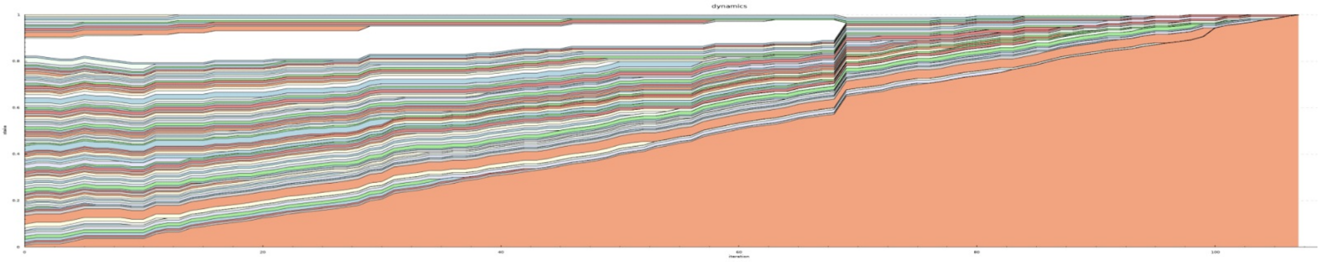
A Deeper Look into the Features of Staking in Cardano

emurgo.io/en/blog/features-of-staking-in-cardano

Proof of Stake represents a fundamental change in the underlying model of blockchain design. Bitcoin introduced the Proof of Work model wherein excessive computing power, and money, was invested in finding a hash above a certain threshold; a miner who met that requirement was granted the right to create a new block on the chain. While this is a time tested method to secure a network and maintain a global consensus, it is also tremendously wasteful in terms of electricity usage. EMURGO, as the official and commercial venture arm of Cardano — the first third generation blockchain to evolve out of a research-driven approach — is helping market a novel blockchain consensus model, named Ouroboros.

All blockchains have an inherent governance model embedded in their design. Researchers at IOHK have determined that, over time, Bitcoin converges into a dictatorship model due to centralization of miners and the underlying reward sharing mechanism, which causes stakeholders to, myopically, choose pools that have minimized their operational costs as there are more rewards available to stakeholders from those pools. This is demonstrated by the Bitcoin convergence simulation image below, which is based on tests run by IOHK.



Source: Kiayias, Aggelos. Stake Pools in Cardano.

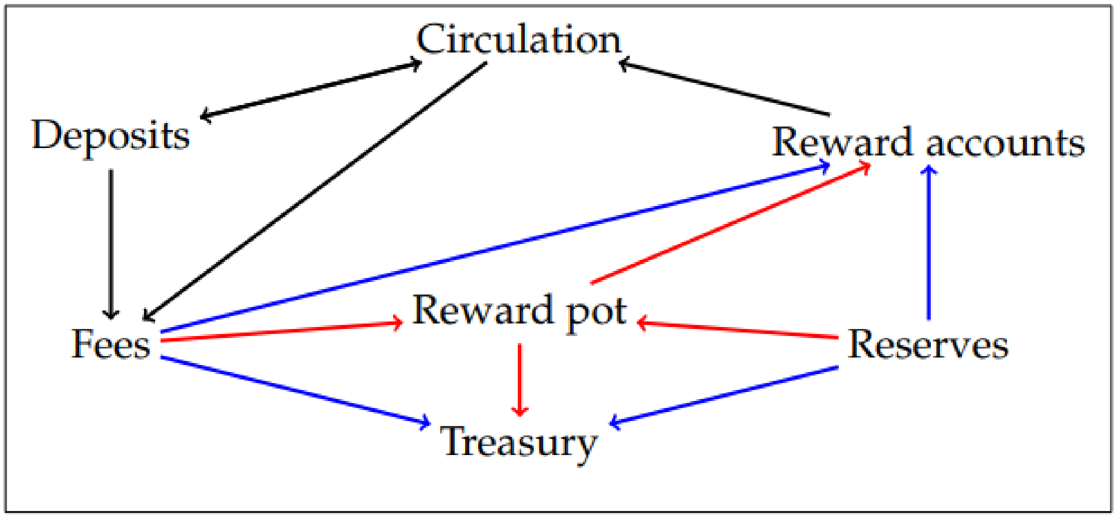
As you can see in the image, over time, in the simulation, the number of pools converge into a single pool.

Logically, one might surmise that geothermal, or government subsidized, pools would win in the long run. Doing a little research shows that this assumption is correct. Eva Xiao states that, "In 2016, for instance, overcapacity from hydropower stations in Sichuan and Yunnan amounted to a whopping 45.6 terawatt hours [of Bitcoin electricity usage]. To put that into perspective, the entire US generated 4,100 terawatt hours of electricity in the same year." As of 2019, 81% of Bitcoin miners are from China. To the visionaries of a novel cryptocurrency based future, that number should sound very troubling.

Cardano's underlying governance model will be significantly more distributed. So how exactly does the Cardano Proof of Stake model work?

Philipp Kant says, "The basic design of Ouroboros is remarkably simple: time is divided into discrete increments, called **slots**, and slots are grouped into longer periods, called **epochs**. At the start of each epoch, a lottery determines who gets to create a block for every slot. Instead of this lottery being implicit, i.e., whoever gets a right hash first wins, the lottery is explicit: a generated random number determines a slot leader for each slot, and the chances of winning for any given slot are proportional to the stake one controls."

The Incentives and Staking in Cardano page says that, "A slot lasts 20 seconds, while an epoch contains 21,600 slots and lasts five days." The probability of being elected a slot leader is proportional to one's stake. The combination of transaction fees and monetary expansion (i.e., reserve funds) are transferred to the reward pool and distributed among stakeholders who were active during that epoch. A portion of the rewards will be allocated to the system's treasury for later use as determined by future governance.



Source: Corduan et al., A Formal Specification of the Cardano Ledger.

There is no minimum stake required to participate, however, users with small stakes will benefit from joining a competitive pool. Pool operators are incentivized to reveal the true cost of their operations by the fact that they are also rewarded as members of the pool in addition to their profit margin. This keeps the incentives of a pool operator aligned with that of its members. The reward function is proportional to the total stake in the pool; this function increases rewards more quickly in the initial phase of the start of new stakers joining a pool, while smoothing out over time. Sebastien Guillemot explains this process in his video review of staking incentives.

The underlying reward scheme is a fundamental piece that secures the protocol and ensures effective decentralization. You don't want a reward scheme that people can game and you don't want a tiny percentage of stake controlling the entire system. Brünjes et al. state in *Reward Sharing Schemes for Stake Pools*, "that the [reward] mechanism can provably lead to a Nash equilibrium with desirable decentralisation characteristics that include a high number of protocol actors and Sybil attack resilience."

So what exactly is a Nash equilibrium? A basic definition says that, "In terms of game theory, if each player has chosen a strategy, and no player can benefit by changing strategies while the other players keep theirs unchanged, then the current set of strategy choices and their corresponding payoffs constitutes a Nash equilibrium." Mutually Assured Destruction is probably the most simplistic, and widely understood, example of this. Cardano ensures that staking pools do not become centralized by introducing what is called a "saturation point," at which rewards are essentially capped. Past the saturation point, rewards will decrease, incentivizing new stakeholders to seek other pools. Rewards are distributed in such a fashion that staking pools do not benefit from competing with one another; this eliminates the incentive for one pool to sabotage the work of another.

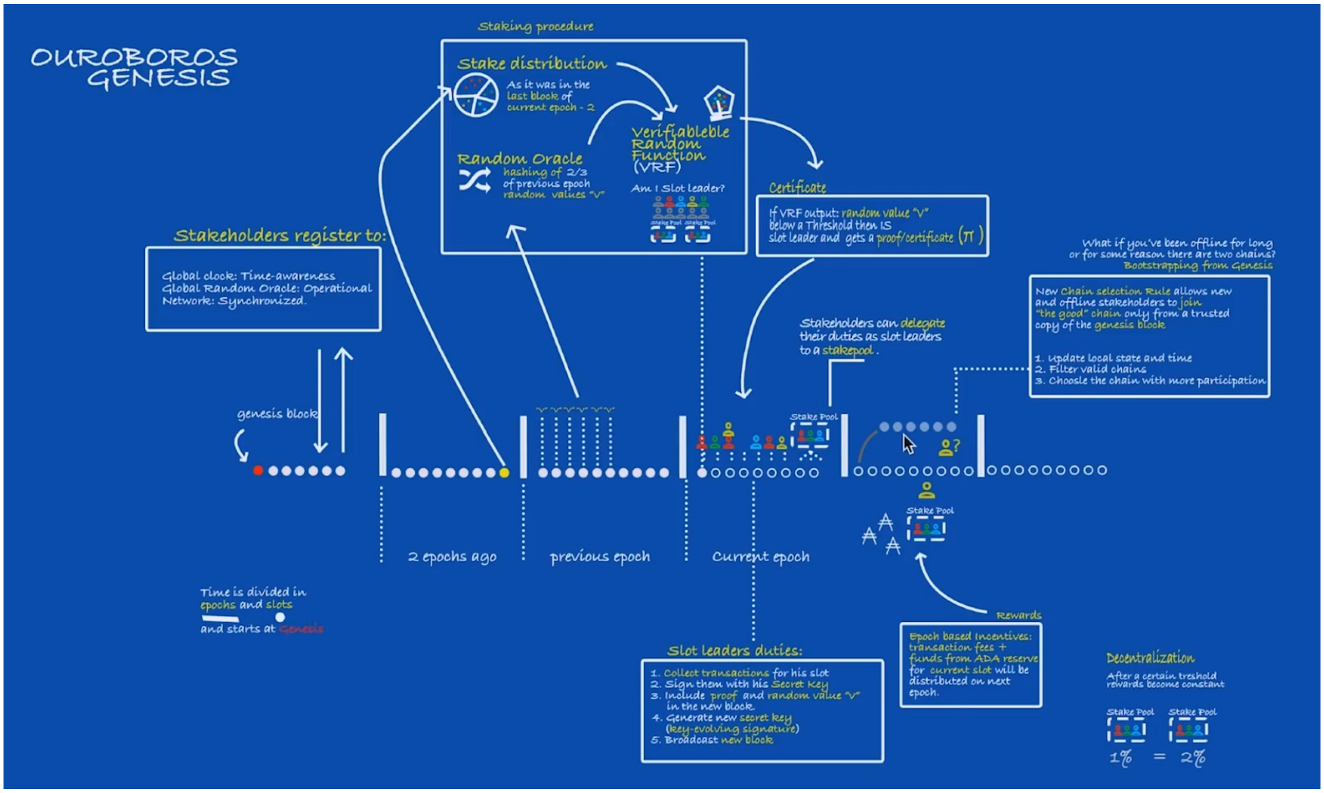
Users will be able to see a pool's desirability rating, provided it will become a successful , saturated, pool. The system attempts to optimize a non-myopic Nash equilibrium and behavior. That means it encourages stakeholders to look at the long term consequences of their choices and choose the strategy that will be in their best interest. It also means that pools will achieve an equilibrium such that stakeholders will not benefit from changing their staking strategy.

Rewards are not distributed per block, like in Bitcoin, but rather per epoch through a "reward pool." Rewards are proportional to the amount of stake you have, in addition to the number of slots/blocks you were able to contribute to during that epoch. Rewards come from transaction fees in addition to funds from the ADA reserve. The funds given away from the reserve will, over time, lessen as they are handed out. The exact percentage of funds that will come from the reserve account is yet to be decided.

EMURGO will be releasing a Staking Simulator for the Seiza blockchain explorer; you will be able to calculate your rewards with the simulator and it will be integrated with Yoroi as well. You will be able to stake from the Yoroi browser extension as well as the Yoroi mobile application.

The Cardano staking system fundamentally works to incentivize two primary activities. The first is making sure that stakeholders are online. The second is participation in the protocol, i.e., block creation. Because there are many people who are either unable to run their own servers with 24/7 uptime or who don't want to create a stake pool, they will be able to delegate their stake to a pool of their choice. Delegation addresses are different from standard ADA addresses.

Unlike Ethereum, or other staking protocols, users funds are not at risk of being "slashed" or destroyed in case they attempt to participate in the protocol in an inappropriate fashion; the design of the system makes that unnecessary. The number of staking pools is something that will likely change over time as the system scales; the initial goal is to have 100 pools and then expand to 1,000 pools. Balancing the need for a decentralized system with performance overhead will be important.


OUROBOROS GENESIS
Staking procedure
Stake distribution
As it was in the last block of current epoch - 2
Random Oracle
hashing of 2/3 of previous epoch random values "V"
Verifiableble Random Function (VRF)
Am I Slot leader?
Stake Pool
Stake Pool
Certificate
If VRF output: random value "V" below a Threshold then IS slot leader and gets a proof/certificate (π)
Stakeholders register to:
Global clock: Time-awareness
Global Random Oracle: Operational
Network: Synchronized.
What if you've been offline for long or for some reason there are two chains?
Bootstrapping from Genesis
New Chain selection Rule allows new and offline stakeholders to join "the good" chain only from a trusted copy of the genesis block
1. Update local state and time
2. Filter valid chains
3. Choosle the chain with more participation
Stakeholders can delegate their duties as slot leaders to a stakepool.
genesis block
Stake Pool
2 epochs ago
previous epoch
Current epoch
Stake Pool
Time is divided in epochs and slots
and starts at Genesis
Rewards
Slot leaders duties:
1. Collect transactions for his slot
2. Sign them with his Secret Key
3. Include proof and random value "V" in the new block.
4. Generate new secret key (key-evolving signature)
5. Broadcast new block
Epoch based Incentives: transaction fees + funds from ADA reserve for current slot will be distributed on next epoch.
Decentralization
After a certain treshold rewards become constant
Stake Pool
Stake Pool
1% = 2%

Source: Lopez De Lara, Carlos. Explaining OUROBOROS, the protocol implemented in the Cardano Shelley testnet. Click here for FULL PICTURE.

Ouroboros will use Verifiable Random Functions in order to select unbiased slot leaders. During each epoch, random numbers are written to the blockchain; those numbers provide a mechanism to randomly select future slot leaders. In essence, this mechanism signifies the symbology behind the Ouroboros name: a snake eating its own tail. Nir Bitansky says, "Verifiable random functions (VRFs) are pseudorandom functions where the owner of the seed, in addition to computing the function's value y at any point x, can also generate a non-interactive proof π that y is correct, without compromising pseudorandomness at other points." Sebastien Guillemot explores the underlying mathematics and assumptions behind these functions in his self titled, and thorough, educational video.

Ouroboros Praos will also use Key Evolving Signatures. Matt Franklin says, "The security of cryptosystems depends on keeping secret keys secret, but this is quite hard to achieve in the real world. The essential feature of this design strategy is that the secret key changes over time, while the corresponding public key remains unchanged." Everytime a block is created, a new private key will be used, even though the public key remains the same. So attackers, who have compromised someone's private key, can not forge transactions like they would be able to with Bitcoin.

Ouroboros Praos, by David et al., clearly explains this concept: "In regular digital signature schemes, an adversary who compromises the signing key of a user can generate signatures for any messages it wishes, including messages that were (or should have been) generated in the past. Forward secure signature schemes [BM99] prevent such an adversary from generating signatures for messages that were issued in the past, or rather allows honest users to verify that a given signature was generated at a certain point in time. Basically, such security guarantees are achieved by 'evolving' the signing key after each signature is generated and erasing the previous key in such a way that the actual signing key used for signing a message in the past cannot be recovered but a fresh signing key can still be linked to the previous one."

Jormungandr is the name for the Cardano rust node. If you are interested in installing the Shelley testnet you can watch this short video walkthrough by IOHK developer, and project manager, Alejandro Garcia. If you are not comfortable building from the source files you can also simply download the release file as shown in this video here. Conversely, you can follow the directions on the Shelley testnet repository. The Jormungandr User Guide is still under development, but should be used as a future reference for understanding the technical details of the Ouroboros protocol.

A number of other cryptocurrency designers have attempted to implement various forms of Proof of Stake, but not all matching the grand vision of Cardano's PoS system. Below we briefly highlight shortcomings of both Tezos and EOS.

Tezos

8,000 Tezos (XTZ) are required in order to participate in the staking protocol as a block producer; otherwise, without meeting the minimum requirement, you can delegate your stake. Tezos allows up to 80,000 validators. One risk inherent in Tezos is that validators may not necessarily pay out rewards to stakeholders. This is because reward payouts are not automatically managed by the protocol, but rather by stake pool operators. With Tezos, as a stakeholder, you absolutely need to do your due diligence to ensure that you get paid. With Cardano, you naturally fit into an ecosystem that will be more secure and guaranteed to be more honest.

EOS

EOS, on the other hand, is highly centralized with only 21 block producers. They reserve the right to freeze accounts and create transactions unauthorized by users and have done so in the past in order to recover stolen funds. While this last point may have certain benefits it is not appropriate for a permissionless mainchain and should be relegated to specific, regulatory compliant, sidechains. Furthermore, such a system does not realistically allow for settlement of off-chain derivatives, or any kind of, legitimate, trade finalization.

Unlike Cardano, EOS uses stake as voting power necessary to elect representatives of equal power. Brünjes et al. says, "This type of scheme differs from ours in that (i) the incentives of voters are not taken into account thus issues of low voter participation are not addressed, (ii) elected representatives, despite getting equal power, are rewarded according to votes received; this inconsistency between representation and power may result in a relatively small fraction of stake controlling the system (e.g., currently EOS delegates representing just 2.2% of stakeholders are sufficient to halt the system, 2 which ideally could withstand a ratio less than 1/3), (iii) it may leave a large fraction of stakeholders without representation (e.g., in EOS, currently, only 8% of total stake is represented by the 21 delegates)."

Given these statistics, and the aforementioned fact about freezing accounts, we believe that Cardano's PoS system and grand vision present large advantages over EOS' technology.

Conclusion

Cryptocurrency is still in such a nascent phase that many institutions still do not truly understand the promise of a decentralized, permissionless, and trustless network. A recent article on asset tokenization by ING researcher Carlo Cocuzzo, sums up this sentiment quite succinctly. He says, "Even in a fully decentralised world where transactions take place on a public blockchain ledger, there needs to be trust in the algorithm, or the coder who designed it. It is difficult to see how a fully decentralised model might work given these issues, which then leaves the door open to trusted intermediaries such as banks and investment funds." The institutions clinging to what has worked in the past will likely face a very difficult transition into the trustless present and decentralized, peer-to-peer, future.

The fundamental conceptual decision comes down to whether to trust mathematics or the full faith and credit of legacy institutions. In this light, Cardano is truly upon the ever-evolving edge of the arc of history. The release of Shelley represents tremendous transformative potential coming to fruition. Proof of Stake is a core part of the puzzle; however, in order to truly be competitive, Cardano will offer significantly more advanced features such as smart contracts, user issued assets, and interoperability with foreign Proof of Work blockchains through NiPoPow.

Looking ahead to the future, it is important to ask yourself: what is your plan for staking? Will you operate a pool or delegate your stake? If you are a developer who is interested in integrating staking into your application or wallet then you will want to browse the js-chain-libs repository, which contains the WASM bindings for Jormungandr.

|| **Click here to subscribe to the EMURGO Newsletter** ||

EMURGO drives the adoption of Cardano and adds value to ADA holders by building, investing in, and advising projects or organizations that adopt Cardano's decentralized blockchain ecosystem. EMURGO leverages its expertise in blockchain R&D as well as its global network of related blockchain and industry partners to support ventures globally.

EMURGO is the official commercial and venture arm of the Cardano project, headquartered in Singapore, with a presence in Japan, the USA, India, and Indonesia. EMURGO works closely with IOHK and The Cardano Foundation to grow Cardano's ecosystem globally, and promote its adoption. Learn more about the project at https://emurgo.io

Follow EMURGO on Social Media
・Official Homepage: emurgo.io
・Twitter (English): @emurgo_io
・Twitter (Japanese): @Emurgo_Japan
・Youtube: EMURGO
・Telegram: EMURGO Announcements
・Facebook: @emurgo.io
・Instagram: @emurgo_io
・LinkedIn: @emurgo_io

About Yoroi Wallet
・Yoroi Twitter: @YoroiWallet
・Yoroi Homepage: https://yoroi-wallet.com/

About Cardano
・Cardano Forum: https://forum.cardano.org/
・Cardano Telegram: https://t.me/CardanoGeneral
・Cardano Reddit: