A BETTER BITCOIN

CHIA NETWORK

- Chia is a better Bitcoin
- Instead of using wasted electricity for security it leverages the already widely distributed large sunk cost of unutilized storage space
- This results in a system which is much more distributed, secure, and green

HOW BITCOIN WORKS

- There's a permanent immutable history which gets added to called 'The blockchain'
- New transactions are in new blocks which go 'on top' of the existing history. New blocks are expensive to produce. Miners prove they have used resources with proofs of work to mint new blocks.
- In exchange they get miner rewards and transaction fees for all transactions they include.
- Once a new block is minted miners collectively switch to mining on top of that new one and the chances of a block every becoming orphaned rapidly approach zero as the number of blocks on top of it increases

HOW ~~BITCOIN~~CHIA WORKS

- There's a permanent immutable history which gets added to called 'The blockchain'
- New transactions are in new blocks which go 'on top' of the existing history. New blocks are expensive to produce. ~~Miners~~Farmers prove they have used resources with ~~proofs of work~~ proofs of space and time to mint new blocks.
- In exchange they get ~~miner~~ farmer rewards and transaction fees for all transactions they include.
- Once a new block is minted ~~miners~~ farmers collectively switch to ~~mining~~ farming on top of that new one and the chances of a block every becoming orphaned rapidly approach zero as the number of blocks on top of it increases

HOW THE BITCOIN NETWORK WORKS

- There is a network of full nodes which all keep the full history and a set of pending transactions. They propagate the single weightiest history they know of to all of their peers.
- When a new block is minted it propagates rapidly to all full nodes and miners start working on top of it. When a miner finds a new block they publish it to the network.

HOW THE ~~BITCOIN~~CHIA NETWORK WORKS

- There is a network of full nodes which all keep the full history and a set of pending transactions. They propagate the ~~singl~~ three weightiest histor~~y~~ies they know of to all of their peers.
- When a new block is minted it propagates rapidly to all full nodes and ~~miners~~ farmers start working on top of it. When a ~~miner~~ farmer finds a new block they publish it to the network. Farmers all find the best proof of space they have. The three best proofs of space rapidly the propagated through the whole network and proofs of time servers start working on top of them. When a proof of time server finishes the proof of time for a proof of space it publishes the whole thing as a fully validated block and publishes it to the netowrk to be built on top of again.

WHAT IS A PROOF OF SPACE?

- A proof of space demonstrates that an amount of space is allocated to a task by answering queries at low latency and amortized cost
- There are always time/space tradeoffs because space can be repeatedly reformatted with new proofs, the goal is to make that be the best tradeoff possible. Since that comes with high cost and latency, it may be enough.
- A simple approach is to fill available space with 'bingo cards' in sorted order. When a challenge comes in, look up the closest bingo card and the distance between that and the challenge is the quality of the response
- This approach fails to Hellman time/space attacks. A subtle new trick foils that attack: https://eprint.iacr.org/2017/893

HOW GRINDING WORKS

- Because it doesn't cost anything to do proofs of space many different histories can be explored in parallel
- For example: Re-farming since genesis. If an attacker has 20% of capacity today but capacity has been growing rapidly so they have 1000% capacity as of a year ago and the system has been around for ten years, they can re-farm an entirely new chain since genesis whose combined weight will be greater than the 'real' chain. Hacks to weight recent blocks create and exacerbated harder to describe but more insidious problems.
- An elegant solution: Alternate between proofs of space and proofs of time.

WHAT IS A PROOF OF TIME?

- A proof of time, or more accurately 'Verifiable Delay Algorithm', is a special type of proof of work which takes a specified number of iterations. Each iteration may be accelerated, but the calculation can't be parallelized across iterations. It further needs the properties that the output is quickly verifiable and canonical: Any two parties who do the calculation will come to the same result, and the verification process ensures that the output hasn't been modified in any way.
- This allows the output of the proof of time for one block to be used as the challenge for the proof of space in the next block
- Given patterns in clock speeds, expectation is that R&D investment will rapidly converge to within a small fraction of the speed of VDA possible
- A good construction for this is known and should be published soon

HOW TO COMBINE PROOFS OF SPACE AND TIME

- Each block starts with a proof of space and is finalized with a proof of time. The product of the quality of the two of them must meet the current work difficulty threshold
- This preserves 'a block is a block'. With no blocks worth more than others, incentive to farm orphan blocks in the hope of catching up is dramatically reduced
- Because correction for improvements in proofs of space and proofs of time are both done the same way in the work difficulty factor, the single observed value (time) can be used to adjust for both
- Attacks where multiple blockchains are followed not just the very best one can be dramatically reduced by having the legitimate network keep track of the top several. Surprisingly, the utility of following multiple ones hits a small constant factor maximum
- Attacks can also be reduced by making the length of proof of work for each block be the arithmetic mean of the last two values rather than based just on the last one, so trying to catch up for a bad value takes a double whammy