in the bank, they have the protection of sovereign government insurance. If they put it in bitcoin, they don't have that protection.

Also, if you encounter somebody who is not knowledgeable about bitcoin and the process or they're in a town where they can't walk into a Bitcoin Embassy and get the kind of community and education they need, it takes all sorts of time and effort to learn the system and participate. They are also dealing in prices, so if they buy now, the price is relatively high. There are many speculators in the market that could potentially deal with much more volatility when, in fact, their costs are in dollars.

Sarah Wiesner: Right. One of the best recommendations I've heard is that if you're buying bitcoins, buy amounts where if it goes down significantly, you won't be tempted to sell it.

C. Austin Fitts: Right.

Sarah Wiesner: That is definitely very true. You definitely have to educate yourself before you store your bitcoins, but there are safe ways to do it. There is a thing called 'multisigs' (multi-signatures). It means that there are a couple of Private Keys protecting your bitcoin instead of one. So supposedly you can put one of them in a bank safe and the other one with a family member and another one you hold for yourself. Then you would need two of them to get the bitcoins out. So that would be a safe solution.

C. Austin Fitts: Has anybody created a bitcoin hedge yet? In other words, has anyone created a bitcoin futures so you could hedge the market risk?

Sarah Wiesner: Yes. There are a couple of exchanges that have futures, and you can also short decline.

C. Austin Fitts: So in theory, there is a way to hedge to protect yourself against a big drop in the price.

Sarah Wiesner: Yes, but it is on exchanges, and those exchanges are not insured. So that's a different problem. But, the bitcoin market is like the Wild West. It's a new world, and it's likely possible to make a private agreement of hedging if you don't want it to be online.

C. Austin Fitts: One other question that I have is: Occasionally you will see an announcement that a big bank or a central bank is considering using block chain or creating a sovereign bitcoin. Are there any developments yet?

Sarah Wiesner: The thing is that when bankers say 'block chain' they don't actually know what they are talking about. They somewhat kidnapped this word and use it to recognize any kind of semi-distributed system that is using encryption and ledgers. A lot of technology existed before, but I think bitcoin woke them up to the need to make more secure systems – something that is cryptographically safe and not just something where anyone can go and only change numbers.

So they are using this method to bring them to the 20th century, and also it's rather like a whitewash for bitcoin by saying, "Oh, we also have bitcoin; we have a block chain," but it's not always necessarily the case. Bitcoin is an open network that anyone can use, and the bank is creating closed networks using some of the ideas from bitcoin.

C. Austin Fitts: Right.

Sarah Wiesner: There is a lot of talk about creating a block chain for sovereign currencies. I know that they want to make something a bit safer than SWIFT, which is being hacked all the time. So they may make a cryptographic system that is somewhat like bitcoin to make more secure systems. Making governments block chain for the country to have their currency on it, they haven't yet published what they actually mean by that. Would people be able to mine the fiat currency?

C. Austin Fitts: Here is the thing: You have a global market of citizens who want a currency which can't be debased and can't be billed in. That's what everybody is looking for. The war on cash is adding to that urge. So the question is: We have a competition between decentralized networks and the central bank over how to satisfy the market, but the central banks are still looking to harvest. This is all part of the ongoing challenge of: Are we going to be free or not?

Let's talk about best practices. You mentioned the importance of not keeping your money on the exchange and keeping it in a wallet. You were talking about how to keep your key private and protected. Do you have any other thoughts on best practices for somebody who is going to hold bitcoin?

Sarah Wiesner: I think it's important that if you're buying it through an exchange where you give your information, it is important to write it in your tax reports. If you want to stay anonymous, you want to make sure that your name isn't involved when you buy the bitcoins. You also should not talk about it because it's similar to gold in that you need to keep it safe.

C. Austin Fitts: That is a good question. Is it clear that if you buy bitcoin at one price and sell it at another what the capital gains treatment is for taxes?

Sarah Wiesner: It's unclear and it's not being enforced yet. It will probably be resolved in the next few years. It might be problematic if they're blaming people for money laundering. The thing is that it's very hard to prove that someone owns bitcoins.

C. Austin Fitts: The other issue is, if I go to Europe and buy euros and then exchange them back into dollars, when I return, I don't treat that as a taxable transaction. So the question is: What makes bitcoin taxable versus the euro not?

Sarah Wiesner: I agree with you on that, but it's all according to the whims of the regulators.

C. Austin Fitts: There is no doubt that sovereign governments can advantage their own currencies by making them not taxable and making everything else taxable.

So let me talk a little about my deep aversion to cryptocurrencies but, also, why I think we're going to keep seeing digital currencies.

Would you describe bitcoin as a cryptocurrency?

Sarah Wiesner: Yes.

C. Austin Fitts: As bitcoin has grown, we've seen the development of other cryptocurrencies around the world, correct?

Sarah Wiesner: Right. Currently only 66% of the market cap of cryptocurrency is bitcoin. The other coins, which are called altcoins (alternative coins), are really picking up. There are hundreds of different coins being traded because anyone can create them. It's somewhat like a penny stock type of market.

C. Austin Fitts: When you say the total market cap, what is the total market cap of all cryptocurrencies including bitcoin?

Sarah Wiesner: I think it's around $30 billion and of that, bitcoin is $20 billion.

C. Austin Fitts: So bitcoin is clearly the only market with any kind of real liquidity here.

Sarah Wiesner: Actually there is a lot of volume in the Sarian System. It's much smaller, but it's still very significant.

C. Austin Fitts: One thing I've always said is that I think the market very much wants digital currencies and cryptocurrencies because the only way you're going to get the transaction costs way down is to have something that can be maintained on a decentralized basis at a very, very low cost. It seems to me that if we are going to have global transactions that are affordable for the frontier and emerging markets, we've got to get the transaction costs way down.

What you're describing has the capacity to do that. Would you agree with that?

Sarah Wiesner: Yes, partially. Potentially, that is what it is going to be like. Right now, because of the limit to the amount of transactions that can be sent across the networks, the transaction fees have been going up. They are still not more expensive than regular admittance, but to bring them down they would need to put in another update to the bitcoin network, and that is being talked about and negotiated now among everybody.

C. Austin Fitts: If I have bitcoins in my wallet and go online and buy something with bitcoin, is the transaction fee to the dealer lower than it would be if we were using regular credit cards?

Sarah Wiesner: It depends on the day, but right now I would say that a standard transaction fee would be up to $2. Until very recently it was much lower. Because many people are using the network, it's gone up.

C. Austin Fitts: So on a big, big purchase, it may be lower if it is a nominal amount?

Sarah Wiesner: The transaction doesn't change by the amount of money you're using. You could be exchanging a large amount of money and still pay the same $2 fee.

C. Austin Fitts: That is going to make it much smaller?

Sarah Wiesner: When improvements to the bitcoin network come through, that is going to push the transaction cost down to what it used to be a year ago, which was a few cents. That's not the situation right now, but that is technically possible.

C. Austin Fitts: Right. Let's talk about my deep aversion because I drive my base. I have a number of avid subscribers who love bitcoin, and I drive them crazy. First, I call it a fiat currency.

Sarah Wiesner: That will drive bitcoinners crazy.

C. Austin Fitts: A fiat currency technically is a currency issued by a sovereign government, but many of us use 'fiat' meaning that it doesn't have an asset category behind it. So it doesn't have a gold standard; it doesn't have an oil standard; it basically has nothing.

Sarah Wiesner: It's somewhat backed by electricity. The miners have to spend money on electricity and hardware to get the bitcoins, so that is possibly a way to see it as being backed by something.

C. Austin Fitts: Right. So they have to work very hard to get a bitcoin. There is no doubt about that, and it's not cheap. But if you're in the United States and leaving something that has both deposit insurance and the backing of a well-capitalized bank, you're moving to something that has no liabilities from the sovereign government or obligation of the sovereign government and has no human institutional backing to protect it.

Sarah Wiesner: That is very true. I heard bitcoin being compared to a bearer bond.

C. Austin Fitts: Right. It's remarkably like bearer bonds in that sense. But now I know if I want to drive a bitcoin enthusiast crazy, all I have to do is insist that it's a fiat currency, and off they'll go.

Sarah Wiesner: I hate fiat and I don't have any fiat.

C. Austin Fitts: I think that's fair because I think it's expressing the deep fury of people who understand what has been done to them with debasement. If you study the wealth that has been stolen, it's extraordinary. So the fury of people who have worked for years and years and store that value and that value gets debased away or even bailed-in away as it was in Cypress, you are constantly feeling like you are putting your money in something that is harvesting you. So I truly appreciate the deep fury.

Here is my big concern, and that is in my whole life I've had many dealings with the intelligence agencies and the secret societies, and I've never met a digital technology that they didn't have a back door into it. I've heard many hours of descriptions by people of why bitcoin is independent and truly decentralized and free.

I had one of my colleagues send you some of his questions about different methods by which the procentralization team has compromised digital systems, including technology that allows them to get various communities to give them back doors or gives them the ability to track what's being input into a computer through the keyboard.

Why don't you talk a little about why the bitcoin community thinks that the system can have integrity and can't be compromised?

Sarah Wiesner: So I guess the first argument is that bitcoin is open source; anyone can see the code. It's possibly the most viewed program in the entire world. You can go through it and see it's coherence and it's not very complicated.

Having an obvious back door like they have in different programs and operating systems is not happening. It's not an option, however, there are a few other problems. The Public Key encryption can theoretically be cracked by a quantum computer. I see that as a real concern but the head of the Bitcoin Israeli Association published an article about this. There is a different kind of encryption that bitcoin could upgrade to if it was worried about the quantum computers cracking it. So this is another factor about it.

I would agree that all the systems are compromised, and to do things in a decidedly secure way, if you think you're being targeted, is very tricky. That is definitely a problem.

It's very convincing that the system as a whole can't be compromised, but you can definitely hack someone. It's extremely hard to hack the mass.

C. Austin Fitts: If you examine the dollar system and if I hold dollars in a bank or a brokerage account, I can also be hacked. In that sense, I think a dedicated hacker looking to target an individual can always do damage. No system is impervious to that.

Sarah Wiesner: Right.

C. Austin Fitts: For a practical matter and for most users, if you're not bitcoin savvy and if haven't learned bitcoin, it takes a certain investment of time to learn how to do it and make sure that you are doing it in a very secure way.

Sarah Wiesner: Yes. Some of the activity we do at the Bitcoin Embassy, as you know, is making sure that people are writing down their keys securely. That's a big file. You need to take the responsibility to do it correctly; no one is going to do it for you.

C. Austin Fitts: Right. So here is the trick question, Sarah: What is going to happen to the bitcoin price over the next ten years? That is what everybody wants to know.

Sarah Wiesner: I don't know. I guess the conventional wisdom is that if it survives for ten years, it's going to be at a much higher price. I would say it would be zero or very high.

C. Austin Fitts: So it's zero or $20,000?

Sarah Wiesner: I think now that there are new cryptocurrencies and some of them have different governance structures and they're more centralized and have better PR, what is definitely true is that this is like Pandora's box. The monster is outside as far as technology, and you can't roll it back. There are definitely going to be cryptocurrencies being traded and being used. The entire market, in general, seems that it has to grow as it picks up more users.

I guess the hope of the bitcoins is that the bitcoin will be the reserve currency of all these other cryptocurrencies. In that case, it does have the possibility of becoming much more valuable.

C. Austin Fitts: At present, the US dollar is the reserve currency. If you look at the current indications, we are waiting for the first full budget of the Trump Administration. But if you study all of the policies and policy statements that have rolled out over the last month, every indication is that the US government is probably going to significantly increase military expenditure, and that means significant debasement of the US dollar. So whether it's the central bank that is buying it or the Treasuries that are selling currency, we are in for a period of inflation.

We don't know what is going to happen to the euro, so that is a question mark. But let's just assume – because I think inflation is probably running much higher than the official statistics – in a world where the reserve currency is being debased, and the bitcoin has been halved, when does bitcoin really approach the point when the law of diminishing returns means it's actually growing?

Sarah Wiesner: I think it's in about 100 years. So in approximately three years it's going to go down to 625. Then in four more years it will be three. So I estimate, in about 20 years, there is going to be very little bitcoin being produced.

C. Austin Fitts: So in the period when presumably the dollar continues to be debased, the rate of growth of bitcoin is going to be slowing very dramatically. That is what it sounds like.

The real questions on the price are: How many people join the community? But ultimately it's: How significantly does the dollar and the big sovereign currencies debase?

Sarah Wiesner: I think that is one of the reasons that draws people to bitcoin. They are really worried about inflation and debasement, and they see it as an insurance policy.

C. Austin Fitts: For many decades people saw gold as the insurance policy, but the reality is that if you look at what is happening, the system has been able to create enormous amounts of paper gold.

It's interesting when you look at people who are buying paper gold. It's easy to argue, "What is the difference between paper gold and bitcoin?" There is nothing behind them."

Sarah Wiesner: There is an unlimited amount of paper gold, and there is not with bitcoin. You can't go into a minus sign with bitcoin.

C. Austin Fitts: Right.

This has been unbelievably instructive. This is the first serious conversation I've had on bitcoin where the other person didn't start screaming at me, so I'm very appreciative.

Sarah Wiesner: I would like to add something more about bitcoin.

C. Austin Fitts: Please, go ahead.

Sarah Wiesner: I could talk about it for hours, but it's about the bitcoin privacy. Right now on the bitcoin block chain, you can see what transaction went from which to which Public Key and just see it. That's not very private, but coming from a cyberpunk mentality, one of the main issues is that they are trying to develop a more private block chain and more things that will secure the history of the coin because they are considered fundability equivalent to every coin. It can't be tarnished, and that is something that is very important about a currency.

So they are developing systems that will decentralize that. Once they are ready in the next year or two, which will allow much more real privacy using bitcoin. So I think privacy will be possible.

C. Austin Fitts: Who is leading that effort?

Sarah Wiesner: The bitcoin developer community. It's called Bitcoin Core, and it's the one true mailing list and anyone can contribute to it. They also have a convention every year, and they present the projects that they are working on and their priorities.

Right now the priority is scaling the network and also creating fundability.

C. Austin Fitts: Where is the conference?

Sarah Wiesner: Every year it's someplace different. It's in Canada and in Hong Kong and Italy. They are actually talking about having it this year in Israel, but it's not confirmed yet but I think it is going to be here.

C. Austin Fitts: Sarah, if we were to look at the population of bitcoin owners – people who have money in bitcoin – where do you think the population is right now?

Sarah Wiesner: It's really hard to tell, but I think most of them would be financially aware people who have some money to invest. They are tech-savvy people. There are a very high percentage of men, usually in their late 20's to early 50's.

There are different alternative communities that catch on to bitcoin, and also there are speculators. It's becoming increasingly more mainstream, but it's really impossible to know.

C. Austin Fitts: Right. I would love to see the statistics on what the percentage of bitcoin holders is relative to the currencies being debased the fastest.

Sarah Wiesner: Yes. Actually, it is much more popular in places that have a very corrupt government. Maybe that is not the right description, but people who have very unstable currencies. For instance, I saw that Zimbabwe has a very high interest in bitcoin, and Venezuela has people smuggling bitcoin miners into the country.

C. Austin Fitts: Really?

Sarah Wiesner: Over the last two months when India cancelled the paper money, bitcoin's price was $100 higher there within a month because people were running into it.

It was the same issue in China. There was a great deal of bitcoin activity in China because people were trying to pass the controls on taking money out of the country because they know the government wants to bring down their currency.

C. Austin Fitts: The indication I've seen is that the recent adoption of bitcoin in China is quite fantastic.

Sarah Wiesner: Yes. They are actually very positive about it and are trying to regulate it. Right now you can't withdraw money from the bitcoin exchanges until the government says you can. They want to have more control because they saw many people trying to move money out of the country with it.

Japan just made it completely legal. There is a lot of volume coming from Japan over the last few months.

C. Austin Fitts: When you say that Japan makes it legal, then it is legal to own and transact bitcoins in Japan?

Sarah Wiesner: Yes.

C. Austin Fitts: Wow! I hadn't realized that.

Let's suppose that I have listened to this, and I say, "I really want to learn more about bitcoin." Where would I go to get myself educated?

Sarah Wiesner: A site that I look where you can learn about bitcoin is called '99 Bitcoins'. That is a blog, and there are explanations and guidelines on it. They also have a bitcoin video course that you can take for free and that is a nice source.

If you want to stay updated about bitcoin, there is a talented Austrian economist on Twitter called Tuur Demeester. He publishes articles for Twitter, and he has his finger on what is happening and he is a very good source for news.

The bitcoin news sites have the same problem that all media has – many of them have a lot of paid content. If you want to see what is going on in the bitcoin world, another good source is the Bitcoin Reddit. That is just www.Reddit.com/r/Bitcoin. So any exciting news would pop up at the top there.

An exceptionally interesting source for learning a deeper background and theory about bitcoin is Nick Szabo's blog. He's considered one of the fathers of the bitcoin, and he has very, very interesting articles on his blog.

C. Austin Fitts: What about Sarah? I want to mention that you also write very well. So how do we keep up with you at the Bitcoin Embassy in Tel Aviv – especially if you have the conference in Israel? There everybody can meet you, right?

Sarah Wiesner: The Bitcoin Embassy is open for visitors. I have a Twitter account, also; it's @CSarahWiesner. The Bitcoin Embassy site is www.BitEmbassy.org.

C. Austin Fitts: Are you tweeting regularly? Do you ever put up articles about bitcoin?

Sarah Wiesner: No, but I might in the future. Anyone who wants to ask me any questions are very welcome to contact me on Twitter.

C. Austin Fitts: Obviously the way to get to know and learn bitcoin is just to buy some and try it. There is nothing like diving in and doing it. So let's assume I've never bought bitcoin and I don't know how to do it. How do I do it? What do I do? How do I figure out how to buy my first bitcoin?

Sarah Wiesner: First of all, you download the app to your phone. Then I would look up bitcoin ATMs in my area. Then you buy a small sum of bitcoins at the ATM, if you're lucky enough to have a bitcoin center in your area. People there are very happy to help you. Bitcoin Meetups are also a good place to go if you have them in your area.

C. Austin Fitts: If I don't want to keep the bitcoin on my phone or my computer but want to keep it in a wallet, where do I get a wallet?

Sarah Wiesner: A hardware wallet? The most trusted one is called the TREZOR. I think it's an American company that has internet sites. You buy their wallets online.

There are also bitcoin debit cards. There are a couple of debit cards that you can charge with bitcoins.

C. Austin Fitts: Right, and you can travel the world with your bitcoin debit card.

How substantial is the expansion of dealers online who will take bitcoin for the normal consumer goods I buy online?

Sarah Wiesner: There are a couple of big sites that accept it – Expedia and Overstock.

C. Austin Fitts: Overstock takes bitcoin? Fabulous!

Sarah Wiesner: With Expedia you can get hotels and airplane tickets with it. Dell Computers also accepts bitcoin.

There are many nonprofit organizations that accept donations of bitcoin and there are directories of sites that accept it. It's becoming more popular, and we're seeing different alternative sites that are accepting it.

C. Austin Fitts: Is there anybody in the group working on innovation and growth efforts to get any big websites like Bookings or Priceline to take bitcoin?

Sarah Wiesner: There was more of an effort a few years ago, and then people realized that it's not really close enough to mainstream for it to be worth their while for the stores to do it. So it's mostly for online services.

A lot of firms like servers and shipping companies use it. When you buy a nice vase and it ships to Israel, many those types of services accept bitcoin.

C. Austin Fitts: It's interesting and very exciting from your point of view because you're experiencing the buildout of the infrastructure of a new market.

Sarah Wiesner: Yes, and it's fascinating!

C. Austin Fitts: It doesn't happen every decade that this occurs. This is a very significant and big buildout, and you're watching what it takes to build the infrastructure to create real deep liquidity in something that is both an investment vehicle and a currency vehicle. So it's quite an education you're getting.

Sarah Wiesner: It's fascinating because something crazy happens every week and it's always surprising. It's really very interesting to watch what is happening in the world.

I forgot to mention that WikiLeaks accepts bitcoin, so when their accounts get blocked, they pick bitcoin.

C. Austin Fitts: I think that bitcoin helped them tremendously when PayPal did them dirty.

Sarah Wiesner: There is also a lot of crowdfunding being done through bitcoin. It's so easy to do it and it's not regulated yet. I don't know if it's impossible to regulate, but people with currency projects just say, "Send me your bitcoins and later I'll send you the new coins or the new project."

It to, some extent, passes the VC (Venture Capital) route where people send it straight through the internet.

C. Austin Fitts: That is fabulous.

Sarah Wiesner: It's also very dangerous because there are a lot of scammy things being done for it. You really need to watch out.

C. Austin Fitts: That's the way it is throughout the markets now, Sarah.

Sarah Wiesner: I was thinking about that. It's clear because it's a smaller world with the amount of scams and greed, but I realized that I understand why this is a scam. I don't understand why some other financial concoctions in the old financial markets are.

C. Austin Fitts: Did you listen to the interview that we did with Helen Chaitman about JP Morgan?

Sarah Wiesner: Yes, I did.

C. Austin Fitts: If you listen to the details of, essentially what JP Morgan Chase did with the Madoff fraud, what you realize is that at some point you would rather take your chances in the Wild West of bitcoin than trust JP Morgan Chase.

Sarah Wiesner: I know and I trust it more for sure.

C. Austin Fitts: I think that there is a very compelling case for why – whether it's debasement or whether it's the fraud – people are very eager to move away from the traditional systems; even the problems of the Wild West sometimes don't seem as bad as the problems in the traditional system.

Part of my feeling is that I want to get away from them and I'll do anything to get away from them. So, to a certain extent, I will take my chances in the Wild West rather than trust the system one more time.

This has been an absolutely fascinating discussion. I know that you've been spending plenty of time learning about the economy and what is going on in the world and integrating that with bitcoin. Could we have a few more minutes with you?

You've been on The Solari Report for a couple of years now. What have you learned about the general economy – whether on The Solari Report or elsewhere – and how does it integrate with what you're learning on bitcoin? Do you have any thoughts on that?

Sarah Wiesner: Wow!

C. Austin Fitts: I wouldn't normally hit you with that one, but I know that you are very smart.

Sarah Wiesner: First of all, I see how much people are hungry for making money. People are looking for a way to get a stake in the systems and make a couple of bucks. Also, I'm seeing the power of the economy pushing things forward into reality.

I think the bitcoin makes us understand how arbitrary and, maybe fake, the financial system is and how bazaar and imaginary money is. In bitcoin, it's true that it's not worth anything, but it's worth money only because people are willing to give you something for it. That's the only thing that gives money value and that's a fascinating thing to understand.

Also, because bitcoin is something logical that makes sense, it gives you a perspective on how bazaar the world has become.

C. Austin Fitts: Touché.

Sarah Wiesner: Another strange thing about bitcoin is that it's a database and a network, but now that it exists, in some ways people are almost enslaved to it. It's like an organism in a way, and if you're pessimistic you can see this as part of, to some extent, the kind of transhumanistic movement we're having as humans when computers are becoming such an important part of our life. They can look at it as uncontrollable computer money and it's really crazy.

C. Austin Fitts: I will say this: I love markets, and one of the challenges right now is watching the central banks and sovereign governments so manipulate and intervene in markets that they are no longer markets. So we have a traditional society that is trying to run everything by micromanaged rules, and it's actually killing the beauty and the power of what happens with shared intelligence that operates through market prices. Not to say that bitcoin is free of any of those influences, but the bitcoin market is still behaving like a market. It's certainly behaving much more like a market than the traditional financial markets.

The human race wants to be free, and they want to be able to transact and communicate. Anything that feels and looks and walks and talks like a market is very attractive now. $25 billion is a tiny flow compared to the global financial markets, but I think people who understand the power of markets and the power of people and are free to communicate and function in a market economy, that is part of the attraction that we're having here.

If you consider my subscribers who are attracted to bitcoin, they are people who appreciate the power of a market. They don't see that in the financial markets anymore; they just see interventions.

I think that part of the fun is when you call it the Wild West; that is what markets are. They are Wild Wests. They are crazy, they are organic, but they work because people are free to come and go and buy and sell as they wish.

Sarah Wiesner: Right, especially in bitcoin where a 12-year-old can trade the markets.

C. Austin Fitts: Touché.

Sarah Wiesner: A UFO can also hook up to bitcoin, and no one will be any wiser.

C. Austin Fitts: Sarah, it's been an absolute delight to talk with you. Thank you very much for briefing us on Bitcoin 101. I'm hoping that your regular message of great intelligence will keep coming in.

If they have the conference in Israel, when will it be?

Sarah Wiesner: It would be in the fall or early winter but there is not a date set.

C. Austin Fitts: So it would be fall of 2017?

Sarah Wiesner: Yes. That would be all the programmer brains coming together.

C. Austin Fitts: That will be exciting. I hope for your sake and the Tel Aviv Bitcoin Embassy that it indeed is in Israel. It would be in Tel Aviv?

Sarah Wiesner: We think so.

C. Austin Fitts: Is there anything else you wish to say in closing?

Sarah Wiesner: I hope I was helpful.

C. Austin Fitts: It was very helpful. Every time I talk with you I understand bitcoin a little better. I think that this has been very helpful, and I think for people who want to learn more, these sources are very helpful.

Ultimately, if you want to understand bitcoin, the way to do it is do a transaction. Get a wallet and try it. That is the way that you really understand something is just dive into it.

Sarah Wiesner: I'll put on my Twitter a few more useful links. Thank you so much for having me on and it's a privilege to be on The Solari Report.

C. Austin Fitts: Just remember that we are inventing the future together, and we need markets to do it. I'm convinced that bitcoin is going to be one of the markets – as frustrated as I get with my wonderful subscribers who think that it solves everything.

Sarah, you have a wonderful day and thank you.

Sarah Wiesner: You, also, and it was really great talking to you.

MODIFICATION

Transcripts are not always verbatim. Modifications are sometimes made to improve clarity, usefulness and readability, while staying true to the original intent.

DISCLAIMER

Nothing on The Solari Report should be taken as individual investment advice. Anyone seeking investment advice for his or her personal financial situation is advised to seek out a qualified advisor or advisors and provide as much information as possible to the advisor in order that such advisor can take into account all relevant circumstances, objectives, and risks before rendering an opinion as to the appropriate investment strategy.