Microchains

New techniques for achieving layer 1 scalability

Intro

+ David Vorick
+ Bitcoin researcher since 2011
+ Co-Founder and lead developer of Sia, decentralized cloud storage
+ Spoke last year about Jute, a braided consensus algorithm

A New Way of Looking at Blockchains

+ Today I am going to introduce a new way of thinking about blockchains
+ Novel applications of game theory allow us to depart from traditional security assumptions about blockchains
+ Biggest breakthrough is a new solution to the double spending problem, which can be used to protect tiny blockchains in ways that Nakamoto consensus cannot
+ Tiny, secure, highly inter-operable blockchains present an opportunity to increase the layer 1 scalability of the blockchain

General Microchains Idea

+ Instead of having a small number of very large, expensive-to-verify blockchains, have a large number of very small, easy-to-verify blockchains
+ “easy to verify” -> can trivially run full nodes on your cell phone
+ Expect users to be on dozens to hundreds of chains, the same way smartphones today have dozens to hundreds of apps
+ Leverage the lightning network to make the chains highly interoperable, so that users on any chain can send money to users on any other chain, without even needing to know what all the chains are

Biggest Issue: 51% Attacks are Easy

+ If you have lots of tiny chains, they will be easily vulnerable to 51% attacks
+ Too expensive to develop a separate ASIC for each chain, so you will have to deal with coin-hopping and low miner faithfulness.
+ Need a new mechanism for securing chains.

New Prerequisites

+ Prereq 1: Open mining. We need a large number of miners to make their hardware freely accessible for the right price. Provide a random header and some payment, and the miner will solve the header for you
+ Prereq 2: High full node participation. Most users need to run full nodes that have high uptime
+ Prereq 3: Mutual Discouragement. Users agree to sell off coins if they observe an attack

Achieving Open Mining

+ Pay miners more for their hashrate than they are making from whatever they are mining by default.
+ If miners get more revenue this way, most miners will transition to open mining or otherwise be outcompeted.

Achieving High Participation

+ Make the chains really tiny. Think 100kb per day instead of 100MB per day
+ At that size, it is reasonable to run a full nodes on your phone
+ Users are generally comfortable running things all the time on their phone, as long as it is nice to their battery and network usage.
+ Chains with low participation will be less secure, which may drive more full nodes from institutional players.

Achieving Mutual Discouragement

+ Chains are very tiny, and users will be on many chains at once
+ Accepting one chain as a total loss is not a big deal overall
+ If a chain is successfully attacked once, it can be successfully attacked again, you really should write it off and accept your losses

Advantage of Open Mining

+ Any user can 51% attack any chain. The mining power is freely available.
+ Freedom to attack means freedom to defend. Any user on the network can respond to a 51% attack.

+ The ultimate result of open mining is that every user can use all of the hashrate at any time. PoW no longer is about 51% attacks, it’s about the amount of electricity you are willing to pay for.
+ With tiny chains in a big network, you can probably dump the entire market cap worth of electricity on the chain in a few hours.

Advantage of High Participation

+ You can observe attacks on the chain in real time and respond accordingly

+ Our threat model is going to require a nontrivial fraction of the network to witness attacks in real time.

+ The largest players (miners, market makers, merchants, lightning network hubs) will have an easy time achieving high uptime, which benefits the whole chain.

Preventing Double Spends

Scorched Earth Counterattack

+ Any double spend has a victim. Whether a merchant, user, miner, or other party, there is a victim.
+ If the victim is online to observe the attack, the victim has both the incentive and capability (due to open mining) to counterattack.
+ Attacker and victim engage in a scorched earth game, which ultimately reduces the incentive to attack.

Mutual Discouragement Disincentive

+ If we assume mutual discouragement, every witness to the attack will begin a coin selloff.
+ If the witnesses include the exchanges, miners, and market makers, the price of the coin will rapidly fall to zero.
+ Miners stop, transactions stop, and many legitimate users leave the chain. The coinprice is permanently degraded substantially

+ **An attacker who is successful inherits ash.** There is no reason to double spend, because your stolen coins will have no value.

Mutual Discouragement **Incentive**

+ Everyone who owns coins knows that a successful attack will zero out the value of their coins.
+ If an honest network participant witnesses an attack, they have incentive equal to the value of their coins to stop the attack.
+ In fact, if an attack happens, mutual discouragement means that there is incentive to defend the chain up to the entire value of the network.

+ A successful chain defense means that the attacker has lost money by spending money on ultimately worthless PoW.

Microchains Don’t Need Mempools

+ If chains are small enough, you essentially switch to a 1 transaction per block model
+ If there is 1 transaction per block, and open mining enables any user to mine their own block, then your fee more or less reduces to the cost of mining a block minus the block reward
+ No mempool means centralized miners have lower revenue and lower utility compared to direct users - a decentralization pressure that reinforces open mining

Microchains are Anti-Fragile

+ If some microchains fail for some use cases due to an inability to match the required prerequisites, it does not impact the microchains which are able to meet the required prerequisites
+ The low-market cap nature of microchains means failure is not as catastrophic as failure for a larger chain

+ It’s okay to experiment. Early microchains can serve as high-risk, high-warning experiments the same as early bitcoin. No forks needed to existing software.

Thank You