Short Guide to Blockchain Consensus Protocols

We hear plenty of talk of how public blockchains are going to change the world, but to function on a global scale, a shared public ledger needs a functional, efficient and secure consensus algorithm.

A consensus algorithm, like bitcoin's proof of work (the one we hear about most often), does two things: it ensures that the next block in a blockchain is the one and only version of the truth, and it keeps powerful adversaries from derailing the system and successfully forking the chain.
In proof of work, miners compete to add the next block (a set of transactions) in the chain by racing to solve a extremely difficult cryptographic puzzle. The first to solve the puzzle, wins the lottery. As a reward for his or her efforts, the miner receives 12.5 newly minted bitcoins – and a small transaction fee.

Yet, although a masterpiece in its own right, bitcoin's proof of work isn't quite perfect.

Common criticisms include that it requires enormous amounts of computational energy, that it does not scale well (transaction confirmation takes about 10-60 minutes) and that the majority of mining is centralized in areas of the world where electricity is cheap.
Bitcoin creator Satoshi Nakamoto woke us up to the potential of the blockchain, but that doesn't mean we can't keep searching for faster, less centralized and more energy-efficient consensus algorithms to carry us into the future.

While not a comprehensive list, the following are a few of the alternative approaches being kicked around out there.

Proof of stake

The most common alternative to proof of work is proof of stake.

In this type of consensus algorithm, instead of investing in expensive computer equipment in a race to mine blocks, a 'validator' invests in the coins of the system.

Note the term validator. That's because no coin creation (mining) exists in proof of stake. Instead, all the coins exist from day one, and validators (also called stakeholders, because they hold a stake in the system) are paid strictly in transaction fees.

In proof of stake, your chance of being picked to create the next block depends on the fraction of coins in the system you own (or set aside for staking). A validator with 300 coins will be three times as likely to be chosen as someone with 100 coins.

Once a validator creates a block, that block still needs to be committed to the blockchain. Different proof-of-stake systems vary in how they handle this. In Tendermint, for example, every node in the system has to sign off on a block until a majority vote is reached, while in other systems, a random group of signers is chosen.

Now, we run into a problem. What is to discourage a validator from creating two blocks and claiming two sets of transaction fees? And what is to discourage a signer from signing both of those blocks? This has been called the 'nothing-at-stake' problem. A participant with nothing to lose has no reason not to behave badly.
In the burgeoning field of 'crypto-economics', blockchain engineers are exploring ways to tackle this and other problems. One answer is to require a validator to lock their currency in a type of virtual vault.
If the validator tries to double sign or fork the system, those coins are slashed.

Peercoin was the first coin to implement proof of stake, followed by blackcoin and NXT. Ethereum currently relies on proof of work, but is planning a move to proof of stake in early 2018.

Proof of activity

To avoid hyperinflation (what happens when too much of a currency floods the system) bitcoin will only ever produce 21m bitcoins. That means, at some point, the bitcoin block reward subsidy will end and bitcoin miners will only receive transaction fees.

Some have speculated this might cause security issues resulting from a 'tragedy of the commons', where people act in self-interest and spoil the system. So, proof of activity was created as an alternative incentive structure for bitcoin. Proof of activity is a hybrid approach that combines both proof of work and proof of stake.

In proof of activity, mining kicks off in a traditional proof-of-work fashion, with miners racing to solve a cryptographic puzzle. Depending on the implementation, blocks mined do not contain any transactions (they are more like templates), so the winning block will only contain a header and the miner's reward address.

At this point, the system switches to proof of stake. Based on information in the header, a random group of validators is chosen to sign the new block. The more coins in the system a validator owns, the more likely he or she is to be chosen. The template becomes a full-fledged block as soon as all of the validators sign it.

If some of the selected validators are not available to complete the block, then the next winning block is selected, a new group of validators is chosen, and so on, until a block receives the correct amount of signatures. Fees are split between the miner and the validators who signed off on the block.

Criticisms of proof of activity are the same as for both proof of work (too much energy is required to mine blocks) and proof of stake (there is nothing to deter a validator from double signing).

Decred is the only coin right now using a variation of proof of activity.

Proof of burn

With proof of burn, instead of pouring money into expensive computer equipment, you 'burn' coins by sending them to an address where they are irretrievable. By committing your coins to never-never land, you earn a lifetime privilege to mine on the system based on a random selection process.

Depending on how proof of burn is implemented, miners may burn the native currency or the currency of an alternative chain, like bitcoin. The more coins you burn, the better chance you have of being selected to mine the next block.

Over time, your stake in the system decays, so eventually you will want to burn more coins to increase your odds of being selected in the lottery. (This mimics bitcoin's mining process, where you have to continually invest in more modern computing equipment to maintain hashing power.)

While proof of burn is an interesting alternative to proof of work, the protocol still wastes resources needlessly. Another criticism is that mining power simply goes to those who are willing to burn more money.

The only coin that uses proof of burn is slimcoin, a cryptocurrency based on peercoin. It uses a combination of proof of work, proof of stake and proof of burn, but is only semi-active at this time.

Proof of capacity

As we've seen, most of these alternative protocols employ some type of pay-to-play scheme. Proof of capacity is no different, but here you 'pay' with hard drive space. The more hard drive space you have, the better your chance of mining the next block and earning the block reward.

Prior to mining in a proof-of-capacity system, the algorithm generates large data sets known as 'plots', which you store on your hard drive. The more plots you have, the better your chance of finding the next block in the chain.

By investing in terabytes of hard drive space, you buy yourself a better chance to create duplicate blocks and fork the system. But with proof of capacity, we still have the problem of nothing at stake to deter bad actors.

Variations of proof of capacity include proof of storage and proof of space. Burstcoin is the only cryptocurrency to use a form of proof of capacity.

Proof of elapsed time

Chipmaker Intel has come up with its own alternative consensus protocol called proof of elapsed time. This system works similarly to proof of work, but consumes far less electricity.
Further, instead of having participants solve a cryptographic puzzle, the algorithm uses a trusted execution environment (TEE) – such as SGX – to ensure blocks get produced in a random lottery fashion, but without the required work.

Intel's approach is based on a guaranteed wait time provided through the TEE. According to Intel, the poof-of-elapsed-time algorithm scales to thousands of nodes and will run efficiently on any Intel processor that supports SGX.

The one problem with this protocol is it requires you to put your trust in Intel – and isn't putting trust in third parties what we were trying to get away from with public blockchains?