BXTB Proof-of-Capacity Consensus and Mining Guide (BLUE PAPER)

What is a Consensus Model?

Blockchains are distributed networks consisting of independent nodes that store data in discrete and immutable units called blocks. A consensus model is a set of rules that determine how these nodes agree on what to include in a block, so that they all contain the same sequence of blocks (the blockchain). It's a set of rules that determines what is stored as true on the blockchain.

What is Proof of Work (PoW)?

Blockchains like Ethereum and Bitcoin do this by asking you to solve difficult cryptographic puzzles (mining). Solving these puzzles requires a lot of work. If you have the solution, and submit an incorrect block, the other participants in the blockchain will use the rules in the consensus model to automatically reject your block, and your work will be wasted. If you submit a valid block, it will be accepted by the other participants, and the rules of the consensus model will provide you with a reward. This is how honest behavior is encouraged, and dishonest behavior is discouraged.

One side effect of rewarding participants for computing an answer to a difficult cryptographic problem, is that they will look for more efficient ways to solve that problem. For Bitcoin and Ethereum, this has led to the development of specialized hardware that uses quite a lot of electricity.

One of the goals of blockchain technology is to provide a secure network by distributing authority as widely as possible. Unfortunately, the requirement for specialized equipment and large amounts of inexpensive power work against that goal by encouraging the concentration of mining efforts in areas with inexpensive power, supportive legal infrastructure, and availability of the specialized hardware. This leads to the creation of centralized *mining farms*, often housed in large factories near inexpensive sources of electricity.

What is Proof of Capacity (PoC)?

Proof of Capacity consensus models are a way to eliminate the need for large amounts of electricity or specialized hardware to participate in a blockchain, without compromising security. One way to do this is to use storage space instead of computing time to solve cryptographic puzzles – most people have some free hard drive space, and hard drives are widely available, and don't consume too much power.

An easy way to think of this is that it works like a multiplication. When we teach multiplication of small numbers in school, we do it in two ways: by memorizing a *multiplication table* and by computing the answer manually through addition (for example 6x4 = 6+6+6+6). Once you have stored the multiplication table in your mind, it's much faster to multiply by looking up the answer on that table as an alternative to computing the answer each time.

This method of trading storage space for time is a common tool to make computer programs run faster. PoC is essentially an extreme application of this method: we store lookup tables that are gigabytes or terabytes in size to speed up computations that are much more complex than

multiplication. Without these tables, solving the cryptographic puzzles required by the consensus model is impractically hard no matter what hardware you have (we've tested this on modern FPGA hardware). Moreover, it's pretty easy to look up a solution using these tables with even modest computer hardware.

Getting ahold of these tables is another matter. You do have to compute them, and they do take a fair amount of time – but you only have to do this once. The resulting tables are tied to your account on the blockchain and can be used over and over.

This makes means that the limiting factor to mining on our blockchain is simply hard drive space, which benefits less from centralization than anything requiring a lot of electricity or special hardware. You probably also don't need to buy anything new – whatever PC or laptop you own is probably good enough, so anyone can participate.

A More Technical Description

The last section, while correct, is a simplification of the underlying methods. You can skip this section if you're not interested in more detail and just want to learn more about how mining will work.

At every block, the blockchain sets a target and a difficulty to try and keep the block time consistent. In other words, the cryptographic puzzles get harder if blocks are being formed too quickly, and get easier if they are not being formed quickly enough. This is how the network adapts to more (or fewer) participants.

When you mine, you look though your local plotfiles for a solution as close as possible to the target. The difference is divided by the difficulty (so higher difficulty values are easier), and the result is the number of seconds after the last block that your result would be considered an acceptable solution (this waiting time is called the deadline). The original data used to compute that result is tied to your account on the blockchain, and a nonce – to form a new block, a node needs a nonce to be submitted along with proof that the owner of the associated account has submitted it. With both of those pieces of information, the node will form a new block after the deadline has passed, and communicate it to the rest of the blockchain. This will cause any block reward and transaction fees to be awarded to the account that produced the winning nonce.

When you generate plotfiles to mine with, you specify a nonce range and an account. Your computer will generate 4096 cryptographic hashes for each nonce that you must store. These 4096 hashes are what lets your computer determine whether a particular nonce is a good solution for the cryptographic puzzle created for each block. The more nonces that you store, the better chances you have at having a good solution that lets you form a block and earn rewards. It is much faster to check if a nonce is a good solution, than to generate a new nonce – this is what lets you mine with a lot of plotfiles. It is also why it takes some time and effort to generate the plotfiles at first.

How Will Mining Work?

Before you can start mining, you will need to generate "plotfiles". These are very large files – they represent the 'storage capacity' you are providing in a proof-of-capacity consensus model.

There are two ways to generate these plotfiles: with your CPU, or with your GPU (graphics card). This only has to be done once to generate a plotfile, then you can mine with it over and over. It is significantly faster to generate plotfiles with a GPU, but using your CPU provides reasonable speed as well.

The plotfiles you generate are *unique to your account* on the blockchain.

We will provide both GPU and CPU plotters when we open up mining. They will work on Windows and Linux.

Once you have plotfiles, you'll need to run a miner. The miner will automatically look through your plotfiles, and if a good solution is found, you will automatically be rewarded for forging a block. The miner does not require much processor power or memory, and can be run in the background while you use your computer for other things. Power consumption is minimal.

We will be providing three miners: one for Windows, one for Linux, and one for single-board computers like the Raspberry Pi.

You can mine from a USB external drive as well. During testing, we found that the speed of USB 3.0 allowed a 2-3 TB drive to work well. Anything more than that would be scanned too slowly by the miner to be useful – but the exact limit depends on the performance of the drive.

You can store your plotfiles on a hard drive. There's very little advantage to using an SSD.

When Will Mining be Opened Up?

We're aiming for Q4/2021 - Q1/2022. We may release the plotting software earlier to help people get started.