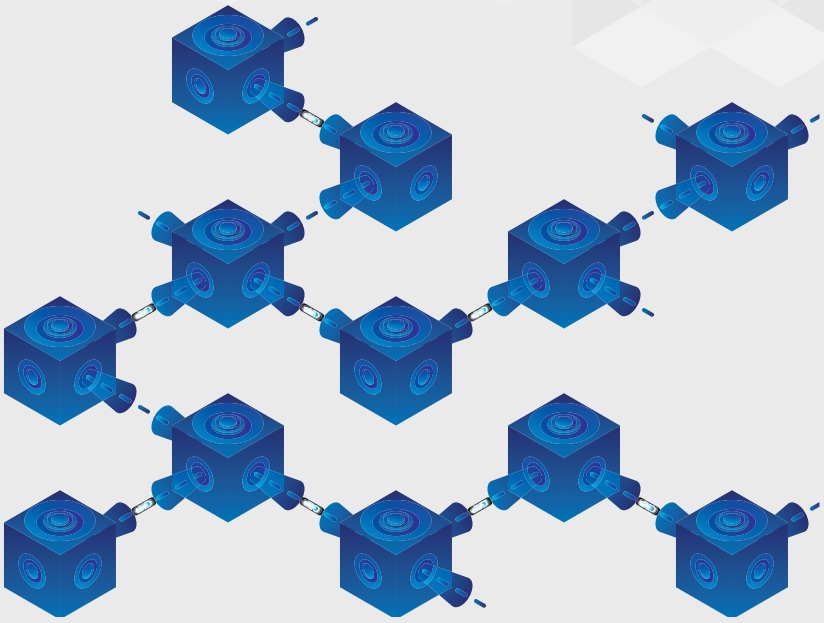
CPUchain: Fast and secure online payment network powered by CPUpower technology.



Min Khang Aung
info@cpuchain.org
www.cpuchain.org

CPUchain Core

Abstract

CPUchain is a widely distributed ledger and a new digital currency that enables modern citizen to receive and spend payments quickly, cheaply, and from anywhere with an internet connection, all without relying on banks, specialized mining hardwares, fraud, censorship, downtime, and centralized forces. CPUchain is fast, secure, and stable platform. We believe any payments created on CPUchain network should be considered as final and complete after 1 minute, no matter how much the payer sends for confirmation fee. Built on a fork of the Bitcoin Core code, CPUchain aims to build free and open-source, community oriented, self-governed platform. CPUchain doesn't have any premined, pre-allocated funds to pay founders, developers, wallet service providers, or exchange to compensate for building something on CPUchain. Instead, we believe anyone can participate on a network and earn reward, build a platform, increase value of CPUchain and pay themselves under fair and transparent, immutable network consensus.

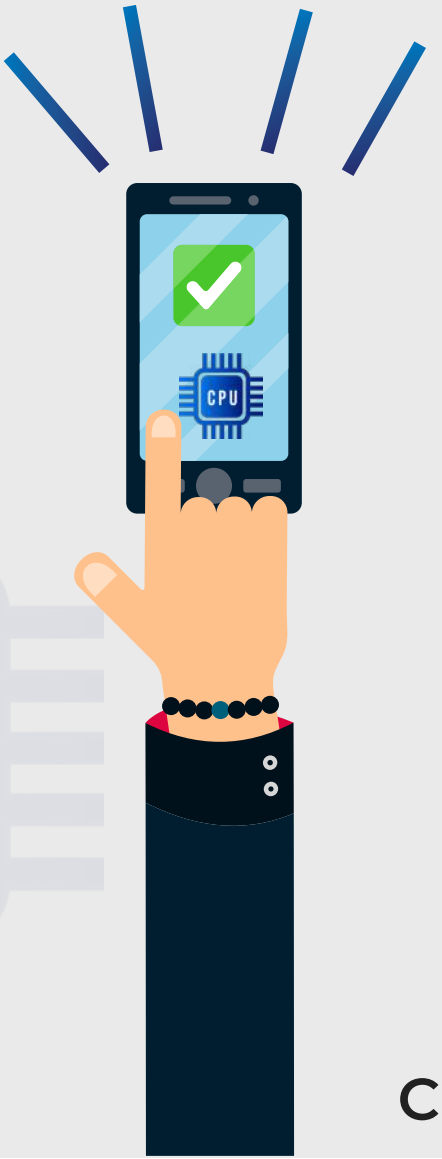
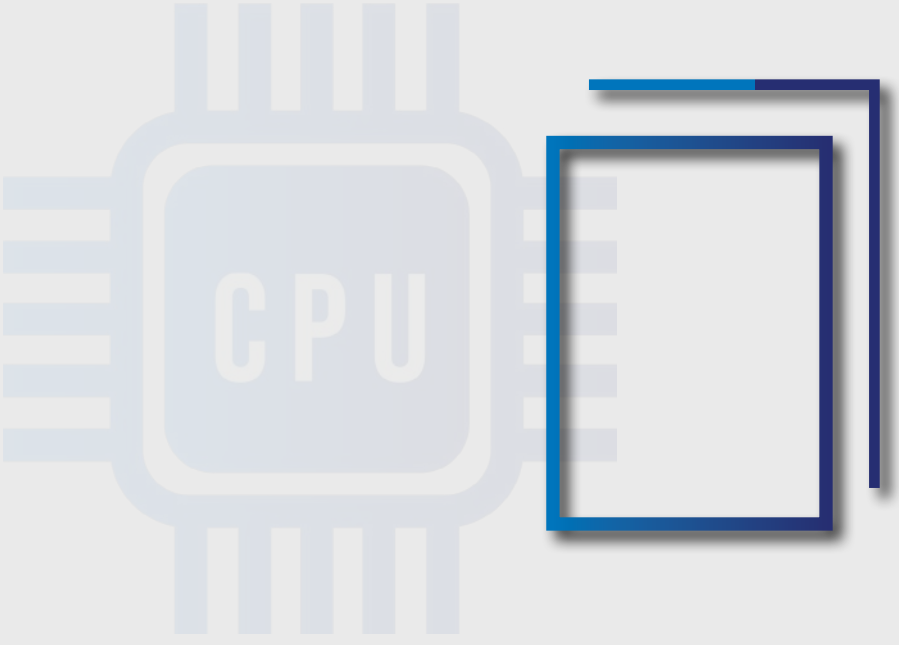


Table of Content



Introduction

What is a blockchain and why it is needed for modern internet? Blockchain, which literally means “chain of blocks”. In other words, it is a database, which in the literal sense of the word is a continuous chain of blocks and transactions and is stored simultaneously on many computers. New blocks in this database chain are constantly being generated by volunteers. Each new created block contains a group of recently accumulated and ordered records (transactions), as well as a header, merkle root, bits, nonce, etc.

Blocks are small unit of blockchain and a collection of various transactions, Transactions that are recorded on public blockchain are any actions that users perform on online network, whether shopping on ebay, paying bills, receiving a bounty, etc. When a transaction is formed by a user, it is sent to the so-called mempool, where it waits until it is being verified and stored to one of the blocks and it turns into a “confirmed” state when a block is formed via competitive mining action, it is checked by other participants of the network and then, if everyone agrees, is connected to the end of the chain. Once this happens, it is no longer possible to revert or modify the transaction where we consider the transaction is secure and immutable.

The technology of the blockchain forces you to take a fresh look at the exchange of values, documents, money, and services. It removes intermediaries and allows users to directly interact with them. That’s why Bitcoin, the first working product of blockchain, has no doubt of being the greatest invention comparable to the discovery of the internet.

Some known characteristics of public blockchain.

1. Decentralized
2. Immutable
3. Transparent

CPUchain leverages blockchain’s solution by adding security, scalability, and stability, which is essential and important in order to build a global currency and a payment network for real-world use and wide adoption.

The main tasks of CPUchain

CPUchain [CPU] is a digital cryptocurrency, which is a direct descendant of Bitcoin or Ripple and is based on the ideas of decentralized P2P network from Satoshi Nakamoto, a founder of Bitcoin.

The main objective of CPUchain is to restore the direct, core purpose of using Bitcoin, cryptocurrency as a store of value and means of exchange.

Bitcoin once used to provide a functionality of fast and cheap global payment network with a characteristic of decentralization without centralized issuer unlike legal tether or simple payment solution like Visa or Paypal. However, current bitcoin network is suffering from 1. Network scaling issue and 2. Network distribution issue which makes Bitcoin or any other cryptocurrencies no longer valuable as before.

Some other cryptocurrencies like Ripple or EOS tend to solve them via an alternative network consensus, however, those consensus algorithms are still not proven to solve centralization and security issues compared with the legacy POW scheme.

That's why CPUchain has improved upon Bitcoin by implementing CPUpower algorithm and Giga block solution to improve public blockchain's well-known weak point which is scalability and security. Without relying on side channel, side chain, non-blockchain solution to complement the network scalability, CPUchain has developed and adopted Giga block size solution, which was first proposed by scientists of Bitcoin Unlimited node, as an alternative of Segregated witness, lightning network proposed by Bitcoin Core and Blockstream company.

To enhance network security and stability, CPUchain uses CPUpower algorithm and LWMA difficulty adjustment rule for the coin's main POW consensus. CPUpower is an exclusive Proof-of-Work algorithm dedicated to CPUchain's new consensus. From the codebase of Yespower pow and Yescrypt hashing algorithm, CPUpower enables CPU friendly and GPU, ASIC, FPGA resistant mining environment which makes possible for CPUchain to issue and distribute only for miners who compute on commodity hardwares where the massive computing power is not only limited to specific hardware vendors but for the people who owns and uses computable devices from x86 desktop computer to arm-based smartphone processors. Anyone with some surplus computing resources may be able to participate on securing the network and receive some bounty in coins as a reward.

CPUchain aims to be a sound money itself, with support of cutting-edge Giga block scaling solution and CPUpower secure algorithm we believe as a complementary currency of Bitcoin, CPUchain can achieve its goal to become a global currency which billions of citizen worldwide can use as a next-generation banking system where low sending fees, instant transaction speed is possible.

CPUchain Core

Supply distribution

To become a sound money and a store of value without any form of guarantee, legal tether, commodity, security, debt, we make this happen as a form of open-source software without any kind of pre allocation of funds or any central authority.

To develop a new kind of currency it is important to have a prominent issuer and supply distribution in order to keep its value and use them as a means of exchange. Modern virtual payments like Paypal uses fiat money to exchange the value for buying goods, shopping on ebay, and security like stock implies an amount of share of corporation where businesses use them to distribute their annual income to major shareholders. Commodities like gold or silver, has its own value because they have finite supply and clear use case.

CPUchain's characteristics is more alike to commodities like gold than securities or legal tether. Full supply is minted by a competitive cryptographic computing activity to find blocks and verify transactions, generate nonce. Like gold or any other valuable commodities anyone can mine a cryptocurrency and trade, exchange them as a price of something. However, this doesn't solve a distribution problem that gold and bitcoin is suffering from. Gold and Bitcoin is only cost effective for mining when they are being mined by specialized hardwares that are exclusive for mining, any they cost a lot of energy resources which are not eco-friendly and waste of natural resources.
In contrast, minting of CPUchain doesn't require specialized hardwares for mining and it doesn't consume a lot of electricity like them. Technology are evolving toward less energy consuming path to protect our nature and addressing toward the distribution problem necessary for a digital currency to achieve widespread, grassroots adoption. As one engineer working on CPUchain, if the mining process is largely controlled by some specialized hardwares created by a far-off foreign manufacture, the coin seems "distant". Mining is an important way for user to participate in a digital currency's community and mining on commodity hardwares , like even the small amount of hardwares like smartphones and even raspberry pi opens the mining process up to a much larger group of community.

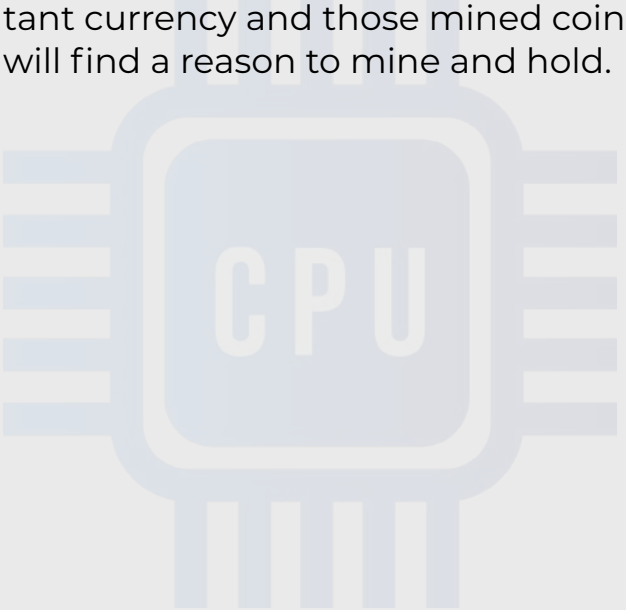
Another key component of CPUchain's approach to addressing the distribution problem is upholding a promise that originated from Bitcoin: that 100% of the coins would be distributed via the public mining process. Every single coin is both unique and identical, which forms an inherit value to be a currency. One of the main characteristics of currency is that it is fungible, full distribution from fair mining makes the coin unique and valuable from miners and the equality of each coin makes users possible to exchange something for their homemade, own mined coins. 100% of the total 105 million CPUchain coins will be allocated via the free market mining process.

But there are several other coins that also build upon the Bitcoin codebase and are also trying to address the distribution problem, what makes CPUchain's distribution structure so unique?

Other cryptocurrencies often have pre-allocation funds or some coins that are not minted via proof-of-work mining process. They often have pre-allocated funds to sustain the development of that coin or having a different consensus, reward distribution structure among pow to complement the disadvantages of proof-of-work mining. For example, proof-of-stake consensus or masternodes enable coin holders to mint coins without additional computing resources, so it is often considered as eco-friendly coin.

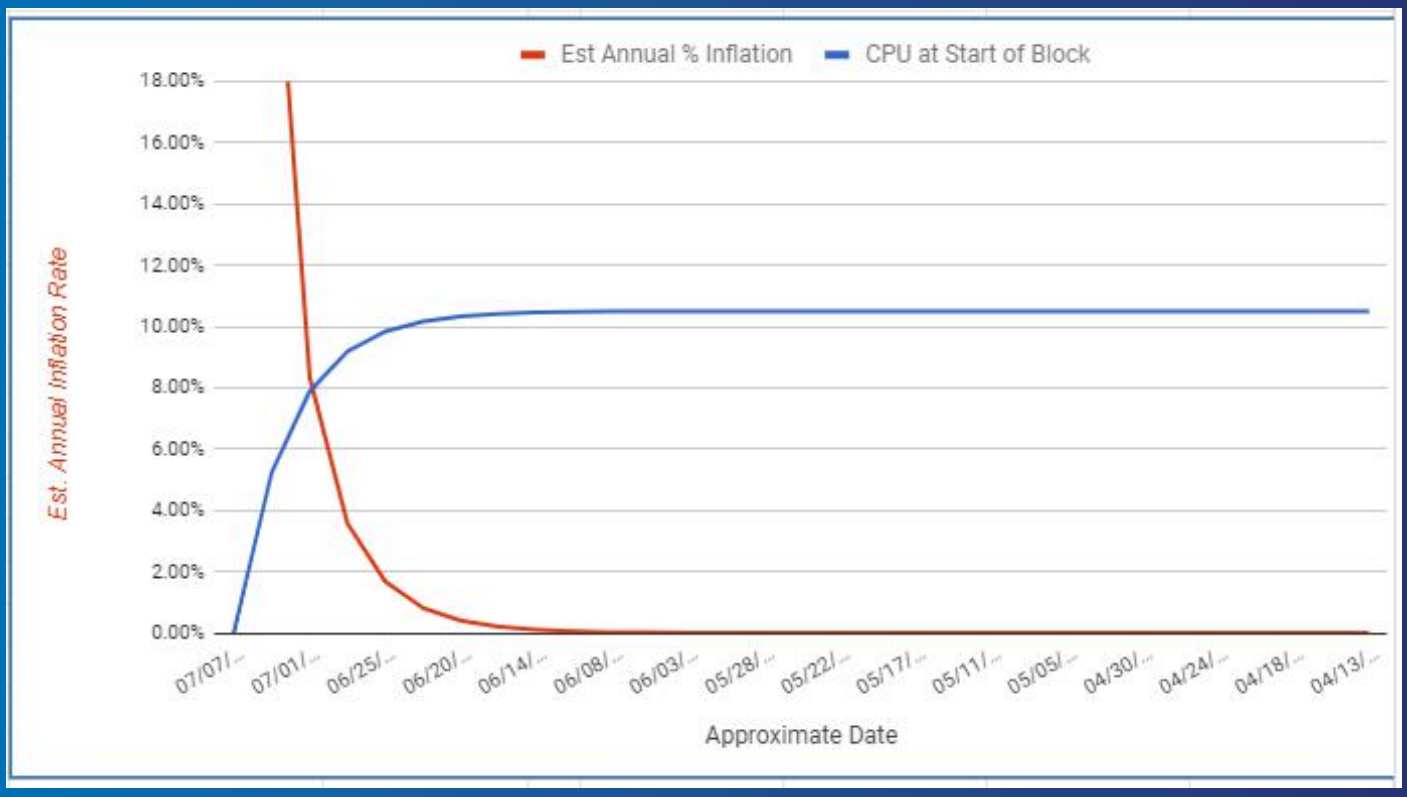
Instead of allocating extra funds for development or implementing additional consensus structure to benefit or complement existing pow consensus rules, we have chosen to evolve the pow algorithm to adapt the features of them without adding them.

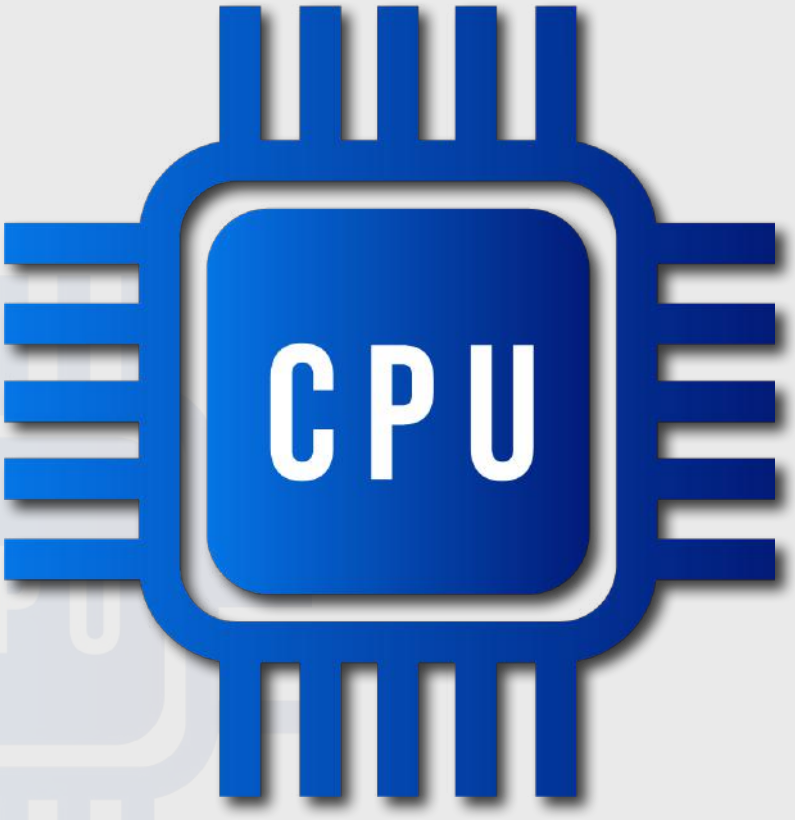
Therefore, CPUchain will have total 105 million supply with fixed schedule of block reward reduction. Every 2 years, miners will receive -50% decreased coin rewards for mining a block, first 2 years miners will receive 50 coins per block, then 25, then 12.5 on 3rd halving schedule. This makes CPUchain inflation resistant currency and those mined coins will be considered as rare therefore people will find a reason to mine and hold.



Block Number	CPU at Start of Block	Max CPU per Block	Block Reward	Est Uncle Reward	Est Total Reward	Inflation % per Era	Est Annual % Inflation	Est Start Date
0	0,00	50	52.500.000,00	0,00	52.500.000,00	#ΔΙΑΙΡ/0!	#ΔΙΑΙΡ/0!	07/07/2019
1.050.000	52.500.000,00	25	26.250.000,00	0,00	26.250.000,00	50,00%	25,03%	07/03/2021
2.100.000	78.750.000,00	12,5	13.125.000,00	0,00	13.125.000,00	16,67%	8,34%	07/01/2023
3.150.000	91.875.000,00	6,25	6.562.500,00	0,00	6.562.500,00	7,14%	3,58%	06/28/2025
4.200.000	98.437.500,00	3,125	3.281.250,00	0,00	3.281.250,00	3,33%	1,67%	06/25/2027
5.250.000	101.718.750,00	1,5625	1.640.625,00	0,00	1.640.625,00	1,61%	0,81%	06/22/2029
6.300.000	103.359.375,00	0,7812500000	820.312,50	0,00	820.312,50	0,79%	0,40%	06/20/2031
7.350.000	104.179.687,50	0,3906250000	410.156,25	0,00	410.156,25	0,39%	0,20%	06/16/2033
8.400.000	104.589.843,75	0,1953125000	205.078,13	0,00	205.078,13	0,20%	0,10%	06/14/2035
9.450.000	104.794.921,88	0,0976562500	102.539,06	0,00	102.539,06	0,10%	0,05%	06/11/2037
10.500.000	104.897.460,94	0,0488281250	51.269,53	0,00	51.269,53	0,05%	0,02%	06/08/2039
11.550.000	104.948.730,47	0,0244140625	25.634,77	0,00	25.634,77	0,02%	0,01%	06/05/2041
12.600.000	104.974.365,23	0,0122070313	12.817,38	0,00	12.817,38	0,01%	0,01%	06/03/2043
13.650.000	104.987.182,62	0,0061035156	6.408,69	0,00	6.408,69	0,01%	0,00%	05/30/2045
14.700.000	104.993.591,31	0,0030517578	3.204,35	0,00	3.204,35	0,00%	0,00%	05/28/2047
15.750.000	104.996.795,65	0,0015258789	1.602,17	0,00	1.602,17	0,00%	0,00%	05/25/2049
16.800.000	104.998.397,83	0,0007629395	801,09	0,00	801,09	0,00%	0,00%	05/22/2051
17.850.000	104.999.198,91	0,0003814697	400,54	0,00	400,54	0,00%	0,00%	05/19/2053
18.900.000	104.999.599,46	0,0001907349	200,27	0,00	200,27	0,00%	0,00%	05/17/2055
19.950.000	104.999.799,73	0,0000953674	100,14	0,00	100,14	0,00%	0,00%	05/13/2057
21.000.000	104.999.899,86	0,0000476837	50,07	0,00	50,07	0,00%	0,00%	05/11/2059
22.050.000	104.999.949,93	0,0000238419	25,03	0,00	25,03	0,00%	0,00%	05/08/2061
23.100.000	104.999.974,97	0,0000119209	12,52	0,00	12,52	0,00%	0,00%	05/05/2063
24.150.000	104.999.987,48	0,0000059605	6,26	0,00	6,26	0,00%	0,00%	05/02/2065
25.200.000	104.999.993,74	0,0000029802	3,13	0,00	3,13	0,00%	0,00%	04/30/2067
26.250.000	104.999.996,87	0,0000014901	1,56	0,00	1,56	0,00%	0,00%	04/26/2069
27.300.000	104.999.998,44	0,0000007451	0,78	0,00	0,78	0,00%	0,00%	04/24/2071
28.350.000	104.999.999,22	0,0000003725	0,39	0,00	0,39	0,00%	0,00%	04/21/2073
29.400.000	104.999.999,61	0,0000001863	0,20	0,00	0,20	0,00%	0,00%	04/18/2075
30.450.000	104.999.999,80	0,0000000931	0,10	0,00	0,10	0,00%	0,00%	04/15/2077
31.500.000	104.999.999,90	0,0000000466	0,05	0,00	0,05	0,00%	0,00%	04/13/2079
32.550.000	104.999.999,95	0,0000000233	0,02	0,00	0,02	0,00%	0,00%	04/09/2081
33.600.000	104.999.999,98	0,0000000116	0,01	0,00	0,01	0,00%	0,00%	04/07/2083
34.650.000	104.999.999,99	0,0000000058	0,01	0,00	0,01	0,00%	0,00%	04/04/2085
35.700.000	104.999.999,99	0,0000000029	0,00	0,00	0,00	0,00%	0,00%	04/01/2087
36.750.000	105.000.000,00	0,0000000015	0,00	0,00	0,00	0,00%	0,00%	03/29/2089
37.800.000	105.000.000,00	0,0000000007	0,00	0,00	0,00	0,00%	0,00%	03/27/2091
38.850.000	105.000.000,00	0,0000000004	0,00	0,00	0,00	0,00%	0,00%	03/23/2093
39.900.000	105.000.000,00	0,0000000002	0,00	0,00	0,00	0,00%	0,00%	03/21/2095
40.950.000	105.000.000,00	0,0000000001	0,00	0,00	0,00	0,00%	0,00%	03/18/2097

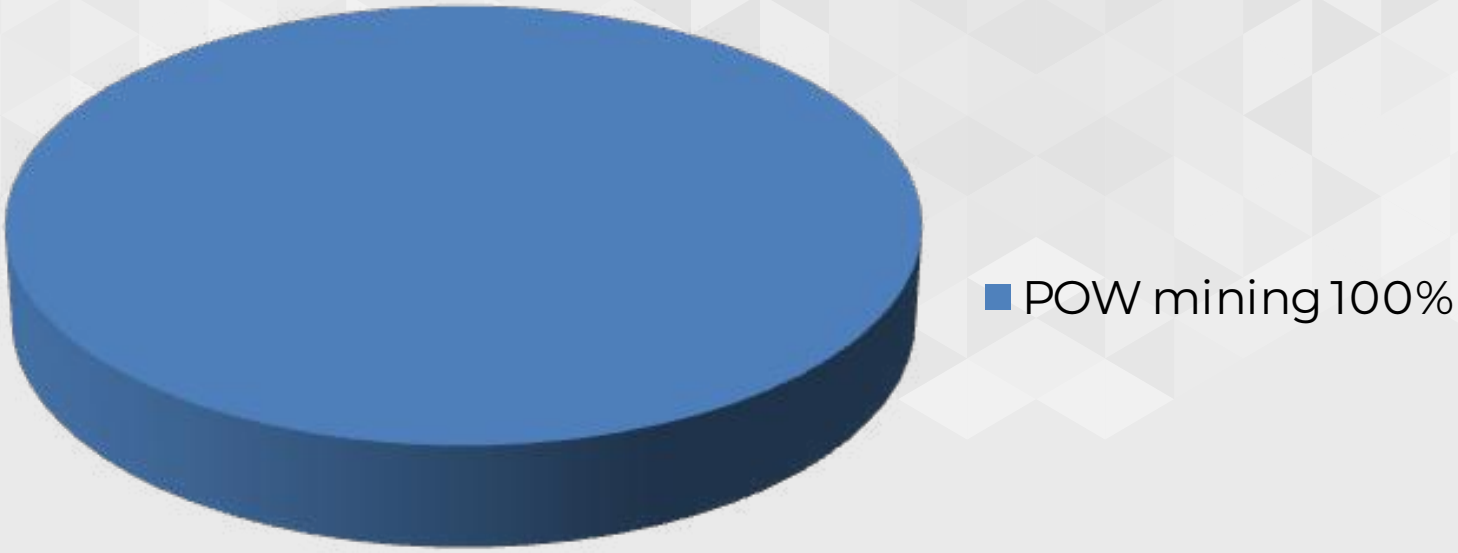
Starting Date	07/07/2019		MAX CPU REWARD PER BLOCK (ERA 1)				
Starting Value	0,00	Emission	Block Reward	Uncle Reward 1	Uncle Reward 2	Total	
		Miner	50	0	0	50	
Block Time (s)	60	Uncle Miner		0	0	0	
Blocks Per Year	525.600	Total	50	0	0	50	
Blocks In Era 1	1.050.000		MAX CPU REWARD PER BLOCK (ERA 2)				
Blocks In Eras 2+	1.050.000	Emission	Block Reward	Uncle Reward 1	Uncle Reward 2	Total	
Blocks Per Epoch	30.000	Miner	25	0	0	25	
Years In Era 1	2,00	Uncle Miner	0	0	0	0	
Years in Eras 2+	2,00	Total	25	0	0	25	
Reduction Rate Eras 2+	0,5	Current Block #		Estimated Cap	105.000.000,00		
		10.000		Hard Cap	105.000.000,00	Estimated Date	
Avg. Uncles/Block Era 1	0			50% Mined	52.500.000,00	07/03/2021	
Avg. Uncles/Block Era 2+	0			90% Mined	94.500.000,00		
				99% Mined	103.950.000,00	04/15/2026	
Epoch Reduction	✖ □			Annual Inflation	0,03	02/02/2026	





CPUchain Core

Allocating Fund



CPUpower Consensus

We've developed and chosen CPUpower algorithm as our main proof-of-work (PoW) mining and block hashing scheme. CPUpower is an transformative algorithm of Yespower and is a proof-of-work (PoW) focused fork of Yescrypt password hashing algorithm, which in turns builds upon well-known Scrypt algorithm. Unlike former Scrypt or Yescrypt algorithm CPUpower is meant to be used for PoW-based blockchains such as block headers and nonce.

Developing cryptocurrency the main reason that we've chosen CPUpower is cause CPUpower is designed to be CPU-friendly, GPU-unfriendly, and FPGA / ASIC resistant. In many years experience of developing FPGA bitstream software to emulate over FPGA cards for mining cryptos, CPUpower is a superior algorithm for combating specialized mining devices.

There are many PoW currencies exist including Bitcoin, Litecoin, Ethereum, Zcash and much more and they are using many different proof-of-work algorithms for computing hashes like SHA256D or Dagger-hashimoto, Yescrypt, Aragon2D, Lyra2v, etc. When we choose hashing algorithms among them, we look for "ASIC resistance", or "GPU resistance".

What is (or should be) meant by that is limiting the computing advantage of specialized Asic devices. For common algorithms like sha256 or scrypt it is normal that ASICs or FPGA take advantages in computing hashes or mining cryptocurrencies compared with commercial hardwares because they are meant to do that.

Specialized hardwares can't do other jobs unlike commercial hardwares, they can't play games or run word processors like normal computers. Instead, they can only do mining cryptocurrencies in effective way. They may also consume less electricity than commercial hardwares because they are utilized for mining activity with old memory chips like ddr3 to lower the manufacture costs.

CPUpower achieves some point of ASIC resistance by disadvantaging specialized hardwares, instead of utilizing the device for algorithm, we have utilized the algorithm to benefit more on cutting edge hardwares and devices. For example an AMD Ryzen 3700X cpu combined with high frequency memory will achieve more hashrate power than xeon server processors or nvidia titan graphic cards that may cost more than a commercial cpu hardwares and have more cores to compute but has lower memory frequency. CPUpower limits a power of multi-core computation to benefit small devices like desktop computers or smartphone devices.

Limiting multi-core performance limits GPU mining performance for computing on CPUchain, Some pro-GPU and anti-ASIC algorithms benefits graphic cards to establish GPU mining ecosystem for the cryptocurrency, although it may secure the network than cpu mining, it consumes more electricity than CPU mining ecosystem and their mining facility is centralized compared with pro-CPU mining ecosystem, Imagine a large GPU mining facility compared with miners mining a currency with their own smartphones instead of investing on graphic cards which is meant for playing video games not mining cryptocurrencies and form a large factory to consume more local electricity.

CPUpower also benefits small miners to mine more coins and form a large group of eco-friendly mining community that raise the value of cryptocurrency. Some group of desktop cpus or cluster of smartphone will be enough to mine CPUchain and you have more choice of cpu vendor to choose, buy and mine with them.

However it is also impossible to estimate the number of cases of exploiting the algorithm for mining on specialized hardwares, some pro-CPU or pro-GPU algorithms failed to achieve the original purpose due to some exploits, so we define here if the case happens for CPUchain / CPUpower algorithm, we may update and patch the pow algorithm to combat those attacks to be resistant again.

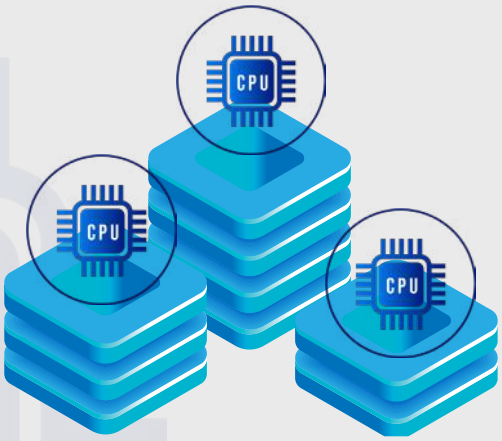
Transaction Scalablity

Almost every existing cryptocurrencies lack support on scaling blockchain network for real use case. This is due to political reason of regarding hardforks, or lack of solution for increased size of transactions from smart contracts, or just a low priority due to low volume of ongoing TPS for altcoins.

As we believe in self-sustainable cryptocurrency that can last for more than hundred years, we take the scaling issue seriously and thus we've implemented a scaling solution that can cover up to 80K transactions per second, which exceeds current visa's 50k tps capacity.

If the cryptocurrency like Bitcoin or CPUchain meets the real use case and transaction demand, to replace simple payments, credit card, cash, or any other payment system, Blockchain network that doesn't meet the tps scaling requirements will be a thing of a past. Like the current OS differs from old computing platforms, that are gone due to lack of computing support, Chains with small tps will be replaced with blockchains with higher transaction capacity.

CPUchain has extended its block size limit up to 1000 MB per block. Although it is not possible to reach the full limit due to lack of parallel computing support, CPUchain may be able to support hundreds of tps with node running on modern computer or servers. It may scale more with support of segregated witness transactions or schnorr signatures attached on utxos.



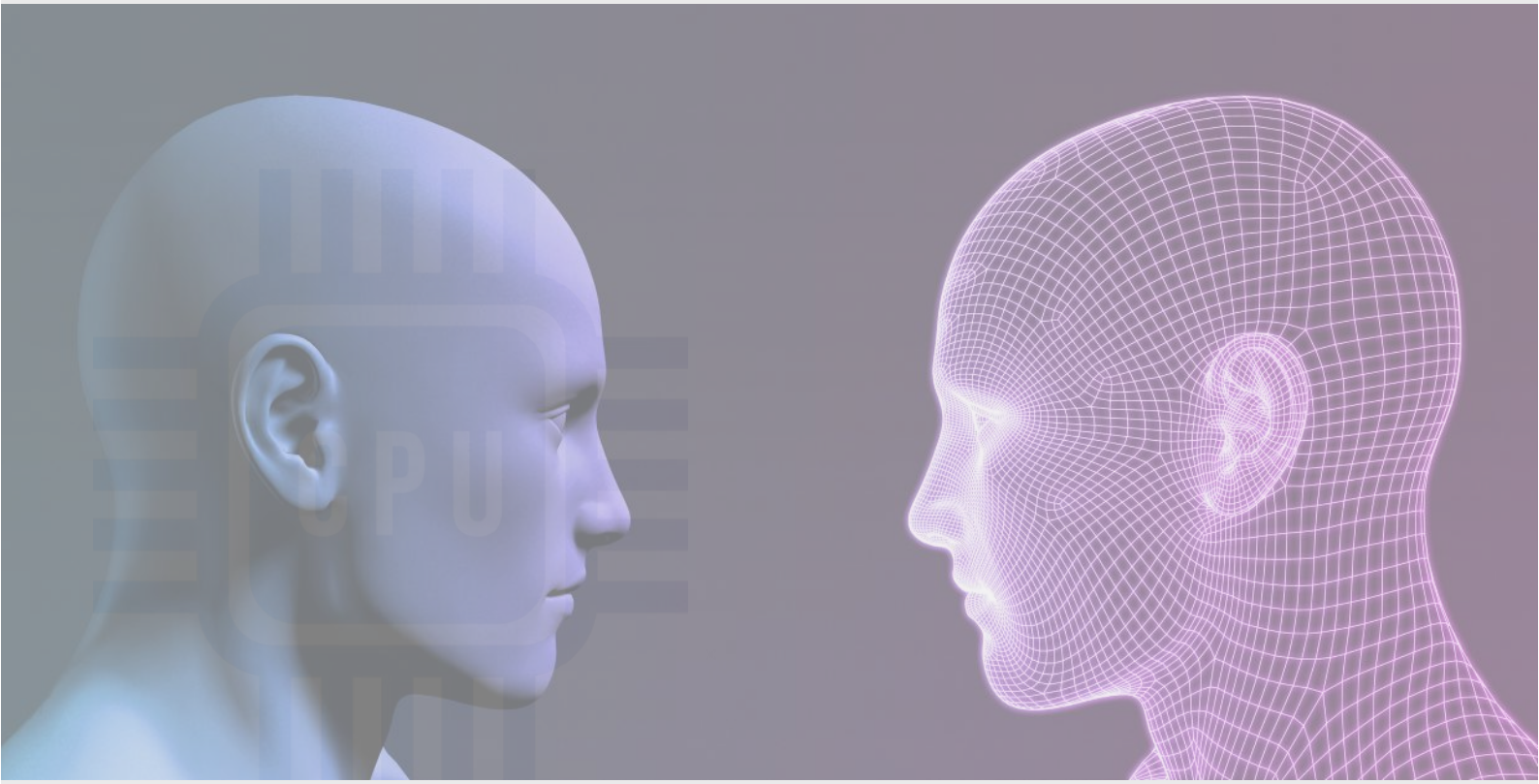
Ecosystem

Our mission for CPUchain is to build free and open-source, community driven , self-governed ecosystem under scaling, decentralized roadmap. As a modern crypto currency, and as a non-ico, non-remine platform, support from community is essential. Therefore we define a win-win business model for CPUchain Core.

Coins may have an ICO or IEO in order to support devs, however, there is an also risk of development discontinuation when devs spend their collected funds from initial launch and this is considered as a bad strategy for coins that should continue the development and maintenance for more than decades. It is also possible for exit scams to collect the money and run without any real development for the coin happen.

Instead of existing ico business models, we define a new business model in aspect of long term, self-sustainable, and community friendly model.

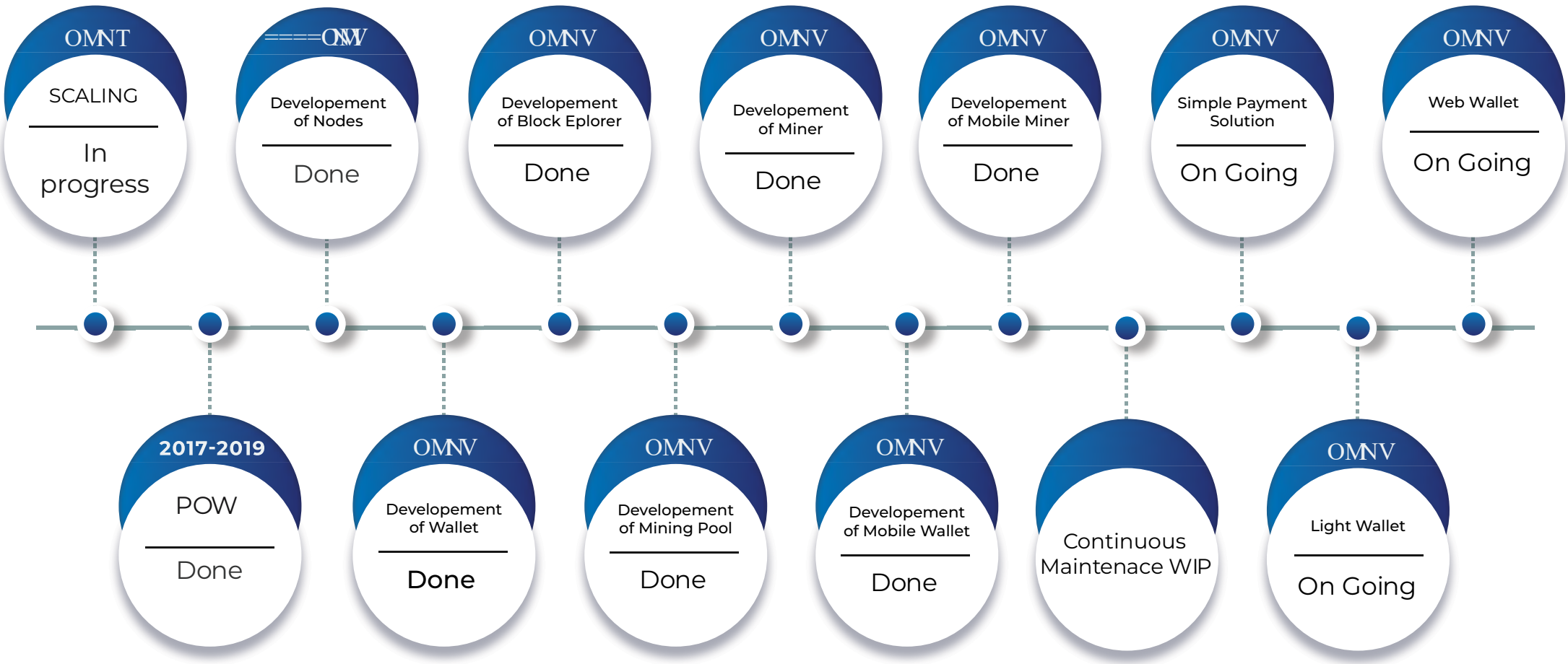
Following the success of non premined crypto currencies like Bitcoin or Litecoin, CPUchain help community to build on self-motivation of evolving the currency, Users who aren't professionals in mining but someone who has an ability of develop something for the coin may find a self-motivation under cpu mining environment. In short the dev can mine a coin and those who want to increase the value of the coin may build something that can attract more users to evolve the currency. Under free market process coin may grow its value, and with growing size of the community, coin's value may double.



Technical specification

•Name	CPUchain
•Ticker	CPU
•Algorithm	CPUpower [POW]
•Block time	1 minute (60 seconds)
•Block reward	50 CPU (50% decrease on every 105m block)
•Halving Every 2 years	(Every 1,050.000 blocks)
•Total supply	105,000,000 CPU coins
•Distribution	100% POW with no ICO or Premine, dev fee.

Roadmap



Github: https://github.com/cpuchain

Medium: https://medium.com/cpuchain

Reddit: https://reddit.com/r/cpuchain

Homepage: https://cpuchain.org/

Twitter: https://twitter.com/cpuchain

Discord: https://discord.io/cpuchain

Telegram: https://t.me/cpuchaincore