Networks: Fall 2023	Updating a Blockchain
David Easley and Yian Yin	Background Reading

Cryptocurrencies, such as Bitcoin or Ether, are based on a public record of all transactions in the cryptocurrency. This record is stored in a globally visible *blockchain*, which consists of a series of *blocks*, each of which confirms for all participants that certain transactions have been performed. In this note we focus on the systems used by cryptocurrencies to update and maintain the blockchain. Participants in the blockchain protocol compete to be in charge of constructing the next block to add to the blockchain. Bitcoin uses a *Proof of Work* mechanism to select the *miner* who will build the next block on the Bitcoin blockchain. Etherium recently switched from Proof of Work to a *Proof of Stake* mechanism to select the *validators* who will construct the next block on the the Etherium blockchain.

In this note and in lecture (December 1, 2023) we describe simplified models of the two systems that are designed to capture the critical elements of each system. We use the models to illustrate issues associated with each system.

1 Proof of Work—Bitcoin

The bitcoin blockchain proposed by Nakamoto (2008) envisions a decentralized trustless network composed of nodes, with each node containing a complete copy of the blockchain. Miners run nodes, validate transactions, and provide security for the blockchain. Mining uses computers with dedicated hardware and software to find a specific hash or string of numbers. The miners race to solve the problem and first miner to do so is compensated with a fixed number of newly issued bitcoins known as a *block reward* and the winning miner also collects the fees attached to transactions in the newly created block. The winning miner posts the block of pending bitcoin transactions to the blockchain. The blockchain grows as each validated block is added.

The block reward is currently 6.25 bitcoins per newly created block and it is halved after every 210,000 blocks are mined.[1] The rate at which new bitcoins are issued is also affected by the difficulty of solving the computational problem. The bitcoin algorithm sets the difficulty so that on average the race between miners results in a block being added to the blockchain every ten minutes. If new blocks are added faster than this desired level (perhaps because of an increase in the number of miners or an advance in mining technology), the difficulty is increased. It is decreased if the rate is too low. This adjustment is made every 2,016 blocks.

Suppose that there are M miners. Let C represent the cost (in dollars) of being a miner and suppose that the reward to a winning miner is R which consists of the block reward and the fees (both in bitcoin). Finally, let p be the price in dollars of a bitcoin. [2] If all miners are the same (a simplification to make our analysis easier) then they all have $1/M$ probability

[1] The total number of bitcoins available for issuance limited to 21 million.

[2] $16,540 on November 27, 2022.

of winning the race to build the next block.[3] So any miner's expected profit is

$$\frac{1}{M}pR - C.$$

There is free entry into the mining game, so miners play an entry-exit game in which any Nash equilibrium must entail zero expected profit. If expected profit is positive there will be entry and similarly if it's negative there will be exit. Ignoring integer constraints, the equilibrium number of miners implied by the zero profit equilibrium condition is

$$M^* = \frac{pR}{C}.$$

However, if no miner can make a non-negative profit even if there are no other miners, $pR < C$, then the value of M^* above is less than one, and the equilibrium number of miners is actually zero. For the blockchain to be secure, some number of miners greater than one is necessary. Debate is ongoing about the maximum fraction of mining that can be controlled by one miner, or mining consortium, before security becomes an issue. For our purposes, it is sufficient to set the minimum number of miners for the mining and the blockchain to be viable at some $\bar{M}$. If the number of miners implied by the zero-profit condition is less than $\bar{M}$ then mining is not viable and the blockchain fails.

There is an obvious issue associated with this system for updating the block: the number of miners is determined by a free-entry equilibrium. M^* is not chosen to provide the needed security at the lowest cost; it may be too low or too high for that. The number of miners increases with the price of Bitcoin or the total reward (bock reward plus fees) and it decreases with the cost of mining. The block reward is slowly declining and will reach 0 in 2140. So, over time, viability of Bitcoin requires the value of fees to increase enough to insure that $M^* \geq \bar{M}$. Fees are chosen by users of Bitcoin to induce miners to put their transactions on a block; whether this process will produce enough fees is unknown.[4] If $M^* > \bar{M}$ then there are more miners than needed for security. This is not a problem for Bitcoin, but as excessive mining wastes resources it is a problem for society.[5]

2 Proof of Stake—Etherium

Etherium uses a Proof of Stake system to select participants who will put the next block on the Etherium blockchain. Owners of the Ether can *stake* their tokens if they want to participate in the process for adding a new block. A user must stake 32 Ether to be eligible to participate. From among those who are eligible to participate a committee is selected to propose a new block and to vote on whether it is a valid block (contains only legitimate transactions). If everyone is honest and follows the Etherium rules only valid blocks will be

[3]See "From mining to markets: The evolution of bitcoin transaction fees" by Basu, Easley and O'Hara, in the *Journal of Financial Economics*, 2019, for more details on this analysis.

[4]On average fees last weekend provided about 3.4% of the total reward.

[5]The total usage of energy by crypto mining changes over time as the number of miners adjusts, but earlier this year the best estimates were that at that point crypto mining used about the same about the same amount electricity as used by the entire country of Argentina.

proposed and the committee members will only vote for valid blocks. But there is the possibility of *Adversaries* who want invalid blocks to be selected or who just want the blockchain to fail. Below we build a simplified model of the process, focusing on voting by members of the committee, known as *validators*.

Suppose the selected committee of validators has N members. Some of these members may be Adversaries who want the blockchain to fail. Others are rational decision makers who want to maximize their payoff. They will follow the rules for validation only if doing so is in their best interest.[6]

The committee uses a voting system to decide whether a proposed block will be added to the blockchain We consider a system in which the proposed block is added only if all committee members vote yes; otherwise, if any validator votes no the proposed block is not added. Etherium uses a quorum rule that is a bit more complicated than this, but the principles are the same.

Suppose that with some probability q the proposed block is Not Valid (NV); otherwise it is Valid (V). If every vote is yes then each voting validator receives a reward of B if the new block is actually Valid. Any committee member who does not vote receives no reward. If any validator votes no then the block is not added to the Etherium blockchain and all validators receive 0. Alternatively, if the committee unanimously votes yes for a block that is Not Valid they each lose S (some fraction of the tokens they staked).

A rational committee member can check the validity of a block by paying a cost C. If checked and found to be Not Valid a rational committee member would clearly vote no and the block would not be added to the blockchain. If a validator checked and found that the proposed block is Valid the validator would clearly vote yes. Let's assume that an adversarial committee member wants the block to added regardless of its validity. So an adversarial committee member never checks validity and always votes yes.[7]

Each validator knows their own type (adversarial or rational) but they do not know the types of the other validators. We assume that with probability $0 < p < 1$ a committee member is adversarial; otherwise the committee member is rational. These validator types are drawn independently.

If all rational members behave honestly(they check validity and vote accordingly) a non-Valid block will be accepted only if all of the validators on the committee are Adversaries. So, in this case, the probability of a non-Valid block being accepted by a committee of size N is p^N which becomes small as the committee becomes large. This suggests that if the committee is large the probability of having non-Valid blocks is small. But this conclusion requires that rational validators behave honestly regardless of the size of the committee.

The rational validators are playing a simultaneous move game in which they each choose to check validity or to not check validity. A validator's choice of whether to check validity

[6]For more on rational validators see Halaburda, He and Li (2021) "An Economic Model of Consensus on Distributed Ledgers," University of Chicago, Becker Friedman Institute for Economics Working Paper No. 2021-137 or Amoussou-Guenou, Biais, Potop-Butucaru, and Tucci- Piergiovanni (2020) "Committee-based Blockchains as Games Between Opportunistic players and Adversaries'.'

[7]More complex Adversaries are possible, but we will consider only these simple ones. Even these simple Adversaries create security issues when the other validators are assumed to be rational rather than participants who mechanically follow the Etherium rules.

can only provide a benefit to the validator if validator is a *pivotal voter*—one whose vote changes the outcome of whether the block is added to the blockchain or not. If any other validator votes no then the block will not be added regardless of the choice and vote by this validator; hence checking costs the validator C and provides no benefit. If no other validator votes no then whether this validator votes yes or no determines whether the block is added to the blockchain or not. So for a validator to chose to check validity it must be that if that all other rational validators would check validity and vote yes (and Adversaries vote yes) then the validator wants to check validity.

Lets ask if it could be a Nash equilibrium for a rational committee member to check the validity of the proposed block. A necessary (but not sufficient) condition for this is that checking is a best response given that all other rational validators check and vote yes. If all other rational validators check validity, and chose to vote yes, and all Adversaries vote Yes without checking, then the block is not Valid only if all other validators are Adversaries (if there was another rational validator that player would have checked the block, found it to be non-Valid and voted no). So by Bayes rule the probability of a block not being valid if $N-1$ others vote yes, and all rational validators would check validity, is

$$Pr(NV|(N-1)yes) = \frac{qp^{(N-1)}}{qp^{(N-1)} + (1-q)}$$

This probability converges to 0 as N grows large. If all rational validators check validity and vote yes then the probability of the block being non-Valid becomes small as the size of the committee grows.

A validator whose vote is pivotal thus would have a small gain from checking validity (the probability of a non-Valid block that received $N-1$ yes votes times the loss from approving a non-Valid block) but would have to pay C to check validity. Thus for large N a pivotal validator would not choose to check validity. A non-pivotal validator simply pays C and has no gain. Thus, a non-pivotal validator would never want to check validity. So for large N there is no Nash equilibrium in which all rational validators check validity.[8]

[8]The potential gain to checking validity only occurs when the validator is pivotal (which happens with probability $qp^{(N-1)} + (1-q)$). So the expected profit from checking validity minus the expected profit to not checking validity (both computed without knowing how others have voted) is $Sqp^{(N-1)} - C$ which is negative for sufficiently large N.