Sentient Chain

A succinct, permissionless, decentralized NIPoPoW blockchain built specifically for play to earn games

https://sentientfoundation.com

Joseph Moran
(Cofounder)
Joseph@sentientfoundation.com

Christian Costantino
(Cofounder)
Christian@sentientfoundation.com

June 3rd, 2022
v1.0

"If I have seen further, it is by standing on the shoulders of Giants."
Isaac Newton, 1675

Abstract

Sentient Chain is the amalgamation of more than a decade of blockchain research and development from an innumerable number of individuals hailing from every corner of the globe. At the end of 2021, cryptocurrency secured its integral position in the financial world with a total market cap exceeding 2.5 trillion dollars. Today, blockchain technology is a recognized academic discipline in many prestigious universities around the world. Blockchain technology has truly come a long way since "Bitcoin: A Peer-to-Peer Electronic Cash System" was first published in 2009; however, there is still a great deal of work to be done.

At the Sentient Foundation, we believe that an academic, collaborative, and prudent approach is the only way to build on Nakamoto's revolutionary work. Fortunately, prominent leaders in the space have solidified blockchain technology as a fundamental pillar of change in our society.

Derived from research conducted by organizations such as IOHK, the Ergo Foundation, the University of Edinburgh, and the University of Athens, we propose a succinct, permissionless, decentralized network which utilizes a novel Proof-of-Less-Work (PoLW) consensus mechanism built within the Ergo UTXO-based ecosystem. Furthermore, we established the groundwork for the next generation of efficient, scalable, and secure blockchain protocols with our implementation of a Non-Interactive Proofs of Proof-of-Work (NIPoPoW) secured sidechain centered around play to earn gaming. Finally, our symbiotic and efficiency centric approach to consensus establishes a new paradigm for Proof-of-Work (PoW).

Introduction

Digital ownership can be esoteric and difficult to understand at first, but our society has been dealing with digital ownership since the advent of the internet. Digital ownership is an individual's right to own their digital fingerprint and associated digital assets. Blockchain technology has allowed digital ownership to become trackable, immutable, and more ubiquitous than ever before. Digital assets can be separated into two main categories: fungible and non-fungible. Fungible assets are analogous to the dollar; where each dollar has a different serial number, but regardless of its identifier each dollar is equivalent in value. These assets can be exchanged like-for-like. Non-fungible assets are analogous to digital collectibles: trading cards, digital images, videos, virtual real estate, domain names, art, music, games and much more.

Our focus at the Sentient Foundation is to establish a NIPoPoW secured sidechain centered around play to earn gaming within the Ergo ecosystem. Sidechains are a mechanism for cross-chain communication and allow smart contracts on one blockchain to receive and react to events that take place on another blockchain. This all is accomplished without the need of a trusted third party.

Video games have been around for decades and provide countless hours of entertainment for children and adults. It is estimated that there are over 2 billion gamers worldwide, which accounts for 26% of the world's population. In 2020, the gaming industry generated 155 billion dollars in revenue and by 2025 analysts predict the gaming industry will generate more than 260 billion dollars in revenue. However, as considerably successful the gaming industry has become, it is also extremely centralized with only a few companies dominating the market. This has led to stagnation of innovation and in some cases straight monopolies over certain gaming genres. Steam, the most popular PC game client, demands a 30% revenue share from game developers, exacerbating the lack of innovation in the gaming industry. Even blockchain gaming companies like Ultra who present themselves as game developer friendly platform take 15% revenue of games developed on their platform.

Therefore, we propose Sentient Chain which is a NIPoPoW secured Ergo sidechain with game developers, crypto miners, and gamers in mind. Play to Earn gaming has been on the rise since 2020 and will only continue to garner attention and momentum going forward (Figure 1,2). The concept of being able to sell a skin bought in Fortnite or a card bought Yu-Gi-Oh Master Duel is an idea every gamer can get behind.

Figure. 1: Worldwide Google searches for "NFT", "Play-to-earn" and "Metaverse". An index equal to 100 indicates the maximum popularity during the analysed period.

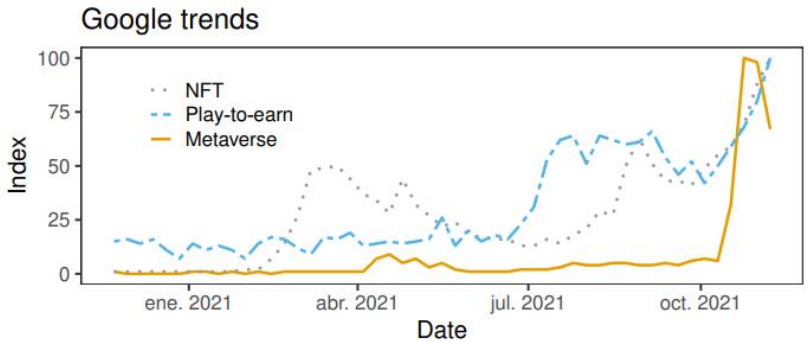


Figure. 2: Number of tokens created over time: a) Play-to-earn, b) Metaverse, c) Metaverse & Play-to-earn.

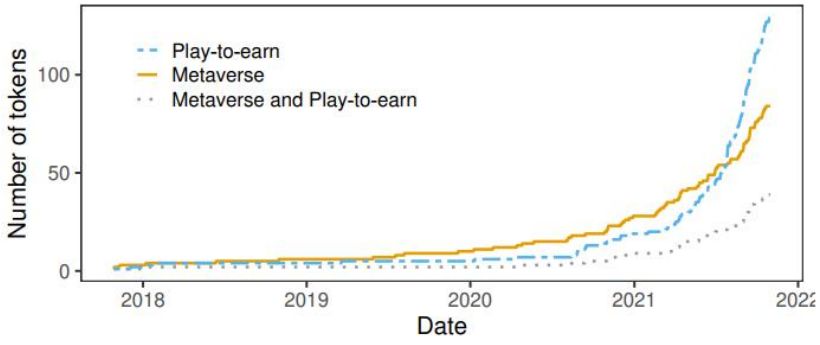


Figure 1, 2. These figures are from research conducted by David Vidal-Tomas, Department of Economics, Spain.

The Social Contract

What drew our team to the Ergo ecosystem was their core principles. These principles are referred to as "Ergo's Social Contract". We have expanded and tailored these principles to align with what we are trying to build with the Sentient Chain. The Bitcoin ethos is at the heart of the social contract and is the life blood for the indelible positive impact blockchain technology has initiated. Our mission is to establish a sidechain specifically for blockchain play to earn gaming.

True Decentralization. The Sentient Chain must be as decentralized as possible. This extends to social leaders, software developers, hardware manufacturers, miners, and any other entity associated with the network. Infrastructure will be established for the community to take action on in order to decrease the impact of malicious actors.

Blockchain For the People By The People. The Sentient Chain is a network for the people regardless of race, creed, national origin, or socioeconomic status. We will accomplish this by utilizing a multifaceted approach. First and foremost, the prevention of the centralization of miners so any individual may participate in the protocol by running a full node and mining blocks. Additionally, protocols and governance will be in place to allow any game developer a chance to launch their game on the Sentient Chain. Finally, we plan to build the Sentient Chain to run on any modern computer and to keep the barrier of entry as low as possible for everyday users.

The Right to Repair. We at the Sentient Foundation will establish procedures and protocols that allow anyone to build one of our gaming devices, which also act as a full node for our network. Furthermore, all our code is open source, and we plan to release schemas of all devices developed by our organization. These devices will be constructed in a modular manner and easy to repair and replace individual components.

Platform For Play to Earn Blockchain Gaming. The Sentient Chain is a sidechain to Ergo with NIPoPow implemented to decrease the hardware cost needed to participate in the network. Furthermore, with our efficiency focus the Sentient Foundation's goal is to establish a more environmentally friendly PoW mechanism, which other chains can adopt.

Long Term Focus. The Sentient Chain is developed with focus on long term survivability, adaptability, and impact. Here at the Sentient Foundation our focus is to establish infrastructure for individuals to build on for generations. This includes providing educational resources for anyone to access and learn about blockchain technology as a whole.

Succinct and Permissionless. Sentient Chain's protocol allows anyone to join the network and participate without any preliminary actions. This aligns with the protocol Ergo developed. However, play to earn games that are launched on the Sentient Chain must provide a minimum viable product (MVP) and go through a community vetting and voting procedure. Play to earn games sold on the Sentient Chain will only be charged 5% of their revenue. This nominal fee will be used to further develop our storefront and assist indie game developers.

Sentient Chain

The Sentient Chain is a hard fork of Ergo with the implementation of NIPoPoW. The Sentient Chain utilizes the same consensus protocol as Ergo, called Autolykos, which allows miners to dual mine Erg and Sent which will add value and security to both blockchains. Autolykos is the first consensus mechanism that is both memory-hard and pool-resistant. Moreover, Sentient Chain uses Ergo's state logic. The client uses a ledger state snapshot from its history instead of using the ledger with all the

transactions that happened before the current one. This methodology follows Bitcoins UTXO design and represents the snapshots using one-time coins. The major difference from Bitcoin is that Ergo's one-time coin, called a box, contains user defined data in addition to monetary value and protecting script. These boxes also store an authenticating digest, called the stateRoot, of the global state after applying the block. A box is made of up to 10 registers labeled R_0,R_1,…..,R_9 which the first four are filled with mandatory values, while the rest may contain arbitrary data or remain empty.

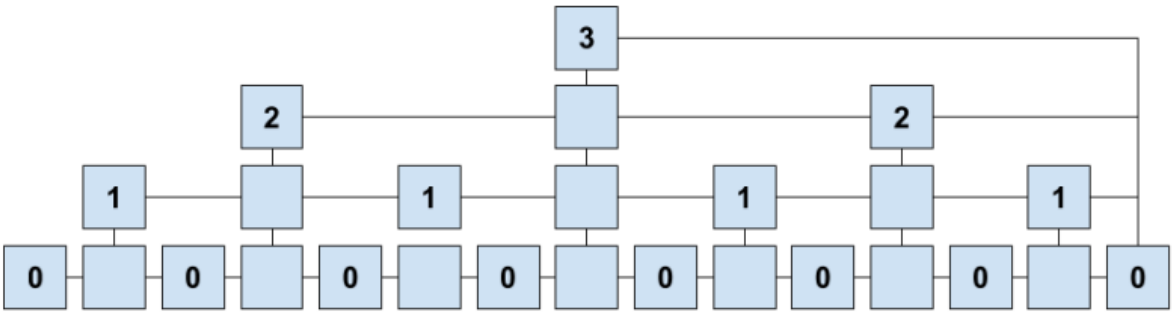
The implementation of AVL+ trees allow for efficient authenticated dictionaries that reduce the proof size and speed up verification by a factor of 1.4 - 2.5. This is highlighted by our proofs being 3-fold smaller than proofs of a Merkle Patricia tree used in Ethereum. Therefore, Sentient Chain chose to utilize Ergo's state and consensus mechanism because it provides an efficient and secure way to prove existence or non-existence of elements within it. In addition to proofs of tree modifications which allow for the implementation of sophisticated contracts.

Briefly, NIPoPoWs are short stand-alone strings that a computer program can inspect to verify that an event happened on a PoW blockchain without the need for connecting to the blockchain network and without downloading every block header. This technology allows for efficient lightweight simplified payment verification (SPV) wallets and full nodes. While SPV clients need to download half a million block headers, NIPoPoW nodes only need around 250 block headers. The sample size for NIPoPoW clients changes but does not grow much in size, as the blockchain grows larger by the years. Even after decades of data has been accumulated. This technology aligns with the Sentient Chain which has an emission schedule that lasts 24 years from the genesis block.

The most compelling use case for NIPoPoW is that it allows blockchains to communicate and interoperate just like APIs. When miners run a blockchain they do not monitor other blockchain networks since this is difficult to do without short proofs. However, if a blockchain supports smart contracts like Ergo, a contract can be written to validate a NIPoPoW which will check that something happened on another blockchain and react to it. This allows the Sentient Chain to work as a sidechain to Ergo. Expanding on this idea, one could create sidechains specific for individual data types, like storage of important historical data, gaming data (Sentient Chain), financial data, and more. This mitigates the load the mainchain must handle, decreasing network congestion and allowing for secure and fast transactions. However, proof about a blockchain can only be produced if the blockchain supports NIPoPoWs in its blocks. This support can be added retroactively without the need for a soft or hard fork and without requiring miners' approval with velvet forks. This makes for malleable blockchains that can adapt quickly to the everchanging blockchain landscape. Ergo has had support for NIPoPoW since its genesis.

NIPoPoW works based on the observation that some blocks achieve a better mining target than others. The core concept of NIPoPoW is that the entire list of block headers does not need to be presented to the network since these blocks capture cumulative difficult on average. Therefore, if a blockchain portion has 128 blocks then on average half of them, 64 blocks, will have an extra zero in the binary representation of their hashes, a quarter, 32 blocks, will have two zeros and so on. Thus, a blockchain can be compressed by only sending these blocks on the network. Figure 3 illustrates the average distribution of blocks using NIPoPoW. The bottom demonstrates the native blockchain and higher-level superblocks show 1, 2, or 3 extra zeros in their hashes. Taking only these blocks forms a super chain. If these superblocks are presented in the form of a proof, each must include a pointer to its previous block. This is no different than regular blocks that include a pointer to the previous block. The connectivity described is called interlinking and is the reason velvet forks are required.

Figure 3. The hierarchical blockchain. Higher levels have achieved a lower target, higher difficulty, during mining. This figure is from Aggelos Kiayias et al, Non-Interactive Proof of Proof-of-Work. 2018



SENT Native Token

Sentient Chain has its own native token, Sent, which was modeled off the Ergo platform's native token, Erg. Like Erg, Sent is divisible to up to 10^9 units and following in the footsteps of Erg theses smallest units are called nanoSent, which is one billionth of a Sent. Sent is the backbone of the Sentient Chain.

The inauguration phase of the Sentient Chain protocol, miners will receive block rewards in Sent according to codified predefined token emission schedule. These coins incentivize miners to participate in the consensus mechanism which secures the Sentient Chain. Additionally, miners will have the ability to dual mine Erg and Sent coins, which adds value and security to both networks. A fixed-rated transaction fee of 0.01 Sent will go to miners and help prevent against spam attacks. Besides network and computational resources, a transaction consumes storage by increasing the state size. The element of the state is stored in a UTXO called a box, same as in Ergo. Once a box is created it possibly lives forever without any compensation to miners and node users. This state is kept in high-cost random-access memory (RAM). To mitigate this misalignment of incentives facilitated by a continuously increasing state size, a storage rent component periodically charges users Sent for bytes included in the state. This storage rent mechanism makes the system more stable by limiting state size, returning lost coins into circulation, and providing an additional reward to miners.

Therefore, the Sentient Chain platform is apt for building applications, specifically gaming applications, that have a monetary system that incentivizes their users. Participating in this system requires Sent, thus users will be highly incentivized to mine, purchase, use and save Sent if they deem the applications built on Sentient Chain to be valuable.

The inauguration phase will last two years, and miner facilitated on-chain voting will be implemented to make the Sentient Chain malleable to the ever-changing global economic landscape.

Emissions

There will only ever by 568.9 million Sent tokens in existence. These are presented in the initial state and are distributed in boxes. Sent will be a fair launch with no premine, no private sale and no ICO. Sentient Chain implemented the same no premine proof logic as Ergo. This proof of no premine box contains exactly one Sent, which is protected by a script preventing it from being spent by anyone. Its purpose is to prove Sent mining was not started privately by anyone prior to the official launch date. Additional registers of this genesis block contain the latest headline from the media in English, Russian and Cantonese, as well as the latest block identifiers from Bitcoin, Ethereum and Ergo.

The foundation treasury is a box that contains 9,481,824 Sent which makes up 1.67% of the total Sent max supply. During blocks 1-2,102,400, the first 2 years, 4.1 Sent will be released each block. After the first 2 years, no Sent will be released to the foundation. This design keeps the foundation's Sent

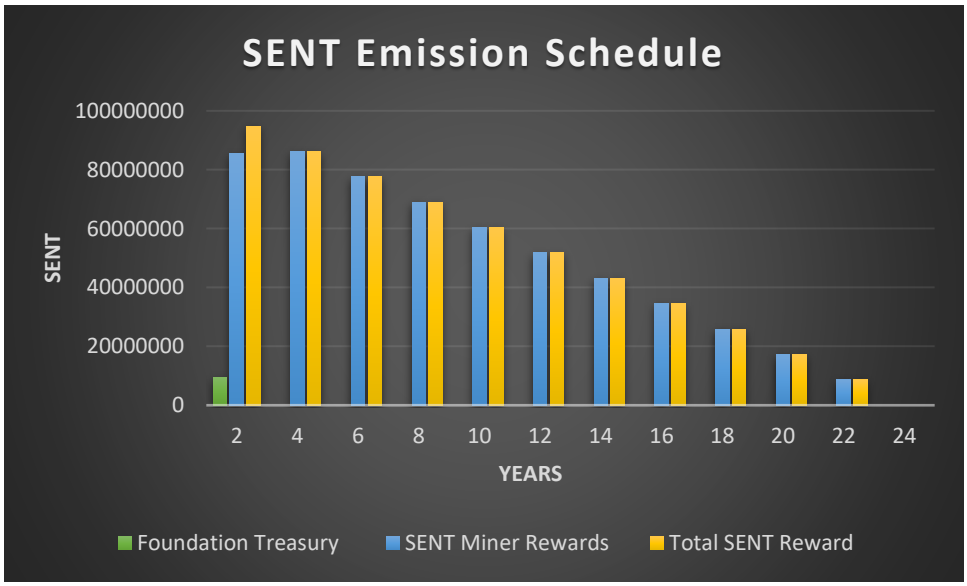
allocation to less than 10% the total circulating supply. This treasury will be used for development and implementation of the Sentient Chain. The first year the funds will be managed by the founders. After the treasury utilization will be voted on by the community in a decentralized manner. The community voting mechanics are still under development.

The miner reward box contains 559,427,616 Sent that will be distributed to block miners as a reward for their proof of work. Its protective script follows the same logic as Ergo, which requires the spending transaction to have exactly two outputs with the following properties:

The first output is protected by the same script and the number of Sent in it should be equal to the remaining miners rewards. During blocks 1-4,204,800, the first 4 years, miners will be rewarded 41 Sent per block mined. After that the block reward will be reduced by 4.1 Sent every 2,102,400 blocks until it reaches zero at block 25,228,800, roughly 24 years from the genesis block.

The second output should contain the remaining coins and can be spent by a miner that solved the block PoW puzzle but no earlier than 480 blocks after the current block.

Figure 4. Mining Reward Emission Schedule



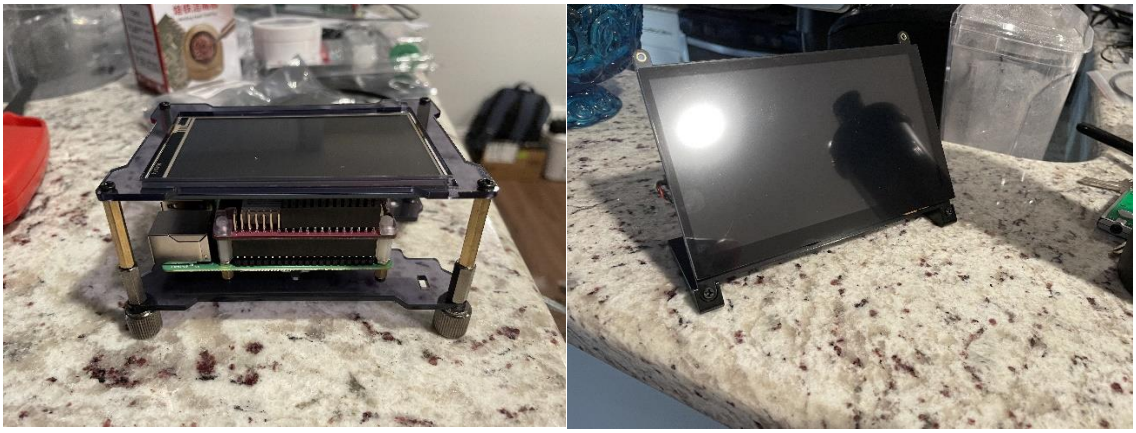
Gaming Nodes

At its core the Sentient Chain is a PoW blockchain and is based on the prover and verifier model. Unlike traditional blockchain clients which verify the entire linearly growing chain, the Sentient Chain is based on NIPoPoW and requires resources logarithmic to the length of the blockchain. Therefore, NIPoPow are succinct proofs and require only a single message between the prover and verifier of the transaction. This model is constructed of three roles: verifier clients, full nodes provers, and miners. Full nodes can be thought of as miners with zero hashpower and maintain the longest blockchain without mining. Full nodes act as the provers in the network. Miners try to mine new blocks on top of the longest known blockchain and broadcast them as soon as they are discovered. Verifiers are stateless clients that connect to provers and ask for proofs regarding which blockchain is the longest.

Currently, there is no monetary incentive for running a node in traditional PoW model. However, Nodes are integral to the security of transactions conducted on the blockchain and play an important role in the decentralized distribution of the ledger. Therefore, we propose using full clients as game clients, such as steam, in addition to their primary role as provers for the network. Incentivizing users to run a

client that also acts as a full node to participate in play to earn on the Sentient Chain. This will increase decentralization, security, and confirmation time for transactions. In addition to adding utility to nodes which are typically overlooked by individuals in the blockchain community. Below are two prototypes developed using Raspberry Pi 4B 4GB which can serve as a full node and game client for retro games the first step in making nodes that are portable gaming devices. These prototypes have comparable specs to the Nintendo Switch.

Figure 5. A 5” and 7” screen prototype for low-cost gaming devices that also run full nodes. Each where constructed with Raspberry Pi 4B in a modular manner to make replacement/repair inexpensive.



Discussion

Proof of stake (PoS) chains have been under a barrage of hacks in the past 6 months. From the 625-million-dollar Axie Infinity-Ronin hack, the Terra Luna nightmare, and the countless hacks on Solana, it’s becoming painfully obvious that PoS is intrinsically flawed. Albeit, PoW has stood the test of time so far, its energy consumption and expensive hardware has hamstrung its success. With the implementation of novel PoW mechanisms like NIPoPoW and PoLW, PoW can become the light on the hilltop it once was.

References

2009. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org
2019. Ergo Developers. A Resilient Platform For Contractual Money. Ergoplatform.org
2019. Ergo Developers. ErgoScript, a Cryptocurrency Scripting Language Supporting Noninteractive Zero-Knowledge Proofs
2021. Kiayias et al. Mining in Logarithmic Space. IOHK, University of Athens
2018. Kiayias et al. Proof-of-Work Sidechains. IOHK
2018. Kiayias et al. Non-Interactive Proof of Proof-of-Work. IOHK
2018. Zamyatin et al. A Wild Velvet Fork Appears! Inclusive Blockchain Protocol Changes in Practice. Imperial College London, UK
2022. Vidal-Tomas. The New Crypto Niche: NFTs, play-to-earn, and metaverse tokens. Department of Economics, Spain
2020. Wang. Proof of Less Work. Alephium.org

2018. Chepurnoy et al. A Systematic Approach To Crypto Fees. Ergoplatform, IOHK, Institute Jena, Germany
2022. Ultra. The Future of Digital Games Distribution. White Paper V1.7
2021. Beattie, How the Video Game Industry Is Changing. Investopedia