THE TAO

TAO The Natural Order

Jul 16, 2022

V2.1

https://thetao.cash

Table of Contents

Introduction

As time flies, it has been more than 10 years since the birth of Bitcoin, and the entire world of cryptocurrencies has been climaxing and troughing with the fluctuation of the price of Bitcoin. During this period, there exist many "rising stars", like Ethereum taking the beating or EOS being totally balls-up. Time flying away, although there have been no perfect coins yet, occasionally some fresh coins turn eye-poppers, such as BHD and Grin. This paper intends to elaborate on the situation of the coin circle in the past 10 years, in order to explain the current landscape and deficiencies of the cryptocurrency world. Then we try to propose a new minable coin based on zk-SNARKs technology, The TAO (DAO), which employs Proof of Capacity (aka, PoC) as its consensus model.

After 1 year of breeding, poc3 came out. poc3 brings brand new features to The TAO, the biggest improvement being the first dual mining mechanism of The TAO and BTC, and other new trends and applications in the industry including DAO, NFT, etc.

TAO (/daʊ/, /taʊ/) is a Chinese word signifying the "way", "path", "route", "road" or sometimes more loosely "doctrine", "principle" or "holistic beliefs". In the context of East Asian philosophy and East Asian religions, TAO is the natural order of the universe whose character one's human intuition must discern in order to realize the potential for individual wisdom. This intuitive knowing of "life" cannot be grasped as a concept; it is known through actual living experience of one's everyday being.

-- Wikipedia（https://en.wikipedia.org/wiki/Tao）

Background

There are three mainstream consensus models in the blockchain world: Proof of Work (PoW), Proof of Stake (PoS) and Proof of Capacity (PoC). Others are all evolutions on these three categories while DAG is not a blockchain at all and beyond the scope of this article. Some others are the home brew ones, which cannot to be mathematically verifiable, nothing but playing to the gallery.

The privacy coin proves its existence value from the perspective of Utility Token.

Three Consensus Models

PoW is the earliest and most mature consensus algorithm, representatives of which are Bitcoin and its fork, Ethereum and its fork, as well as Litecoin, Zcash, Monero, etc., and its main feature is that miners follow diverse types of cryptography hash algorithms specified by the blockchain networks to find a nonce value in some brute-force way within the certain time, in order to have the accounting right and get the reward by generating blocks. PoW is often criticized due to its significant waste of the electricity. The growing trend of hash algorithms built in ASICs has made PoW mining become heavy-asset projects, which daunts small and medium-sized retail investors while only capital predators can afford mining.

Proof of Stake, PoS, exists for quite a long time, but the price of PoS tokens has been flat. The reasons are as follows. First, all coins are generated and distributed in the "Genesis Block", and no longer needed to be mined. Secondly, excessive concentration of stakes is prone to bribery elections. The community differentiation of Steemit is the latest example. This is neither the first nor the last time. It is just a rather famous one. Thirdly, the total amount of PoS coins is usually huge. Considering the incentives of block producers, the inflation model is generally used. Fourthly, PoS has not find its practical application purposes so far. Even if Ethereum 2.0 is about to adopt to PoS, the community still cannot see a bright future for the time being. Fifthly, Staking cannot save PoS. However, PoS is not utterly useless. PoS is more suitable for being the stake of an enterprise-like community governance rather than a Utility Token.

PoC, Proof of Capacity, is destined to stand out from others since its birth. PoC is divided into two major categories. The first is represented by Burst, which leverages the principle of space-time conversion. The cryptographic hash value in PoW is computed in advance and written to harddisks. When mining, the miner program only needs to scan harddisks to obtain all nonce from special scoop and submit a smallest deadline of its own. The owner of the minimum deadline from the entire network in each round gets the accounting right, generates the block and gets the incentives at the same time. This type of PoC has a low entrance threshold. Ordinary computers can participate in mining as long as equipped with hard drives. The electricity consumption is extremely low while under certain computing power, it can be as safe as PoW. Burst, as the first complete and operational public chain based on PoC, proved the feasibility of PoC. But the poor operation in the later stage led to its failure. As a rising star of PoC, BHD testifies its value when nurturing the market in a large amount. The other is the PoC + PoW hybrid consensus model represented by Filecoin. Although belonging to the PoC category, it requires the capacity of harddisk to match enough PoW computational power (graphics cards or ASICs), which makes the entire consensus algorithm extremely complex. It sets a high technical threshold for miners, and the threshold of initial investment is as high as that of pure PoW consensus model.

Privacy Coins

When it comes to privacy coins, everyone will immediately think about of Zcash, Menero and Grin.

Zcash is a fork of Bitcoin, which changed the hash algorithm of consensus model and added zero-knowledge proofs (zk-SNARKs) into the business logic. It made a splash once and ranked the first place in privacy coins. But its good times did not last long. Currently it has reached the point where the computing power has dropped to be quite vulnerable to the 51% attack.

Menero chooses the privacy algorithm of ring signatures. It has stumbled over the past few years and been constantly patching up to fight against ASICs. It is also the preferred coin for zombie botnet mining networks in mixed reviews.

Grin is a promising new star of privacy coins in 2019. The basic principle is to add the additively homomorphic encryption to the Bitcoin codebase to realize privacy. Due to the privacy only established on the premise that everyone is online, which can be regarded as an online tumbler, that brings much trouble in practice.

The privacy coins above have one thing in common, that is, they all employ PoW consensus and require huge power consumption to maintain the security of chains.

But privacy coins have always been a "pretty rigid demand" in the cryptocurrency world! As a Utility Token, privacy should be a natural and inherent property of cryptocurrencies. Unfortunately, mainstream cryptocurrencies such as Bitcoin and Ethereum are neither private nor anonymous, which leads to the continuous chasing of privacy coins.

Bitcoin eco-system

In the past year, BTC has gone from a record $69,000 all the way to $20,000 today, with big ups and downs, and a bloody rain, who is the master of the sink. The infamous GBTC dragged 3AC and other institutions into the bottomless abyss, the so-called success is leverage defeat is also leverage.

But BTC's dominant position cannot be shaken, no matter from the technical consensus strength to the social consensus strength, BTC is deservedly No.1, therefore, in the future for a long time, any token will inevitably have a direct or indirect relationship with BTC, poc3 is created based on this thinking.

The TAO

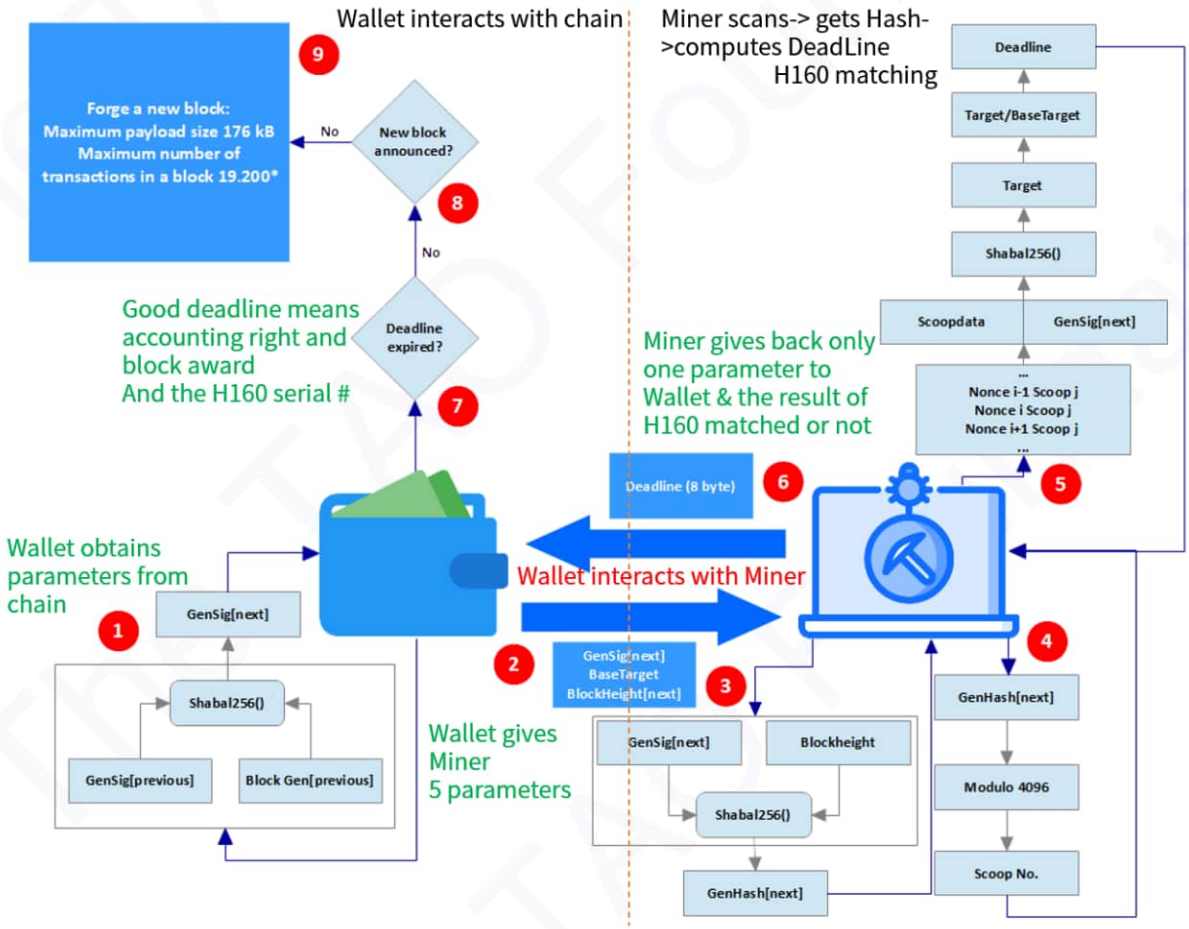
Proof of Capacity (PoC) is an excellent consensus algorithm, with the attributes of low barriers to participation, low power consumption, ASICs tamperproof, and public transparency. Zero-knowledge proof (zk-SNARKs) has experienced the baptism of time and proved to be a reliable algorithm for privacy transactions. The TAO is a combination of their advantages. The underlying mining algorithm employs PoC consensus and the upper business logic adopts to zk-SNARKs. Although there are some

public chains claiming to realize PoC + zk-SNARKs, it can be found to be a totally fake privacy coin after an easy verification. The TAO is the world's first privacy coin built with PoC + zk-SNARKs!

Technical Architecture

1. Mining Process

Mining is a process of having the accounting right and obtaining the token incentives by submitting minimum deadlines specified by blockchain networks. The mining process of The TAO is that miners plot harddisks in fixed time, get nonce, calculate deadlines, match the H160 and submit to wallet or pool. Miners Start mining with either solo or pool mode. They can choose as they want freely.

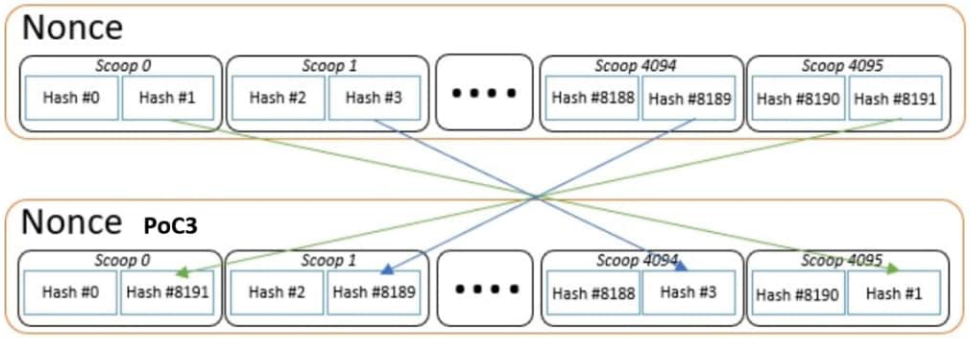


As shown in the figure, mining is divided into 9 steps: 1) Wallet interacts with the chain to obtain current chain parameters; 2) Wallet sends 5 chain parameters to the miner program; 3) Miner program calculates the nexthash value according to the current chain parameters; 4) Miner program calculates the current Scoop number according to the nexthash value; 5) Miner scans all nonce per the current Scoop number within his harddisk capacity and calculates the deadline value; also trying to matching the H160 6) Submit the smallest deadline value of its own and the H160 matched result to the wallet; 7) The wallet makes a local judgment whether the received deadline value is greater than the default maximum value set by itself. If the deadline is greater than this value, it will be dropped directly and will not be submitted to the chain; 8) Wallet submits the deadline value to the chain; 9) Chain judges whether the accepted deadline is the smallest of all the current ones. If it is the smallest, the accounting right and token reward are given; Otherwise, the submitted deadline value is dropped. If any of the H160s has been matched, the serial # will be provided to the chain, too.

During mining process, the wallet can be on the same physical machine with the miner program, which is called the solo mode. Or it can be on the remote site, thus it is in the pool mode. The TAO will make joint efforts with the community to run an official pool. It does not require all miners to participate in the official pool compulsorily while everyone is encouraged to join in it. There are two categories of miner programs: C ++ and Rust, which can be run under both Windows and Linux platforms respectively. The miner program will be available on the official website, and it is strongly recommended that the community only downloads the related programs from the official website.

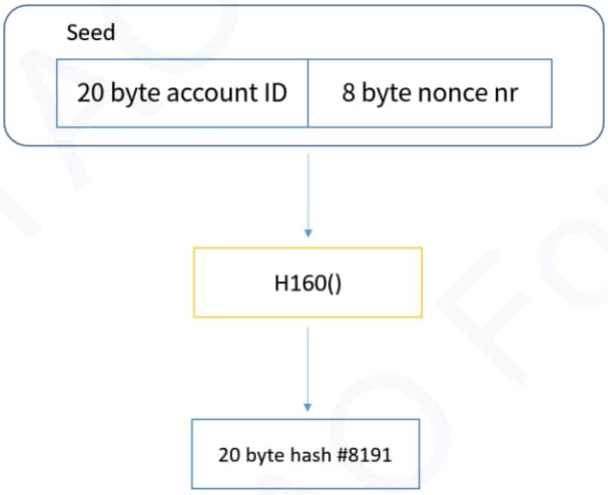
2. Plotting Process

The TAO adopts the PoC consensus, which means a process of making a plot file is required before mining. This process is called plotting harddisks. The plot files of The TAO use the PoC3 format, which is different from PoC format as follows:

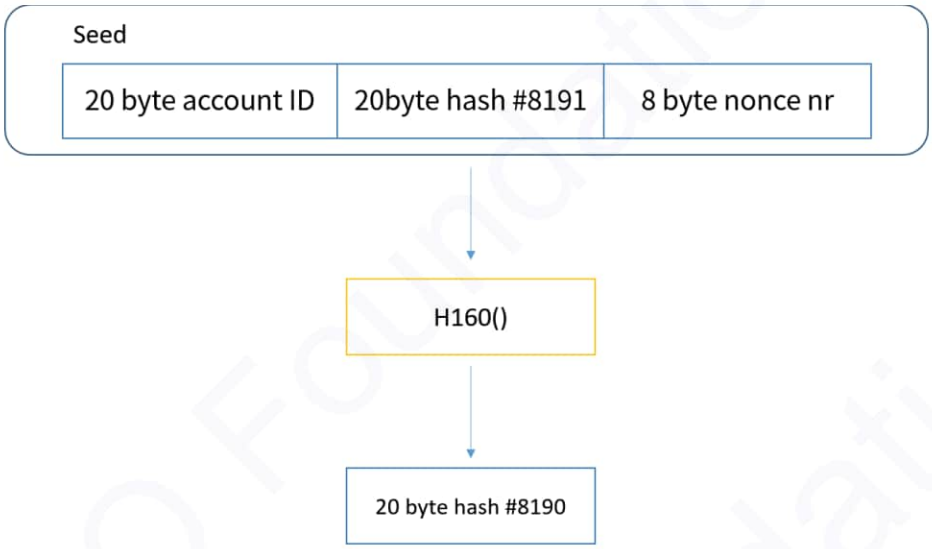


For the purpose of reducing the frequent addressing action of harddisk heads, PoC3 format is optimized. It puts the nonce of the same Scoop number together to improve efficiency and benefits lives of harddisks. And poc3 also creates the concept of ‘useful storage’.

The nonce calculation of The TAO is heavily different from Burst, BHD, etc., which is embodied in the generation of seeds. The TAO uses a 20-byte account ID instead of the usual 8 bytes while is not simply extended from 8 bytes to 20 bytes. The specific algorithm will be reflected in the open source plot program. The cryptographic hash algorithm employs H160. The nonce calculation process of The TAO can be listed as follows:



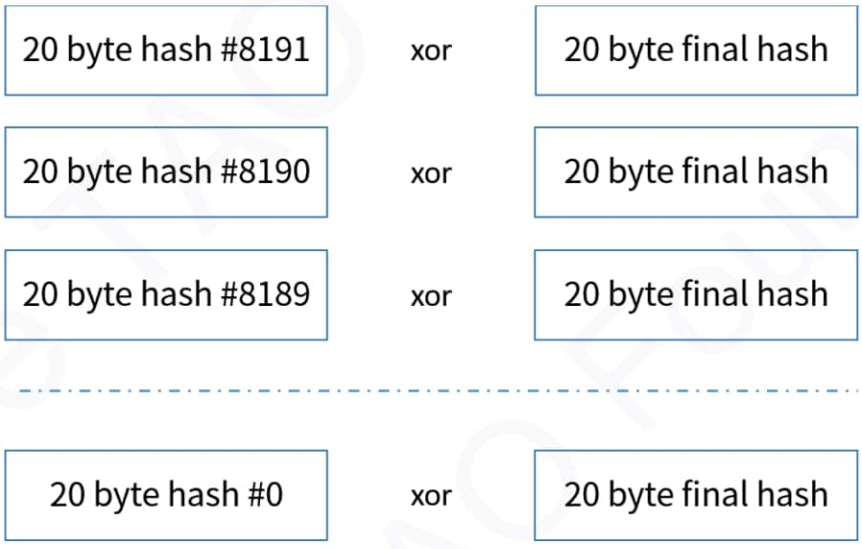
Leveraging the seed, use the H160 algorithm to generate the first hash, that is, the hash with the number 8191. Then take the result as part of the seed to generate the second hash, #8190, by using the same algorithm, H160:



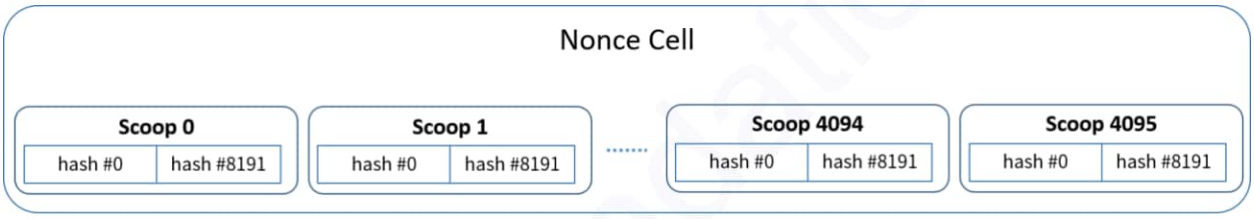
Make recursions consecutively until all 8192 hashes are generated. At this time, a hash called final hash needs to be generated, whose seed is all 8192 hashes plus the original seed with the earliest 28 bytes, namely:

Final hash = H160（Hash #0~8191 + startedseed(20byte account ID+8byte hash nr）)

At last, final hash does xor calculation on each hash generated before, so as to get the final nonce:



The 8192 hash results are arranged in groups of two adjacent ones. Each group is called a Scoop then to get 4096 Scoops, which are filled in the Cell. Thus, the Cell structure is completed.



In the process of generating the Cell, the computer must use the cache to record all intermediate results for obtaining the final nonce result. As you can see, SSD can be used to improve the efficiency of harddisks plotting.

Since each Cell contains 8192 hash results of H160 and the length of each nonce is 20 bytes, each Cell will take up fixed space of 160KB.

Repeat the operation of generating Cells, and then optimize the arrangement of all Cells to fill the Plot files.

The TAO will provide the plot program with graphic cards acceleration based on the Rust language to the community for free.

3. Useful Storage

From Burst to BHD to Chia, and the initial version of The TAO, all these well-known PoC projects have chosen useless hash or "garbage" hash for two purposes: firstly, they inherit the idea of PoW, but turn PoW into a two-step calculation and reuse the existing "Garbage" Hash, this move in security can rival PoW, but energy consumption is greatly reduced, which is already the big step from PoW to PoC; Second, the use of Shabal256 Hash function is only to increase the difficulty of the P disk process, to a certain extent to reduce or slow down the 51% attack.

TAO's poc3 algorithm has made revolutionary, industry-leading improvements.

1) About H160

H160 that is Hash160, is the product of the generation process of BTC classical address (i.e. address starting with 1), is also an important Hash for locking assets on the bitcoin chain, H160 or P2PKH address format locks millions of BTC assets! For example, the infamous hacker address

1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF, long ranked in the top10 of the top100 richest addresses of BTC, locked nearly 80,000 BTC, its ATH value reached 5 billion dollars, even now, still worth 1.6 billion dollars! How can you take this wealth? Let's look at the on-chain locking script:

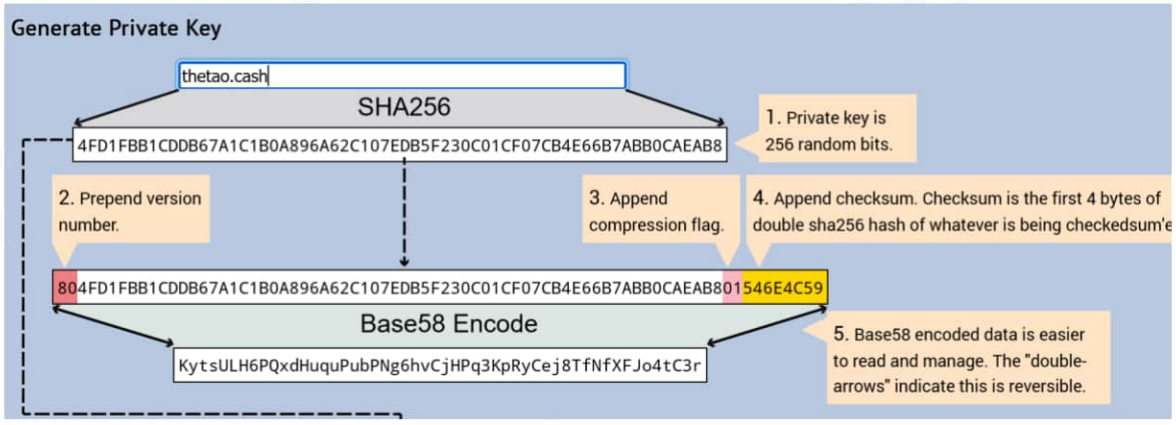
Index	0
Address	1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF
Pkscript	OP_DUP OP_HASH160 a0b0d60e5991578ed37cbda2b17d8b2ce23ab295 OP_EQUALVERIFY OP_CHECKSIG

(https://www.blockchain.com/btc/address/1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF)

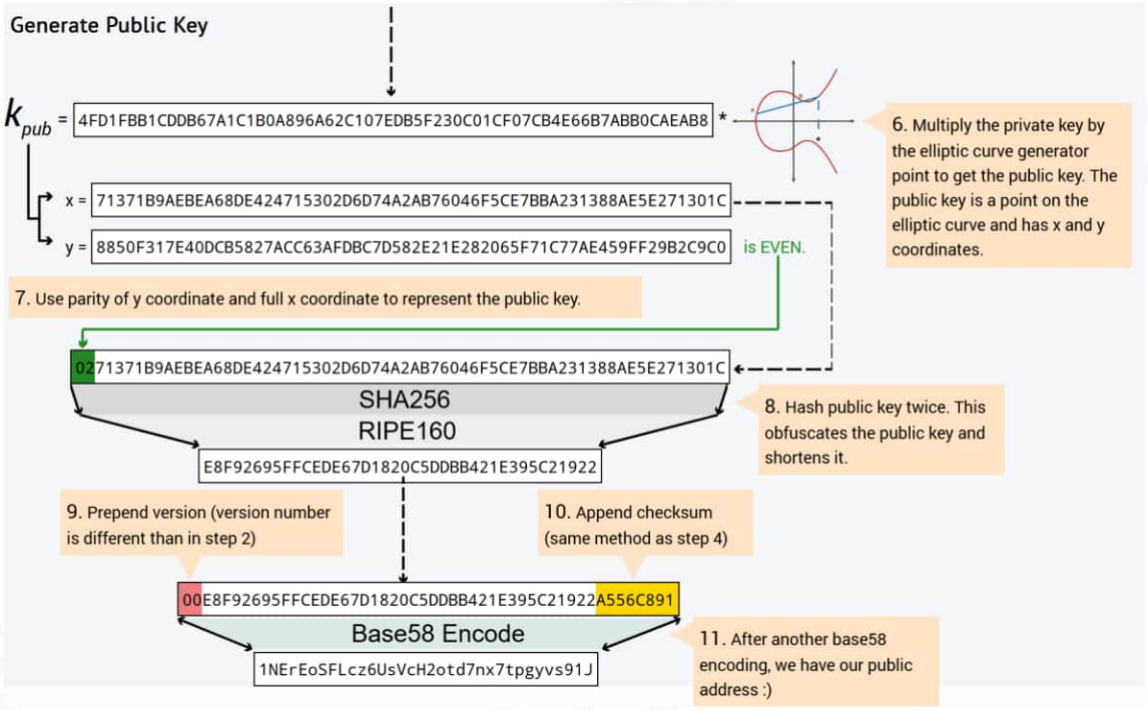
You read that right! As long as you have a0b0d60e5991578ed37cbda2b17d8b2ce23ab295 of Hash 160, you can take it all without any other requirements! In the bitcoin chain, all the assets locked at the beginning of the 1 address are the same, and this is exactly the wealth that poc3 will "mine"!

2) Brain Wallet

Bitcoin's brain wallet, which had been popular in the early days, was slowly abandoned because the entropy was too small and too easy to be brute-forced, but many early wallet addresses were generated by the way of brain wallets, for example, the process for a classical address generated with thetao.cash as the seed is:



The private key in WiF format is KytsULH6PQxdHuquPubPNg6hvCjHPq3KpRyCej8TfNfXFJo4tC3r which is not our interested point. What is interesting is the process of address generating.



As you can see, the final address is 1NErEoSFLcz6UsVcH2otd7nx7tpgyvs91J, which is the classical 1-prefix address. But the most existing thing is the send to last step how it generates H160：e8f92695ffcede67d1820c5ddbb421e395c21922.

$$H160 = RiPEMD160(SHA256(ECC(PrivateKey)))$$

This is one of the cores of poc3's disk-plotting algorithm. poc3 replaces the previous "garbage" hash with a useful hash of H160, which not only meets the needs of PoC consensus hard drive based mining, but also reuses the already generated H160. reuse? Yes! More energy efficient and effective reuse than PoC! But why?

3) Pigeonhole Principle

Looking closely at the steps of classical address generation, the ECC public key is hashed RiMEPD160 once after SHA256! This is designed to resist pre-image attacks, but according to the pigeonhole principle, it is known that each RiMEPD160 result corresponds to 2^{96} inputs, that is to say, each

classical address or H160 corresponds to 2^{96} private keys, a lock that locks a huge amount of wealth can be opened by 79228162514264337593543950336 keys! You need only 1 key to take the wealth!

4) What makes poc3 unique

Since there is such a problem with bitcoin's classical address design, and also huge amounts of wealth locked by just H160, why is nobody trying to brute-force crack it?

Yes, and there are a lot of people doing this, they are all using PoW, i.e., using CPU or GPU to brute-force private keys to collide with one or several H160s with huge balances. Huge energy consumption or, rather, electricity costs are required here, and the result is that very few people stick around until the collision yields results. poc3 is different in that one calculation is reused! As mentioned above, 1 H160 corresponds to 2^{96} private keys, and poc3 stores the calculated private keys and H160 information on the hard disk, so a single H60 can be reused multiple, infinite times; and poc3 does not target only one or some H160s, but traverses all classical addresses with balances on the bitcoin chain, synchronizing the attack without discrimination. This is the maximum cost effective in terms of energy consumption and probability!

Since classical addresses are so insecure, hurry up and move to multi-signature addresses! Yes, but many of the earlier addresses have lost their private keys and become "locked-in" wealth. No one can move them, but they have become the prey of poc3. They cannot move. What they can do is only waiting to be burst by poc3!

#	addr.	h160	balance	1st in	live
1	1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF	a0b0d60e5991578ed37cbda2b17d8b2ce23ab295	79,957.21	2011-03-01	×
2	12tkqA9xSoowkzoERHMWNKsTey55YEBqkv	14c1ed72d09150b8e5f49d94d53070d2c1f1db36	28,151.05	2010-04-05	×
3	12ib7dApVFvg82TXKycWBNpN8kFyiAN1dr	12d5a845f2b212ce0c3bd65a4035881d9219090e	31,000.07	2010-05-13	√
4	1PeizMg76Cf96nUQrYg8xuoZWLQozU5zGW	f8753559cd673046044baf06725c7a94bcb8a592	19,414.43	2010-07-24	×
5	1f1miYFQWTzdLiCBxtHHnNiW7WAWPUccr	0730733b14f38b9ffd71c7af91d5bd42f6f91eee	10,009.26	2011-05-04	×
6	1BAFWQhH9pNkz3mZDQ1tWrtKkSHVCkc3fV	6f711c825976d3e171f52d1255bf4729a5a786c2	10,000.07	2011-05-04	×
7	14YK4mzJGo5NKkNnmVJeuEAQftLt795Gec	26d45a268d236f025aab79f69aa30fffcb2c623c	10,000.03	2011-05-04	×
8	1KbrSKrT3GeEruTuuYYUSQ35JwKbrAWJYm	cc09aca7e05eb5a3519b535ece40cafc7157386e	10,000.01	2011-04-02	×
9	1P1iThxBH542Gmk1kZNXyji4E4iwpvSbrt	f175606e5002520a4b8f34c9eebe2dec38e71cfd	10,000.01	2011-05-04	×
10	12tLs9c9RsALt4ockxa1hB4iTCTSmxj2me	14adec07961b45af6b9b9a353d279d737047f4c1	10,000.01	2011-04-02	×
11	1ucXXZQSEf4zny2HRwAQKtVpkLPTUKRtt	09f349307b923b61145029efdc5c9ba5b7ebde52	10,000.01	2011-05-04	×
12	1CPaziTqeEixPoSFtJxu74uDGbpEAotZom	7ceee99631098c391869241768b354601be45201	10,000.01	2011-05-04	×
13	167ZWTT8n6s4ya8cGjqNNQjDwDGY31vmHg	381642c97cbdcf66aa4b2d13f7e31468ef9c7437	8,999.00	2010-08-09	×
14	198aMn6ZYAczwrE5NvNTUMyJ5qkfy4g3Hi	592fc3990026334c8c6fb2b9da457179cdb5c688	8,000.00	2009-02-22	×
15	18Hp8j2JMvwtPs1eqNaYEEVvuFpjQJRFVY	4ff6e173d27de706193bdb01a07486fbf17bf2d6	4,333.00	2011-08-08	×
16	16eb495TbiCRbRbZv4WBdaUvNGxUYJ4jed	3df4724b043ea82dd77058f137ff3ac9850f1bcb	4,322.33	2011-08-08	×
17	18hFBPU81kC8V4Dp4iwdwQHakKa5TW2ZkJ	54655ae5c48c9db6a3f34dafe11bfe795c1e3655	4,175.77	2011-01-29	√
18	1ALXLVNj7yKRU2Yki3K3yQGB5TBPof7jyo	666a5bcac99eb29e521abcf864bd08617c8cc2c2	4,000.00	2010-07-24	×
19	18eY9oWL2mkXCL1VVwPme2NMmAVhX6EfyM	53e24676b17804707d0eed7cbd2c0815552ea415	4,000.00	2011-06-27	×
20	1LwBdypLh3WPawK1WUqGZXgs4V8neHHqb7	daa9bb4c40a22cabd24f63609e8394f9ff1d38a9	4,000.00	2011-05-17	×

4. Zero-Knowledge Proof（zk-SNARKs）

A zero-knowledge proof is a digital protocol that allows for data to be shared between two parties without the use of a password or any other information associated with the transaction.

In its most basic sense, a zero-knowledge proof (also commonly referred to as ZKP) can be thought of as a protocol through which a digital authentication process can be facilitated without the use of any passwords or other sensitive data. As a result of this, no information, either from the sender’ s or receiver’ s end, can be compromised in any way.

This is quite useful, especially since such a level of safety provides tech enthusiasts with an avenue to communicate with one another without having to reveal the content of their interactions with any third party.

The idea underlying zero-knowledge proofs first came to the fore back in 1985, when developers Shafi Goldwasser, Charles Rackoff and Silvio Micali presented to the world the notion of “knowledge complexity” — a concept that served as a precursor to ZKPs.

As the name suggests, knowledge complexity acts as a metric standard to determine the amount of knowledge required for any transaction (between a prover and verifier) to be considered valid.

The basic of Zero-Knowledge Proof protocol is interactive. It requires the verifier to constantly ask a series of questions about the “knowledge” the prover possess.

Non-interactive Zero-Knowledge Proof, as the name implies, do not require an interactive process, avoiding the possibility of collusion, but may require additional machines and programs to determine the sequence of experiments.

Zcash is the first widespread application of zk-SNARKs, a novel form of zero-knowledge cryptography. The strong privacy guarantee of Zcash is derived from the fact that shielded transactions in Zcash can

be fully encrypted on the blockchain, yet still be verified as valid under the network' s consensus rules by using zk-SNARK proofs.

The acronym zk-SNARK stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge," and refers to a proof construction where one can prove possession of certain information, e.g. a secret key, without revealing that information, and without any interaction between the prover and verifier.

zk-SNARK converts the transaction content that needs to be verified into a proof that two polynomial products are equal, combined with homomorphic encryption and other advanced techniques to protect the hidden transaction amount while performing transaction verification. Its process can be briefly described as:

- Disassemble the code into verifiable logical verification steps, then disassemble these steps into an arithmetic circuit consisting of addition, subtraction, multiplication, and division.
- Conduct a series of transformations to convert the code to be verified into a polynomial equation, such as t(x)h(x)= w(x)v(x).
- In order to make the proof more concise, the verifier randomly selects several checkpoints,s, in advance to check whether the equations at these points are true.
- By homomorphic encoding/encryption, the verifier does not know the actual input value when calculating the equation, but can still verify.
- On the left and right hand sides of the equation, multiply a secret value k that is not equal to 0. when verifying that (t(s)h(s)k) is equal to (w(s)v(s)k), The specific t(s), h(s), w(s), and v(s) cannot be known, so the information can be protected.

The core math model is:

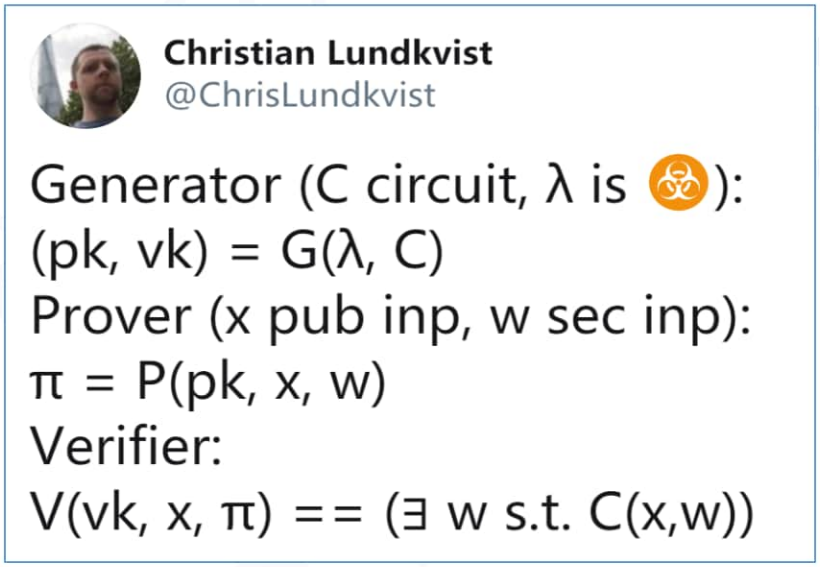
$$\Pr\left[\sigma \leftarrow \mathrm{Setup}(1^k) : \mathcal{A}^{\mathrm{Prove}(\sigma,\ldots)}(\sigma) = 1\right] \equiv \Pr\left[(\sigma,\tau) \leftarrow \mathrm{Sim}_1 : \mathcal{A}^{\mathrm{Sim}(\sigma,\tau,\ldots)}(\sigma) = 1\right]$$

Here $\mathrm{Sim}(\sigma,\tau,y,\omega)$ outputs $\mathrm{Sim}_2(\sigma,\tau,y)$ for $(y,\omega) \in R\sigma$ and both oracles output failure otherwise.

The TAO generates 5 parameters through the MPC (Multi-party Computation) protocol. The first 2 parameters are the proving key (pk for short) and the verifying key (vk for short). The following 3 parameters are the circuit parameters.

pk and vk are generated by generator G according to λ and C.

λ: Random factor, which is also called poison pill.



(From：https://twitter.com/ChrisLundkvist/status/799807876982251520)

During the process of generating pk / vk , multiple participants contribute their own random numbers, and the sum of shared randomness is λ. The MPC protocol works that as long as only one participant actually destroys the random number contributed by himself honestly afterwards, the security of pk and vk can be guaranteed, which means no one can forge the proofs.

C: Circuit transformation function, Circuit.

The code demonstrates as r1cs or cs, rank-1 constraint system.

P: Proving function.

V: Verifying function.

The three steps of zero-knowledge proof are as follows:

1. G calculates pk and vk according to the input λ and C. For some specific blockchains, pk and vk only need to be calculated once and revealed publicly.

2. The prover calculates the proving value π = P (pk, public input x, secure input w).

3. The verifier calculates V (vk, public input x, π) to be true, then confirms that the prover holds the secure input w to make C (x, w) true.

The r1cs parameter file is generated by running the Taod program with command-line parameters:

```
taod -savesproutr1cs -experimentalfeatures
```

We will hold a Trusted Setup Ceremony to generate privacy proving parameters for zk-SNARKs.

5. Wallet

We do not reinvent the wheel. Our wallet is compatible with the standard bip39/32/44 protocols, which means we have a universal Mnemonic and a Hierarchical Deterministic (HD) derivation sub-address protocol. Under the premise of guaranteeing the security, it not only greatly increases convenience and usability, but also lay a good foundation for wallet on mobile APPs. We will also launch our own hardware wallet as the first hardware wallet in PoC ecosystem to escort the community's assets.

Our wallet addresses are divided into two categories: transparent addresses starting with 7- and privacy addresses starting with tao-. All addresses support HD sub-address derivation.

6. Others

The TAO will provide the community with a complete ecosystem of tool chain and facility tools from plot programs to miner programs, from desktop wallets to mobile wallets, from block explorers to mining pools. All programs will be open source.

The TAO will be the first to creatively adopt the approach of delayed open-sourcing process of the source code. We package the source code and calculate its SHA512, and this hash value will be written to the genesis block. This move can not only make the source code delayed open-sourcing for about half a year to resist copycats in the TAO's young fragile ecosystem, but also prove that the code was genuine from the day of the genesis block generated.

Economic Model

The TAO adopts an economic model of deflation. It belongs to Utility Token, and the symbol is TAO.

- Total Supply：21,000,000 TAO
- Initial Block Reward：50 TAO
- Block Interval：5 minutes
- Deflation Strategy：Block reward halves every 210,000 blocks
- No pre-mining

Countermeasures

Any public chain is facing various types of attacks, and The TAO is no exception. We have taken the following countermeasure policies:

1. Gang of Miners Attack

In PoC ecosystem, gang of miners is not uncommon. They savagely loot PoC mining coins like locusts, grab short-term economic benefits, and cause serious damage to the ecosystem. Keep this in mind, we have made a countermeasure policy. First is the plot parameters. We have modified the plotting algorithm, the length of account ID turns from 8 bytes to 20 bytes which is not a simple digital expansion. It disables mining bully to switch on large amount of computing power for benefits by using harddisks already plotted in early stage when the computing power of entire network is not big enough.

Secondly, we split the mainnet into pre-mainnet and mainnet phases which is ruled by the whole net capacity power and block height.

2. 51% Attack

PoC algorithm has a 51% attack problem similar to PoW. To end this, we will adapt the latest algorithm.

3. Privacy Disclosure

We keep close track of the cutting-edge zk-SNARKs and zk-STARKs algorithm and adopting the latest research results in real time to maintain the robust stability and privacy of The TAO network.

4. Cold Startup

The startup of TAO mainnet splits into two stages, the pre-mainnet and the mainnet. The difference is the whole net' s 'capacity-power'. The trigger value is 500P and the block height. The block reward during pre-mainnet is split:

(0, 1P) && height<2016 miner vs foundation 1:9

[1P, 10P) && height<6048 miner vs foundation 2:8

[10P, 50P) && height<14112 miner vs foundation 3:7

[50P, 100P) && height<22176 miner vs foundation 5:5

[100P, 500P) && height>22176 miner vs society fund blind box mode, miner gets a random reward between 25 and 50

[500P, ∞) miner : 100%

That is to say, when we have 500P capacity-power, we enter mainnet stage.

Our Team

The TAO is the first anonymous coin from PoC ecosystem. we are geeks and white-hat hackers from all over the world. Although coming of a noble background, we would like to keep anonymous instead of letting the great fame behind become a burden to The TAO. We dedicate our math and crypto skills to the community of blockchain and the whole society.

Our email address is thetao[at]riseup[dot]net.

Don’ t call us, we will call you if you are special enough.

Community

The health, stability and sustainable development of ecosystem are closely associated with the community. We value and respect the community. The core team will make joint efforts with the community to guide and promote the development of The TAO. The evangelists of the PoC have already laid a small space for us. With greeting to them, we start the global recruiting of community manager and volunteers.

Let us work together to create the glory of PoC + zk-SNARKs!

Roadmap

The TAO will launch the mainnet directly to make a privacy coin for PoC ecosystem and even the whole world.

In the next step, we will complete the integration with the private IM tool at a rate of a large version updating every 6 months, introduce NFT, DeFi and Oracle, realize a real privacy coin wallet with zero-knowledge proof for mobile app and a privacy stable coin base on PoC consensus, and so on.

In Q3 2022, we will list in DEX. In Q4 2022, launch in 1 ~ 2 renowned big exchanges.

All glorious things are happening quietly, so stay tuned ...

Acknowledgements

Greeting to Satoshi Nakamoto，Xiaoyun Wang，Vitalik Buterin，Zcash Core Team，Burst Core Team，BHD Core Team &Community，and countless friends and families behind us.

The journey of a thousand miles begins with a single step.

- Lao Tsu in Chapter 64 of Tao Te Ching

References

https://bitcoin.org/en/bitcoin-paper

https://ethereum.org/learn/

https://z.cash/technology/

https://www.burst-coin.org/

http://www.btchd.org/

https://royalforkblog.github.io/2014/08/11/graphical-address-generator/#thetao.cash

https://bitinfocharts.com/bitcoin/address/1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF

https://en.wikipedia.org/wiki/Pigeonhole_principle