Paul Bohm Follow
May 25, 2015 · 4 min read · Listen

Bitcoin: The Byzantine Generals' Problem

Originally published 6/17/2011

Byzantine General Belisarius

Bitcoin is a theoretical and practical breakthrough that makes it possible to decentralize services we couldn't previously decentralize.

To elaborate: Bitcoin isn't just a currency but an elegant universal solution to the Byzantine Generals' Problem in computing, one of the core challenges in reaching consensus in distributed systems. Until

The Byzantine Generals' Problem goes roughly as follows: N Generals have their armies camped outside a city they want to invade. They know their numbers are strong enough that if at least half of them attack at the same time, they'll be victorious. But if they don't coordinate the time of attack, they'll be spread too thin and will all die. They also suspect that some of the Generals might be disloyal and will send fake messages. Since they can only communicate by messenger, they have no means to verify the authenticity of a message. How, then, can such a large group reach consensus on the time of attack without mutual trust or a central authority, especially when faced with adversaries intent on confusing them?

Bitcoin's solution is this: All of the Generals start working on a mathematical problem that statistically should take 10 minutes to solve if all of them work on it. Once one of them finds the solution, she broadcasts that solution to all the other Generals. This solution then becomes the next problem. Everyone then stops to work on the previous problem, and proceeds to use the previous solution as the next problem — which again should take another 10 minutes. Every General always starts building upon (using as the problem) the longest chain of solutions he's seen. After a solution has been built upon (extended) 12 times, every General can be certain that no attacker controlling less than half the computational resources could have created another chain of similar length, because it took a lot of computational resources to extend the chain 12 times. The existence of the 12-block chain of solutions is proof that a majority of Generals have participated in its creation. This is called a proof-of-work scheme.

If this sounds confusing, don't worry. What it means is simply that consensus is reached because computational resources are scarce. You vote with work. So to rig the vote, an attacker would need to control more computational power than the honest participants have. Also, to ensure that it's more expensive for an attacker to purchase the computational power needed to attack the system, Bitcoin adds an incentive scheme. Users who contribute computational power get rewarded for their work. Thus, if the value of a Bitcoin rises and attacking the system becomes more profitable, it also becomes more profitable for honest users to add computational resources. Here's an example of how this works: At any given point, one would expect miners to invest as many resources into mining as is profitable for them. Bitcoin then also is a currency, because it needs incentives to protect the consensus process from attackers. This computational process ("mining") is not wasteful, but an incredibly efficient way to make attacks economically unprofitable. Bitcoin never uses more computational resources than necessary to protect the integrity of its interactions.

Now let's return to discussing the value provided by Bitcoin. Essentially it's a means to make consensus in highly distributed large-scale systems that would otherwise never be able to accomplish




DNS (Domain Name System). Every Bi es with a cryptographic key pair, which also allows us to solve the PKI (Public Key Infrastructure) problem: every name you connect to, has an encryption key associated with it that can be verified without having to trust a central authority. Moreover, in case network traffic monitoring prevents people from accessing information either at all or anonymously, Bitcoin makes it feasible to pay for internet relays that anonymize or reroute traffic — that is, it makes it easier to remove central control and fight censorship. The list of benefits goes on, and I've been hard-pressed to find any decentralization schemes that would not benefit from Bitcoin integration.

The pattern here is that almost all of these applications can already be built in centralized form. But often the centralized solution comes with many weaknesses. In the PKI case, you have to trust over 300 Certificate Authorities every time you make an https:// connection, many of which are located in countries with repressive governments. If any of those 300 entities are compromised, malevolent attackers will be able to read your email, access your bank account, and violate your privacy. DNS is being censored by governments simply because they can do it. And every time you store value in currency, you're trusting a central authority to ensure that it isn't mismanaged and won't depreciate in value.

So is there really value in Bitcoin? The answer depends entirely on your perspective. Let me ask a counter question: Is decentralization valuable? If you think we'll increasingly lose trust in the central authorities that manage the infrastructure we rely on, you might expect Bitcoins to rise a lot in value. If, however, you believe that authorities will be able to tackle the challenges of the future better in centralized form, then from your perspective Bitcoins don't add value. Time will tell which viewpoint is correct.