Stanford eCorner

The Downsides of Crypto

Balaji Srinivasan, *Coinbase*

13-02-2019

URL: https://ecorner.stanford.edu/?post_type=snippet&p=62949

Coinbase CTO Balaji Srinivasan discusses two potential challenges facing the global adoption of cryptocurrency. He shares how cryptocurrencies will need to overcome national firewalls (like China's) that can create synchronization problems, and addresses the possibility of undiscovered security vulnerabilities within Bitcoin.

Transcript

- You know what are the risk scenarios, What are the down side cases for Crypto? I'd give a few, right.. I think it's gotten pretty far, so as of 2019, you know for example 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 what not right.. In so far as I think there are future risks I'd put them in a few buckets.. First is partition tolerance, so at least right now the Bitcoin block chain is not built to handle extended partitions.. So if for example, the great firewall goes and blocks port 8333, and then there's like a back and forth, and eventually becomes difficult for the block chain to synchronize across borders, then you could have a peek-a-boo problem, where the chain is extended in China by mining, but most transactions are happening in the rest of the world and synchronization is not happening fast enough.. Now there's work arounds for this.. There's a satellite which is pumping, you know the blocks from Bitcoin into China, because China has control over air space, but not space space right.. There is other work arounds where you could like steganographically encode packets and bring them into China, but we would have to run the experiment to see if it was possible for the great firewall to actually inrodite it.. Now that firewall would have to be so tight that it would have to introdite not not just the service, but any one megabite transfer like in all of China across billions of people, so that would be hard but possible..

So lets call that one approach, the partition tolerance.. Second is if there is some CVE, you know like really critical vulnerability that we have not seen that allows people to counterfeit large numbers of Bitcoins and you know like break the value of the system, and 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 was serious security issues, I think it would set back the industry at least five years or so, like people would have to rebuild around it.. With all that said though, I think those kinds of issues I just mentioned are technological issues where it could set the thing back, but I think the fundamental concept of block chains of decentralized currency is out there, and then folks, what they'll do is fix that, and then have the more robust version in the future...