SafeTitan

V1.5.1 WhitePaper

Those who have a reasonable understanding of the various popular crypto Blockchains know that we are living in exciting times. We are witnessing the metamorphic transformation of global finance, money & civilization. The impact of digital money on every living soul on this planet will be huge. Money-related Blockchains will exponentially enhance and transmute wealth, finance and online security. Overtime crypto will transform the entire notion of trust.

SafeTitans core pillar will ultimately be a highly secure & private digital token that will be simpler to use than the world's fiat currencies. Safe Titan tokens will be designed in such a way that private keys will be simple to recover, anyone with a standard PC will be able to participate in validations transactions and easily mine tokens (rather than massive organized mining operations that are becoming more and more centralised into huge, expensive, environmentally destructive farming pools.) .

We have come a long way since Satoshi's white-paper was released for Bitcoin. Safe Titan will build on the older previous cryptographic technology such as Rivest, Hellman Wuille, Merkle and others. SafeTitan will use a new refined cryptography that will take us into the next chapter of the Bitcoin experiment. Satoshi will be proud that a new team of engineers, developers, blockchain enthusiasts and core community members will be implementing some of Satoshis ideas that have not yet been realised (such as natural log governs key blockchain constants related to work difficulty resets). In the same way as the Internet developed from the early ARPnet days and how the Facebooks stood On the shoulders of MySpace, Safe Titan will stand on the shoulder of the current Blockchain giants and propel the crypto world into the future.

Ultimately, Safe Titans Proof of Time & Proof of Space consensus algorithm a will bring a private, highly secure, environmentally friendly and fully decentralized alternative to both proof of stake & proof of work. Regular users will be able to mine , preventing issues such as mass pooling and 'centralization creep' that has happened with some of the current popular Blockchain. Furthermore, regular users would not need to spend a huge amount of money staking (e.g. the 32 Ethereum required to stake ETH 2.). And, of course, our key feature is ease of use. This will help propel Safe Titan to mass adoption.

Proof of Space

This protocol works by a verifier sending a challenge to a prover and the prover confirms to the verifier that a certain amount of storage space at that exact time. Space is initialized by plotting, the amount of space that can be used is not limited. It's performed only once and can last for several hours or even days. The actual plot size is determined by a k parameter space = 780 * k * pow(2, k - 10), with a minimum k of 32 (101.4 GiB). This is based on Beyond Hellman (https://eprint.iacr.org/2017/893.pdf); to ensure its nested function and contains heuristics.

2.2.1 Algorithms for PoS

A proof of space is specified by the four algorithms given below 15

PoS.init on input a space parameter $N \in \mathcal{N}$ (where $\mathcal{N} \subset \mathbb{Z}^+$ is some set of valid parameters) and a unique identifier pk (we use pk to denote the identifier as in Chia it will be the public key of a signature scheme) outputs[10]

$S = (S.\Lambda , S.N = N , S.pk = pk) \leftarrow \text{PoS.init}(N, pk)$

Here $S.\Lambda$ is the large file of size $|S.\Lambda| \approx N$ the prover needs to store. We also keep N, pk as part of S as it will be convenient.

PoS.prove on input S and a challenge $c \in \{0, 1\}^w$ outputs a proof $\sigma = (\sigma.\pi , \sigma \sigma.N = S.N , \sigma.pk = S.pk , \sigma.c = c) \leftarrow \text{PoS.prove}(S, c)$

Here $\sigma.\pi$ is the actual proof, the other entries in σ are just convenient to keep around. PoS.verify on input a proof σ outputs accept or reject

$\text{PoS.verify}(\sigma) \in \{\text{reject, accept}\}$.

We assume perfect completeness

$\forall N \in \mathcal{N} , c \in \{0, 1\}^w$, $\Pr[\text{PoS.verify}(\sigma) = \text{accept}] = 1$ where $S \leftarrow \text{PoS.init}(N, pk)$ and $\sigma \leftarrow \text{PoS.prove}(S, c)$

Proof Of Time

This is also referred to as a verifiable delay function, it confirms the execution of a sequential function was run X number of times. Essentially this is similar to multiple hashing of a number. This differentiates from Bitcoins proof of work, i.e.

it would not be possible to simply purchase additional processing power to expedite the calculations. The repeat squaring must be proved x T times, so time must be Θ(T). Furthermore it must be proven that this was done correctly.

A POT is specified by the two algorithms given below.

POT.solve on input a challenge $c \in \{0,1\}^w$ and time parameter $t \in Z^+$ outputs a proof

$\tau = (\tau.y , \tau.\pi , \tau.c = c , \tau.t = t) \leftarrow$ VDF.solve(c, t)

and runs in (not much more than) t sequential steps (what a step is depends on the particular VDF). Here $\tau.y$ is the output and $\tau.\pi$ is a proof that $\tau.y$ has been correctly computed. For convenience we also keep (c, t) as part of τ .

POT.verify on input τ outputs accept or reject.

POT.verify(τ) $\in$ {reject, accept}

Verifying must be possible in t steps, for existing POTs verification just takes log(t) [Pie18] or even constant [Wes18] time. We have perfect completeness.

$\forall t, c$: POT.verify(POT.solve(c, t)) = accept

The two security properties we require are

uniqueness: It is hard to come up with any statement and an accepting proof for a wrong output. More precisely, it is computationally difficult to find any τ^0 where for $\tau \leftarrow$ POT.solve($\tau^0.c, \tau^0.t$) we have

POT.verify(τ^0) = accept and $\tau.y \neq \tau^0.y$.

Note that we only need $\tau.y$ (but not $\tau.\pi$) to be unique, i.e., the proof $\tau.\pi$ showing that $\tau.y$ is the correct value can be malleable. This seems sufficient for all applications of POTs, but let us mention that in the [Pie18, Wes18] POTs discussed below also $\tau.\pi$ is unique.

sequentiality: Informally, sequentiality states that for any t, an adversary A who makes less than t sequential steps will not find an accepting proof on a random challenge. I.e., for some tiny

Pr[POTs.verify(τ) = accept $\wedge$ $\tau.c = c \wedge \tau.t = t$: $c^{rand} \leftarrow \{0,1\}^w, \tau \leftarrow A(c, t)$] $\leq$

Let us stress that A is only bounded by the number of *sequential* steps, but they can use high parallelism. Thus the POT output cannot be computed faster by adding parallelism beyond what can be used to speed up a single step of the POTcomputation.

SafeTitans First Steps. Mass global Awareness.
Titan, Saturn's largest moon, will be our destination! Strap yourselves in and join us on this rocket ship! We'll be launching a global marketing campaign in multiple regions culminating in promotion through dozens of influencers & numerous other channels to two of the world's most popular crypto locations. China & South Korea. We welcome you to join a truly global community of crypto enthusiasts.

Our secret sauce for community strength is direct access to hundreds of millions of crypto enthusiasts from both China & South Korea. Recent competitors have ignored this lucrative region, our marketing and promotion efforts will reach hundreds of millions of potential community members via multiple marketing funnels. We have an experienced team who understands the Chinese & South crypto market/communities ensuring significant community engagement.

SafeTitans Initial Launch

Valuation bubbles tend to become somewhat exuberant with the high APY averages we all know and love, however, there are traps along the way and many DEFI players have been caught out. The continuous increase in popularity of DEFI has resulted in sky-high APY's. APY LP farming rates have lured many of us into the inevitable trap, being nudged out the way by those who got in early with higher staking rewards. Anyone who has at least dipped their toes into this space knows that those APY rates with multiple digits lure us in like the sirens of old. Then suddenly, bam, the valuation bubble explodes and the price hits the floor. Many have now adopted static rewards to avoid such issues. Static rewards, also known as reflection, virtually eliminate many of the issues caused by farming rewards.

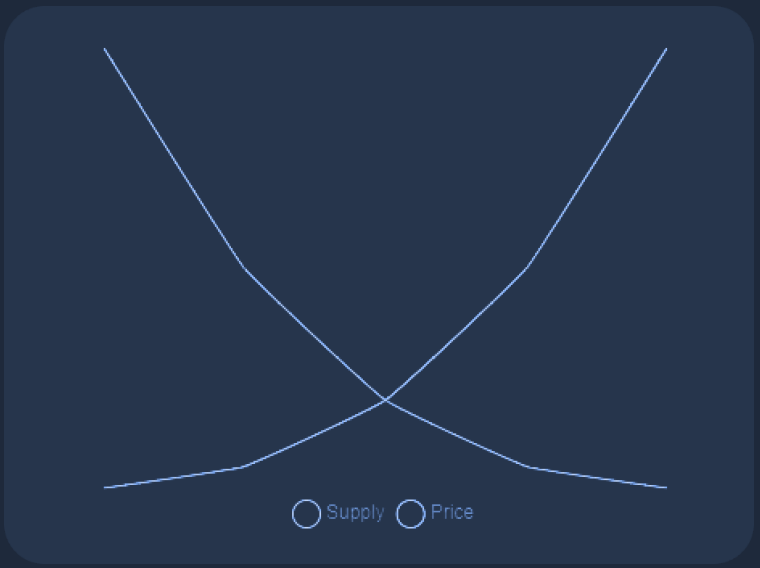
The Auto liquidity Pool (LP) -

Users of the platform will benefit from automatic LP. This is one of our initial key areas of focus. Our contract will ensure tokens from buyers AND sellers are added to the LP ensuring a rock-solid floor on the price of the token. This guarantees a mechanism that is resistant to arbitrage thereby securing the volume of Safe Titan as a reward for holders. This will increase Safe Titans stability i.e. the additional LP adding is 'tax' to the overall liquidity of the token. This is separate from the burn function and other reflection tokens that are usually only of benefit in the short term from the granted reduction of supply.

While the Safe Titan token LP goes up, the stability of the price equates this

function with the benefit of a hard price floor and cushion for holders. Our objective here is to stop the huge dips caused by whales who may have accumulated the token and decide to sell later in the game. This ofcourse keeps the price from fluctuating as much as if there was no automatic LP function.

This will remove many of the issues we've seen with the current DeFi reflection tokens. Our model & protocol will prevail over many of the now outdated, troublesome reflection tokens for these reasons.



The Static Option -

Several problems are immediately solved with static rewards. The reflect mechanism nudges holders to keep their tokens to benefit from higher returns that are based on percentages carried out and depend upon the total tokens held by the owner. Furthermore, the number of rewards is conditional on the volume of traded tokens. This process will alleviate most of the downward sell pressure put on the token caused by early buyers selling tokens after farming wacky super high APY's.

Manual Burns.

Burn baby burn will become a Safe Titan meme. For the most part burns matter, not always. For example, a continuous burn is often beneficial shortly after token release, however, the burn cannot be finite or controlled.
Team-controlled burns that are promoted on achievements ensure the community is aware and rewarded. The specifics of manual burns and the figures will be traceable and advertised.

Our burn strategy will be mostly of benefit to long-term token hodlrs. The number of tokens burned will be advertised on our site and across social media. This ensures total transparency in identifying the current supply in circulation at any given time.

Safe Titan Protocol
Safe Titan employs 3 simple functions: Reflection + LP acquisition + Burn In each trade, the transaction is taxed a 10% fee, which is split 2 ways.

5% fee = redistributed to all existing holders
5% fee is split 50/50 half of which is sold by the contract into BNB, while the other half of the Safe Titan tokens are paired automatically with the previously mentioned BNB and added as a liquidity pair on Pancake Swap.