

URL: https://ecorner.stanford.edu/?post_type=video&p=62945

Opportunities in the cryptocurrency sector extend well beyond simply investing in Bitcoin or Ethereum, says Coinbase CTO Balaji Srinivasan. He compares the digital currency landscape to the early days of mobile—a space poised to create an entirely new set of innovations and business models. For entrepreneurs looking to make a play in everything from social networking and banking to collectibles markets and real estate, he suggests, crypto's underlying blockchain technology is worth investigating.



Transcript

- [Narrator] Who you are defines how you build.. - Alright, why do we think blockchain is the most important technology in this decade? Tom gave my bio, I won't belabor it but basically, currently CTO of Coinbase.. Prior to that sold a company to Coinbase, Earn.. Prior to that General Partner at Andreessen Horowitz, you may be familiar with the firm.. I also sold a company for about \$375 million, it's a genomics company literally it came out of Bio-X just down the street over there, with my brother and a bunch of our friends.. I'm basically just a Stanford guy through and through, so I kind of know your pain.. So that's me.. But enough about me, let's talk about Bitcoin and launching.. I like this particular image because I think it motivates.. This is a screencap of Wireshark and you can see the Bitcoin protocol literally as a protocol on screen..

What's amazing about this is you can see that payments have been turned into packets.. This is a transmission, this is a Bitcoin block.. You can see the bytes over here and what's remarkable about this is what's absent.. There's no HSBC, there's no Wells Fargo.. There's no countries.. There's no licenses or anything like that.. What we have done is literally digitize the transmission of value.. And if you think about how big a deal it was to digitize books, and music, and movies, and newspapers, and so on and so forth, the underlying technology behind blockchain allows us to digitize now cash, stocks, bonds, mortgages, loans, derivatives, and all kinds of new things, financial instruments that you haven't even maybe thought of yet.. This is the motivating thing, once we've got something into the realm of computer science well all you folks can go to town.. This is going to be a lot of fun over the next ten years..

Alright, I'm going to give basically ten things about blockchain, ten things about Coinbase and go through a FAQ and certainly answer all of your questions.. Just about blockchain I want to review Bitcoin, blockchain, and Ethereum and then talk about Coinbase a little bit and do a Q&A.. First just for those folks, just to level set 'cause I know there's varying backgrounds, I want to give the very very very basics.. In particular, this slide over here is if you only remember one slide and you don't want to remember anything else this is the motivation behind why even invent Bitcoin in the first place.. With physical cash, if I have a dollar bill and I hand Tom that dollar bill, there's an implicit property to the dollar bill which is when A hands that dollar bill to B, A no longer has it and B has it.. I had it then now Tom has it.. And anybody whose observing that can see that that physical bill was handed over.. If I tried to naively transplant that to the digital realm, if I take the Federal Reserve serial numbers on that dollar bill and I just go and email them to Tom, well I still have a copy of those serial numbers and I can go and email them to somebody else.. And that is the fundamental issue with a naive representation of digital cash.. It is the double spend problem..

I could have spent those serial numbers with Tom and then with somebody else and somebody else and so simply using serial numbers alone that's not sufficient for risk scarcity in the digital realm.. Until the invention of Bitcoin, the way that we represented digital cash was with a bank.. A centralized actor that we trust in the middle and this actor over here is where the scarcity enters the system.. When A sends money to B digitally, C is trusted to debit A and to credit B.. This is where the scarcity enters the equation.. The thing about this is you're putting a lot of trust in C.. They can debit and credit anybody.. They can choose not to debit or credit.. They can not allow a transaction to go through.. In extremis as in 2008 they can print billions of dollars for themselves..

This is something which is inelegant from a computer science perspective to have a trusted central node, if you can avoid

it.. What Satoshi Nakamoto did is he came up with D the decentralized digital cash.. Essentially this central actor, this bank, was replaced with a network of miners and any one of those miners could approve that transaction, that debit or credit between A and B.. Since any one of them could approve it one of them disapproving it all it would do is just be giving up some Bitcoin that they would have mined otherwise.. Basic way to combined a transaction approval and in seigniorage currency printing in the same unit.. The details of this aren't super important, like technically at least for a talk like this but the concept is important.. Which is we took physical cash, we tired to naively turn it digital cash.. That didn't work so we had the centralized actors and Bitcoin dispenses with those centralized actors by having anybody in theory who can connect to the Internet with sufficient computation power can now approve transactions and push them through.. The cool thing about Bitcoin is once people understood this once people understood what a breakthrough it was they said oh well this data structure that these miners are updating that blockchain that fundamental innovation behind Bitcoin that's essentially a tamper resistant database for storing arbitrary things of value.. You can use it for storing cash, and you can use it for storing stocks and bonds, and so on an so forth..

But Bitcoin itself wasn't that easy to work with.. It wasn't built for programming, or it was actually but Satoshi turned off a lot of the more sophisticated opcodes early on just to keep it simple and attack proof.. What happened was more recently a new blockchain was launched in 2014 called Ethereum about five years after the launch of Bitcoin.. And to understand the improvement that Ethereum gives here's an example of a scripted Bitcoin which is kind of almost like an assembly language, which is like a stack-based language.. Here's what Ethereum's solidity looks like which is a little more like English or JavaScript or what have you.. This programmability led to a huge new surge in crypto activity and in 2017 this massive ICO Boom.. This went up from under 10s of billions of dollars to many 100s of billions of dollars and then down to 100 billion dollars.. But the thing about this is even though the ICOs came up and they went down you would think of it today it's the winter for price but the summer for innovation.. A lot of this stuff that kind of got started back then is starting to work.. For example you've got decentralized prediction markets and decentralized loans, and decentralized derivatives..

That stuff is all starting to work.. The winter for price, the summer for innovation.. One thing that I see as themselves by the way is they represent in my view the simultaneous disruption of venture capitals, SWIFT, crowdfunding, and cap tables.. I'll come back to that point but essentially you can invest in something internationally with a group at the same time and have all of the property rights recorded in the blockchain so anybody can see.. That's like such a big deal and so many innovations at once that people can sometimes lose the forest from the trees 'cause they say oh what are you funding? You're funding all of this crazy stuff but if you just look at it as an innovation in crowdfunding, or in VC, or SWIFT, or cap tables, it's actually a pretty big deal.. This brings us to the present day.. It was Bitcoin, then the blockchain, then Ethereum, ICO boom, and now the present day.. Crypto winter, winter for price, summer for innovation.. The way to think about the blockchain as a technology is it improves fundamental financial primitives.. One way to think about this is a blockchain as I mentioned is a database for storing things of value and it started with cryptocurrency which is like digital gold..

More recently we've had these so called ERC-20s, these tokens which represent like equities but you can also use it for other stuff.. You can use it for non-fungible assets and it's very technical sounding in-game items, like swords, and potions, baseball cards, collectibles or even eventually pieces of real estate.. You can use it for representing identity and frankly you can use it for representing almost anything scarce.. Anything scarce you can think of you can represent in a blockchain.. And you might say, well why use a blockchain for things that are scarce? Once you've got a database that represents all the money in the world, the first thing someone's gonna try to do is write themselves a million dollars.. You have to actually say well first I want that to be tamper resistant, second I don't want one party to be able to write themselves a million dollars.. I want it to be decentralized so that the power is split.. No one person can write themselves a million dollars.. It might need more than a million dollars to write themselves a million dollars.. And once you start thinking of those kinds of constraints like a database that represents things of value you start to be led to the kinds of properties that blockchains have..

And once of course you can solve the problem of preventing someone from writing themselves a million dollars, you can stop them from writing themselves a million potions, or a million acres, or a million of anything else.. As I mentioned before Bitcoin turned all this stuff into packets.. There are literally protocols Bitcoin, Ethereum in these things that you can open up Wireshark and see the raw packets that update the underlying blockchains.. It's actually completely amazing when you think about that.. Anybody who's on the Internet can send and receive cryptocurrency back and forth, just send packets back and forth.. One consequence of this is people talk about the unbanked it's an important problem that I think crypto can solve in the longterm.. There's another group of unbanked which are machines.. We give machines telephone numbers in the form of IP addresses.. It used to be that you had to have a human who is associated with a telephone number.. When you give a machine an IP address the machine could then autonomously communicate back and forth..

You do that all the time whenever you've written a bot that goes and interacts with Twitter or scraper like that spider's web and connects to other computers autonomously.. Autonomous machine communication was a really big deal.. We believe that autonomous machine transaction where machines can hold and send money on your behalf will likewise be a very very big deal.. Here's just a simple GitHub gist that string over there represents money.. If you can now transmit a string, you can transmit an arbitrary amount of value which is pretty awesome.. A lot of the stuff in the late 90s that people talked about when they talk about intelligent agents or bidding entities and so on that's all actually starting to happen.. The primary context in which it's happening are things like exchanges, especially decentralized exchanges.. You can go and write a program on your laptop that will literally make you money as you sleep by arbitraging these decentralized exchanges.. I think

over time in like the 10, 20, 30 year timeframe every price on the Internet, every Amazon.com product will have a cryptocurrency interface.. If you have some arbitrage strategy for wool versus fleece sweaters or whatever you can actually arbitrage anything 'cause everything will be priced in crypto..

That's I think where the arbitrage stuff goes in the medium to longterm.. Okay, fourth point.. People talk a lot about the potential of blockchain and I do think it has a lot of potential but it's actually something where in some ways it's over-hyped and in some ways it's actually under-hyped.. That's to say there are fundamental financial primitives that the blockchain has already delivered and like had 10x improvement on.. I mean a quantifiable 10x.. The easy one, the obvious one is gold.. Bitcoin is infinitely lighter than gold.. It's faster to transfer internationally, it's cheaper to custody.. And to give a concrete example of this when the German Bundesbank tried to repatriate a bunch of gold from New York it took them years it cost them millions of dollars to bring back billions of dollars in gold.. While that might be an infrequent operation it's an extremely important and valuable operation that frankly underpins a big chunk of the world's economy..

If you've improved on that, that's a big deal.. Gold is a 2 trillion dollar industry.. If that was the only thing that blockchain ended up doing, that'd be a pretty big deal.. But it's more than that.. Tom's going to buy some Bitcoin now.. - [Audience] (laughs) - It's more than that.. With Ethereum and other kinds of cryptocurrencies that represents the 10x improvement over SWIFT.. SWIFT if anybody sent a wire internationally that takes days to clear typically, whereas with Ethereum I can be on the phone with somebody and just like I can wait for that email to hit I can wait to just see it in the blockchain and I can say oh that transaction's done, boom.. I can now I can get the deal closed.. The speed difference here is the difference between a physical mail sending a letter which takes two to three days versus an email which takes minutes..

Think about how big a difference that made, right? When you went from physical mail to email just the metabolism of business changed.. When you go from two to three days for international commerce to minutes the metabolism of international business changes.. Third point, crowdfunding.. In 2015 if you go to Wikipedia and you look at the list of the largest crowd funders you will see that it's like maybe 10 million, 15 million dollars.. By 2017, 2018 a large crowd funder was four billion dollars.. That's like a 400x improvement in about two to three years and that's more than the 10x that's like 400x.. Now you might argue, well what are those things funding? They're all funding ICOs and crypto stuff it's all this uroborus.. It's actually something where you could fund a building.. You could fund pretty much anything.. Now that folks are accustomed to using crypto to do this kind of thing it's a powerful new innovation in crowdfunding..

I can go on and on and I'll probably write an article on this.. Just a few more examples, Delaware Incorporation.. In many studies, the World Bank has this study called Doing Business.. And in this study they actually say hey, how long does it take you to incorporate in your country? Does it take you weeks, or months, or does it take you days? And if it takes you days well you're a great country for business, great country for startups.. Ethereum's shattered that, destroyed that because it's not days anymore, it's minutes.. You could literally get a smart contract into the blockchain in minutes.. That's amazing, that works internationally.. You're not incorporating in Delaware, you're incorporating on the blockchain.. It might seem like an apposite comparison today but lots and lots of stuff, all these VC terms, all of these bits of Delaware law are currently as we speak being encoded into smart contracts so that incorporation on the blockchain will become probably the default in I don't know 10 or 15 years.. There's more, like the time to set up bank accounts, the time to audit..

In 2013 people talked about Bitcoin as a scam but today the big four when they've audited a blockchain firm they used the blockchain as the source of ground truth that they check all of your transactions against.. From a scam to the gold standard in like five years.. The point here is we're 10xing all these financial primitives like basic basic fundamental things and how we move money, how we think about money and that's going to have consequences, good consequences hopefully.. Literally not only have blockchains 10xed lots of things they've already created many billion dollar entities.. Three that have risen in particular, the folks who founded new coins, the miners who run these gigantic server farms, and the exchanges.. Each of these three groups has created and captured billions of dollars in total revenue.. It's comparable sort of to the 90s Internet when it was kind of the infrastructure stage and search engines and Akamai and AOL and so on were getting built out at that time.. Sixth.. Now people talk about blockchains as being trustless and Bitcoin as about no trust.. I think a much better way of thinking about it is that they give you a choice of who to trust..

Before you just had to trust a bank.. You had to store your money at a bank.. You can't just go and withdrawal a million dollars from the bank or you could but you'd be on a lot of lists.. Today what you can do is you can certainly still store it at a bank should you so desire you can store it with a company like Coinbase or and this is very new you can store it on your computer you can store it on a USB key.. You can store it in the cloud you can basically self-custody an arbitrary amount of money.. And that's a major innovation because you can't carry a bunch of gold bricks around with you.. You might be able to carry around suitcases full of cash but it's a little bit conspicuous.. And now you can carry an arbitrary amount of money so that's a very new thing you don't have to trust a bank if you don't want to.. And places like Venezuela this is actually truly a killer app.. Number seven..

I hinted at this before but just to drill into this point, one can argue that the single most important data structure in Silicon Valley is the cap table.. Namely the very simple table that shows which people or entities own what shares of the company.. Your common stock, your series seed A, B, et cetera.. That data structure, that little table, that Excel spreadsheet maintained thing is what has aligned people from every country around the globe to build Silicon Valley.. The scale of which it's aligned

them is 10s, 100s, sometimes 1,000s of people pre-IPO and then you build this huge company and then everybody hopefully does well together.. The state of the art for managing the most important data structure in Silicon Valley is an Excel spreadsheet or a Google Sheet.. Which is kind of amazing.. Now what we've got with the blockchain is you can 10, or 100, or 1000x that number of people.. Something like BAT for example is 54,000 addresses that hold BAT and you can see exactly who owns what when and this is fully programmatic.. One way I think about it is if aligning a few hundred people at a time built Silicon Valley what does aligning a few hundred thousand people at a time or a few million people at a time what can that build? You can now align human beings and incentivize them like never before..

That's a really a big deal.. Number eight.. One way to think about this is some of you will be like I got to Stanford too late I missed mobile, you know it's over.. No, it's not over, it's just beginning.. One thing we think of as blockchain first or crypto first is like the new mobile first.. It provides a weapon with which to go and attack and open many industries or areas that were either closed to competition or seemingly impregnable or not even thought of as the kind of thing you can innovate on.. I already mentioned international wires, and precious metals and messaging and I'll talk about the social bit in a little bit more.. There's also other areas that you normally wouldn't think of as things you can even innovate on.. For example DNS.. With crypto you can innovate on DNS..

You can innovate at the protocol level with things like Blockstack, or ENS, or Handshake where you can register domain names these are also scarce entities you can register them in a blockchain and you can route things through them.. You can have incentivized versions of BitTorrent, incentivized versions of SMTP, all these protocols that you previously thought of as kind of non-monetizable are now potentially improvable and monetizable.. There's also commons like Wikipedia, open source projects where you can now take a fresh gloss to them and think okay how could I maybe tokenize this, how can I make this even better? There's so many different crypto first companies that are kind of swarming in and attacking these different verticals that I couldn't even enumerate all of them.. This gives you some of the flavor of them.. Coinbase Ventures alone has made like 40 investments over the course of the last year.. Ninth point.. Blockchains break network effects and to give a completely new tool a can opener for going after skilled social networks and two-sided marketplaces.. One way of thinking about this is if you think about Metcalfe's Law you think about network utility.. Typically the larger the network, the higher the value to the user.. So Facebook you have 2 billion people supposedly in a runaway advantage you can't displace them..

But there's something really interesting about crypto which is that if you have a token whose value is associated with the startup the tokens upside is maximal when the size of the network is smallest.. For example an early investor in Snapchat had more upside than somebody who invested in the series D round where it already had 10 million plus users.. Upside is itself valuable and now you've got a second term in the equation which can balance out that first term.. Some kind of hypothetical future value that for the first time you can programmatically issue to your users for sign up and other kinds of actions that they take within your app.. Imagine if Facebook had something where the folks who signed up for it the first 100,000 or 200,000 or million users or end users received some slice of Facebook's equity for doing that.. Well, that would be a very big deal.. You could actually start making money by signing up for all these dumb social apps.. That's actually something which I think is a very powerful tool for going after scaled social networks, two sided marketplaces, and things like that.. Split some of the upside with the user.. Tenth..

Blockchains, I believe, are going to transform social networks.. The last ten years people have been liking, and poking, and messaging each other wasting time.. The next ten years we're done making friends it's time to start making money.. Basically those edges we think are going to now have money on them, cryptocurrency.. And you're going to have new kinds of social networks.. What are we going to call them? Maybe digital economies or crypto economies.. The fundamental difference being that your time with them is not wasted your time with them is actually like a form of work where you're actually remunerated for it.. Some of these maybe existing social networks might be able to retrofit but I think you're going to have to construct wholly new social networks that are based on these kind of behaviors from the beginning where earning is part of the equation.. Finally, just on talk of blockchain, blockchain is like a partial move away from the cloud and towards privacy.. An amazing stat from earlier this year is that Ledger sold it's millionth hardware wallet..

Actually this is earlier last year, early 2018.. I think of a hardware wallet as being a pretty arcane kind of thing but when a million of them have been sold you're probably eventually going to have a billion sold in some form or the other.. One possibility is hardware wallets like a phone charger are bundled with a phone so you get three devices, the phone, the phone charger, and the hardware wallet rather than two.. There's lots of different distribution models you can imagine but the fundamental concept is I think hardware models are going to become very popular and that's a move away from the cloud and towards privacy because the whole concept of the hardware wallet is you're not keeping your keys in the cloud you're keeping it locally.. One possible future model is something where you're data's on the cloud but it's encrypted with the private keys that you're using in your hardware wallet and so nobody can read it other than you and it's only de-encrypted and re-encrypted just in time.. I think things like homomorphic encryption and so on will make that possible.. Let me briefly just give ten things about Coinbase then I'll take some questions.. Doing well on time I think.. You can think of Coinbase itself as the IntraBase between fiat and crypto and you know we have both a retail and a professional interface.. And on the fiat side we're building a Wall Street 2.0, custody, and indexes, and commerce..

And on the crypto side we're doing blockchain first apps like Earn, and Coinbase Wallet and we work closely with regulators.. Our goal is to remain the safe, legal, and trusted part of crypto.. And you get all of these licenses and so on,

money transfer license all that stuff.. Our mission is basically to create a more open financial system for the world and what that means is kind of two different groups of users that would benefit from that.. The first group are developers, investors, power users of money who are trying to move money around in different kinds of way, do fancy things with money.. The second group are the marginalized, the folks who are unbanked, the folks who do not have bank accounts.. Both of these folks in different ways are pushing on the financial system to make it more open and those are our folks.. What does that mean? By the way what does a more open financial system mean? It does mean upside, it sometimes means downside.. Upside is that you can raise 35 million dollars in 30 seconds or disrupt remittances.. The downside is there's new kinds of hacks and new kinds of scams and so on but I do believe in the medium term will mitigate the downsides with things like multi-saver or what have you..

At Coinbase we're kind of thinking of ourselves as bridging from the investment phase to the utility phase.. Which is to say that crypto has sort of the opposite emergence model of social media.. Social media piled up the users first and then had to prove out monetization and crypto proved that monetization first in almost the most literal sense and now needs to prove out utility.. We're seeing that happen, I can go into lots of different things with earned and decentralized finance and we think that's a big part of the next five years or so.. Coinbase was actually named after where the blockchain starts so the so-called coin based transaction is where the new crypto is created in Bitcoin and that why we think it's also where the blockchain starts for users.. Windows you started using it with the Start button or Google Search is where you started browsing the Internet log onto Facebook how you started using social media.. Coinbase is where you start using crypto.. We think of ourselves as kind of this on-ramp this Start button for crypto.. We've been making headlines, you can read more about us online.. That's about it and I'll be happy to take questions..

- [Audience] (applause) - Yes.. - [Speaker 1] You mentioned about blockchain breaking a network, so I was just wondering from an investments perspective, do you think that would encourage more short-term behaviors because surely all the benefits are currently front-loaded as opposed to the longer game and so on.. - [Speaker 2] Can you repeat the question? - Sure, absolutely.. Her question is does this kind of model encourage short term behavior among users? And I'd say maybe but they'll only really realize this value if the network is scaled.. That is to say it has theoretical future value you might be able to flip to somebody but you're not going to get 10,000x unless the thing is scaled.. And so while it's true that liquidity does present some short-term issues I think on net it does align people toward longer term things.. - [Speaker 3] How is Coinbase handling the emerging proof-of-stake systems? - So question is how is Coinbase handling the emerging proof-of-stake systems? We are close to looking at everything I can't talk about any specific assets we're adding.. We did publish a blog post in December talking about specific assets we were looking at and that included several coins that implement proof-of-stake in different ways.. - [Speaker 4] Could you provide a more sort of fulsome picture of what the downside scenarios for crypto looks like? You've been generally positive in your presentation but obviously there's another side to your craft and could you add what that might look like.. What, who would be the cause of death? - Excellent questions, what are the risk scenarios what are the downside cases for crypto? I'd give a few..

I think it's gotten pretty far.. As of 2019 crypto has sort of withstood the crackdown of the Chinese government in 2017, it's withstood enormous numbers of articles proclaiming Bitcoin dead and so on.. And tons of bubbles and whatnot.. Insofar as I think there's future risk to put them in a few buckets.. First is partition tolerance.. At least right now the Bitcoin blockchain is not built to handle extended partitions so if for example the Great Fire Wall goes and blocks port 8333 and then there's a back and forth and eventually it becomes difficult for the blockchain to synchronize across borders then you could have a peekaboo problem where the chain is extended in China by mining but most transactions are happening the rest of the world and synchronization is not happening fast enough.. Now there's workarounds for this like there's a satellite which is pumping the blocks from Bitcoin into China because of China's control over airspace but not space space.. There's other workarounds where you could steganographically encode packets and bring them into China but we'd have to actually run the experiment to see if it was possible for the Great Firewall to actually intranight it.. Now that firewall would have to be so tight that it would have to intranight not just the service but any one megabyte transfer in all of China of course billions of people so that'd be hard but possible.. Let's call that one approach, the partition tolerance..

The second is if there's some CVE, like really critical vulnerability that we have not seen that allows people to counterfeit large numbers of Bitcoins and break the value of the system.. By the way, the reason I keep focusing on Bitcoin here is it is sort of like the fundament of the system.. If it was hacked if there were serious security issues I think it would set back the industry like at least five years or so if people would have to rebuild around it.. With all of that said though I think those kinds of issues that I just mentioned are technological issues where it could set the thing back but I think the fundamental constant of blockchain as a decentralized currency is out there and then folks what they'll do is they'll fix that and then have a more robust version in the future.. That's kind of where I'm at and open to other thoughts.. - [Speaker 5] You talked a little about banks serving as a trusted source for recordkeeping but the other main role banks have is a monetary policy that's why we have Federal Reserve banks and so I can see how Bitcoin does the recordkeeping function of banks but I'm not seeing anything replacing the monetary policy function and if economists have learned one thing in the last 200 years it's that that's really critical to an economy's wellbeing.. How are you envisioning Bitcoin functioning as a currency without a monetary policy? - Great questions, so the question is if I can paraphrase, how does Bitcoin interact monetary policy how can it function as a currency without a monetary policy? What I think is we are engaged in a grand experiment which is what I think of as empirical macroeconomics.. Basically, and I'm sure I'm going to offend some macroeconomists in the audience.. I think that microeconomics is pretty empirical in the sense of you've got the theory of the firm and venture capitalists are running

lots of experiments all the time and you have a thesis on how a company should be organized or not and if you're wrong you lose money..

With macroeconomics because it involves assemblages of very large numbers of people it's hard to do a reproducible experiments until relatively recently.. I actually have these supplemental slides.. I've got every question, okay.. Blockchain's a big macroeconomics experimental sciences so virtual economies have been a topic of discussion for about 15 years where this guy Edward Castronova a smart guy, a professor, has been looking at this in the context of World of Warcraft and things like that.. And in those kind of economies you print money, EVE Online, you see what the effect is on prices and so on and it's pretty cool where you can run experiments with a system of people who are actually trying and responding to incentives.. What I think is going to happen is that type of work is going to linkup with crypto economies and we're going to start to get a lot of real life empirical economic data on what life is like without a central monetary policy in this opt-in kind of system.. One of the really good things about this is it's like a bonanza for econometrics people.. There was this vague concept of six degrees of separation in the late 90s then we got this digital data structure of the social network.. So there was a vague concept of six degrees of separation and then you've got something that was digital and computable you could think of it as a graph and so on.. In the same way we have this sort of vague concept of the economy and now we've got a blockchain which is the record of every single transaction that's ever happened down to the penny back to $t=0$..

Every economic theory that one has about transactions, or price support can be tested and importantly one can also develop blockchains that have inflationary policies that are connected to central banks and so on.. I think what we're going to see is just a ton of different kinds of economic experiments some inflationary, some deflationary, some demurrage, some weird kinds of combinations that resist political classification.. I think we're gonna run the experiment and see what happens.. Yes.. - [Speaker 6] You mentioned a Coinbase acting in Venezuela and there's somewhat of a controversial bank.. Could you (muffled speaking) and how emerging economies are distressed economies? - Yeah, sure.. I think you asked, what did Coinbase do in Venezuela and so on.. I think we've announced this but we basically gave away money to folks on the ground in Venezuela.. There's a lot of theories on international aid but one theory is just give the money to people directly.. Now they've got phones you don't necessarily need intermediaries..

People are often good judges of what to do with money and now you can actually, via the fact that all these people have Smartphones, just give them money directly.. We have this site GiveCrypto.org which is funded by Brian our CEO and co-founder and a bunch of other folks.. We're trying this experiment to see can we get the money to Venezuelans? Is Bitcoin something they can use or borrow against? Is it considered currency-like in that environment? And if so then what are the consequences? And if that works well then maybe we can scale it up.. So that's what we're doing there.. Sir.. - [Speaker 7] On the environmental impact on currencies.. So I've read that (muffled speaking) \$1,000 Bitcoin what that means physically is that somewhere in China \$500 will (muffled speaking) to a miner mining farm.. That doesn't seem sustainable if you want to expand and so what's the solution to that? - Yeah, so a couple of thoughts.. - [Speaker 8] Could you repeat the question, please? - Sure, of course, of course.. Yeah so what is the environmental impact of Bitcoin? Is it something where we're consuming tons of energy for it and so on? That's a complex issue but let me offer a few thoughts on that..

First is that a lot of Chinese mining is actually happening at night and the reason it's happening at night is you have hydroelectric plants, geothermal plants that are basically spinning a water wheel at night because power can't easily be stored in the grid.. What happens is power comes up which is usually maximal at 12 noon and then it kind of drops off at 4 a.m.. then it comes back up.. It's got this sort of sinusoidal cycle.. And at night that power is off and just wasted.. Now what's interesting is folks are using Bitcoin mining as almost a kind of battery.. Where what you do rather than just throwing away that excess power is you mine Bitcoin.. In theory what could happen and we're starting to see some of this is you can have markets where while you might not be able to store power in a normal battery you store it in the form of mined Bitcoin.. And then you can have aftermarkets where it kind of it trades and you might be able to balance the power grid better.. It may actually be something that leads to interesting innovations and a form of energy storage..

That's kind of one answer.. The second answer is if you think about what Bitcoin represents I don't think it's correct to compare it to let's say PayPal which some would say is so cheap.. PayPal you're just minusing and plusing things on a central server.. I compare Bitcoin more to like a system of property rights.. More analogous to let's say the miners are more analogous to the police and the military.. All these extremely expensive things that maintain American property rights.. If you think about the energetic cost of that it's actually very substantial.. This system of property rights which is developed in a different way you can measure the amount of energy that goes into it.. I think it's probably less than the police, the military, and the banking system and all the things that enforce all offline property rights but I think that's a second comparable that's interesting.. Sir, in the back..

- [Speaker 9] There's so many amazing use cases for blockchain, some of them you alluded to, some of them out there for banks and whatever what is stopping companies to adopt a more widespread scale today? Blockchain and also banks that are as (muffled speaking) Bitcoin and so on.. - Yeah, what's stopping companies from adopting on a widespread scale, what's holding blockchain back? In some sense the industry is actually already fairly large in the sense of you saw how many people here held a cryptocurrency.. The first killer app for cryptocurrency as gauche as it sounds is hold cryptocurrency as an investment and hope it goes up.. But that speculation phase was necessary and the reason we think of it as necessary is speculation was instillation.. That is to say before you have this decentralized finance environment with decentralized loans,

and derivatives, and so on people have to treat those packets moving back and forth as money.. The last 10 years what that did is you have an environment where 80% of Americans have heard of Bitcoin.. Everybody kind of knows it's valuable, they know a good chunk of Americans also know that Ethereum is valuable and so on.. Once they treat it as money then you can actually develop apps on top of that but you need to have that speculative phase to install it in people's heads.. Now why aren't businesses using it yet? I think what you're going to see is it's going to radiate out from the crypto sector.. That is to say that businesses within the crypto economy miners, exchanges, blockchain companies, new asset issuers, et cetera..

This is actually a large enough set right now where folks pay each other back and forth in Bitcoin and Ethereum.. The folks who are on the border of the crypto economy are folks like prop traders who are guys in Chicago who invest their own money or Fintech developers, Square has gotten into the game a bit, Robinhood's gotten into the game.. Those are the folks on the border who are like crossing the chasm.. They weren't founded on crypto but are starting to get into it.. That environment, those folks, they'll grow for the next three to five years then it will kind of go out one more set and so on.. I think it's going to be a gradual process but I think over time you start to get more businesses involved as we build it out.. Yes.. - [Speaker 10] Can you hear me alright? - Yes.. - [Speaker 10] Great.. We have a Stanford Journal of Blockchain Law and Policy at the law school which I'm (muffled speaking) that I read that..

I was curious what do you think would be some creative articles would you like to see covered in the legal or policy space that would kind of push further the (muffled speaking) this area.. - Great, so the question was articles on governance, policy, philosophy.. Well it so happens I have some supplementary slides on that.. - [Audience] (laughs) - So basically, let me give you one concept that I think is a very powerful one.. One concept I think a lot about is that a blockchain it's not just like a database.. It's a database with a community which is very different.. It's like a database plus a social network in some cases plus a protocol and a compiler.. Which is actually pretty complicated interplay.. A blockchain value derives from its community meaning you've got Bitcoin Maximalists, your Ethereum developers, like a million people are at these meetups now, you've got your XRP army, and so on and so forth.. The thing about this is just like within a country the Estonian's there's the butcher, the baker, the candlestick maker they all interact..

They have the Estonian kroon, or they used to before they had the Euro and then they can just use that within themselves and then has an exchange rate with the outside world.. That exchange rate is their API with the outside world.. They use their own currency within their own kind of country and then the exchange rate outside.. In the same way once you've got a critical mass of enough people online who just believe in something they can just transact amongst themselves in this crypto and value it.. Offline you may think you're crazy for valuing XYZ coin but you're happy to buy and sell XYZ for USD for them, maybe sell.. Blockchain's value derives from this community and one of the consequences of this is if you just take three random people they're not economically aligned.. Any one of them can lose or win together.. Or rather lose or win on their own.. But if they all hold the same cryptocurrency then they either all lose together or they all win together.. This is a way of economically aligning human beings..

When VCs talk about alignment this is the underlying data structure that underpins that.. The thing about this is you have this community-forming behavior online and that community-forming behavior leads to these tribes.. Overtime what it does I can talk about this bit also overtime it leads to is experiments in self-governance where once you've got a system of property rights in the blockchain you can start doing experiments with other kinds of things.. That's the type of I think you could cover.. Sir.. - [Speaker 11] We've heard a lot of cases where people just lose their private keys and then there's grossing Bitcoin that cannot be accessed anymore.. How with the Bitcoin number being capped is industry thinking about a solution to generate more liquidity? - The question is basically folks lose their Bitcoins and the Bitcoin number's capped and how does the industry think about that? Bitcoin is meant to be like cash, if you lose \$100 you can't message the U.S.. Government to give you another \$100.. It's a dollar bill down the drain.. That's what Bitcoin is kind of intended to be like..

In a sense it actually benefits slightly every other Bitcoin holder because it's like re-normalizing the cap table.. If you lose 1% of Bitcoin everybody else's is somewhat more valuable.. The solution for this, there's a few, one of them is store your crypto with somebody else if you don't want to handle it yourself and a lot of people do that.. That's certainly an option.. The second option is something like multisig where you have a few different folks who have keys to it.. There's yet other kinds of sophisticated password resets social reset schemes that make it harder to just lose your crypto by accident but it's something that's being worked on.. We'll do one more, yeah.. - [Speaker 2] One quick one.. - Yeah, okay great.. Hi, yep..

- [Speaker 12] You mentioned earlier that blockchain is hard to move away from cloud privacy.. When do you see a point where is the tipping point where it is a full move (muffled speaking)? - I think you need like hundreds of millions or billions of people to have crypto and you need homomorphic encryption and I think that's what starts to tip it but that's like at least 10 years out maybe 20.. - [Audience] (applause) (energetic electronic music)..