Proof of Work, Explained (Part 1 - POW for Non-Techies)

Author	josh
Date	2017-11-29 23:55:27

Overview

Personally, I'm fascinated by both the technical and financial implications of cryptocurrencies like Bitcoin, Bitcoin Cash, and Litecoin (to name a few). The way these currencies work is a complex topic, with lots of moving parts to discuss. One of the core components of cryptocurrencies like Bitcoin is the mechanism by which an entirely decentralized system of money can securely verify transactions as well as issue new currency, all while preventing fraud and issuing at a predictable rate.

Most of these currencies solve this problem using a concept called "proof of work" by which nodes solve a computationally difficult but easily verifiable mathematical problem. This concept goes beyond cryptocurrencies as well, and actually originated as an anti-spam measure.

Proof of Work - The 10,000 foot view

What is Proof of Work?

Proof of work, fundamentally, is the solving of a computationally intensive mathematical problem. This problem has two very important properties - the solution to the problem is both:

> Difficult (computationally intensive) to find
> Easy to verify once found

The idea is this: for an application like cryptocurrency or anti-spam, a "node" or computer is challenged to find a solution to this puzzle. The solution can only be found by brute-force guessing. However, once the solution is found, all the other nodes on a network or a server can verify the solution in one step. Since the answer can only be found by brute-force computation but can easily be verified as correct, the solution to the problem serves as *proof* that a certain amount of computing work was done - hence the term "proof of work".

Why is it Useful?

First, let's look at the original application of proof of work: anti-spam. The original idea was implemented in a system called HashCash, invented by Adam Back. Back's system works like so: Before performing an action like posting to a forum or sending an email, the user of a site is made to do a small proof of work problem. This problem only takes half a second or so of computing to solve, and of course is almost instantaneous for the system to verify. For a legitimate user of a forum or email system, the half second of computing is no obstacle to completing his or her task. However, for a spammer trying to send hundreds of thousands of spam messages, the task suddenly becomes very uneconomical since it would tie up their computer for minutes or even hours at a time!

Now how does this system apply to cryptocurrencies like Bitcoin? In this system, transaction verification and currency issuance is totally decentralized - no third party is trusted to create new value tokens or verify that transactions are legitimate. This of course presents a massive fraud-prevention challenge - how can the network ensure that malicious parties don't create "counterfeit" currency or send through transactions that aren't valid?

Proof of work helps to solve this problem. On the Bitcoin network, new transactions are broadcast to computers running what is called "mining" software and accumulated into "blocks" of transactions that will be validated at one time. Every time a new block is waiting to be verified, all the nodes on the network running this software essentially "race" to solve a proof of work problem first. The Bitcoin network adjusts the difficulty of this problem so that about once every ten minutes, one miner wins the race and finds a solution to this problem. Once one node finds the answer, it tells all the other nodes on the network that it's found an answer, and the other nodes can instantly verify that the answer is correct.

The node that finds proof of work for this block is rewarded with brand new Bitcoin (issued at a predictable rate) as well as all the transaction fees in that block. This computationally expensive proof of work problem creates an excellent system of economic incentives- the reward of new Bitcoin drives miners to to verify transactions are correct, and also make fraud more expensive than legitimate mining. If a miner were to try and cheat, all the other nodes running the legitimate software would instantly reject the new block since it doesn't meet the rules of the network, and all of the time and computing power of the malicious node would thus be wasted.

Proof of Work - Powering Cryptocurrency and Thwarting Spammers

The idea of proof of work has incredible value for multiple applications. This system allows computing to be used as a precious resource in a purely digital economy; a way to both secure monetary transactions and prevent the waste of resources like time and storage space. In an anti-spam setting, proof of work allows the operators of a curated space to reduce the impact of spam on their systems, reducing wasted time, clutter, and storage space. In a cryptocurrency application, proof of work allows the secure verification of transactions and the issuance of new currency without the need for a trusted third party, the often fatal flaw in fiat systems.

The applications of this technology are incredibly interesting. In the case of cryptocurrencies, I would say its application is part of a system that is *revolutionary*. Now, as a software engineer, I find the actual technical workings of proof of work to be even more interesting than the surface description. In the next article, I'll walk through how these algorithms work from a more technical perspective.