Whitepaper

Octopus Network: Where Web3.0 Happens

octopus network

Appchain

Bitcoin is an application-specific blockchain (appchain) — The first and the most successful one. Inspired by the decentralization tactic invented by Bitcoin, a bunch of appchains were developed from 2011 to 2015. Some aimed at becoming a better Bitcoin, while the others targeted areas other than currency. The former left us with dozens of cryptocurrencies, such as Litecoin, Monero, Stellar, to name a few. But the latter, such as Colored Coins and Namecoin, achieved next to nothing. The commonly agreed reason is that the Bitcoin blockchain is purpose-built and unsuitable to address other use cases by being forked or extended. We may call this period the "1st cryptonetwork innovation wave."

Ethereum is a general-purpose public blockchain equipped with a Turing-Complete virtual machine, which could theoretically execute any computation, as long as it remains within the complexity limitation (gas limit). The major EVM programming language Solidity, with Javascript-like syntax, is easy to learn and very good at controlling on-chain assets. The combination "EVM + Solidity" and associated tools propelled the 2nd wave of cryptonetwork innovation, from which emerged thousands of decentralized applications. Unfortunately, none of them could retain many users for an extended period until the 2020 DeFi explosion.

While it's not surprising to hear some of the brightest minds in the crypto space declare that blockchains should be designed and managed over time primarily as DeFi development platforms, — How pathetic if it turns out to be true! For we're looking forward to seeing various kinds of cryptonetworks around, coordinating mass volume interactions and transactions between people, bypassing company-owned platforms, and driving the Internet into a more open, fair, and secure era, aka Web3.0.

The Evolution of Web3.0

Web3.0 hasn't happened yet. But based on first principles, we're sure it ultimately will. Trading always flows to the market with lower transaction costs, just like water always flows downhill. Decentralized protocols are minimally extractive coordinators of exchange. Cryptonetworks are digital service marketplaces with minimized transaction costs, which will inevitably absorb and retain economic exchange activities.

What's more, cryptonetwork participants get the privilege of sharing the value accumulated via magical network effects by being rewarded in the token, which represents a piece of ownership of the cryptonetwork.

Web2.0 platforms just have no way to resist being replaced by cryptonetworks. Web2.0 platforms are owned and run by companies whose goals are directly aligned with maximizing shareholder value. To put it bluntly, Web2.0 platforms extract as much profit as they can from

the economic activities they coordinate. A company's governance, especially if publicly listed, would ensure its Web2.0 platforms continue in that manner.

But Web2.0 platforms are fantastic for Internet Users. They are easy to use and free in most cases. How many conveniences would Internet Users be willing to sacrifice in exchange for trustless, permissionless, and censorship resistant? Not so many. All applications that have harnessed decentralization as their primary selling point have thus far failed to attract mainstream Internet Users.

A great Web3.0 application has to be a great Web application in the first place. That is to say, a great Web3.0 application must provide user experience at a comparable level with its Web2.0 counterparty. Good UX is the hardest part of Web3.0 application development because distributed ledger technology involves more complexities, increased costs, and ultimately downgraded UX.

The 3rd Innovation Wave of Cryptonetworks

Fortunately, a secret weapon has been forged for Web3.0 applications in the past few years. Blockchain frameworks such as, Substrate and Cosmos SDK, provide an unprecedented colossal design space to Web3.0 application developers.

Do you want users NOT to rely on browser extension wallets? Sure, you can decide.

Do you want to omit the gas fee for certain types of transactions, or do you want users to have a choice on token types to pay gas, maybe in stable coins? The choice is yours.

There are tons of optimization options for developers, including those on the lowest layer in the tech stack.

The secret lies in vertical integration — what Apple has done behind all those shiny app icons for many years. In short, developers can deliver a fully optimized Web3.0 application by building an appchain. To illustrate, while thousands of other applications might share a standard set of configurations on a generic smart contract platform, each appchain in a PoS setting could easily achieve 1K+ TPS throughput and fast finality — and this transaction processing capacity is dedicated to one application.

Another advantage appchains have over smart contracts — and perhaps the most critical in the long run — is that appchains can evolve quickly with legitimacy. Each appchain is a self-governed economy with code-defined explicit processes to reach agreements on protocol upgrades, either for eliminating software defects or changing the economic rules.

Thanks to Substrate, the primary function of on-chain governance is ready to use, and any cryptonetwork could mirror the governance process from others by copy-paste code. Blockchain governance in itself could evolve like open-source software. Once we consider cryptonetworks as codified institutional species where evolutionary laws apply, there appears a certain level of predictability on success or failure. According to Darwin's On the Origin of Species:

"It is not the most intellectual of the species that survives; it is not the strongest that survives, but the species that survives is the one that is able best to adapt and adjust to the changing environment in which it finds itself. "

History always spreads like an ascending spiral. Blockchain technology evolves from purpose-built to generic-purpose, then from generic-purpose to purpose-built. We believe appchains will be the 3rd innovation wave of cryptonetworks.

But we shouldn't rush to extremes regarding appchain's supremacy. Smart contracts are good for asset trading use cases, i.e., open finance or DeFi. Because smart contracts run based on the same security assumptions, composability between them is the essential recipe for the DeFi explosion.

While DeFi's UX is not as bad as online banking and has been proven acceptable by many users, it still has ample room for improvement, especially when considering a more capable layer1 blockchain than Ethereum, such as NEAR Protocol.

Octopus

While Substrate and Cosmos SDK have decreased the development cost of appchains to a comparable level with smart contracts while stepping into their mature phases, it's time to shift attention to an even more significant hurdle to Web3.0 innovation: Appchain bootstrapping is a complex job for developers and it's quite capital consuming.

We are introducing Octopus Network — A brand new multichain network born to bootstrap and run appchains. By providing flexible leased security, out-of-box interoperability, one-stop infrastructure, and a ready-to-be-engaged community, Octopus Network is unleashing an innovation wave on Web3.0.

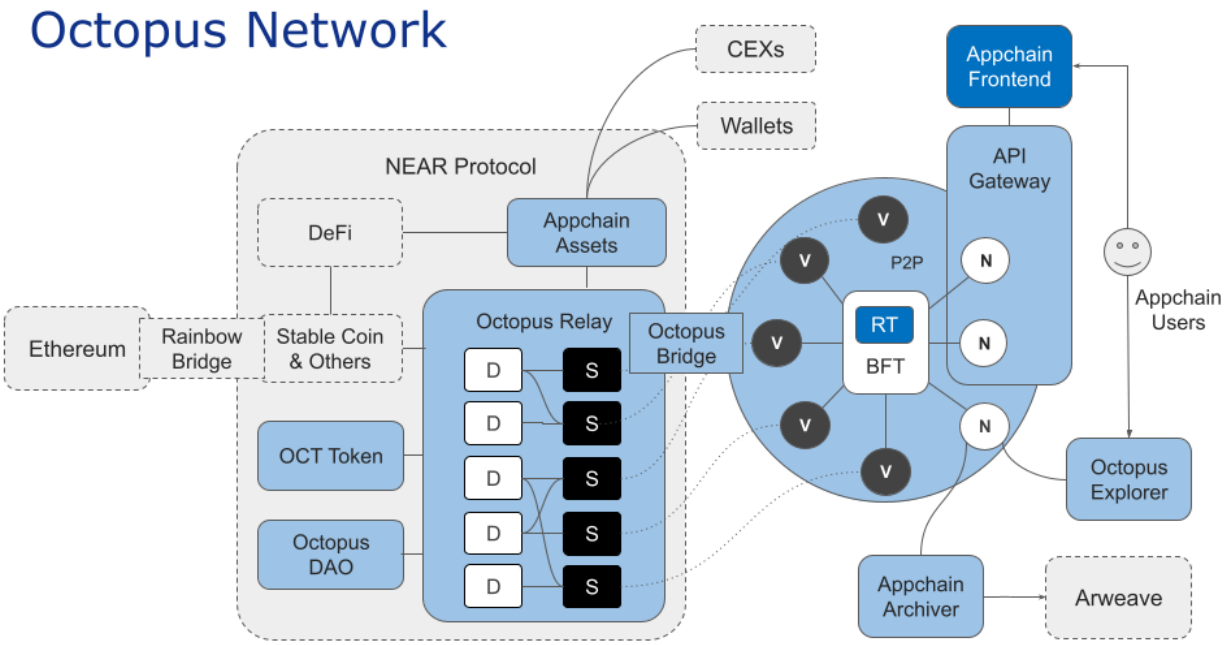
Why bother to invent another multichain network while Polkadot and Cosmos have been around for years? Because there is still no network designed for appchains.

Although Polkadot is the natural choice for Substrate based blockchains to join, its architecture and economic model do not accommodate appchains. A Polkadot parachain must afford the consensus cost of one shard of the network, which could equate to tens of millions of dollars a year. While a generic platform parachain could host thousands of applications to share the security cost, it does not make sense for an application-specific parachain to bear the cost on itself.

For a Cosmos zone, its developers have to bootstrap PoS/Tendermint security by obtaining the value recognition of its native token in the crypto asset market and bootstrapping an active validator community from the ground up.

Polygon and Skale may seem like options, but they are still smart contract-based and not designed for appchains. Appchains offer far more than dedicated transaction processing capacity. Once an application has its blockchain, it's absurd to give up customizability and evolvability by sticking to the smart contract paradigm.

Appchains need security, but bootstrapping PoS security is time-consuming and laborious (not to mention PoW security.) When the token of an appchain has a low and unstable market price at the initial stage, few people will take the risk of accumulating a large number of tokens to be appchain validators. The appchain team would have to spend a lot of money to promote the project and gain acceptance by the crypto community, and then maybe some professional miners would validate the chain. It commonly takes several years and a few million dollars to bootstrap an independent appchain with sound security.



Within the Octopus Network, each appchain decides its own economic model, including how many tokens it's willing to pay validators for security. Because it's the $OCT (the native token of Octopus Network) holder's responsibility to decide which appchain they'd like to stake on, the Octopus Network works as a free market, where appchains can lease the security needed at market price any time.

Overview

The core of the Octopus Network is the Octopus Relay — a set of smart contracts running on the NEAR blockchain, aka mainchain, that implements the security leasing market. Octopus appchains sit on the demand side of the market. They pay rent in their native tokens to lease security from $OCT holders.

Security

There are two types of participants sitting on the supply side of the market, appchain *Validators* and appchain *Delegators*. Validators will stake $OCT on an appchain in the Octopus Relay and set up a node to run the appchain's protocol, while Delegators delegate their $OCT to Validators for rewards sharing. Staking rewards will be distributed to Delegators directly after Validators collect a unified commission, e.g., 20%. All punishments are applied to Delegators proportionally when their Validators get slashed.

Validators that fail to keep their nodes up and running will lose a part of the rewards. If any Validator acts maliciously in the appchain consensus process, anyone (but most likely honest Validators) can challenge them by submitting fraud-proof to the Octopus Relay. Upon the submission of verified fraud-proof, a malicious actors' staking will be slashed. As appchain security is ensured by the staked $OCT, the security level of an appchain is proportional to the total value of the staking.

Interoperability

Appchains require interoperability. In most Web3.0 application economies, there is a demand for payment methods. However, widely accepted stablecoins, such as USDT and USDC, have very high requirements on transaction volume. It would be almost impossible for appchains to meet stablecoin criteria at their initial stage.

Another approach to the interoperability requirement would be to build a cross-chain bridge between appchain and Ethereum, enabling Ethereum assets to be transferred into the appchain and utilized as a payment method or for other purposes. But a reliable and usable Ethereum bridge is a monstrous headache for most layer1 public blockchain teams, let alone any appchain team. And it is very uneconomical to run and maintain a complex cross-chain system separately for appchains.

The Octopus Relay enables appchains' interoperability with NEAR protocol and Ethereum via the Rainbow Bridge. Additionally, appchains can utilize an out-of-box IBC pallet to connect with any IBC enabled blockchains directly. Any asset issued on Ethereum, NEAR, or any IBC

enabled blockchain can be transferred into and utilized by Octopus appchains trustlessly. Conversely, assets issued on appchains can be transferred trustlessly out to Ethereum, NEAR, and any IBC enabled blockchain.

Infrastructure

What's more, the Octopus Network provides a complete set of infrastructure for appchains — including API Gateway, Blockchain Explorer, Archive Gateway, etc. The Octopus Bridge will deploy a NEP141 wrapper contract on NEAR for each appchain native token. Then wallets and exchanges can integrate standard wrapper tokens rather than integrating with appchains one by one. So, appchain teams only need to focus on Substrate runtime and front-end development while the Octopus Network handles all the other technical necessities.

Community

Beyond its role as a cryptonetwork that provides leased security, interoperability, and infrastructures to appchains, Octopus also acts as a meta-community to hatch Web3.0 application communities. It's a focal point where Web3.0 application developers, i.e., appchain founders, can display the merit of their cryptonetwork to attract a variety of supporters, such as investors, Validators, Delegators, and market participants. Octopus is a community-base for appchains to support their own journey of building active communities around them.

Security

What is security in the context of blockchain? Simply put, security is the level of certainty that the predefined protocols, whether at the base layer or application layer, will be applied as most stakeholders expected.

Blockchain security is usually a quantifiable property, roughly speaking. For there is no such thing as absolute or unlimited security. If a blockchain has absolute security, it must be both unusable and unaffordable. Octopus Network is willing to explore a new balance point on multichain security since existing designs are inadequate for appchains.

Limitations of Current Security Solutions

The first model has each appchain relying on its PoW or PoS security. Vitalik Buterin coined this "easy solutions," and Cosmos falls into this category. Because of the very high cost of tape-out ASIC, bootstrapping a secure PoW public blockchain is extremely hard. Though it's much easier

for a PoS based blockchain to achieve self-contained security, its security becomes fragile when a substantial amount of cross-chain assets exist. In that situation, manipulating the consensus often turns out to be profitable.

The second model is a “hard solution.” Sharding, wherein the same security level (potentially very high) is shared among the whole network, can be seen in Polkadot, for example. But Polkadot faces difficulties with resource allocation. Considering the overhead of coordination, the total amount of shards is limited. Ethereum V2 will have 64 shards, whereas Polkadot will have less than 100 shards.

Suppose a network allocates one shard per each application. In this case, it could only support a few tens of applications, with each application having to pay a few tenths of the total network consensus cost, which does not make sense for either the network or the applications. A Parathread may seem like a workaround, but it still lacks elaboration. At least for some types of applications, such as decentralized gaming or social media, an underlying blockchain without liveness guarantee, like a parathread, is meaningless.

In a computation system, higher security doesn’t necessarily equate with better security, because a higher level of security always comes with a higher level of cost. So, what a computation system needs is appropriate and adequate security. In Polkadot, developers can’t decide what the appropriate level of security is for their parachain. They only have one choice — win a slot in the auction.

Even if a parachain wins the auction, it usually overpays for security because a cryptonetwork, in its initial stage, simply does not need a multi-billion dollar level of security. The security cost burden may cause those parachains to become trapped in hyperinflation, for they have to promise to issue a big chunk of native tokens to Crowdloan lenders. At the very least, this burden leaves the parachain very little space to incentivize the real value-creators of their protocol — the participants who help build the network effects of the cryptonetwork.

Security in Octopus Network

In the Octopus Network, each appchain decides its own economic model, including how many tokens it’s willing to pay to Validators for security. It’s the $OCT holder’s responsibility to determine what appchain they’d like to stake on, thereby assuming the risk of either earning a bag of valueless shitcoins, or enjoying the rewards of token price appreciation. So, in the Octopus Network, market participants do their planning with price mechanisms coordinating their decisions.

Or to put it another way, the Octopus Network attempts to commercialize blockchain security by providing an abundance of interchangeable commercial services — and reducing the difficulty and cost for appchains to obtain sufficient security. To this end, Octopus Network is developing

a series of tools for security providers, such as appchain validator node automatic deployment and management tools, network economic views, and statistical analysis tools. In this respect, Octopus makes security providers' work more like professional investors rather than IT maintenance companies because they provide capital to promising businesses and share the risks and benefits with them.

Fraud-proofs

As mentioned above, in a multichain network, the major blockchain security issues arise from cross-chain assets because in PoS settings, attackers can hardly profit from a purely internal attack. In Octopus Network, if Validators act maliciously in the appchain consensus process, anyone can challenge them by submitting fraud-proof to the Octopus Relay. There are two types of fraud-proof corresponding to two types of malicious actions that can be challenged:

1. A group of appchain Validators signed two different headers at the same height.
2. A group of appchain Validators voted on a block that included invalid transactions.

The 1st type of fraud-proof can be verified by the Octopus Relay directly, and it's pretty straightforward since the Relay tracks all the Validator's public keys and uses the same public-key cryptography and curve (secp256k1) with appchains. Once the challenge is verified, a slashing process is invoked automatically.

All Validators who signed the duplicate header will be slashed. The severity depends on the summed voting power of the faulty Validators. If the voting power is 33% or more, 100% of the stake will be slashed. These penalties are transferred to an on-chain treasury. The Octopus Relay will then halt the corrupted appchain, and its future would be dependent upon a governance decision.

The 2nd type of fraud-proof can't yet be verified directly by the Octopus Relay. So, once this type of fraud-proof is received, the Octopus Relay pauses the staking/delegation operation and any cross-chain asset transfers into and out of the appchain. A governance process is then triggered to make a judgment and take corresponding action.

Data Availability

Another problem is data availability for which Octopus has also developed a new design. While other methods rely on a data availability proof — which is complex and expensive — Octopus uses a challenge-response game.

All Octopus Validators must continually observe the Octopus Relay, more specifically, the light client corresponding to its own appchain inside the Relay, which acts as the Root-of-Trust for

cross-chain asset transferring. A malicious Validator group could forge a header and update the light client in the Octopus Relay, but hide block content from honest Validators. By doing that, the malicious group may steal cross-chain assets from the mainchain that are locked on the Octopus Bridge, or transfer fake appchain assets to the mainchain.

Suppose an honest appchain Validator finds a newly committed block header in the appchain's light client in the Octopus Relay, but doesn't have the corresponding block data. In this case, he would submit a query transmission to the Relay expressing doubt. If he receives the block afterward, he would then withdraw the query. (Depending on network conditions, it's normal to see some queries come and go.)

But if one appchain accumulates a considerable number of queries on the same height, the Relay will emit data availability challenges. In this situation, it is the header signers' responsibility to submit a valid block that justifies the header. Should they fail to do so, their staking would be slashed.

As long as the duration of this challenge-response game is significantly shorter than the unbonding period — and the total staking on the appchain caps the cross-chain assets — there is no chance for attackers to profit by hiding blocks.

In the future, there will be a Substrate runtime environment on the NEAR blockchain, in the same way that NEAR supports EVM. (After all, NEAR and Substrate are both WASM-based.) With the proper runtime environment, the 2nd type of fraud-proof could be processed inside the Octopus Relay without involving any human intervention.

The technology behind it would be similar to what the Polkadot Relay validator and parachain collator do now, where Relay validators are stateless clients of the parachain, and it's the parachain collector's responsibility to pack and submit the Proof of Validity (PoV) block — which includes the transactions and state data needed to execute or verify these transactions. We are also considering leveraging a dedicated data availability layer once it shows maturity.

The Advantages of Leased PoS (LPoS)

The new blockchain consensus described above is called Leased PoS (LPoS). Compared to Polkadot parachain's shared security model, Octopus appchain's leased security is far more scalable and flexible. Because security leasing is essentially capital leasing or collateral leasing, even though capital is a scarce resource, it scales without physical limitations.

In the Polkadot case, each parachain will accommodate a certain number of validators in the pool exclusively in any given epoch. The consensus algorithm limits the total size of the pool. That is why the total number of parachains is expected to be under 100.

What's more, Octopus's leased security is much more cost-effective than Polkado'st. Since Octopus does not have its own blockchain, and the Octopus token is issued and managed by a smart contract, Octopus itself does not need to pay for consensus costs directly. That is why the $OCT inflation rate could be set to zero, which means the base interest rate of the Octopus economic system is zero.

When the base interest rate is zero, a 3%-5% APY is a decent annual return, which is the range we expect an appchain will pay for their leased security. In contrast, a Polkadot parachain has to pay 20% or more APY to make itself attractive to crowdloan $DOT lenders because staking on the Polkadot Relay will give investors a 14% risk-free annual return.

Imagine two economies in the multichain network context — one has a zero base interest rate and the other has 14% — It would be much more difficult for startups in the latter category to raise capital to lease security.

Decentralization via Forkability

Octopus appchains have both high-performance and cost-effective leased security. *According to the impossible trinity theory, have we chosen to sacrifice decentralization?* Of course not! On Octopus, high-performance, cost-effective leased security, and decentralization are not mutually exclusive.

The vision of ordinary users running full nodes on their laptops is idealistic and would be impractical, especially in a multichain future. In ten years, ordinary people may be using super-sovereign SoV, DeFi world computers — and at least a dozen appchains for social media, media streaming, blog, classified ads, etc. They could not run all these blockchain nodes on their commodity laptops.

Fortunately, decentralization can be fostered another way. People used to vote with their feet rather than their hands, and it's workable in crypto, under one condition: forkability.

Forkability refers to how easy it is for a cryptonetwork to be forked. Given good forkability, even if a few plutocrats controlled governance, it would be meaningless for them to seek rent by changing the rules. If they did, users who'd contributed a significant portion of economic activity could leave the cryptonetwork and settle down on a new fork with fairer rules. In this case, users would remain unharmed, while plutocrats would lose the resources they put in to control the network. For example, just imagine an alternative outcome for Freenode IRC protocol, had it been built as a forkable cryptonetwork?

Yes, forking requires social coordination, and this time the effort will be on ordinary users' side. *But how could one expect to control his assets, identity, and data without paying attention?* If a user isn't concerned with fairness, openness, or privacy, and has no issues with remaining on

an oligopolistic platform, so be it. But internet users who deserve Web3.0 don't have to set up and run a blockchain node on their PC. Ordinary users just need to keep an eye on those cryptonetworks they care about, choose the fork they think has legitimacy, and give up on those that don't. In this way, user awareness ensures decentralization.

The Octopus Network limits the number of appchain validators to a two-digit range, where pBFT-like consensus works very well and the total IT cost is almost negligible. At the same time, Octopus will serve all its appchains with great forkability by archiving the appchain block history to Arweave — a decentralized permanent storage protocol.

Based on the archived block history, every appchain can be forked at any height to become a new appchain once the Octopus community supports the fork. What's more, since Substrate is the most widely adopted blockchain framework, any appchain core team is replaceable if it loses the trust of its community.

Interoperability

The Oxford English Dictionary defines "interoperability" as "the ability of computer systems or software to exchange and make use of information." Since the only way for a blockchain to use information is to make a state transit by executing transactions, blockchain interoperability could be defined as "a certain state transit on one blockchain (source chain) triggering a specific state transit on another blockchain (target chain) in a pre-defined way."

Basically, any system that is to facilitate blockchain interoperability needs to solve two problems. The first problem refers to how a target chain can know that a state transit it cares about has happened on the source chain. Since blockchains are computational systems that passively handle requests, they need an off-chain process to update them. The second problem addresses how the target chain can make sure a message carries the true, unaltered information about the state transit on the source chain.

Cross-chain Messaging and Asset Transfers

Generally speaking, there are two types of commonly recognized blockchain interactions: cross-chain asset transferring and cross-chain messaging. At first glance, cross-chain messaging seems to be a much more powerful and generic primitive, which means a smart contract on one chain can call its peer on the other — and a cross-chain asset transfer could be implemented based on that. But once we dig in deeper, we may see that cross-chain messaging is not so applicable.

Because different blockchains have different security levels and assumptions, almost all cross-chain interactions generate risk exposure — either on the source chain, target chain, or both. Those risks should be covered by on-chain collateral in a trustless environment, (ideally over 100%,) to mitigate the risk of under-collateralization caused by asset price volatility. But the risk involved with cross-chain messaging usually can't be quantified. In other words, no one knows how much collateral is needed to cover the exposure.

Basically, no notable cross-chain messaging practice exists in the public blockchain space. While some might cite the Polkadot XCMP as a counterexample, XCMP is a cross-shard messaging protocol with each shard having the same security level assumption. Because each Polkadot parachain is a shard of Polkadot, the Polkadot relay chain validators are able to guarantee the passage of messages between shards in a trustless environment. This is fundamentally different from real cross-chain cases.

In the real world, cross-chain asset transfers have been widely adopted. While they may seem to restrict functionality, cross-chain asset transfers are much more powerful than is commonly thought. In this paradigm, vouchers are created on the target chain to represent assets locked on the source chain. These vouchers can then be utilized by any application protocol as if they were local assets. Theoretically, all types of financial transactions can be supported once cross-chain asset transfer capability is provided since all financial transactions involve exchanging various kinds of vouchers between entities.

On the Octopus Network, we aim to support trustless, secure, and easy-to-use cross-chain asset transfers between the appchains, the mainchain, and any other public blockchains alongside Octopus.

Current Interoperability Solutions

Vitalik Buterin described the classic blockchain interoperability taxonomy in 2016, which is somewhat outdated by the current standard. A more recent framework proposed by the World Economic Forum in 2020 outlines three approaches unique to blockchain interoperability — cross-authentication, API gateway, and oracles.

The cross-authentication approach is further classified to notary schemes, relays, and hash-locking. Oracles are not so different from notary schemes in the context of blockchain interoperability. For when oracles feed data that originated from other blockchains, they essentially act as notaries. Therefore, in the following paragraphs, we will use notary and oracle interchangeably. (We purposefully omitted API Gateways since they have to rely on a trusted third party to run the gateway and can't be utilized in a trustless environment.)

As both Vitalik and the World Economic Forum have pointed out, hash-locking has the most limiting functionality, supporting only digital asset swaps. But neither of them have noticed that a

Hashed Time-locked Contract (HTLC) is not a meaningful way to support a trustless cross-chain asset swap because the swap initiator has Optionality that her counterparty does not have. This creates an element of unfairness.

To illustrate, B, who locks his asset after the swap initiator A does, essentially gives out his option for free allowing A to speculate without punishment. The option's value is determined by the timeout span set by B and the relative price volatility of the two assets that are put into the swap. A could choose to abort the swap if not to her advantage without having to pay a premium for the option. Though B will try to limit the timeout span, the option's value will never be zero. So, B has to rely on A not to take advantage of B. More simply, B must trust A.

Relays are considered trustless by nature. A source chain light client runs on the target chain, giving the target chain the capacity to verify a message representing state changes on the source chain without resorting to a trusted party. State-of-the-art blockchain interoperable systems and protocols such as Rainbow Bridge and IBC protocol are all in this category.

But relays are not a perfectly trustless cross-chain approach. The relayer — the off-chain process responsible for feeding the light client on the target chain with block headers, (or the equivalent of the source chain) — turns out to be the Achilles' heel. Because there must be at least one honest relayer to keep light clients updated, the system is only as decentralized as its most centralized component. The relayer incentive mechanism is complex and remains an unresolved problem even for the most advanced protocols.

Cross-chain Mechanism from Mainchain to Appchain

Notary schemes and oracles are often considered trust-based approaches. But this is not necessarily always the case. Suppose the oracle data feeder set is replicated from the target chain's validator set, and they reach agreements in the same way. In that case, the oracle scheme wouldn't introduce any extra entity that would need to be trusted. In this respect, oracle or notary schemes should be considered trustless. What's more, the oracle data feeders or notaries would not need an extra incentive model other than the one prepared for validators.

Octopus needs every honest appchain Validator to act as a fisherman by staying ready to challenge those who are malicious. Being a fisherman also requires that a validator be equipped with a reliable way to observe and submit transactions to the Octopus Relay on the mainchain. These facilities could then also be utilized as an oracle about *any* event emitted by the Octopus Relay, including staking-related events.

Therefore, the cross-chain mechanism from the mainchain to appchain is as follows:

1. Each appchain Validator sets up a reliable RPC connection to a mainchain full node (or indexing service) and subscribes to all staking cross-chain events that happen in the Octopus Relay by using Substrate off-chain workers.

2. Once an event is observed and identified targeting the appchain, all Validators of the appchain will vote with their voting weight proportional to staking, thereby reaching a consensus on the appchain about the event's existence.
3. When a consensus is reached, corresponding actions, such as a mint voucher token or an updated validator set, will be executed.

This novel design has the advantage of eliminating independent relayers and related complex incentive and reliability problems. Validators use off-chain workers to pull event data from the mainchain and agree on these data with the appchain consensus mechanism, (which is exactly the "trustless oracle" described above.) And this mechanism does not increase the cost because validators, when acting as fishermen, need to observe the mainchain anyway.

Cross-chain Mechanism from Appchain to Mainchain

The other direction, appchain to mainchain, is different for it is not possible to customize the NEAR stack to embed an oracle. We therefore chose the relay approach instead. In its early implementation, the Octopus Foundation will run a set of relayers to update the block headers, (MMR roots) of each appchain to Octopus Relay. In the future, appchain Validators will do the work through off-chain workers, and the performance of the header relay will be considered a factor for block rewards.

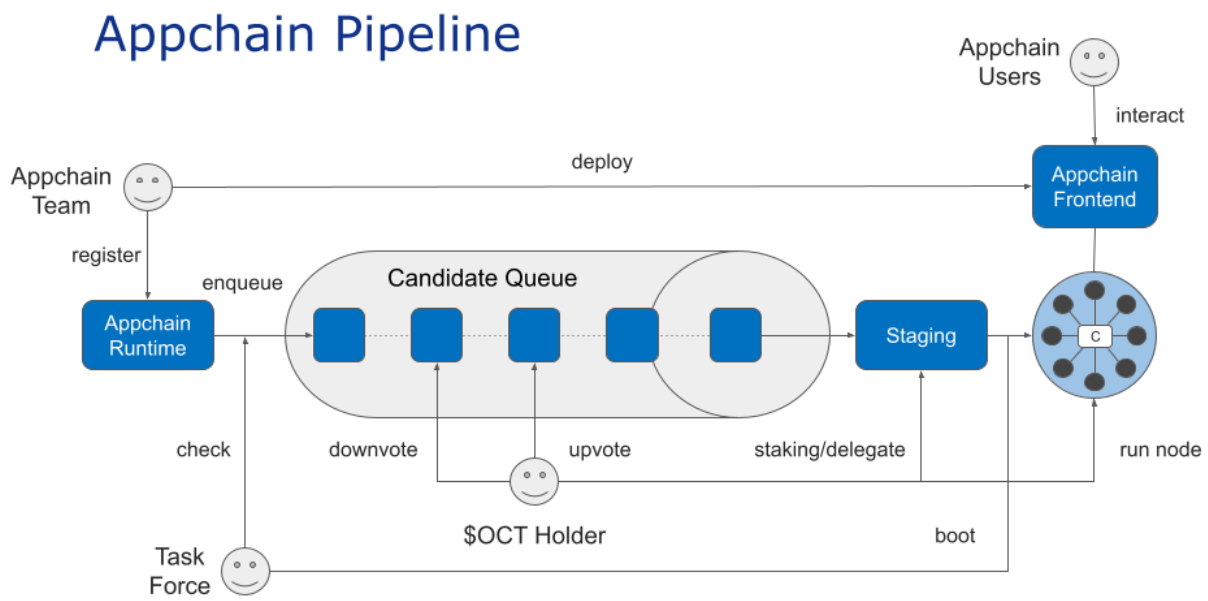
Trustless cross-blockchain interoperability sits at the core of the Octopus Network protocol stack. The Octopus Relay enables appchains to be interoperable with the mainchain, or NEAR protocol. Furthermore, appchains can interoperate with blockchains outside the Octopus Network, either by bridges on NEAR, such as with Ethereum via Rainbow Bridge, or by utilizing the out-of-box IBC pallet to connect with any IBC enabled blockchains directly.

It's not a controversial statement that all public blockchains and multichain networks will be interconnected, forming the Internet of Blockchains. The Octopus Network is specifically designed to be a part of this. The Octopus team, previously known as Cdot, has been working on universal blockchain interoperability protocol IBC and cross-chain integration for quite some time.

Community

Nowadays, anyone can deploy smart contracts on a public blockchain and host a front-end UI to bring a Web3.0 application alive with relatively meager costs. The greater challenge is how to make their applications known by potential users. The Octopus Community solves this challenge by virtue of its role as the focal point of Web3.0 applications.

How Appchains Go Live in Octopus



The architectural design of the Octopus Network — coupled with the processing power of the NEAR Protocol — makes it easy to host hundreds of appchains. But this doesn't mean we want to see just any appchain join the Octopus Network without proper selection, (which could result in a lemon market where bad coins drive out good coins.) For this reason, the process of appchain selection is a part of the Octopus protocol and the decision-making power is given to the Octopus Community, or $OCT holders.

The Octopus Network is a decentralized two-sided platform for Web3.0 investors and Web3.0 application teams. Besides being appchain Validators and Delegators, $OCT token holders have the right to select the best appchain projects by upvoting or downvoting in an on-chain candidate queue.

Registration

Any Substrate-based chain can register and apply to become an Octopus appchain. Registration requires a white paper or spec and a runtime release that has been internally tested and audited. To prevent abuse, the registration requires a small deposit of $OCT.

Audit Stage

After the appchain is registered, members of the community task force will audit it. The purpose of the audit is to ensure that the appchain has no known security vulnerabilities and that its application logic is consistent with its white paper or spec.

Appchain auditing is currently an unmet need. Only a few companies in the industry have the relevant experience and the services they provide are expensive. Auditing performed by the Octopus Network can not only greatly reduce the cost of an appchain launch, but also contributes to the accumulation of relevant knowledge and professional capabilities.

Voting Stage

Once an appchain has passed the auditing phase, it enters the candidate queue where it will be upvoted or downvoted by $OCT holders. In a rolling period that lasts one to two weeks, the appchain that ranks first in the number of upvotes minus downvotes in the queue will enter the staging state as the the most supported appchain by the Octopus Community.

Staging Stage

In the staging stage, $OCT holders can stake or delegate on the appchain. When the staging period ends, if the appchain has attracted enough staking beyond the security bottom line, it will enter the booting state.

Booting Stage

In the booting stage, task force members will run four bootstrapping nodes to start the appchain. Then Validators should run their nodes to join the appchain consensus. Octopus Network will also run a full node cluster for each appchain and provide API access services to the appchain's front-end. Appchain developers just need to update the front-end configuration, and then the appchain is ready for end-users.

Appchain Rewards

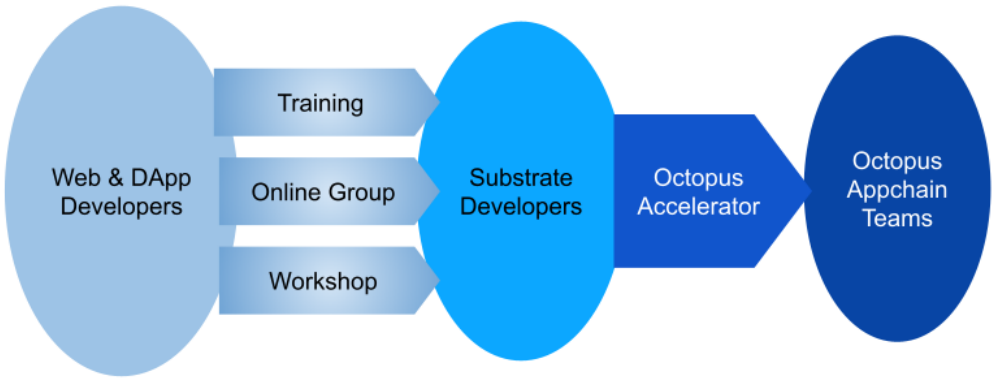
Octopus recognizes that appchain projects are the value creators of the network. While other multichain networks charge admission for appchains, Octopus considers appchain teams to be the most critical part of the community and is very happy to share the benefits of network effect expansion. Therefore, the first 100 launched Octopus appchains will be directly rewarded by 100k $OCT vested gradually over three years after the launching event. In addition, the foundation has decided to provide an additional 1M $OCT rewards for the first ten appchains to recognize them as founding appchains.

A cryptonetwork is owned by its community. This is the essence of decentralization and the fundamental difference from Web2.0 platforms. The Octopus Network is a meta-community, which will nurture hundreds of Web3.0 application communities. Users interested in different Web3.0 applications will pay attention to their favorite applications through events such as the Octopus appchain launchings.

Beyond infrastructure and initial stages, the Octopus Network provides forkability to all its appchains, making it meaningless for any type of tycoon to takeover an appchain without agreement from the community.

At the same time, the whole Octopus Network is a part of the NEAR ecosystem. Based on seamless interoperability between the Octopus Network and NEAR, a variety of crypto assets issued on Octopus appchains will also contribute to the prosperity of NEAR's DeFi ecosystem.

The Octopus Accelerator Program



The core community-building problem faced by the Octopus Network is how to find and attract outstanding appchain projects. In the entire Internet industry, blockchain is just a small branch. And within the blockchain space, Solidity developers still occupy the mainstream. So, the first task is to transform web developers and Solidity smart contract developers into Substrate developers. In this regard, we are very experienced.

Two years ago, the Octopus team, along with some community enthusiasts, initiated the first global Substrate online training course. This nearly free course trained the first batch of Substrate developers in China and was also the genesis of the Chinese Substrate Community.

Our course is now an official course funded by Parity, Inc. To date, many members of the Octopus team have served as teaching assistants for the course. Based on these experiences, we are negotiating with partners worldwide, including the NEAR education team, to provide similar training courses to regions beyond China.

But even with qualified Substrate developers, there is still a long way to go to form a mature appchain team. Web3.0 applications are not only about technology, but also involve a wide range of topics. This is why we aim to launch the Octopus Accelerator Program — a collection of open and composable courses and seminars available to Substrate developers and teams worldwide.

The Octopus Accelerator Program will hold a batch of courses every quarter, each lasting ten weeks. During each period, learners and mentors will study several topics including Token Economics, Web3.0 Product Design, Community Building, Blockchain Governance, Crypto Regulation, and Crypto Project Fundraising. We will extensively invite experts to provide videos on specific topics and participate in seminars as mentors. Anyone can apply to provide videos on particular topics and participate in seminars.

At the end of each batch, there will be a Demo Day event. The Octopus Foundation will select the top five appchain projects and provide them with a $250k total reward. In this way, the Octopus Foundation will directly fund 20 appchain projects through the Octopus Accelerator Program each year, providing them $1M in total.

Tokenomics

$OCT is the native token of the Octopus Network — a fungible, non-inflationary utility token with three utilities in Octopus Network:

- Used as collateral to guarantee the security of appchains
- Used for the governance of the network
- Used for endorsing appchains by upvoting them in the candidate queue

Security Collateral

The core role $OCT plays in the Octopus Network is appchain staking. Holders put their $OCT at risk (via staking) to provide security to appchains and earn rewards in the respective appchains' native tokens. The staking also acts as a disincentive for malicious participants who would be penalized by having their $OCT slashed, which is the source of leased security for Octopus appchains.

When Octopus runs in its full capacity, 30-50 appchains will be launched in the network annually. At the initial stage, an appchain would commonly be paying around $500k worth of security rent in its native token to Validators to ensure the appchain receives above several million dollars security. In most cases, this security level would be adequate for a newly born

appchain. If the long-term equilibrium rate of return of appchain staking is 5% per annum, newly launched appchains alone will bring in about $400M in collateral demands each year.

Some appchains will inevitably fail, paying out the cost of innovation. Some will succeed and continually expand their economic scale. When an appchain consistently attracts economic activity, its token price will increase. Accordingly, its rent increase will attract more collateral and the appchain will automatically obtain a higher level of security. Thus, as the total economic value of an appchain accerates, so do its security/collateral demands.

Governance

The second function of $OCT is to entitle holders to control the governance of the network, (more specifically, the Octopus Relay where all economic rules apply,) by forming the Octopus DAO.

There is excellent quantitative research on governance token valuation which concluded that stake size and decisiveness (the possibility that a single token holder's vote can determine a referendum's result where the relative value of said voter's stake to token distribution represents a relative value of governance power) are positively correlated, and in some cases, result in an exponential relationship.

While the Octopus DAO Council has a maximum of 100 members, it's most likely to grow from a few members in the beginning to a few dozen when stable. Each Council member's governance power is valuable but still dispersed enough to avoid collusion. The relative value of governance power is shown below, assuming 25 members in the Octopus DAO council.

```
macbook-pro:governance-model liuyi$ python3 ./model.py 100 100 100 100 100 100 100 100 100 100 100 100
 100 100 100 100 100 100 100 100 100 100 100 100 100
    tokens     stake  decisiveness
0    100.0  0.038462      0.154981
1    100.0  0.038462      0.154981
2    100.0  0.038462      0.154981
3    100.0  0.038462      0.154981
4    100.0  0.038462      0.154981
5    100.0  0.038462      0.154981
6    100.0  0.038462      0.154981
7    100.0  0.038462      0.154981
8    100.0  0.038462      0.154981
9    100.0  0.038462      0.154981
10   100.0  0.038462      0.154981
11   100.0  0.038462      0.154981
12   100.0  0.038462      0.154981
13   100.0  0.038462      0.154981
14   100.0  0.038462      0.154981
15   100.0  0.038462      0.154981
16   100.0  0.038462      0.154981
17   100.0  0.038462      0.154981
18   100.0  0.038462      0.154981
19   100.0  0.038462      0.154981
20   100.0  0.038462      0.154981
21   100.0  0.038462      0.154981
22   100.0  0.038462      0.154981
23   100.0  0.038462      0.154981
24   100.0  0.038462      0.154981
25   100.0  0.038462      0.154981
```

In our opinion, a token's governance value can not be decoupled from its utility value in most cases. A sound and widely participated-in governance will give token holders more stable value expectations and suppress extreme fluctuations in the token price, thereby reducing the implicit option cost of appchain staking.

Appchain Voting

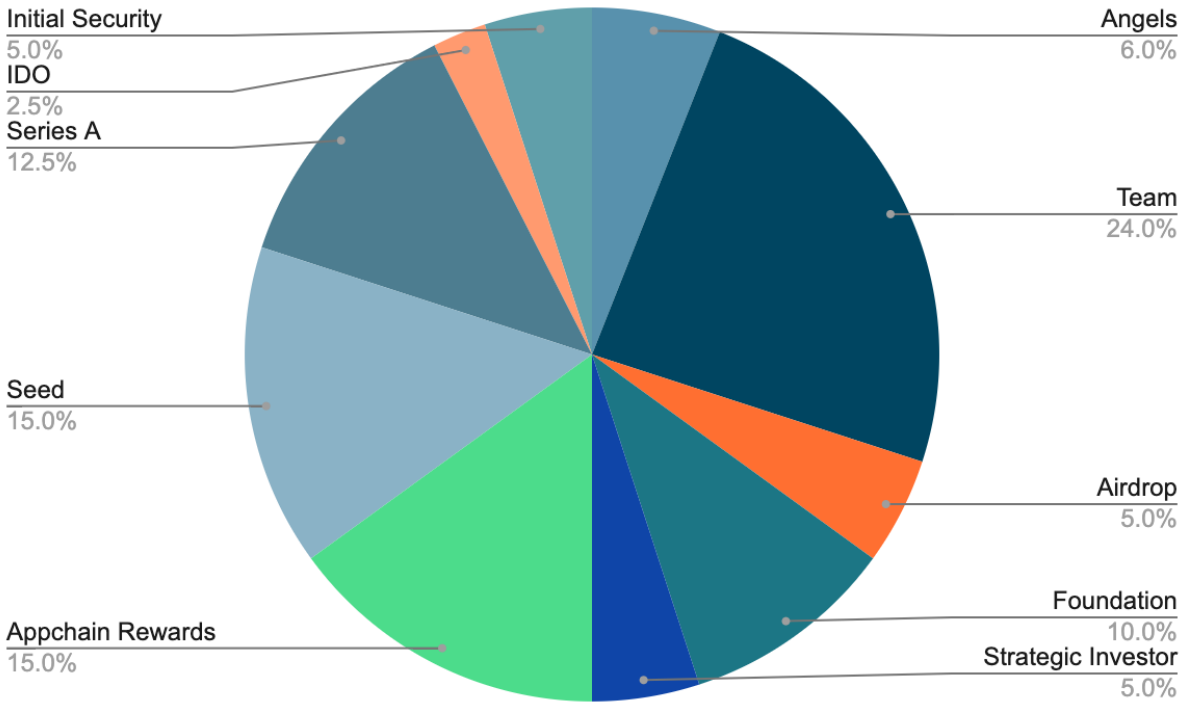
The third function of $OCT via $OCT holders is the selection of which appchains will go on to live in the network by the upvoting or downvoting on candidates. Appchain teams will need to convince the Octopus community that their Web3.0 application is meaningful and will create continuous value streams for investors who stake $OCT on their appchains. $OCT holders will select which appchains they support carefully, for there is an opportunity cost of missing those which could be more valuable.

While downvoting low-quality appchains or Ponzi scheme ones may not bring direct economic benefit to voters, the long-term goal of forming a set of social contracts by embracing good appchains and expelling evil ones will. Until such time, the Octopus Foundation and founders certainly won't hesitate to use their voting power to downvote evil appchains.

Though it may be difficult to evaluate the influencing power of $OCT quantitatively, it's certain that most institutional investors engaged in the Octopus ecosystem will spare a chunk of $OCT to support the appchains in their portfolio.

Some appchain teams may choose to raise $OCT by themselves or implement some kind of reward mechanism to win the support of $OCT holders. As long as the economic design of the appchain itself is based on value creation, we are happy to see all kinds of innovation via appchain-$OCT holder interaction.

$OCT Distribution



The total supply of $OCT is fixed at 100 million. 41% of $OCT are to be distributed to investors: 6% to angel investors, 5% to a strategic investor (NEAR foundation), 27.5% to institutional investors who participate in seed and Series A private sales, and 2.5% to IDO investors.

It's a common headache for a cryptonetwork to identify its actual community members when distributing tokens. We can observe this in several unsuccessful attempts by projects such as Stellar, Handshake, and Edgeware, to name a few. A community should be consistent with the actual participants of the cryptonetwork. For Octopus, this community is meant to consist of Web3.0 investors and Web3.0 developers. So, we will do our best to distribute $OCT to qualified and long-term thinking investors who are devoted to Web3.0 to form the basis of the Octopus Community rather than mere speculators.

$OCT belongs to the Octopus Foundation. 30% of the total supply will be used to incentivize upcoming Octopus community contributors. 24% $OCT is to reward the core team over 5 years

starting from April 2019. Finally, 5% of $OCT over 5 years after the mainnet's live is allocated for social media users who help share the value proposition of Octopus Network. The Octopus core team is working on executing precision airdrop since no existing platform can meet our requirements.

All $OCT will be minted before the Octopus mainnet goes live. 30% supply will go into circulation right after that, including tokens belonging to IDO, Seed, and Series A investors. 5% $OCT belonging to the foundation will be used to provide initial security for appchains. 65% of the total supply, including tokens distributed to angel investors, the strategic investor, core team, and foundation, will be released linearly over 3 years after the token generation event.

"Show me the incentive, and I'll show you the outcome." This famous quote from Charlie Munger gets straight to the point regarding the behavior of individuals and organizations. By distributing $OCT to Web3.0 investors and appchain developers, which form the two-sided market of the Octopus Network, we expect the Octopus Network to grow into the most successful multichain network that enables Web3.0.

Governance

Participation in cryptonetwork governance is a right, but there is always a cost to exercise this right. The highest cost of exercising governance is the cognitive cost. When stakeholders can exit quickly, participating in governance to change dissatisfaction is usually not rational. This raises another question: *Who are the real stakeholders of cryptonetworks?* It seems that the amount of stake and the duration of the correlation of interest should both be considered.

In a multi-sided market coordinated by a cryptonetwork, service providers are usually long-term stakeholders because their interests surpass income expectations. More importantly, service providers typically need to learn market rules and operating methods in order to formulate strategies that suit their characteristics. These cognitive investments usually translate to a cryptonetwork with stronger stickiness for service providers.

Service users, on the other hand, are more inclined to continuously compare prices and quality of various cryptonetworks. Should they find a better option, they will leave a cryptonetwork. So, although the network effect of cryptonetworks is built by service providers and users, the service providers are usually considered the long-term stakeholders of cryptonetworks. Therefore, cryptonetworks should design governance structures primarily around service providers.

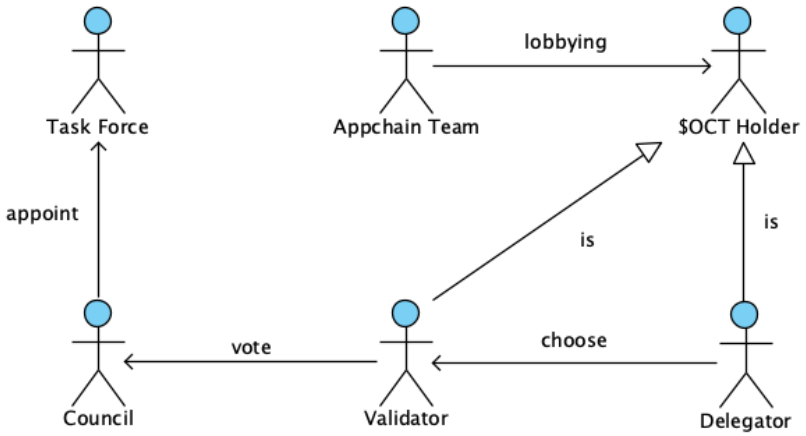
In the economic system of cryptonetworks, native tokens should be distributed to service providers with a token locking mechanism utilized. Voting power should only be given to those locked tokens that compensate token holders for liquidity loss. This enables service providers to declare themselves long-term stakeholders of the cryptonetwork.

In Octopus Network, things become relatively simple. The essence of the Octopus Network is a security leasing market. Service providers are those who pledge $OCT to provide security, and

users are appchains that require security. Therefore, the Octopus Network assigns governance voting rights to the $OCT in the staking state.

To go one step further, we merge the two processes of staking and voting. That is, when staking, the Validator designates votes to a Council member or a candidate. The cancellation of a separate voting process is expected to increase the turnout rate. The Delegators do not have the right to vote individually, for they have granted the right to the Validator during the delegation process.

Since the fixed commission rate is drawn by the Octopus Network's Validator, assuming that all validating nodes can maintain a 100% online rate, we hope that the Delegators primarily consider two factors when choosing a Validator. The first is the proportion of staking. For staking that is much larger than average, the unbonding period should be extended accordingly, increasing the Validator/Delegator's options' cost. The second is the political factor wherein Delegators would be most inclined to choose those Validators whose governance views are closest to their own.



The Octopus Council is the governing body of Octopus Network, responsible for reviewing and deciding on proposals from the community. The proposals primarily dictate the expenditure of the on-chain treasury and upgrades of the Octopus protocol — including the governance process itself.

Council members are elected by the Community through the method outlined above. A NEAR account supported by at least 1M $OCT can become a Council member. Due to the flexibility of NEAR accounts, a Council member can be an individual, an organization, or even a DAO. Council members have equal voting rights on proposals, with no fixed term or term limit. The Council can be regarded as a type of liquid democracy.

The Task Force is a group of professionals appointed by the Council through the approval of proposals. The Task Force is responsible for the daily maintenance of Octopus Network and

Task Force members receive salaries from the on-chain treasury. Task Force members who misbehave or lack ability will be dismissed by approving proposals.

Each Octopus appchain implements on-chain governance that meets its own needs. On-chain governance has the ability to make decision-making transparent, accountable, and binding, and the potential to create innovative governance mechanisms. The main criticism of on-chain governance, the inability to resist plutocracy, has already been addressed by forkability. With the emergence of Octopus appchains and Polkadot parachains in significant amounts, there will be a Cambrian explosion of governance designs where hundreds of cryptonetworks will try hundreds of approaches in parallel at hyperspeed.

It's important that Validators and service providers operate in the same groups for a base layer protocol where security is the service provided, but in distinctive groups for an appchain where security is a service needed. Providing that the security level is high enough, it's in an appchain's best interest to keep the security cost as low as possible.

Appchains should never allow Validators to gain control of governance since rational Validators would continually attempt to maximize their gain from the appchain economy, which directly conflicts with other participants' interests and is antithetical to the concept of cryptonetworks working as minimally extractive coordinators.

Due to the incentive structure, an independent PoS blockchain can be very easily controlled by its validator which would be catastrophic for appchains. So, appchains should use leased security or shared security to achieve a long-term economic balance. In the Octopus Network, appchain Validators are not involved in the appchain's governance. They are merely providers of security services through a free market. Each appchain is free to choose its governance structure, which is usually based on its native token voting.

LPoS is more conducive to the long-term development of appchains than independent PoS. But more importantly, the right to choose always belongs to the appchain community. The Octopus Network will even provide the tools to support appchains who choose to cease using leased security in order to transform into an independent PoS blockchain. Once an appchain community makes such a decision, its connection with the Octopus Network will be downgraded to that of a standard IBC bridge, and existing cross-chain assets will not be affected.

Coda

Octopus is a multichain network for bootstrapping and running appchains. By providing cost-effective leased security, out-of-box interoperability, complete infrastructure, and a community ready to be engaged, Octopus Network will decrease the capital expenditure to bootstrap an appchain by 100X — from several million dollars to less than one hundred thousand dollars — unleashing the 3rd innovation wave of cryptonetworks.

Besides cryptocurrency and DeFi, it is yet to be seen in which areas cryptonetworks will develop on a grand scale. But if the most dominating force in the whole universe, the theory of evolution, has any say in the matter, the market will filter out the winners. The Octopus Network decreases the total cost of cryptonetwork innovation, enlarging the incentive, while absorbing the most creative minds into the Web3.0 space to prompt an exuberant and highly diversified ecosystem.

If you don't expect one chain to fit all needs, you are like us. If you don't believe that one chain can rule them all, you are among us. And if you believe Web3.0 is more than DeFi, you *are* us. Let's deliver decentralized applications for every online business field that the Web2.0 traditional middleman has controlled and return value to the real creators. Whether in gaming, NFTs/digital collectibles, DAO, advertising, the creators' economy (video, audio, graphics, text), prediction markets, or the token curated registry (TCR), now we can build Web3.0 applications with great user experience by leveraging appchain technology. The possibilities are only limited by imagination.

We named the Octopus Network after the most fiercely intelligent marine benthic creature. Rather than a centralized nervous system as vertebrates have, two-thirds of an octopus' neurons are spread throughout its body, distributed amongst its arms. Scientists have recently determined that those neurons can make decisions without input from the brain, essentially making the octopus a decentralized intelligent life form. From an evolutionary perspective, octopuses, which consist of some 300 species, are incredibly successful. They have been around for 155 million years, live in every ocean, and different species have adapted to different marine habitats.

We would like to see multichain networks emulate the octopus. Each blockchain has its own intelligence and decision-making mechanism, empowering its efficient adaptation to ever-changing environments. When connected as a whole, all members benefit from much more significant network effects and economies of scale.

The octopus is a successful alternative form of intelligence. We expect the Octopus Network to be a successful alternative form for multichain networks. Go, Octopus! Be a unique animal in the crypto sea, and enjoy your journey!