SpiderDAO

White Paper version 0.1

The First Hardware-based DAO on Cosmos

Table of Contents

Executive Summary

SpiderDAO is the industry's first hardware-enabled DAO that bundles multi-layered hardware and software tools on top of a decentralised network protocol. This enables members to ring-fence against Dark DAO attacks and establishes an inherently democratic governance mechanism so that the evolution of the network, development decisions and the subsequent value capture created is distributed fairly amongst its members instead of a centralised party.

A common problem in decentralised networks occurs when large investment bodies (or "whales") create an oligopoly by accumulating and staking a significant portion of tokens and subsequently gaining majority voting rights to influence the development of the network for personal gain. SpiderDAO seeks to solve this problem by introducing a dual governance structure whereby users of the network utilise hardware devices (routers) as Proof of Use to retain representative voting rights and thereby restricting voting participation for non-users.

Combining hardware safeguards and building on top of the Cosmos Tendermint consensus protocol enables SpiderDAO builds in whale-resistant mechanisms whilst creating a highly scalable, interoperable and stable decentralized governance system.

What is a DAO?

A DAO (Decentralised Autonomous Organization) is an organization represented by rules encoded as a transparent computer program, controlled by the organization members and not influenced by a central government. A DAO's financial transaction record and program rules are maintained on the blockchain. The core component of this system is a decision-making system that allows members of the community to collectively own and manage assets within the DAO through consensus rather than relying on centralised party.

Every member of the community is able to submit proposals to fund projects. The DAO then enables the community to collaboratively come to a decision on which projects receive funding. Through this process, a community is able to self-organise and scale regardless of growth whilst maintaining accountability, agility and transparency in the decision-making process.

The wide benefits of DAOs are beyond the scope of this paper but additional information can be found here.

Current problems with DAOs

Whilst smart contracts have long been hypothesised to be effective mechanisms for running on-chain elections in a transparent, autonomous and decentralised way, unfortunately, the last few years of implementing these models have revealed key vulnerabilities that threaten the entire system if not addressed.

One of the biggest problems DAO's have faced since inception is on-chain vote-buying, which has led to the rise of “Dark” DAOs. The foundations of the vulnerability stem from the low barriers to entry for malicious actors (whether individuals or larger entities) to skew the democratic voting process by buying up large amounts of tokens to achieve an unfair share of the voter's rights and influence the decision making in an unfavourable way.

Ethereum founder, Vitalik Buterin and core ethereum researcher, Vlad Zamfir have both criticized how on-chain voting mechanisms have a tendency to descend into plutocracies whereby the wealthy who have the power to accrue more tokens, have the biggest say.

In this section, we will look at the points of weakness in current systems, likely attack vectors and the implications of a successful attack.

Blockchain vs Traditional Voting

There are various flavours of blockchain voting schemes utilised by multi-billion dollar projects like EOS, Tezos, Tron, Polkadot and Decred in an effort to formalize the decision making processes in their ecosystems. The majority of these schemes utilise a form of delegated Proof of Stake model - this requires selected nodes to validate transactions on a network. Token holders are allowed to stake their tokens, to demonstrate their ownership of the token to the network, which subsequently gives them voting power based on the number of tokens staked.

And whilst current on-chain voting schemes have faced many challenges such as privacy, latency and scaling, these haven’t been as critical to the future of the DAO as the issue of vote-buying.

In traditional political systems, vote-buying is a corrosive form of election fraud that has had detrimental impacts of undermining election integrity. Nevertheless, academic research demonstrates that malicious vote-buying schemes usually breakdown in normal market conditions for several reasons:

1. Vote-buying, in most cases, is a crime and punishable by law. In traditional systems tracing the source of the vote back to the individual is a relatively easy endeavour and thus is infrequently practised;

2. Where secret ballots are used, compliance is difficult to enforce;

3. When a voter does sell their vote, there is no guarantee that the counterparty will pay, essentially relying on a high-risk trust-based system.

No such blockers exist in blockchain systems where vote-buying schemes can be run effectively through smart contracts that by-pass the pseudonymous, jurisdictional, legal and trust complications disincentivizing this from occurring in traditional systems.

Various solutions have been proposed by the likes of David Chaum, Benolah and Tuinstra looking to resolve these problems through the implementation of software logic mechanisms from “vote receipts” to second-layer solutions to mitigate the challenges of vote-buying and coercion attacks but have had limited success thus far.

Attack Vectors

Let’s look at how voting can be skewed. In the simplest dPoS models, where token holders are allocated one vote per token staked and have the freedom to seamlessly buy or sell tokens right until the closing block number when the vote is cast.

1. **Smart Contracts:** This form of attack entails the malicious party either “borrowing” or buying the smart contract for a period of time necessary to influence the vote. In order to qualify for voting, this party will simply need to accrue the appropriate amount of ERC20 tokens until the vote date, take part in the voting and subsequently dump their tokens once a consensus has been reached and enforced by the underlying blockchain. Whilst some governance mechanisms require additional criteria to partake in the voting process, these are often circumnavigated based on the low levels of friction to buy and sell voting power.

2. **Trusted Hardware**: Another form of vote-buying involves the use of trusted hardware. Such hardware utilised a feature called remote attestation - a trusted computing mechanism that allows user A to prove to user B that they are running a certain piece of code. Whilst this was initially designed to prove that the code you're running is not malicious (e.g. the user isn't copying files that they have temporary access to, like a TV show), nefarious actors have flipped this paradigm on its head. Using the same trusted hardware, they are able to shackle cryptocurrency users that restrict their space of allowed behaviours and gives the vote-buyer a limited use of the token owner's wallet key. Within this structure, the vote-buyer is able to utilise the voting power of the tokens in the token owner's wallet, without having the ability to withdraw funds. In exchange, the vote buyer makes a payment to the token holder in a trustless manner.

3. **Dark DAOs:** Whilst smart contract attacks are a low-complexity form of executing such an attack and can be more easily detected through on-chain activity, a more concerning attack vector arises from the creation of a Dark DAO. In its simplest form, a Dark DAO is an entity constructed using smart contracts that would be undetectable, systematically buying user votes to overwhelm a governance system, issue false signals and engage in market manipulation. The Dark DAO often uses trusted hardware to run the computations in an "enclave" (i.e. private setting) which makes it very difficult to detect. Similar to the staking reward mechanisms on decentralised exchanges, Dark DAO attracts vote sellers by paying users to run their custom wallet software in exchange for "lending" their voting power until some threshold is reached to execute an attack on the DAO. Most damaging is that the turnout for on-chain voting in DAOs has been historically low and thus token holders who do not wish to exercise their voting rights or feel their vote doesn't matter, have an incentive to "lend" their voting right to the Dark DAO in exchange for a reward.

   In such a setup, is difficult for a DAO's creator to counteract this attack because the untraceability fo the Dark DAO makes it difficult to distinguish between the "real" DAO voters and Dark DAO votes including the total amount of money pledged, the number of participants and precise logic of the attack.

Implications of Dark DAOs

Even the primary implications of Dark DAOs can be catastrophic and expose participants to manipulation, coercive forces and can result in token holders, unknowingly, responding to false signals created by the unscrupulous forces to further amplify decision-making in the wrong direction. These forces often de-legitimize the outcome of elections and create mistrust in the entire system.

As the sophistication of Dark DAOs evolves, the implications can be even more far-reaching. Consider the use case in identity theft, for instance, where a Dark DAO is used for getting through credit checks secured by key-based identities by borrowing such keys from users with good credit.

A key conclusion drawn from these problems shows that permissionless e-voting requires trusted hardware that increases the friction points associated with vote-buying. However, having a hardware model where a user is able to generate their own keys is not enough (as detailed above). The hardware needs to act as an integral part of the governance mechanism where together with a token design that makes it inherently difficult for voting right transfer to occur to avoid the inevitable plutocracy we have seen develop in previous governance systems.

SpiderDAO has found a solution to this new-age problem by introducing a set of rules that must be abided by to qualify for the right to an on-chain vote via the DAO.

Product Offering

By deploying a combination of hardware and software tools on top of the Cosmos Governance protocol, SpiderDAO bakes-in an inherently democratic, whale-resistant governance mechanism. This enables the evolution of the network, feature development decisions and the subsequent value creation to be distributed fairly amongst its users instead of being manipulated by a well-resourced, centralised party.

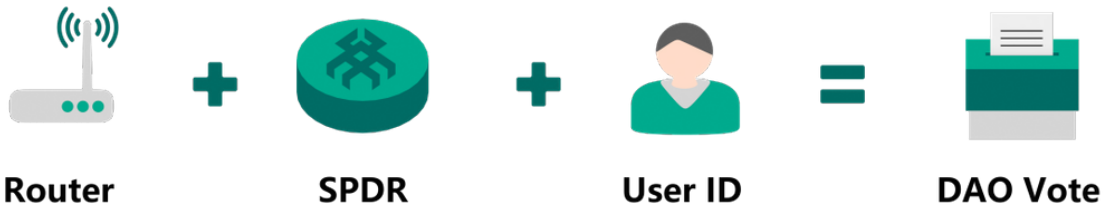
This is achieved through the introduction of a unique dual-governance model with three components - the SPDR token, SpiderNetwork and the SpiderConnect Hardware Router. The SpiderDAO utilises this dual-speed model to shift the voting

power away from DAO token holders (as is in traditional DAOs) and towards the hardware owners.

The SpiderConnect Hardware Router is purchased and distributed to each community member where it can then be connected to the SpiderNetwork via the Spider Dashboard.

The Spider Dashboard is a simple setup tool that enables members to plug and play their router by registering their MAC address and unique serial number, syncing up their hardware device with the rest of the network and setting up their SPDR Wallet. Spider Dashboard will provide a centralised interface where members can easily access the DAO, stake their tokens, view the status of the network as well as submit, review and vote on community proposals.

The SPDR tokens will act as the utility key to partake in the voting. An initial portion of the SPDR tokens will be distributed to early adopters through a seeding cycle after which additional tokens can be mined both through staking and participation in the DAO. The SPDR tokens may also be converted into LP tokens through liquidity provisioning and thus may also be staked to qualify for the voting process (see more in SPDR Tokenomics).



In order to gain the right to participate in the voting process, the DAO member will need to satisfy the following criteria:

1. They must have a SpiderConnect Hardware Router connected to the SpiderNetwork.
2. They must have a minimum amount of LP tokens or staked SPDR for a set period of time - the parameters of which will be determined by the DAO.

Upon registering on the SpiderDAO Dashboard with dVPN Identifier, SPDR Wallet and receiving approval from the Validator Node (see “Validator Node” below for more details), the member will be able to raise proposals, vote on existing proposals and partake in the voting mechanism of the DAO.

Once a member has successfully qualified to partake in the DAO, the weighting of the vote will be determined by the hardware router and **not** the quantity of tokens being staked via a members' wallet (as with other DAOs). Thus, one approved SpiderConnect Hardware Router will equate to one on-chain vote, enabling demonstrable decentralisation to be maintained at a hardware level.

This dual system, therefore, introduces additional safeguards into the voting process that greatly benefit organic supporters whilst penalising, making it difficult (and costly) for short termist outside parties to "buy" uneven voting rights through token purchases on the open market.

Validator Node

To ensure the access criteria are satisfied, SDPR will be running a validator node to ensure DAO members hardware devices are online and the wallet address associated with the requirements voted by the DAO have been met. Once the validator node has confirmed this, the user will unlock the right to vote.

The SpiderDAO validator node will be checking for a Unique Identifier which will be the Router MAC Address & Serial number (SpiderIdentifier) along with the SPDR Wallet address of the holder to ensure they meet the DAO's pre-defined standards.

To negate any hardware vulnerabilities or hardware manipulation (for example MAC Address Spoofing) this validator node will be running constantly, checking the integrity of the Unique Identifiers. If a cloned SpiderIdentifier is found, the validator will remove the right to vote, brick the device and remove it from the network. Additional measures will be built-into the distribution system, monitoring both volumes of routers by shipping volumes and activation of devices per IP address to provide early warning signs of potential malicious activity.

As a final layer of protection, a distributed ledger will be used to create a Hash Table Director on the Cosmos base chain where all the MAC addresses and serial numbers for Spider stock inventory would be stored. Only the Routers with the correct SpiderIdentifier may be activated as members of the DAO, presenting an additional physical barrier to entry for malicious intent.

Governance

SpiderDAO will be supported by Cosmos Governance by utilising the BFT Tendermint as the consensus mechanism enabling us to combine proof of stake, on-chain governance and hardware anchoring within the governance system.

To enable the continuous development, DAO members will coordinate both formally on-chain (see below) and informally off-chain to collaborate on proposal evaluation before a formal election is cast. We have selected to partner with Cosmos instead of Ethereum in augmenting this governance structure given the on-chain governance features that we expect to drive increased member engagement within the decision making process (seeking to address the problem of low DAO member engagement observed across other DAOs).

Additionally, Cosmos provides flexibility in changing parameters in how the DAO itself runs - examples of this may include inflation rate of the network, how rewards are distributed, how slashing parameters are applied, level of quorum required, how long the unbonding period is etc.

Voting Process

The voting process itself will be conducted through a 3-stage process - Deposit Stage, Voting Stage, Tallying Stage.

1.*Deposit Stage*

Any registered member can submit a proposal for others to view. The only cost associated with submitting a proposal is a small transaction fee for operating on the network. However, throughout the voting period, a proposal must have quotes amount of SPDR deposited to it for it to proceed to a vote. This period lasts 2 weeks, but if the minimum amount SPDR is reached sooner the proposal will pass to voting immediately.

2.*Voting Stage*

The voting state lasts 2 weeks. Rather than depositing SPDR, participants in this governance stage are actually voting Yes, No, No(With Veto) or Abstain. If a proposal reaches quorum **or** the minimum threshold defined by the protocol of votes, it will pass to the next stage for tallying. Only members satisfying the voting eligibility

criteria (see previous) are eligible to partake at this stage. Each hardware router is allocated a maximum of one vote assuming the voting eligibility criteria have been met. Voters can also change their vote right up until the closing period.

3. *Tallying Stage*

After two weeks the proposal voting will end and the following condition will be taken into consideration to determine if it passes or not:

- Quorum: more than 40% of the total staked tokens at the end of the voting period need to have voted
- Threshold: More than 50% or a majority of the tokens that participated in the vote, excluding “Abstain” votes must have voted “Yes”
- Veto: Less than 33.4% of the tokens that participated in the vote, not counting “Abstain” votes, have vetoed the decision “No (With Veto)”.

If any of these conditions are not met, the deposit associated with the denied proposal will not be refunded. These funds will be sent to the SpiderPool.

SpiderPool

To fund the continued development of the DAO, a SpiderPool will be created which will accumulate 2% revenues generated by Spider VPN services. These resources will be used to fund the improvement of the DAO which, in turn, will incentivise the evolution of the project. As the DAO grows in sophistication, more advanced consensus and voting systems may be introduced to act as the incentive mechanism to reward participants for contributing to the DAO and driving the right behaviours. Smart contracts can be added to the DAO to add new features and ensure further improvements. It is envisioned that multiple products will be developed to leverage the SpiderDAO, each of which will be asked to make a revenue to the DAO to fund future development.

SpiderVPN: The First DAO-Governed VPN

Overview

The SpiderDAO provides a unique governance infrastructure layer for a hardware-enabled DAO and can be applied in a variety of use cases. As the first use case, Spider will leverage its well-established presence in the hardware VPN market

together with a partnership with Sentinel, an established dVPN provider and BPSAA Alliance member, to create a fully self-governing decentralized VPN network called SpiderVPN.

In the first instance, the SpiderVPN will provide centralized VPN services with DAO eligibility (assuming qualification criteria are met). As SpiderVPN successfully integrates with Sentinel, a private cloud will be used to serve decentralised VPN access with enterprise-grade security running on the SpiderNetwork utilising Sentinel's infrastructure. SpiderVPN will enable users to augment the privacy benefits of leveraging VPN connectivity with distributed ledger technology that decentralises the governance structure and removes the single point of failure that is the weakest link in traditionally centralised systems. In 2021, the SpiderVPN will run premium nodes on the dVPN, serving higher amounts of bandwidth for enterprise clients.

Once setup, SpiderVPN will offer the ability to tunnel user bandwidth through a decentralized VPN network which introduces a whole new level of security beyond traditional VPN services, whilst offering multi-functionality to easily plug and play various devices with a simple configuration.

It will integrate a host of features such as Network Monitoring, Parental Controls, IP Filtering/Blocking, Kill Switch Control, Geo Filtering for Gamers, AdBlocker, Deep packet inspection (DPI) and Band Steering. Relay nodes can be used to run DNS ZONE servers, which can be implemented at the hardware level and use domestic IP's. This can be used as a blockchain relay network with random exit nodes which can co-exist with the Sentinel dVPN Network. This will run on the SpiderVPN Network powered by Sentinel and will make GEO Unblocking unstoppable by any 3rd Party, government or authority.

Furthermore, military-grade encryption using both SOCKS5 or Wireguard Servers will enforce quantum level encryption standards such as AES 256 or Poly1305; the complete transparency of the code base will be available for full provability, and distributed nodes across the globe, enabled by the community, allow users to choose the optimal servers based on geographic location and speed. Advanced router features will enable users to benefit from seamless connectivity, full protection from IP leakage should a VPN fail all at a cost-effective price.

This ultimately provides users with unrivalled private, open and unrestricted access to the internet whilst empowering them to contribute to the SpiderVPN community, host nodes and influence the direction of development through the SpiderDAO governance mechanism.

Modes of Participation

"Service Only" - Users wishing to primarily utilise the dVPN services without participating in the DAO can pay for the service either with SPDR tokens or FIAT currency. A portion of the revenue accrued for payment of the service will be redirected to the SpiderPool to fund community developments. Passive users who opt-out of the governance mechanism may still stake their SPDR tokens through the SpiderDashboard to provide liquidity in the network and receive LP tokens in return (see SPDR Tokenomics for further detail).

"Active Participants"- Users wishing to proactively participate in the voting mechanism will be rewarded with additional SPDR tokens for their involvement which can be utilised either for either providing liquidity to the network through staking or paying for the rendered VPN services.

Secondary Marketplace

SpiderVPN users will have the ability to resell unused VPN bandwidth to back to the community. The marketplace will be available via an addon in the SpiderDashboard which will provide an order-book style model of available bandwidth.

All transactions on the marketplace will be denominated in SPDR tokens and buyers/sellers will be able to perform transactions provided they are connected to the SpiderNetwork with corresponding SpiderWallets.

A small fee will be charged for all transactions occurring in the marketplace and collected funds will be assigned to the SpiderPool for re-allocation to community projects.

Distribution of the Hardware

The initial distribution of the hardware routers will be executed by an Alliance Partner who has agreed to cover the cost of the first 1000 devices to seed the SpiderVPN Network. Early participants in the token sale who contribute $2000+ will receive the tokens + one free router (up to a maximum of the 1000 free devices available for distribution).

Should a member partake in the initial token sale and choose to contribute less than $2000, they will not receive a free router. However, they may still purchase the router separately via the SpiderVPN website (https://spidervpn.org/).

Once the hardware device has been bought, setup and all the prerequisite criteria satisfied, the member will have the ability to opt-in to vote on future developments once the DAO has been launched.

SPDR Token

Decentralized Finance is here to stay and will change the way we approach and judge the value of digital assets. We believe there is value in implementing aspects of typical “DeFi token economics” into the SPDR token.

In addition to enabling token owners to purchase services and contribute to the community via the DAO, the SPDR token design allows for additional features to be integrated as the system evolves. The key aim of the SPDR token will be to capture the value created within the ecosystem such that the SPDR token’s value will reflect the increase in ecosystem usage. Thus, a rise in usage volume increases SPDR staked, leading to greater SPDR demand which will subsequently increase the value of SPDR given the deflationary token mechanics.

The initial use cases for the SPRD token will be as follows:

1. Eligibility for voting rights in the DAO (in conjunction with hardware) (DAO participant)
2. Liquidity Mining: Distribution of 60% of the network to liquidity providers
3. Liquidity as Utility” (LAU) - Free dVPN access to LPs.
4. Substitute payment for SpiderVPN services (Service consumer)

A multi-layer utility token

Layer 1: DAO Governance

- The purpose of SpiderDAO is to direct the flow of resources towards projects and proposals that offer the best route for growth. SpiderDAO holders are incentivised to assess different proposals and vote to fund the most promising initiatives to evolve the community. If no consensus is reached during the

voting process (see Voting Process), the outstanding SPDR tokens will be returned to the SpiderPool for future developments.

- Setting up a node in the SpiderDAO requires compatible hardware (like the SpiderConnect Router) as well as staking a set base amount of tokens. Once the node has been setup, other token holders may amplify the voting power of a node by staking more tokens on it (similar to a delegated proof of stake (DPoS) consensus algorithm would work).

Layer 2: Liquidity Mining

- 60% of SPDR supply will be unlocked through liquidity mining. Participants will be able to mine this supply by staking LP in the SPDR/ETH or SPDR/USDC liquidity mining pools. We believe that the network should be distributed to holders of the tokens instead of the investors that happened to be early but decided to renounce their stake in SpiderDAO. This is reflected by tying the release of over half the tokens to holding and staking the token for the duration of the liquidity mining program.
- Through the SpiderVPN “Liquidity as Utility” program, token holders can participate in liquidity mining while also enjoying the benefits of SpiderVPN Utility Mining (see Layer 3).

Layer 3: Liquidity as Utility (LAU) - Free dVPN access for LPs

- SPDR tokens are required to receive LP tokens by providing liquidity to SPDR/X pairs on decentralized exchanges. Greater depth of the SPDR market means lower slippage and a better buying experience for investors and traders. Therefore, some of the SPDR utility will be attached to SPDR-based LP tokens instead of the token directly. Due to SPDR being required to receive those LP tokens, any utility the LP tokens have is also inherent to SPDR itself. We call this mechanism **“Liquidity as Utility” (LAU)**. We want to encourage token holders to lock their tokens in liquidity and stake their received LP tokens by attaching utility to the LP tokens.
- Everyone dealing with blockchain, DeFi, and digital assets should be using a dVPN to protect their data, privacy, and assets. SpiderVPN is offering a unique way to access its dVPN network for its token holders: SPDR Liquidity Providers receive access to the SpiderVPN by staking the equivalent of at least $500 in liquidity in the form of LP tokens. Acting as a liquidity provider is an act by an individual that benefits the entire community. Via this service will not only be rewarded with liquidity mining rewards and LP profits but also with free access to the SpiderNetwork.

SPDR Utility Development

Over the lifetime of the SPDR token, the ratio of importance for the different Utility Layers will gradually shift from Liquidity Mining towards “Liquidity as Utility” and DAO Governance. As Liquidity Mining gradually recedes, the overall adoption of the DAO ecosystem and everything in it will start to determine the long-term token utility.

We believe that the LAU model is a truly unique approach to token economics. By centring utility around LP tokens, we believe that token velocity issues are addressed by creating an incentive to lock tokens for the benefit of both the entire community while being rewarded by a combination of LP profits and token utility.

Leadership Team

Our overall experience as a team gives us a cutting edge when it comes to the development of diverse technologies. We all have a drive and passion for success and this motivates us to achieve originality in the blockchain space.

Nathan Varty - CEO

Nathan is an experienced entrepreneur specialized in IoT development and operations, Skilled in management of onsite and remote IT Help Desk Administrators and Developers. He has been successfully overseeing SpiderVPN since 2017. He also managed the full oversight of multiple projects from start-up to completion.

Žiga Flis - Co-founder

Before joining SpiderDAO, Žiga was the Chief Technology Officer at RiveX, where he contributed to the development of various blockchain technologies. He is experienced in on and off-chain tech and has a passion for developing decentralized solutions.

Anas Sayed - CTO

Acting as Project Manager and working with teams of Developers and Administrators. Anas has a background in hardware engineering, full network stack development and computer science working with embedded systems for Open Source network/entertainment Operating Systems design. Previously worked for A-Solutions, Pensil Media, FuboTV.

Advisors

Dr. Alfie Zhao - Hardware Advisor

Chief Technology Officer, GL Technologies (Hong Kong) Limited. Winner of CES innovation awards in 2019 and 2020. His PhD in engineering management compounds has a proven track record in hardware IoT since 2012.

Pierre Laurent- Blockchain Technology Advisor

Pierre holds a Master of Engineering in Computer science from a French Engineering School, he joined the cryptocurrency exchange Gatecoin in 2018 to oversee the development of the European office as Blockchain Partnerships Manager. After that, he Co-founded Atka advisory.

Strategic Partners

GL.iNet is a leading developer of reliable networking devices.

Kyro is a deep media search engine.

Sentinel is an interoperable networking layer for distributed services.

Atka is an advisory firm for blockchain projects.