Stanford eCorner

Bitcoin Basics

Balaji Srinivasan, *Coinbase*

13-02-2019

URL: https://ecorner.stanford.edu/?post_type=snippet&p=62958

Why invent cryptocurrency in the first place? It's all about decentralizing transactions, says Coinbase CTO Balaji Srinivasan. He walks through the basics of Bitcoin, explaining how monetary transactions can be decentralized and how digital currency establishes trust through user verification.

Transcript

- So first, I know there's varying backgrounds, I wanna give the very very very basics.. And in particular, this slide over here, if you only remember one slide and don't wanna remember anything else, this is the motivation behind why even invent bitcoin in the first place.. So, with physical cash, if I have a dollar bill and I hand Tom that dollar bill, there's an implicit properly 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, now Tom has it.. Anybody who's observing that can see that physical bill was handed over.. If I try 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, okay, 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've 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 basically scarcity in the digital realm..

And so, until the invention of bitcoin, the way that we represented digital cash was with a bank.. Like a centralized actor that we trusted 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 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 let a transaction go through.. In extremes, as in 2008, they could print billions of dollars for themselves.. So this is something which is inelegant from a computer science perspective, to have a trusted central node if you can avoid it.. And so, what Satoshi Nakamoto did, is he came up with D, decentralized digital cash.. And so 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.. And so since any one of them could approve it, one of them disapproving it, all they would is just be giving up some bitcoin that they would've mined otherwise..

It's basically a way to combine transaction approval and currency printing in the same unit.. So the details of this aren't super important, technically at least for a talk like this, but the concept is important, which is, we took physical cash, we tried to naively turn it into digital cash, that didn't work, so we had these centralized actors, and bitcoin dispenses with those centralized actors by having anybody, in theory, who can connect to the internet with sufficient competition power, can now approve transactions and push them through...