2021

Blockchain Emergencies & Open-Source Software Governance: Is "Rough Consensus" a Suicide Pact?, Blockchain Emergencies & Open-Source Software Governance: Is "Rough Consensus" a Suicide Pact?

Angela Walch
St. Mary's University School of Law, awalch@stmarytx.edu

word managers are really important. You don't want that to be broken into, but you want someone to be able to access your passwords. Using hardware keys is important. Don't knock the centralized exchanges, like Coinbase and Kraken. Those exchanges have built–in ways to pass on your account to somebody else. So for someone who wants to invest in cryptocurrencies but is not digitally savvy, that's a perfectly valid solution. Ledger is probably the hardware wallet of choice, and then a Liberty Safe and good old pen and paper does wonders. For some of my clients, they write down with a pen and paper what their private keys are, all of their passwords, etc., they put it in an old–school safe that only they have the combination to, knowing that when they die their personal representative will have to go to court, they will have to be named personal representative by the court, and at that time, they will hire a locksmith to come and break that safe open. So that's what some of my crypto elite clients are doing.

SETH ORANBURG: Thank you, Carly.

CARLY HOWARD: That will wrap it up. Thanks, Seth.

SETH ORANBURG: Yes, marrying the high tech and the low tech, that's practical right there, and so absolutely great advice. You definitely need to have a plan because if you forget that private key, that Bitcoin disappears. People have lost millions by losing just a 64–bit number.

CARLY HOWARD: Yeah, and I think we're going to see more of that too as people start passing away and then their representatives can't find their keys.

SETH ORANBURG: Right. I can't even find my car keys, so, I mean, this is going to happen certainly.

PRESENTATION 3: ANGELA WALCH—BLOCKCHAIN EMERGENCIES & OPEN–SOURCE SOFTWARE GOVERNANCE: IS "ROUGH CONSENSUS" A SUICIDE PACT?

SETH ORANBURG: So, next we have Professor Angela Walch. I would love to hear from you about software and governance and how blockchain fits into that as well. So please take it away, Angela.

ANGELA WALCH: Hi. Thank you so much for having me today. I've enjoyed these earlier presentations. Again, my name is Angela Walch, and I'm a professor at St. Mary's University School of Law in San Antonio and a research associate

at the UCL Centre for Blockchain Technologies. It's great to be with everyone here today. A lot of this stuff that we have heard discussed ties in with what I am thinking about. My talk is probably a little bit less heavy on the legal intricacies and more on thinking about how lawyers need to be concerned about mechanics that underlie these systems and the "who is doing what" at the base level of these systems.

So my talk here today is called Blockchain Emergencies and Open–Source Software Governance: Is "Rough Consensus" a Suicide Pact? I am fascinated by worst case scenarios, and so that's what you're going to get today. Basically, how we're going to proceed in this talk is to situate ourselves with what I'm referring to here. I am concerned with the governance of these protocols at the base level. I'm concerned with, "How is Bitcoin run? Who gets to make decisions about Bitcoin? How is Ethereum run? Who gets to make decisions about Ethereum?" Why does this matter? Well, it matters because—I think we've already heard a great demonstration of why it matters—these protocols at the base are supporting this whole DeFi structure that Aaron was discussing earlier, right? All the complexities and different complex financial products that are being built there, they sit on top of these infrastructural base level protocols. I think we need to be aware of how these things work and the systemic risks that they can pose if we're not really pressing on assumptions and practices in those areas.

So I will talk about what the normal protocol governance looks like in some of these systems, of course keeping in mind that every one is slightly different. I'll talk about how their governance might differ in emergencies in the systems, and then post some open questions that I think we need to come up with answers to so that the systems we're building atop of the base level are reliable if we're putting big financial systems on top of that.

This was the best picture I could come up with to just kind of show you what I'm thinking about. I wish that it were actually the other way around, that you would have the thin layer at the bottom and go up into this bigger triangle at the top. But basically, I'm concerned with what's happening at the bottom of a structure. When things go wrong at the bottom, at the foundations, that can then make things on top of it fall apart,

for instance the decentralized finance infrastructure. So I'm thinking about the very bottom level.

We've heard discussion today about how the systems are decentralized and there's been a lot of writing about how power is shared across the system and there are lots of checks and balances involved so that no one can really force anyone to do anything. So we have software developers who are involved in writing software and maintaining it, looking for bugs, and helping to figure out what upgrades would be helpful to the system and socializing those with the larger community and ultimately proposing those to be adopted. You have people who are running the software in these systems, the nodes in the system, who do not have to run anything that they don't want to run. We've heard also that the code that runs Bitcoin, Ethereum, most of these crypto systems, I would guess all of them—although Aaron noted that there's some new developments in that area—the code is open source. So the idea is that everyone can read the code, they can decide if they want to do a proposed upgrade or not. It's on them, it's their choice, so checks and balances, the developers don't have ultimate power. Same with the mining pools and the miners who are in these networks—the ones that bundle up the transactions and add them to the common ledger that everyone is keeping.

So there's been talk about how, well, look, this is actually a lot like constitutional systems like we have, like in the US. You have different parties who are active in the governance system and power is not absolute in any one of those settings. So here on the screen, you're wondering what I'm talking about of "BIPs" and "EIPs." This is the standard way that changes to the software are made in, for instance, Bitcoin and Ethereum. So we have a BIP, which is a Bitcoin Improvement Proposal, and an EIP, Ethereum Improvement Proposal, that anyone can make if they have a suggestion for how the software of the systems should change. It's important to remember that software is how the systems run—it implements the governance. Software implements the policy choices that people make and that they then reflect in the code that is run on the system.

So there are processes within this open–source software development context that are used in standard situations. Proposals are made, there's a lot of vetting of these proposals by other developers in the system as to whether they are techni-

cally sound, they might be a good idea, there's a lot of community discussion about them. Then we go from here to more community discussion. Finally, once there's enough community discussion and the [developers ("devs")] are comfortable with it, they say they've reached kind of "rough consensus" on whether this upgrade is a good idea and the devs will finalize that new software release and push it out to the network for people to choose whether they want to run it or not. So the nodes and the miners don't have to run it—as I said, they get to choose—and the outcome is that either the network will fork or it will stay together. So that's the typical process of software governance. People generally say checks and balances, it's a pretty decentralized system.

So in theory, in non–crisis times, power is decentralized, right? These things that I just said here: checks and balances, no one can force anyone to upgrade, the code is transparent (anyone can look at it and decide for themselves whether they want to run it, and you don't have to upgrade if you decide you don't want to), and if it's a type of software upgrade that would not allow you to stay with the existing blockchain, you can fork, right? You can go on your own and you don't have to be governed by the new proposal. So this is the theory for non–crisis times.

There are also crisis times, and these are the ones I'm really interested in. I like this picture because it was called the apocalypse or something in the database I found the pictures on. So, blockchain emergencies, what are these? They are events that happen such as a bug in the code, a flaw that's discovered perhaps in the cryptographic proofs that help to support the blockchain's operation and they can bring down the system if people exploit them. And we have had a number of blockchain emergencies that have occurred in major blockchains over time.

Just a few examples of these. We saw in Bitcoin, in the fall of 2018, an inflation bug that if exploited could have blown past the famed 21 million limit on Bitcoin. People discovered it in time and worked to fix it. So don't worry. As far as I know, the 21 million cap is still safe. But it was a critical bug in the software. Similarly, we saw in Zcash, another more private crypto system, that there was a flaw in the cryptographic proof that if exploited, again, could have essentially broken the system, made it uncredible and made it lose all its value. This was

revealed by the Electronic Coin Company—the people who had discovered this flaw and managed its resolution. They revealed that in 2019.

What's different in these emergencies when these events come up? Well, the normal standard governance processes that I talked about go out the window. Remember, transparency is a big deal in these, socializing with the community, taking time to review, people understanding what they're getting into. All of that goes out the window in emergency situations. In each of these situations—you can go and read the bug reports, and there's lots of very interesting discussion put out by the people who are involved in resolving these issues—only a few people were told about the flaw or the emergency. They determined the severity of the issue and how to handle it. They didn't tell the public the truth about the situation until later on when they were sure that the situation had been fixed by people upgrading their software already. So the fix was kind of hidden in the name of saving the blockchain. Key mining pool operators were told to upgrade first, again, to save the network.

So I know I'm coming probably close to the end of my time. I think we really need to think about these situations given the billions and billions, if not now soon to be trillions of dollars in value riding on these systems, on these base level protocols. What's a blockchain emergency? How do we know when we're entering into this state of exception and go outside our standard governance practices? Who gets to decide? How much has to be at stake? Is it enough for people to lose money? Is it that the core principles of the system, like the cap of 21 million, is at stake here? Who decides what is an emergency? What practices are okay in a state of emergency that are not okay in normal times? Can you forego this critical, crucial tenet of transparency in order to save the system? Who needs to be informed about the problem? Who needs the truth about the problem? And what obligations do those who are running these emergency protocols owe to users and the public? So, if you are familiar with any of the discourse around states of emergency and the discussion around US constitutional law, when do we suspend our normal practices and who's the boss then? Very analogous . . . .

SETH ORANBURG: I think we may have frozen on you, Angela. What a cliffhanger. I think Angela might have frozen just

as she was wrapping up, so we'll allow her a minute to respond at the end of our panel. Sorry about that technical issue. But quite an interesting presentation and really reminds me of that miniseries, Chernobyl, where they just didn't want to talk about what was happening at the nuclear power plant and that led to a further disaster and creating the wrong incentives. I love to think about incentives.

PRESENTATION 4: ZACH SMOLINSKI—SMART CONTRACTS

SETH ORANBURG: Let's now hear from Attorney Zach Smolinski. He's going to talk to us about smart contracts and practices in this area. Also a registered patent attorney. Zach, if you would please, we'd love to hear your thoughts on the impact of blockchain.

ZACH SMOLINSKI: Thank you, Seth, and thank you also to Isabella for your work in organizing this event and also to the NYU Journal of Law & Business and to the Classical Liberal Institute for hosting today. I'm going to take a little different approach. I'm not going to refer to slides during my talk here and I'm going to try to keep things relatively simple and a little more freeform.

Let me just go over briefly what my goals will be in my discussion today. I'd like to give the audience an overview of what smart contracts are and why lawyers and law students might care about them. I have a secondary underhanded goal, which is to instill a little bit of skepticism in these topics. There's a lot of boosterism in this space and the boosterism can lead to a lack of clarity around some topics. I'd like to encourage everyone in the audience today to take this discussion as a series of hooks into this topic. Almost everything I say is going to refer to a bunch of other topics. As you've heard from the presenters up to this point, there's really no such thing as an isolated topic in this space. You quickly get into, what are the technical backgrounds behind what we're talking about? What are the legal connections? What are the business and governance issues around these things? For all these topics, it's definitely has gotten to the point where it's an irreducibly complex area. My hope would be that we can just very simply go through some of these topics. Of course, any real questions that remain bring to the breakout sessions after-