EPISODE 894

[INTRODUCTION]

[00:00:00] JM: Andreas Antonopoulos is the author of several books about cryptocurrency engineering, including mastering Bitcoin and mastering Ethereum. In these books, Andreas lays out the systems of economics and computer science that underpin the two most mature, decentralized monetary systems.

When Andrea's originally discovered the Bitcoin white paper, he had witnessed the repeated mismanagement of government-backed fiat currencies. Andreas has a Greek background and the financial collapse of 2008 had led to an economic crisis in Greece. Andreas' first-hand observation of the weaknesses of centrally planned government currencies, together with a degree in computer science and distributed systems have made him a dedicated evangelist for Bitcoin. Andreas joins the show to discuss the Bitcoin ecosystem and the relationship between decentralized crypto economic systems and centralized corporations.

Facebook has recently announced a cryptocurrency project called Libra, and Andreas suggests that Libra changes everything. Not necessarily because Libra will make it to production or because Libra itself will upend the world of finance, but because it allows us to further call into question the very nature of what makes a modern currency valuable and valid. After all, if a government has the right to back a currency, why shouldn't a large corporation have that same privilege?

Andreas is also a cohost of one of my favorite Bitcoin podcasts, Let's Talk Bitcoin. The cohost of that show, Adam Levine, has been a previous guest on this show, and if you are looking for more Andreas content, check out his podcasts.

[SPONSOR MESSAGE]

[00:01:51] JM: When I'm building a new product, G2i is the company that I call on to help me find a developer who can build the first version of my product. G2i is a hiring platform run by engineers that matches you with React, React Native, GraphQL and mobile engineers who you

can trust. Whether you are a new company building your first product, like me, or an established company that wants additional engineering help, G2i has the talent that you need to accomplish your goals.

Go to softwareengineeringdaily.com/g2i to learn more about what G2i has to offer. We've also done several shows with the people who run G2i, Gabe Greenberg, and the rest of his team. These are engineers who know about the React ecosystem, about the mobile ecosystem, about GraphQL, React Native. They know their stuff and they run a great organization.

In my personal experience, G2i has linked me up with experienced engineers that can fit my budget, and the G2i staff are friendly and easy to work with. They know how product development works. They can help you find the perfect engineer for your stack, and you can go to softwareengineeringdaily.com/g2i to learn more about G2i.

Thank you to G2i for being a great supporter of Software Engineering Daily both as listeners and also as people who have contributed code that have helped me out in my projects. So if you want to get some additional help for your engineering projects, go to softwareengineeringdaily.com/g2i.

[INTERVIEW CONTINUED]

[00:03:43] JM: Andreas Antonopoulos, welcome back to Software Engineering Daily.

[00:03:46] AA: Thank you so much for having me, Jeff. I really enjoyed our previous interview, looking forward to this one.

[00:03:50] JM: Awesome. Next year, Bitcoin will undergo a halving, where the block reward will decrease by half. Why do Bitcoin block rewards decrease over time?

[00:04:02] AA: Well, Bitcoin has a very unique monetary policy, which is part of its DNA if you like. It's part of the rules that were set in place when it was launched in 2009 and that are preserved by all of the participants in the Bitcoin ecosystem.

This monetary policy is intended to be deflational, to create digital scarcity. Meaning that Bitcoin is intended to be rare and finite, emulating in many ways the model of mining for gold, but an even more strict digital form of scarcity that doesn't exist in nature, where at some points, no matter how much people want more Bitcoin to be issued, it simply won't. So every four years, or actually every 210,000 Bitcoin blocks, the amount that is issued is divided in half.

[00:04:59] JM: How has this halving historically affected Bitcoin?

[00:05:05] AA: Well, interestingly enough, even though it happens suddenly. So in a single block, the reward suddenly goes from whatever was to half that. The market really anticipates this halving a long time in advance. So it's priced into the expectations. The effect of this halving is really from an economics perspective a supply and demand fact. If you think about it, it's almost like the Federal Reserve's monetary policy. Only you know exactly what's going to happen at any point in the future because it's built into an algorithm.

So just like the markets react to the Federal Reserve announcements about interest rates, the markets react to the halving, because effectively the issuance determines the interest rates on Bitcoin. So the difference of course is with the Federal Reserve, you don't know until they announce it, whereas with Bitcoin, you know well in advance.

Every time the halving has happened, it's had an impact on the market, basically a reduction in supply. If the demand remains the same, a reduction in supply causes the price to go up, because there's less Bitcoin available for the same amount of buyers. This particular halving is even more interesting, because with this halving, the issuance rates of Bitcoin will correspond to a 1.8% increase per year. So it's almost like the interest rate goes down to 1.8%.

Now, that is below the 2% target that central banks have as part of their mandate in most countries. So that means that the inflation rate, if you like, of Bitcoin will now be below pretty much every currency in the world.

[00:06:59] JM: Could you describe the difference between block reward and transaction fee?

[00:07:06] AA: Yes. So, essentially, the reward is made up of two parts, which we call the block subsidy and the transaction fees. The block subsidy is essentially new coins issued as part of the block reward, and the transaction fees are the sum of all of the fees, of all of the transactions, included in the block, and the fees are paid by the person initiating a transaction, and they act as a mechanism. A market pricing mechanism to determine the priority of each transaction for access to the blockchain, which is by definition a scarce resource. Meaning that there is a limited amount of space to fit transactions and somehow we need to decide which transactions are more important than others.

There's really only two ways to do that. One is to start to allow someone to make a decision as to whether a transaction is important or not by classifying transactions. The other way is to allow a marketplace to develop and essentially allow each person who issues a transaction to decide for themselves how important that transaction is to them and signal that choice using the price of a transaction fee.

So if I am in a hurry, if my transaction is important to me and I feel an urgency, I include a higher fee so that my transaction is more competitive, vis-à-vis all the other transactions, and gets included sooner. If I'm not in a hurry, I include a low fee and my transaction will be included eventually or maybe not if there's not enough capacity. That way, we use a market-based mechanism. So those transaction fees are collected by miners so that the miner who produces a block collects all of the fees for all of the transactions that are in that block.

[00:08:59] JM: Are there any ways in which the balance of transaction fees and block rewards could go haywire at some point in a sense that the transaction fees might end up getting so high that nobody would actually want to transact with Bitcoin?

[00:09:19] AA: Well, the transaction, it's a self-correcting mechanism, because if the transaction fees get so high, that means that there is a lot of demand for limited block space. If that's the case, people don't want to pay those transaction fees. They stop issuing transactions and transaction fees drop, because there's lots of competition for space until people want to issue transactions again. So the market kind of prices the transaction fee to accommodate all of the people's demand for transactions. It's almost like saying, "Nobody goes to that restaurant because it's too busy."

© 2019 Software Engineering Daily

[00:09:56] JM: All right. Taking a step back, you are highly engaged with the community of people who pay attention to cryptocurrency around the globe, and that community grew massively in the last bubble. Then the community shrunk a little bit. It subsided a little bit. Now, cryptocurrency is entering the mainstream once again. It does have this ebb and flow, and every time the audience seems to be slightly different, the mainstream element seems to be slightly different. Tell me about the audience in a typical speaking event that you're putting on these days. Who is interested in cryptocurrencies today?

[00:10:34] AA: That's a great question. I mean, it very, very much depends on where I'm doing this talk and the context of the talk. So I noticed very big differences. Usually about a third to half the audience are people who are new to cryptocurrency. By new, I mean, less than a year, or just over a year of being involved in cryptocurrency.

Then there's of course the people who come again and again and again and have been part of this for more than a year or two and are consistent. Now, in some countries, people are interested in Bitcoin primarily as a speculative investment, and in cryptocurrencies in general, and that's not necessarily a bad thing. It depends on what access to investments they have.

So, for example, when I'm in certain countries in South America where they have very high inflation and currency controls, Bitcoin represents an investment that people can access that the government can't stop them from investing their money and which protects them from inflation. So that's a store of value speculative investment, which is for capital protection.

In other countries, countries where people for the most part have plentiful access to financial services and investment opportunities, people are more interested in the social and political implications of Bitcoin. So there's people who have much more interest than the long-term impact that this is going to have on the relationship between individuals in the state, so empowering individuals.

Often, people who come to my events are privacy activists, or interested in various political movements and social movements, and many, many of the people who come to my events are

also interested in the technology itself. So they're software engineers, or web developers, programmers, etc., who are interested primarily in the technology.

[00:12:37] JM: What are the hardest engineering problems facing the Bitcoin community today?

[00:12:41] AA: So there's many interesting and hard problems, because this is a pioneering technology, some of the rebalancing competing interests or tradeoffs and design tradeoffs. For example, there's an an interesting design tradeoff, which is called the trilemma in blockchains, which is tradeoff between security scaling and decentralization.

So looking at blockchains in general, they present a situation whereby you can optimize for two of the three of those design objectives. You can have something that is secure and scalable, but it won't be decentralized. You can make it secure and decentralized, but it won't scale very well, and you can make it scalable and decentralized and it won't be very secure. So that's called a trilemma, and there's a lot of engineering challenges, as well as tradeoffs as to how you optimize for each one of those or how you lessen the degree of tradeoff you might have between those three competing interests.

[00:13:42] JM: It makes me think of – This may be a bad mapping, but makes me think of the CAP theorem. You have the trilemma of consistency, availability and partition tolerance. When I think about the CAP theorem, this is something that has – It's not like it's ever been fixed completely, but it has been ironed out by increasingly pragmatic systems over time and it has been the story of iteration and incremental technology improvements.

I don't know enough about the Bitcoin community and the engineering solutions that are being built therein, but I can easily imagine just minor incremental progresses accumulating over time that alleviate that trilemma.

[00:14:28] AA: Absolutely. So, the other aspect of this is that like many of these laws, if you like, these trilemmas exist within a specific system or a subsystem within the technology but don't necessarily exist within the kind of overall user experience. Same thing that applies to the internet, for example. Within a single layer of the protocol, you may experience design tradeoffs, which are then hidden or resolved by other layers within the protocol, right?

So if you're routing something over UDP versus TCP on the internet, you have to choose between reliability and low latency. Gradually, these tradeoffs have been smoothed out, as you said, by combining features with different layers, reducing some of the harsh tradeoffs by various optimizations and improvements by pragmatic choices, such as using non-optimal heuristics, but heuristics that are good enough for each solution, we can solve them.

When we're looking at engineering decisions, things that appear impossible in a theoretical basis may be somewhat possible at a practical basis to a degree that the end-user doesn't really see the difference. A classic example of that is the traveling salesman problem. A theoretical problem in computer sciences says that there is no way to find the combinatorially explosive solution, the perfect solution, to routing between say 10 different cities on the shortest possible path a dozen return through one of those cities. Because the number of combinations explodes in your face as soon as you have even a small number of cities, and yet we have Google Maps.

So from a user experience, it kind of looks like we've solved it, but of course the difference is that you can approve, and in fact, it's clearly theoretically impossible to find the perfect path between two cities. But can you find 100 perfectly good paths that still are good enough for the person who's actually trying to get from A, to B, to C, to D that are not the optimal path, but they're good enough? Of course, you can.

In blockchains, these problems are a lot about what you want to achieve in the end with the blockchain. For example, in Bitcoin, we very, very strongly care about decentralization, because decentralization is a means to an end, and the end is to prevent anyone from taking over co-opting, controlling, and ultimately concentrating power over the system to the detriment of the participants.

So decentralization is a cherished property. Many other blockchains kind of will solve the trilemma by simply reducing decentralization, because it's something that's both hard to measure and its impact is more long-term. Same thing as we've seen on the internet, right? You don't notice that decentralization is going away until your grandpa tells you that Facebook is the

internet and you're like, "Oh! We've gone way too far." It's that unnoticed creeping slippery slope.

So in Bitcoin we really care about that. So we do that to the cost of scalability. So Bitcoin solves the trilemma by emphasizing decentralization and security at the cost of being able to scale easily on layer one, and sometimes you see that reflected in fees where it gets expensive to transact on the first layer of the blockchain.

But then one of the interesting developments in the last year has been developing protocols as a second layer above that that allow us to route payments in a way that they're not broadcast and verified by everyone, but instead are truly peer-to-peer through a system of routed payment channels. This technology is called the lightning network, and that allows us to get very, very good scaling properties in layer two even if the underlying layer one doesn't scale very well. So we pushed some of the problem up a layer and solve it in a different way.

It's very similar to solving the fundamental routing problems in the IP layer on the internet and not caring too much about reliability and end-to-end streaming and then solving those at the TCP layer and not caring too much about application and encoding and solving those at the HTTP layer. That's a fundamental way of looking at engineering, which is maybe cancel the problem in this layer, but you can create a user experience where that problem is less noticeable.

[SPONSOR MESSAGE]

[00:19:30] JM: SQL has been around for a very long time, and the basics of SQL might not change very much from year-to-year, but the underlying technology that implements those queries is undergoing constant innovation. The Distributed SQL Summit is a full day of talks about building and scaling distributed SQL systems in the cloud.

The Distributed SQL Summit is September 20th, 2019 in San Jose, California. Distributed SQL databases can globally distribute data and elastically scale while also delivering strong consistency and acid transactions.

The Distributed SQL Summit includes speakers from Google Spanner, Amazon Aurora, Facebook, Pivotal and YugaByteDB. To find out about the latest innovations in large-scale distributed systems infrastructure, mostly with a focus on distributed databases, check out the Distributed SQL Summit, September 20th, 2019 in San Jose.

[INTERVIEW CONTINUED]

[00:20:40] JM: You alluded to the occasional – Well, not so occasional confusion, that some people believe that, for example, Facebook is the internet. I had a kind of a disturbing conversation a couple days ago with an engineer from India, and we're just talking about what we do and he asked me what I do, and I said I run a podcast. It's called Software Engineering Daily. He said, "Oh, how can I find it on YouTube?" I was like, "No, it's a podcast," and he's like, "Yeah. How do I get it on YouTube?" I was like, "Podcasts, these are disjoint – I mean, not disjoint, but they're overlapping kind of things."

I have really come to respect the ethos of decentralization as it could potentially apply to a variety of forms of communication, including money. I wonder – There's clearly market demand for decentralized communications platforms, and I wonder how your current line of thinking is on how the other platform, like other communication mediums other than money will develop.

You could hypothesize that these things will all be built on top of Bitcoin, and then there's all kinds of gradations beyond that, like maybe it's actually going to be Ethereum, because the base programming language is more flexible or maybe it's like some other kind of protocol or something that are built on top of these systems or built entirely separate from these systems. Have you started to get a belief set around how these other communications mediums, like social media, or video, or audio sharing. How these things will manifest in decentralized fashions?

[00:22:26] AA: Yeah, I think that's been one of the primary drivers for the Ethereum blockchain, and in Ethereum speak, that's called web3, web3 is intended to be kind of the next generation of the web. It's kind of a play on the web 2.0 social media and interactive web generation that happened a decade ago.

Web3 is supposed to be the decentralized we. I prefer to call it the re-decentralized web, because when we started the web, tt was decentralized. You ran your web server if you wanted to publish content.

Gradually, it became more and more and more centralized, and now I think we're looking at re-decentralizing the web. That's one of the core principles within the Ethereum community and is one of the driving goals of the Ethereum blockchain, is this concept of web3. The idea is to build applications where control over many of the trusted components that today are primarily run by trusted third parties, or semi-trusted third parties, that provide institutional mechanisms of trust. Instead are replaced by smart contracts that provides protocol mechanisms of trust.

So if you think about it, if you want to publish contents and you want to control who accesses it and create a network of friends, then you can't trust how you publish that unless you have some form of identity management, or reputation management, or access control. We trust companies like Facebook and Google and Apple and others to provide us these access control mechanisms and identity and reputation mechanisms, and they provide them as centralized institutions and third parties.

So the idea with Ethereum is if you can replace those with protocols, so you have mechanisms for reputation that are based on protocols and smart contracts, mechanisms for identity that are based on protocols and smart contracts and methods for access control and governance that are based on smart contracts, then you don't need these centralized institutions.

It's fairly easy today to decentralized data storage. We already have tons of protocols that do that, Bittorrent, I PFS and many newfangled protocols that do that, and yet a lot of our personal content tends up being in these walled gardens and centralized platforms like Facebook. Part of the reason is because we don't have protocols to do the identity, the reputation, the access control and many of the other things we care about. I think that's a core part of the Ethereum version.

On the other hand, however, I think in order for the those types of platforms to be built, we first need to get payments in money done right. We need robust, open global systems of payments and money. Part of the reason is because not only do those provide a foundation for security

and trust, because people care enough to protect their keys when their keys are used for controlling money, but they also provide the platform to fund all of these other activities.

Without that platform and without that censorship persistent money, it becomes very difficult to build the next layers, which is why I think all of the kind of rivalry and competition between platforms like Bitcoin and Ethereum is mostly just misguided, because I think, in fact, they work very well together and need each other to do things that cannot be done in a single platform and should not be attempted in a single platform because the tradeoffs are different.

[00:26:25] JM: Why is that? Because I look at Bitcoin and, yes, obviously the language it is different, but to me it just looks like a very basic Turing machine and you can build all kinds of things on top of it like sidechains and lightning networks and things with like longer confirmation times where you could have different scripting languages and so on. What couldn't you just import all the innovation into Bitcoin? Why do you need these other languages and other platforms?

[00:26:58] AA: I think, primarily, it's two reasons. One is that Bitcoin itself is not Turing complete, and that's quite deliberate. It's actually a hard fact to achieve and difficult to maintain, and it's deliberate because that provides a much more predictable platform for execution of much more – Let’s call it mission-critical security code.
If you're going to build a robust nation state resistance, censorship resistant, denial of service resistance global platform for money, which is a very tricky proposition, because governments are very serious about controlling money worldwide. You really need to focus on very conservative, robust security development. That restricts both the range of activities you can do on the platform, as well as the pace and speed at which you can do development. Things have to be very slow, very conservative, very carefully reviewed before they are deployed, because you're talking about something that needs to be very robust.

Now, that's not suitable for developments of all of these other things we’re talking about. They need a much more experimental, much more fast-paced style of development, and that will necessarily happen at others layers and other chains. Can those chains be connected to and interact with Bitcoin? Absolutely.

But the other issue also is that the security of model of Bitcoin, the consensus mechanism involves verifying only the security primitives of Bitcoin itself, which means that if you build a sidechain or something else that links to it, it's is very difficult to rely on the security guarantees of Bitcoin if what you're doing is outside of that purview. If it's not being validated or verified by the same security mechanism.

So if you build the sidechain that does you no fancy, smart contracts, etc., and those smart contracts are anchored or connected to Bitcoin but they're not being verified by the Bitcoin security mechanism, then you have to provide that security mechanism in your sidechain or in whatever else you're doing. If that's not robust, then neither are your smart contracts. This is the fundamental dilemma that caused or led Vitalik Buterin to decide to launch Ethereum as a separate chain.

[00:29:37] JM: I think I see. So I was imagining, "Oh, you can just engage in 250 transactions on a sidechain and then eventually compress that into something that fits into the core of Bitcoin blockchain, but then all 250 of those transactions are not subject to the security constraints of Bitcoin." So you're going to have to figure out some totally alternative security mechanism for securing them, unless you want to wait for the Bitcoin confirmation. That wouldn't work, right? You just wouldn't have security guarantees.

[00:30:11] AA: Well, it depends on what you're doing in the sidechain. If what you're doing in this other chain or layer is payments and you can summarize the entire security state in a Bitcoin script, then yes, you can basically take all of the security guarantees of Bitcoin and essentially connect them to this other state, and therefore you can inherit all of those security guarantees, and that's what the lightning networks does. Because what the lightning networks is doing is summarizing the state of payments, and so that's fine.

The problem is if you want to do more complex things involving smart contracts, then the state of those smart contracts cannot be expressed in Bitcoin script. Therefore, you can't leverage the security guarantees of Bitcoin. You need to bootstrap a whole different security mechanism that actually inspect the execution of the smart contract and the state transitions of the smart contract, and it's exactly what Ethereum does.

In doing so, however, it sacrifices some of the robustness in order to be able to move faster and develop and experiment more, and that means the things that should be simple or not and things that can be done very simply and very secure in Bitcoin can't be done very simply and very secretly in Ethereum.

Here's a very good example, multisig. Multisig is part of the fundamental primitives of Bitcoin script. So you can implement it directly in Bitcoin script, and multisig has existed almost since the very beginning in its modern form since 2012, which is called paid script hash, and it is extremely robust, because it's implemented at the core layer of the protocol. It's validated by everyone, and it's very, very simple, and simplicity and security are very closely related, right? The simpler you can make something, the harder it is to find a way to introduce a vulnerability or fool the protocol as validators.

Multisig in Bitcoin, very, very robust. Multisig in Ethereum has failed repeatedly, because multisig in Ethereum is not part of the base protocol. It's implemented as smart contracts. People have been, unfortunately, rather verbose in their implementations. Rather than doing a very, very simple multisig, they've added features, right? They've made it more flexible. Some of those features resulted in bugs, and those bugs exploited, caused failures in multisig.

This has happened more than once, and there is currently some multisig contracts in Ethereum that have been very carefully audited and have been used for a while without the vulnerability. I don't trust them. I wouldn't put my money in them, even though other people have put hundreds of millions of dollars. The reason is simply because there's much more room for errors, and that's exactly the kind of tradeoff that makes it difficult to implement the same level of security in Ethereum as you can in Bitcoin.

[00:33:30] JM: This is what kind of confuses me about the idea that we wouldn't want to or that we couldn't build everything on top of the Bitcoin ecosystem. If you're going to need a reliable multisig system regardless, and if you can build – I guess maybe what it comes down to is the question of can you build abstractions on top of Bitcoin that are Turing complete and have the sufficient guarantees that you need, such that your Bitcoin-based system is equivalent, yet superior in terms of its proven stability to Ethereum, or is there just something about Ethereum?

[00:34:24] AA: It's a fundamental design tradeoff. The flexibility you need to do expressive, compostable and flexible smart contracts undermines your security robustness, and that doesn't mean you can't do security. It simply means that security takes a lot more iterations and a lot of time to mature. Eventually, once you have a smart contract that has been polished to a level where it's being relied on an attack and attacked and attacked and no one can find any problems with it, then you can rely on that, and then it's robust enough, but it takes a lot more iterations to get to that point, because it's more complex and more expressive.

By comparison, you can do that more easily with Bitcoin, because it's simpler, but the problem is you can't be very expressive. So you can't develop the kinds of smart contracts, and there's a gap between those two design tradeoffs, and you don't really want to try and close that gap. If you make Bitcoin expressive enough to do smart contracts, you lose some security, and if you tried to make your smart contract less expressive, you gain a bit of security, but you lose the ability to develop interesting things beyond the basics.

I'll give you another example, and I should probably do a talk about this. Think of Bitcoin as inorganic chemistry and think of Ethereum as organic chemistry, right? Bitcoin is an inorganic chemistry. You can make steel out of it, and it's incredibly robust. There are a number of chemical reactions that can happen, but they're fairly limited. You can, in fact, list all of the chemical reactions that can happen to it, because it will react in a very predictable way with a very specific set of elements, and that set of elements is finite. So you can predict its properties.

From a quantum level, you can predict it's properties, exactly what it's going to do, even if you've never seen a molecule like that before in inorganic chemistry, even before it's discovered, even before an atom is discovered, a specific chemical element is discovered, we already know it's properties. You can derive its properties from its composition, right? You can predict its properties even before it exists.

Now, compare that to organic chemistry. Organic chemistry is freaking messy. You can have an infinite variation of elements that combine in different ways, and it's not just what they're made of. It's also which way they're twisted and what shape they're in and how they fit into another molecule. It has a different shape, and whether the left-handed or right-handed. You can never

predict how they will respond to interacting with another element, and that makes them very unpredictable, but it also makes life.

So that's the tradeoff, and when it comes to doing money and stuff like that, I'd much rather stay firmly in the inorganic chemistry that is predictable and finite and its implications. But when it comes to doing more interesting things, I'd much rather stay in the organic side. There's a bit of overlap, but they're two fundamentally different routes.

[SPONSOR MESSAGE]

[00:37:48] JM: Instabug is a feedback system that helps teams improve their app quality. Instabug allows your users to give feedback inside the app by shaking their phone. Users can take surveys and help you understand their perspective about your app.

If your users encounter a bug that they want to report themselves, they can just shake their phone and send feedback to you and your development team. This level of communication is great for beta testers. Or if you have a live app where you're in close contact with your users, you will also receive automated crash reports, which means that every crash on a user device is going to be reported to you and your development team.

Go to instabug.com/sed and try Instabug for free for 14 days. If you like it, you can use code SED19 for 20% off of any of the Instabug plans. Instabug lets you get feedback from your users inside your app. When your app has an issue or a bug or a UI glitch, your users should be able to report it, and they should be able to have a dialogue with you.

Go to instabug.com/sed to try Instabug for free for 14 days. Just thinking about it makes me want to get Instabug for the SEDaily apps. We should probably check it out in more detail, because companies like Lyft, and PayPal, and Samsung all use Instabug and they want to improve the quality of their apps. Well, I want to improve the quality of my apps too. If you want to improve the quality of your apps, you can check out instabug.com/sed.

[INTERVIEW CONTINUED]

[00:39:37] JM: I'd like to discuss mastering Ethereum a little bit. I read Mastering Bitcoin a couple of years ago and I never programmed with Bitcoin. I never spun up a node or anything, but the book was really useful to me, because you can read the white paper and you can read cryptotwitter. But until you kind of see some code and you see just the engineering beauty and finesse that has gone into Bitcoin, it's difficult to really get – I found, like I had so much more appreciation for what Bitcoin is from reading that book, and my sense was that in writing it, also your regard and how much you were in awe of the technology increased as you were writing it, because it is so well put together.

I'm wondering what that process was like for mastering Ethereum, because I'm sure you we went very deep into the technology and probably had some insights about what made the technology beautiful. So I'd love to know more about that writing process and any insights you had.

[00:40:49] AA: Yeah. I mean, for both of these books, the purpose of writing them was learning, for me. When I first entered the space in Bitcoin, I craved a way to be able to get a very high-level, but detailed enough picture of the whole things that I could grasp it. But all of the information was scattered all over the place, and it took forever to put it together and figure out if the information was up-to-date and if it was relevant, and connect the dots between all of these different pieces and see them as a whole and how they work together and why they work together. The why is very important, because it gives you an insight into the how. There wasn't such a resource. So I set out to write it.

Of course, when I started that journey, I didn't understand Bitcoin. I mean, I kind of understood it, not to the depth of the core developers who had obviously internalized all of this information the hard way, but I didn't understand it to that level of depth. Writing the book not only allowed me to collect all of the information and understand how it fit together and why, but also to learn, and learn and really understand Bitcoin to a level of depth I'd never had before.

So I was fascinated with Ethereum for the very beginning when I first saw the white paper that Vitalik wrote, December 2013, and I wanted to learn more about it. I was writing Mastering Bitcoin at the time, so I wasn't involved in the early days. I was keeping tabs on it and trying to

learn, and I found that I only understood it on a very surface level, and I had trouble understanding some of the concepts and they fit together.

So I decided to repeat the same process, which is the best way to learn this would be to write about it. I don't have a book like Mastering Bitcoin to learn Ethereum. There isn't such a thing. It was much harder to write. Part of the reason it was much harder to write is Ethereum moves so much faster, and there's so many, let's say, tendrils and offshoots, right? It's a much bigger ecosystem. There's a lot happening at the edges.

So as I was writing it, it was changing at the same time. So I tried to capture what are the things that are essential and continuous or eternal about Ethereum. What's the real essence of it? The DNA of it? What's kind of on the surface and changing quickly that might not be relevant in a couple of years?

Again, a lot of that involves focusing on why. Why are certain choices made? Why does it work this way and not another way? Because that gives you an insight into what's going on. Again it was a huge learning experience. It took me two years, and at the end of it, I'm quite proud of the book, because to me it feels like the book I wish I had when I first started learning about Ethereum, and that was my goal. It was almost immediately out-of-date just like with the first Bitcoin book. The first edition is good, but not great. Again, just like the first edition of Mastering Bitcoin. The second one was much better. So I expected some time, I'm going to write the second edition for Mastering Ethereum and it's going to be much better than the first, and I'll learn it to even more depth.

[00:44:29] JM: I want to talk a little bit about Libra with you. I watched a talk that you gave about Libra. You touched on Libra. It was very shortly after Libra came out. Have you had more time to take a closer look at it or have you taken a closer look at it?

[00:44:45] AA: Yeah. I mean, I read the white paper, and I did a talk at a university in Edinburgh about it. It's mostly about the social, political, economic implications. Not so much about the paper, and part of the reason for that is because I predicted at the time that while the paper was written by people who strongly believe in decentralization and a lot of the principles we talk

about in cryptocurrency, in fact, they quote “The Internet of Money,” which is the title of two of my books in the first paragraph, I believe, or second paragraph of the paper.

That vision would never make it into production. The reason it would never make it in production is because it would come into contact first with Facebook headquarters, then Facebook lawyers, finally, government regulators. It didn't take more than two or three weeks from when I made that video for the full impact of that to come through. I made a prediction that such a system would be unacceptable in countries that have currency crises and needs strict central-bank control.

I used India as an example. India came out the next week and said, “This is not to be allowed here,” and many different governments immediately pushed back hard against Facebook. The recent hearings I think were an eye-opener, because it offered a very strong juxtaposition against crypto, real crypto, like Bitcoin.

The concepts that I talk about to differentiate between the crypto that I care about, the open blockchains and these other things that pretend to be, but are not really, and I talk about the five pillars. The five questions you need to ask when someone says the word blockchain. You need to ask is it open? Is it borderless? It is publicly verifiable? Is it neutralist censorship persistent? The answer for all five of those for a Facebook's system is no. Tey could never make it be any of those things, because they would immediately come under pressure to start backpedaling from those positions. That's exactly what happened. You can have a system that exhibits those properties on the five pillars that is owned by someone who can be coerced. It's impossible, because they will be coerced immediately.

[00:47:06] JM: Regardless of the viability of Libra, it has been a nice thrust of political and public discourse about the nature of crypto currencies.

[00:47:20] AA: Oh, yeah. It changes the game completely.

[00:47:23] JM: Why is that?

[00:47:25] AA: The funny thing is that Libra changed the game just by writing a paper. They didn't even need to deploy anything, because they force people to start making comparisons. So I think, essentially, Libra was the second strike against the nation state money. First strike was Bitcoin, right? That suddenly forced people start asking questions about the nature of money and can you have money that's viable, that's valuable, that's usable without state-backing? The answer after 10 years is clearly yes.

Libra now creates other questions, which are really important, which is what is the role of private corporations in the formation of money? Can private corporations create private money? If so, what are the rules by which they operate since they're not controlled by democratic institutions? That creates juxtaposition. It creates comparisons between both corporate money and state money, but also between corporate money and people money.

So now we have these three players. You have state money, traditional fiat. You have people's money. Open, public, blockchains and crypto currencies, bitcoin, of course, being the foremost example of that, and corporate money. These three are going to provide three very different perspectives to the world. I think people are beginning to realize that privately controlled money is dangerous and creepy and fascist and laden with surveillance. Once they realize that, they realize that a lot of our state money is also heading in that direction. Maybe we shouldn't be eradicating cash.

So we're having a long-needed conversation about the fact that cashless society is freedom-less society and democracy-less society. You can have a cashless society that's free. The idea of eradicating cash and going to completely digital currencies that are controlled by governments, inexorably leads to governments that are less accountable, and that's dangerous too. So it's created some very interesting conversations.

The other conversation it's creating, which is really useful, is the juxtaposition against the people's money, because very, very quickly people saw that governments are highly motivated to stop Libra from happening and to stop Facebook from doing this. Not only are they motivated, they are able. The moment they noticed that, they immediately also noticed that they are unable to do the same for Bitcoin, and that juxtaposition is really important.

[00:50:08] JM: That's profound. What kinds of response are you seeing to that kind of like – Or are they waking up? Are they waking up to, “Oh no! This Bitcoin thing.” Like, “Oh no! This is actually much more problematic than Libra. What are we going to do?” Are they starting to have that actualization or is Bitcoin still to nascent and kind of un-actualized in its effects on the real world for governments to really start freaking out?

[00:50:38] AA: I think it's un-actualized and still too nascent, and that's really, really great. Because the problem here is that at some point, governments will realize that this is no joke, that this is not going away, that this is not going to be stopped, and that this is not something that they can control. Not even if they take extreme undemocratic measures as some governments have already taken and still fail to control it.

We’re beginning to see what happens when determined governments tried to ban it and then fail, or as I like to say, you can take your country out of Bitcoin, but you can't take Bitcoin out of your country. So when you bad it, all you're saying is, “We will not have any legitimate or positive involvement with Bitcoin.” Great! So that goes away, but then what are you left with? You still have all of the other contacts was Bitcoin, because it doesn't go away. It doesn't leave your country. It’s already there staying there. It's everywhere.

So if you ban legitimate user from using it, you lose all of the benefits, but it doesn't stop the illegitimate uses of it. In fact, it accelerates those and makes them even more profitable. So pushing it under the rug, pushing it into the shadows doesn't really work, and that’s being demonstrated a number of times.

That won’t stop governments from trying to do that again and again and again. But for the time being, they’re underestimating the threat this will have, essentially, on sovereignty, on their sovereignty, and on their ability to control monetary policy. We’re beginning to hear some whispers. But, I mean, pretty loud once. When the secretary of treasury in the United States says, “This is a threat to the U.S. dollar’s supremacy.” You’re damn right it is. You have no idea how big of a threat is.

Of course, the narrative is still, “But we can ban it anytime we want,” which is the kind of narrative you can persist with as long as you don't actually try to execute on it. In fact, it's

dangerous for governments to try, because the one thing that's worse than kind of vaguely tolerating it and spreading misinformation about the fact that it's like used by terrorists and drug dealers is to actually try to ban it and then fail. If you try to ban it and then fail, you provide an enormous boost to the narratives that you can't ban it. That's even more damaging, because then you show the impotence, right?

It's really funny, because when I talk to regulators, and government people, and bankers, when I say you can't regulate this, the usual response is, "But we have the authority." I was like, "No. I wasn't questioning your authority. I was questioning your ability. There's two different things." You have all of the authority in the world. Sure, you have the authority. What you lack is the technical capability to exercise that authority, and that's confusing to them, because in all of the regulated systems that I've seen so far, legal authority translated into capability one-to-one. They've never seen a system where the legal authority does not translate into the capability.

So when you say you can't, they think that you're somehow questioning their legal authority. I'm not. I'm questioning their technical capability to actually affect change, and that's a huge difference. That really hasn't been well-understood, and I'm glad I'd rather they continue to misunderstand that for another decade. I'm really glad for Libra, because what it's done is it's distracted, right? It's drawing all of the attention and the ire of regulators and government officials, as it should, because it's far more dangerous and insidious. But it's distracting from the thing that's really going to be a thorn in their side in a decade.

[00:54:46] JM: Last question. You are the author of the Internet of Money. This is a book that's – I read it a couple of years ago. If I recall it's, it's a collection of talks. The highlights from talks you've given. You touched on a lot of visions and ideas around cryptocurrencies, some of which have come to fruition. Other of which are still probably prescient. If you were to update Internet of Money today, what concepts would you add? What are the new areas you would focus on?

[00:55:12] AA: First of all, there is to Internet of Money books. There is Internet of Money Volume 1 and Volume 2, so we have updated it, and Volume 3 is being planned for this year.

[00:55:21] JM: Oh, okay.

[00:55:22] AA: So the nice thing about this is they're not in any way continuous. You don't have to read them in order. Every talk in them is standalone. It was given to a live audience. It's improvised and unique, and it touches on some aspect of this technology in a social economic political impact, the philosophy behind it, etc., and they're structured so that you can read them in a 5 to 7-minute sitting, a single chapter. It's a fun read that you don't have to start at the beginning and go to the end. You can just jump in at any point in read one short story, and it's not technical. It's for broad audience, just like my talks.

So Internet of Money Volume 1, Volume 2, which have now been translated in I think more than a thousand languages, are collections of my talks. There are 12 talks in each book or 11 talks, I think, in each book, and we're doing more.

How would I update them? I mean, essentially, these are almost like a continuous biography of my journey through crypto. Each volume contains newer talks in the previous volume. So you can see kind of a historical progression from book-to-book. Has things changed? But I'm continuing to do talks. I just did a European tour where I delivered nine different talks in seven cities, all of them unscripted, improvised to live audiences. Those are eventually going to end up in the next volume. One of them might be the Libra talk that I did in Edinburgh.

[00:56:51] JM: Okay. Andreas, thank you so much for coming back on. Thanks for being a great emissary of Bitcoin. I continue to get a lot of value out of your content.

[00:56:59] AA: Oh, thank you so much. I really appreciate it. I'd like to add kind of for your audience that all of the content I produce is available on the free and open licenses, including all of my videos, Mastering Bitcoin and Mastering Ethereum books. You can find them online. You can download them and read them for free. You can watch my videos on YouTube.

I am not sponsored by any corporations or seeking corporate endorsements or anything like that, because I'm funded directly by the community. So through Patron, which provides me with a steady income stream for me and my staff. I fund my activities which allow me to take this message of education to as many people as possible in as many languages as possible. You can find all of that under my username, which is AANTONOP, AANTONOP. You can find me as

AANTONOP on Twitter, AANTONOP on YouTube. My website, aantonop.com, and also if you want to support me on Patron with a monthly subscription, patron.com/aantonop.

[00:58:04] JM: Beautiful. Thank you adding that information, Andreas. Great to talk with you, and best of luck in the continued talks. I'll be watching.

[00:58:11] AA: Thank you so much, Jeff. We'll talk soon I hope. Have a good one.

[END OF INTERVIEW]

[00:58:17] JM: When I was in college, I was always looking for people to start side projects with. I couldn't find anybody. So, I ended up working on projects by myself. Then when I started working in the software industry, I started to look for people who I could start a business with. Once again, I couldn't find anyone. So, I started a business myself, and that's the podcast you're listening to. But since then, I've found people to work with, on my hobbies, and in my business, and working with other people is much more rewarding than working alone. That's why I started FindCollabs.

FindCollabs is a place to find collaborators and build projects. On findcollabs.com, you can create new projects or join projects that are already going. There are topic chat rooms where you can find people who are working in areas that you're curious about, like cryptocurrencies, or React, or Kubernetes, or Vue.js, or whatever software topic you're curious about.

We now have GitHub integration. So it's easier than before to create a FindCollabs projects for your existing GitHub projects. If you've always wanted to work on side projects or you want to find collaborators for your side projects, check out FindCollabs. I'm on there every day and I'd love to see what you're building. I'd also love if you check out what I'm building. Maybe you'd be interested in working on it with me.

Thanks for listening, and I hope you check out FindCollabs.

[END]