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, Sellar, to name a few. But the latter, such as Colored Coins and Namecoin, almost achieved nothing. The commonly agreed reason is that the Bitcoin blockchain is purpose-built and therefore not suitable 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.

Now, it's not a surprise to hear some of the brightest minds in the crypto space declared that blockchains should therefore be designed and managed over time first and foremost as DeFi development platforms. How pathetic if it turns out to be the truth! For we are 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 phase, aka Web3.0.

Web3.0 hasn't happened yet. But based on the 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, for they're owned and run by companies whose goals are commonly recognized to be maximizing shareholder value. That is to say, Web2.0 platforms would extract as much profit as they could from the economic activities they coordinate. And the company's governance, especially those public listed companies, would ensure Web2.0 platforms continue in that manner.

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 resistance? Not so many. All applications that take

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 provides user experience at a comparable level with its Web2.0 counterparty. Good UX is the hardest part of Web3.0 application development which relies on distributed ledger technology that inevitably involves more complexities, raised costs, and ultimately downgraded UX.

Fortunately, a secret weapon has been forged for Web3.0 applications in the past few years: blockchain frameworks, for example, Substrate and Cosmos SDK, which 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 those shiny app icons for many years. In short, developers can deliver a fully optimized Web3.0 application by building an appchain. In contrast, thousands of other applications share a standard set of configurations on a generic smart contract platform. Meanwhile, 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.

Appchains have the 3rd supremacy over smart contracts. And in the long run, this factor matters the most: 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 and have stepped 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.

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 cryptoasset market and bootstrapping an active validator community from the ground. Polygon and Skale may seem like options, but they are still smart contract-based and not designed for appchains. Appchain offers 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.
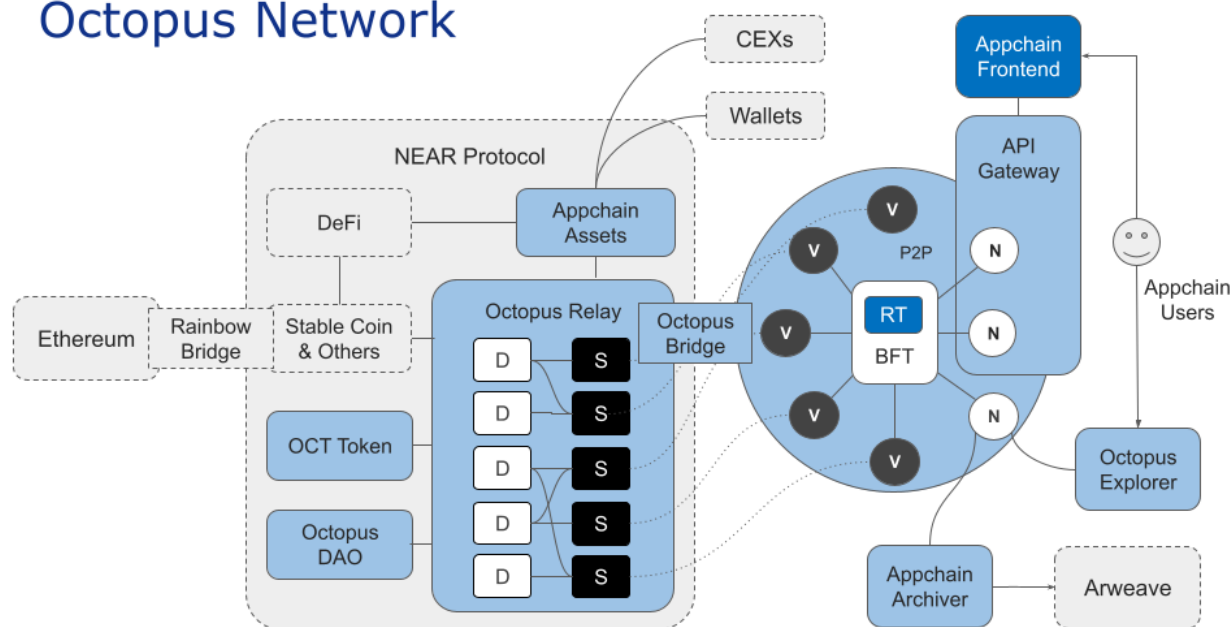
Within the Octopus Network, each appchain decides its economic model, including how many tokens it's willing to pay to validators for security. Because it's the OCT (the native token of Octopus Network) holder's responsibility to decide which appchain they'd like to stake on, the Octopus Network works as a free market, where appchains can lease the security needed at a market price at any time.

The core of 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 are sitting on the demand side of the market. They pay rent in their native token to lease security from OCT holders.

There are two types of participants sitting on the supply side of the market, appchain validators and appchain delegators. Validators will stake OCT to an appchain in 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 commission. All punishments are applied to delegators proportionally when their validators get slashed.

Validators that failed to keep their nodes up 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 Octopus Relay. Then malicious actors' staking will be slashed. By working in this way, appchain security is ensured by the staked OCT. And the security level of an appchain is proportional to the total value of staking.

Appchain needs interoperability. In most Web3.0 application economies, there is a demand for payment methods. However, the widely accepted stablecoins, such as USDT and USDC, have very high requirements on transaction volume. Appchains are almost impossible to meet the criteria at their initial stage. The other way is to build a cross-chain bridge between appchain and Ethereum, enabling Ethereum assets to be transferred into appchain and utilized as a payment method or for other purposes. But a reliable and usable Ethereum bridge is a big headache even 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.

Octopus Relay enables appchains interoperable with NEAR protocol and with Ethereum via Rainbow bridge. At the same time, appchains could utilize an out-of-the-box [IBC](#) pallet to connect with any IBC enabled blockchains directly. That means any asset issued on Ethereum, Near, or any IBC enabled blockchain could be transferred into and utilized by the Octopus appchains trustlessly. Vice versa, assets issued on appchains could be transferred trustlessly out to Ethereum, NEAR, and any IBC enabled blockchain.

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

Octopus is not only a cryptonetwork that provides leased security, interoperability, and infrastructures to appchains but also a meta-community to hatch Web3.0 application communities. It is a focal point where Web3.0 application developers, aka appchain founders, can show the merit of their cryptonetwork, attracting various kinds of supporters, such as investors, validators, and delegators, and market participants. Octopus is a community for appchains to start the journey to build 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 usually is a quantifiable property, at least roughly. And 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.

The first model is that each appchain relies on its PoW or PoS security called ["easy solutions" by Vitalik Buterin](#), 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, in which the same security level, potentially very high, is shared among the whole network, as Polkadot does. But Polkadot faces difficulties in resource allocation. Considering the overhead of coordination, the total amount of shards is limited. Ethereum V2 will have 64 shards, and Polkadot will have less than 100 shards. Suppose the network allocates one shard for one application. It can only support a few tens of applications, and each application needs to afford a few tenths of the total network consensus cost, which does not make sense both for the network and applications. Parathread may seem like a workaround, but it still lacks elaboration. At least for some types of application, such as decentralized gaming or social media, an underlying blockchain without liveness guarantee, like parathread, is meaningless.

In a computation system, security is not the higher, the better, because a higher level of security always comes along with a higher level of cost. So what a computation system needs is appropriate security or good enough security. In Polkadot, developers can't decide what the appropriate security level for their parachain is. They only have one choice, win a slot in the auction. Even 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 trapped in hyperinflation, for they have to promise to issue a big chunk of native tokens to crowdloan lenders. At least this burden leaves the parachain very little space to incentivize the real value creators of their protocol, aka participants who help build network effects of the cryptonetwork.

In Octopus Network, each appchain decides its economic model, including how many tokens they're willing to pay to validators for security. And it is the Octopus holder's responsibility to determine what appchain they'd like to stake on, taking the risk of earning a bag of valueless shitcoin while enjoying the rewards of token price appreciation at the same time. So in Octopus Network, market participants do their planning, and it is the price mechanism that coordinates their decisions.

As mentioned before, in a multichain network, the major blockchain security issues arise from the 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 but most likely honest validators can challenge them by submitting fraud-proof to Octopus Relay. There are two types of fraud-proof corresponding to two types of malicious action deem to 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 includes invalid transactions;

The 1st type of fraud-proof could be verified by Octopus Relay directly, and it's pretty straightforward since Relay knows all 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 have signed the duplicated header will be slashed. The severity depends on the summed voting power of faulty validators. If it is about up to or beyond 33% voting power, 100% stake will be slashed. These penalties will be transferred to an on-chain treasury. Octopus Relay will halt the corrupted appchain, and its future is upon the governance decision.

The 2nd type can't be verified directly by the Octopus Relay at present. So once this type of fraud-proof is received, the Octopus Relay will pause staking/delegation operation and cross-chain asset transfer into and out of the appchain, then trigger a governance process to make a judgment and take corresponding actions.

Another problem is data availability, on which Octopus would also try a new design. While other methods rely on data availability proof which is complex and expensive, Octopus resorts to a challenge-response game. All Octopus validators keep observing Octopus Relay, especially the light client header chain which acts as the Root-of-Trust for cross-chain asset transferring. A malicious validator group could post a header to the light client but hide block content from honest validators. By doing that, the malicious group may steal cross-chain assets from the mainchain that is locked on Octopus Bridge or transfer fake appchain assets to the mainchain. Once an honest appchain validator finds a newly committed block header in the appchain's light client in Octopus Relay, but he doesn't have the corresponding block data, he should submit a query tx to the relay for showing doubt. If he receives the block afterward, he should withdraw the query. Depending on network conditions, it's normal to see some queries come and go. But if one appchain accumulates a considerable amount of query on the same height, the relay will emit data availability challenges. In that situation, it is the header's signers' responsibility to submit a valid block that justifies the header. If they fail to do so, their staking will 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, just like the way NEAR supports EVM. After all, NEAR and Substrate are all WASM-based. Providing the proper runtime environment, the 2nd type of fraud-proof could be processed inside Octopus Relay without involving human intervention. The technology behind it will be just like what Polkadot Relay validator and parachain collator do now, where Relay validators are stateless clients of the parachain, and it is parachain collector's responsibilities to pack and submit Proof of Validity(PoV) block, which include transactions and state data being needed to execute or verify these transactions.

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. Why is that? Because security leasing is essentially capital leasing or

collateral leasing. Though capital is a scarce resource, it scales without physical limitations. In the Polkadot case, each parachain will occupy a certain amount 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 Polkadot. Since Octopus does not have its own blockchain, and 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. That means the basic interest rate of the Octopus economic system is zero. When the basic interest rate is zero, a 3%-5% is a decent annual return, which is the range we expect an appchain will pay for their leased security. But for a Polkadot parachain, it has to pay 20% or even more annual return to make itself attractive to crowdloan DOT lenders because staking on Polkadot Relay will give the investors 14% risk-free annual return. Just imagine two economies: one has zero basic interest rate, the other has 14%, it will be way more difficult for startups in the later one to raise capital. In the multichain network case, to lease security.

Octopus appchains have high-performance, cost-effective leased security. According to the impossible triangle theory, have we chosen to sacrifice decentralization? Of course not! The envision of ordinary users running full nodes on their laptops is too idealistic and will turn out to be impractical, especially in a multichain future. Ten years later, ordinary people may all use a super-sovereign SoV, a DeFi world computer, and at least a dozen appchains for social media, media streaming, blog, classified AD...etc. They could not run all these blockchain nodes on their commodity laptop.

Fortunately, decentralization could be kept in another way. People used to vote with their feet rather than hands, and it's workable in crypto, on condition that one thing provided: forkabililty. Forkabilitiy means how easy a cryptonetwork could be forked. Given good forkability, even if a few plutocrats control governance, it's meaningless for them to seek rent by changing the rules. Once they do that, users who contributed a significant part of economic activities could leave the cryptonetwork and settle down on a new fork with fair rules. In this case, users stay unharmed, while plutocrats lose the resource they put in to control the network. Imagine what will happen on Freenode, if IRC is a forkable cryptonetwork.

Yes, forking needs social coordination, and this time the effort will be on the ordinary users' side. But how could one expect to control his assets, identity, and data without even noticing what's happening here? If someone does not care about fairness, openness, privacy, and would like to stay on any oligopoly platform, just let them be. Internet users who deserve Web3.0 do not have to set up and run any blockchain node on their PC. Just keep an eye open on those cryptonetworks you care about, choose the fork you think has legitimacy, use them, give up others, and sell out their token. By doing that, you help ensure decentralization.

Octopus Network limit appchain validator amount in the range of two digits, where pBTF-like consensus works very well and total IT cost is almost neglectable. At the same time, Octopus

will serve all its appchains with great forkabilitiy by archiving appchain block history to [Arweave](#),
a decentralized permanent storage protocol. Based on 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 they lose 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 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." Then basically, any system to
facilitate blockchain interoperability needs to solve two problems: The 1st is how the target
chain knows a state transit that it cares about has happened on the source chain? Since
blockchains are computation systems that passively handle requests, they need an off-chain
process to update them. The 2nd problem is how the target chain could make sure a message
carries the true, unaltered information about the state transit on the source chain?

Generally speaking, there are two types of commonly recognized blockchain interaction:
cross-chain asset transferring and cross-chain messaging. At the first look, 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 cross-chain asset transfer could be
implemented based on that. But when digging in more profound, it is showing 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 by cross-chain messaging usually can't be quantified. In
other words, no one knows how many collaterals are needed to cover the exposure. So
basically, there is no notable cross-chain messaging practice in the public blockchain space.
Maybe some people would like to cite the [Polkadot XCMP](#) as a counterexample. But actually,
XCMP is a cross-shard messaging protocol, and each shard has the same security level and
assumption, fundamentally different from real cross-chain cases.

In the real world, cross-chain asset transfer has been widely adopted. It may seem restrictive on
functionality. But cross-chain asset transfer is much more powerful than people commonly think.
In its paradigm, vouchers are created on the target chain to represent assets locked on the
source chain. Then these vouchers can be utilized by any application protocols as if they are
local assets. Theoretically, all types of financial transactions are supported once cross-chain
asset transfer capability is provided since any financial transaction is about exchanging various
kinds of vouchers between entities. In Octopus Network, we aim to support trustless, secure,

and easy-to-use cross-chain asset transfer between appchains, the mainchain, and any other public blockchains alongside Octopus.

Vitalik Buterin described the classic blockchain interoperability taxonomy in 2016, which is somewhat outdated by the current standard. In a framework proposed by World Economic Forum in 2020, there are three approaches unique to blockchain interoperability: cross-authentication, API gateway and oracles, and cross-authentication approach, which is further classified to notary schemes, relays, and hash-locking. Oracles are not so different from notary schemes in the blockchain interoperability context. When oracles feed data that originated from other blockchains, they are notaries essentially. In the following paragraphs, we will use notary and oracle interchangeably. And we left out API Gateway since it has to rely on a trusted third party to run the gateway and can't be utilized in a trustless environment.

As Vitalik and WEF have pointed out, Hash-locking has the most limiting functionality, supporting only digital asset swaps. But none of them have noticed, hash-locking is not a meaningful way to support trustless cross-chain assets swap. Because B, who locks his asset after counterparty A does essentially give out an option for free. 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. Though B will try to limit the timeout span, the option's value will never be zero. So more or less, B has to rely on A not to take his advantage, aka trust A.

Relays are considered by nature trustless. 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. No wonder state-of-the-art blockchain interoperation systems and protocols such as Rainbow Bridge and IBC protocol are all in this category. But relay is not such a perfect trustless cross-chain approach as many people think. Relayer, the off-chain process responsible for feeding the light client on target chain with block headers or the equivalent of source chain, turns out to be Achilles' heel. Though relayers can not cheat light clients, there must be at least one honest relayer to keep light clients updated. A system is as decentralized as its most centralized component. The relayer incentive mechanism is complex and remains an unresolved problem even for the most advanced protocols.

On the other side, notary schemes and oracles are often considered trust-based approaches, which is not necessarily 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, essentially, the oracle scheme does not introduce any extra entity that needs to be trusted. In that situation, oracle or notary schemes should be considered trustless. What's more, the oracle data feeders or notaries do not need an extra incentive model other than the one prepared for validators.

Octopus needs every honest appchain validator acting as a fisherman, being ready to challenge malicious ones. Being a fisherman requires a validator equipped with a reliable way to observe and submit tx to Octopus Relay on the mainchain. These facilities could also be utilized as an oracle about any event emitted by Octopus Relay, including staking-related events. Therefore,

the cross-chain mechanism from the mainchain to appchain is: each appchain validator sets up a reliable RPC connection to a mainchain full node(or indexing service) and subscribes all staking cross-chain events happen in Octopus Relay by using [Substrate off-chain worker](#). Once an event is observed and identified targeting the appchain, all validators of the appchain will vote with voting weight proportional to staking, reaching a consensus on the appchain about the event's existence. Once a consensus is reached, corresponding actions, such as mint voucher token or update 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 a trustless oracle we have described before. And this mechanism does not increase the cost, because validators when acting as fishermen, need to observe the mainchain anyway.

The other direction, appchain to the mainchain, is different, for it is not possible to customize the NEAR stack to embed an oracle. We choose the relay approach instead. In the early implementation, the foundation will run a set of relayers to update the block headers, [MMR roots](#) actually, 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 a considered factor for block rewards.

Trustless cross-blockchain interoperability sits at the core of the Octopus Network protocol stack. Based on it, Octopus Relay enables appchains to be interoperable with the mainchain, that is to say, NEAR protocol. Furthermore, appchain can interoperate with blockchains outside Octopus Network, either via bridges on NEAR, such as with Ethereum via Rainbow bridge or utilize the out-of-the-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, which Octopus Network is designed to be a part of. Octopus team, previously known as Cdot, has been [working on universal blockchain interoperability protocol IBC](#) and [cross-chain integration](#) area for a long time.

Community

Nowadays, anyone can deploy smart contracts on a public blockchain and host a front-end UI, essentially making a Web3.0 application alive, all with meager costs. But the problem is, how could they make their applications, even if astonishingly good, known by potential users? The solution is to set up a focal point of Web3.0 applications, which the Octopus community aims to be.

Appchain Pipeline
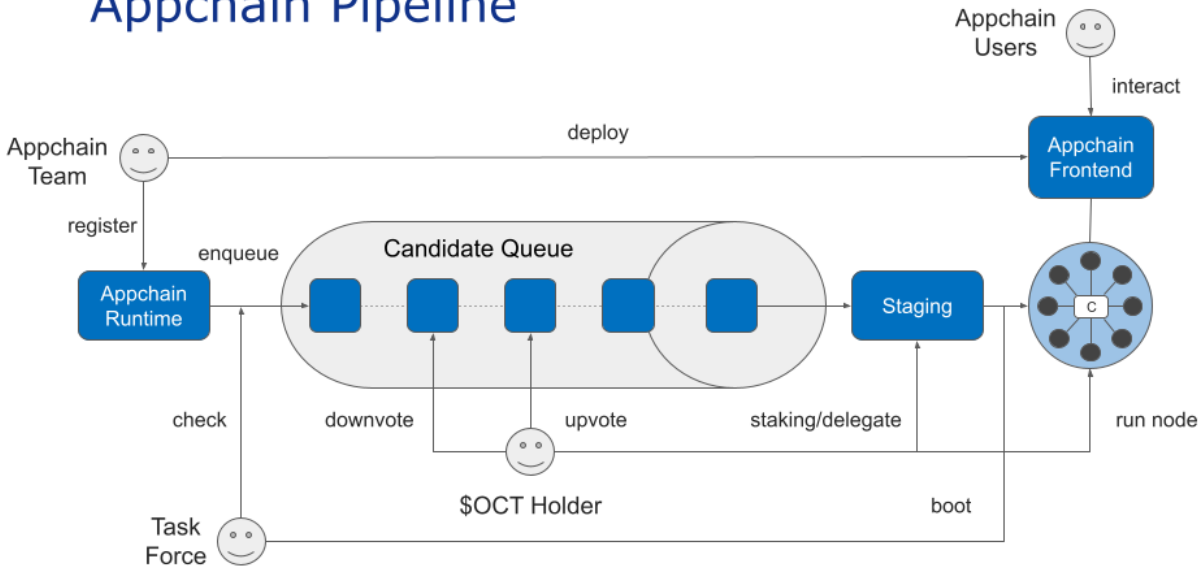
The architecture design of Octopus Network, coupled with the processing power of the NEAR Protocol, makes it easy to host hundreds of appchains. But we don't want to see appchains to join the Octopus Network without proper selection, which will usually form a lemon market where bad coins drive out good coins. We implement the process of appchain selection as part of the Octopus protocol and give decision-making power to the Octopus community, that is to say, OCT holders.

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

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. 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 the white paper or spec.

Once passed the auditing, the appchain 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 ranked first in the number of upvotes minus downvotes in the queue will enter the staging state. This one is the most supported appchain by the Octopus community. In the staging state, OCT holders could stake or delegate on the appchain. When the staging period ends, if the appchain has attracted enough staking, which goes beyond the security bottom line, it will enter the

booting state. In the booting state, task force members will run four bootstrapping nodes to start the appchain. Then validators could run their nodes to join appchain consensus. Octopus Network will also run a full node cluster for each appchain and provide API access service to the appchain front-end. Appchain developers just need to change the front-end configuration, and then the appchain is ready for end-users to use.

Octopus recognize appchain projects are the value creator of the network. The first 100 launched Octopus appchains will be directly rewarded by 100K $OCT in three years after the launching event. While other multichain networks charge for admission to appchains, Octopus takes appchain teams as the most critical part of the community and is very happy to share the benefits of network effect expansion. In addition, the foundation has decided to provide an additional 1 million $OCT rewards for the first ten appchains and recognize them as founding appchain.

Cryptonetwork is owned by its community, and this is the essence of decentralization and the fundamental difference with Web2.0 platforms. 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. Besides infrastructure and an eye-catching stage, Octopus Network provides forkability to all its appchains, making it meaningless for any rich man 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 Octopus Network and NEAR, various kinds of crypto assets issued on Octopus appchains will contribute to the prosperity of DeFi eco on NEAR.
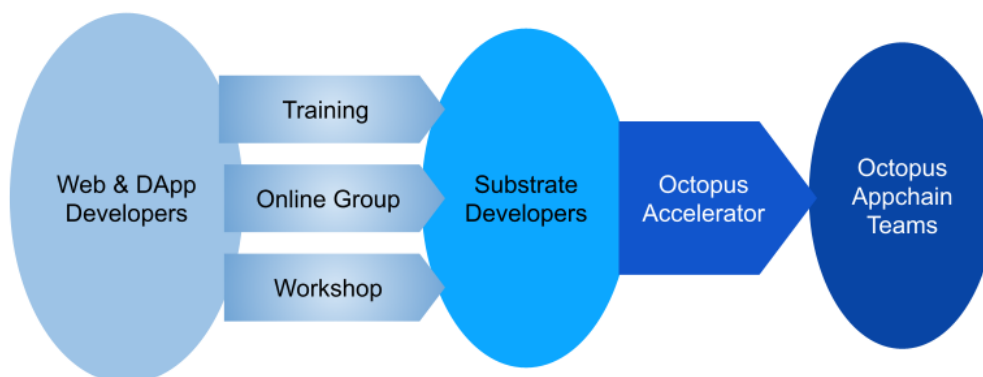
The core community-building problem faced by Octopus Network is: how to find and attract outstanding appchain projects. In the entire Internet industry, blockchain is just a small branch. And in the blockchain space, Solidity developers still occupy the mainstream. So the first task is to transform web developers and Solidity smart contract developers into Substrate developers. In this regard, we are very experienced. Two years ago, we and some community enthusiasts

initiated the first Substrate online training course worldwide. The almost free course trained the first batch of Substrate developers in China and also the origin of the Chinese Substrate community. It is now an official course funded by Parity Inc. 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 in regions besides China.

But even with qualified Substrate developers, there is still a long way to go to form a mature appchain team. Because 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 plan is to hold a batch every quarter, each lasting ten weeks. During this period, learners and mentors will discuss 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 5 appchain projects and provide them with a $250K total reward. In this way, Octopus Foundation will directly fund 20 appchain projects through the accelerator each year, providing them $1 million in total.

Tokenomics

OCT is the native token of Octopus Network, a fungible, non-inflationary utility token with three utilities in Octopus Network:
- to be used as collateral to guarantee the security of appchains;
- to be used for the governance of the network;
- to be used for endorsing appchains by upvoting them in the candidate queue.

The core role OCT played in Octopus Network is appchain staking. Holders put their OCT at risk (via staking) to provide security to appchains and get rewards in appchain native token. The staking acts as a disincentive for malicious participants who will punish by getting 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, the common practice for appchain will be paying $400K-$600 worth of security rent in its native token to validators, which makes sure the appchain gets above several million dollars security at the point. In most cases, this security level is enough for a newly born appchain. According to this calculation, only newly launched appchains will bring about $200M 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 attracts more and more economic activities, its token price will increase. Then the rent increase will attract more collateral

accordingly, which means the appchain will automatically obtain a higher level of security. For anyone who believes in the necessity of Web3.0 and takes appchain as the correct form of Web3.0 application, it is reasonable to project that the total economic value of appchains grows at a fast pace, and so their security/collateral demands.

The 2nd function of OCT is to entitle holders to control the governance of the network, more specifically Octopus Relay, where all economic rules apply, by forming Octopus DAO. There is excellent quantitative research on governance token valuation, which concluded that stake size and decisiveness(the possibility a vote determines the referendum's result, representing the relative value of governance power) are positively correlated, and in some cases, result in an exponential relationship. Octopus DAO Council has a maximum of 100 members, while it's most likely to be a few dozens when stable, going from a few at the beginning. Each council member's governance power is valuable but still disperse enough to keep from collusion. The relative value of governance power showed as 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, token's governance value can not be decoupled from the utility value in most cases. A sound and widely participated governance will give token holders more stable value expectations, then suppress extreme fluctuations in the token price, thereby reducing the implicit option cost of appchain staking.

The last but not the least function of OCT is to decide which appchain will go live in the network by upvoting or downvoting on candidates. Appchain teams 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 appchain to support carefully, for there is an opportunity cost of missing more valuable ones.

While downvoting low-quality appchains or Ponzi scheme ones will not bring economic benefit to voters, we believe there is faith in justice and fairness around, and people will fight evils even if it's not economically rational for them. The long-term goal is forming a set of social contracts on embracing good appchains and expelling evil ones. Before that, the Octopus Foundation and founders will not hesitate to use their voting power on downvoting evil appchains. But don't ask me the standard of evil appchains. I know it when I see it.

Though it's hard to evaluate the influence power of OCT quantitatively, one thing for sure is that most institutional investors engaged in the Octopus ecosystem will spare a chunk of OCT to support 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 on appchain-OCT holders interactions.
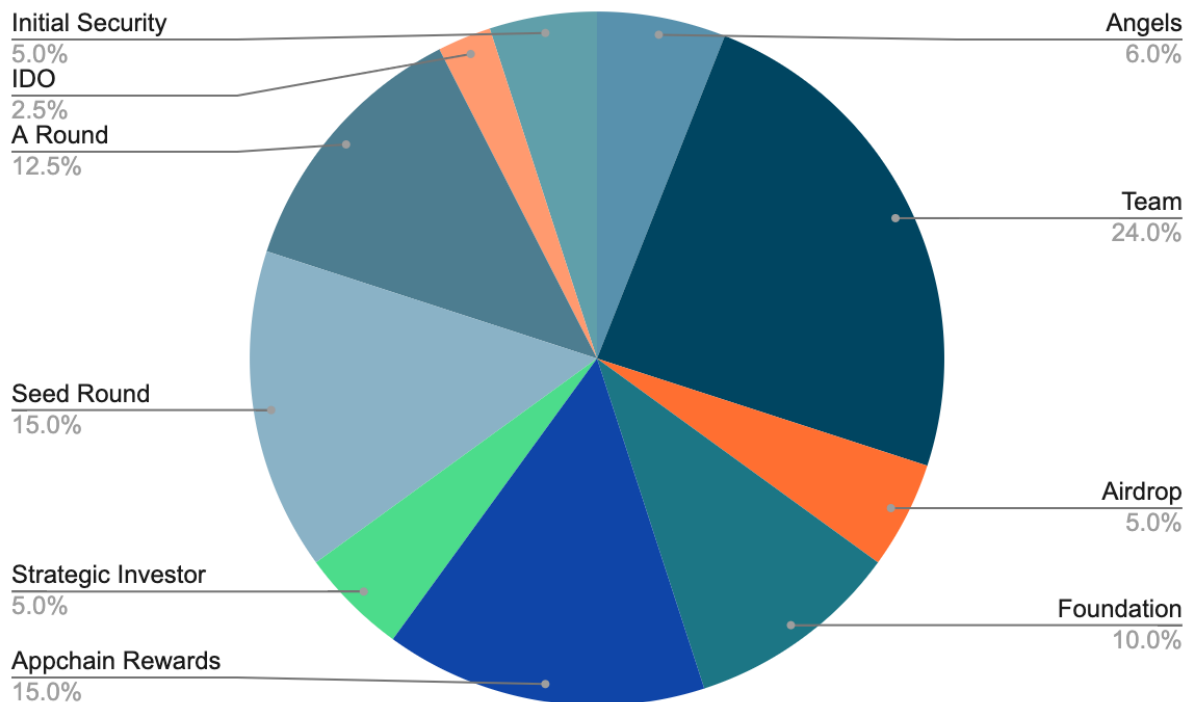
The total supply of OCT is fixed at 100 million. 41% of OCT are distributed to investors, 6% to angel investors, 5% to a strategic investor (NEAR foundation), 27.5% to institutional investors who participate in seed and round A private sales, and 2.5% to IDO investors. Besides these, 24% OCT is to reward the core team in 5 years starting from April 2019.

It's a common headache for a cryptonetwork to identify its actual community members and distribute tokens. Some tried in various ways but were not so successful, such as Stellar, Handshake, Edgeware, to name a few. A community should be consistent with the actual participant of the cryptonetwork. For Octopus, they are web3.0 investors and web3.0

developers. So we will try our best to distribute OCT to qualified and long-term thinking investors who're devoted to Web3.0 and form the basis of the Octopus community rather than speculators.

OCT belongs to Octopus Foundation; 30% of the total supply will incentivize the upcoming Octopus community contributors. The initial plan is to airdrop 5% OCT in 5 years after mainnet to social media users who help spread the idea and value proposition of Octopus Network. The Octopus core team is working on executing precision airdrop since no existing platform can meet our requirements.

The first 100 launched Octopus appchains will be directly rewarded by the Foundation. Each appchain team will receive 100,000 OCT respectively in three years after the launching event. Yep, you're reading this correctly! While other multichain networks charge for admission to appchains, Octopus takes appchain teams as the most important part of the community and is very happy to share the benefits of network effect expansion with them.

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 round 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 in 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 Octopus Network, we expect 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 the right. The highest cost of exercising governance is the cognitive cost. When stakeholders can get off quickly, participating in governance to change dissatisfaction is usually not rational. Then there 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 all be considered.

In a multi-sided market coordinated by cryptonetwork, service providers are usually long-term stakeholders because their interests are not limited to current income and income expectations for a long time in the future. More importantly, service providers typically need to learn market rules, operating methods and formulate strategies that suit their characteristics. These costs usually mean that cryptonetwork has stronger stickiness to service providers.

As for service users, they are more inclined to compare prices and quality continuously. Once they have a better choice, they will leave cryptonetworks. So although the network effect of

cryptonetworks is built by service providers and users, the service providers should usually be taken as the long-term stakeholders of cryptonetworks. Therefore, cryptonetworks should design a governance structure around service providers.

In the economic system of cryptonetworks, native tokens should be distributed to service providers as much as possible, and they need to perform some kind of token locking. Voting power should only give to locked tokens that compensate token holders for liquidity loss. By doing that, they declare themselves as long-term stakeholders of the cryptonetwork.

In Octopus Network, things become relatively simple. The essence of 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 the votes to a council member or a candidate. The cancellation of the separate voting process is expected to increase the turnout rate. The delegators do not have the right to vote individually, as 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 consider two factors majorly when choosing a validator. The first is the proportion of staking. For staking that is much larger than the average value, the unbonding period will be extended accordingly, increasing the validator/delegator's options cost. The second is the political factor: to delegate to those validators whose governance views are closest to them.
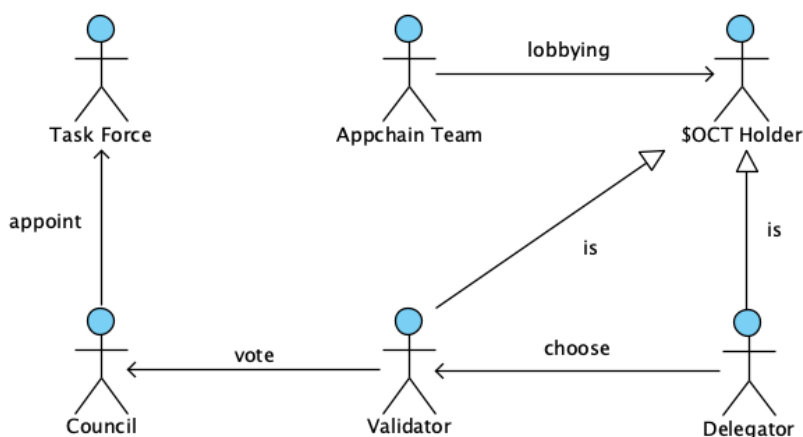
The Octopus Council is the governing body of Octopus Network, responsible for reviewing and deciding on proposals from the community. The proposal mainly covers the expenditure of the on-chain treasury and the upgrade of the Octopus protocol, including the governance process itself. Council members are elected by the community through the method mentioned above, that a NEAR account supported by at least 1 million OCT becomes a council member. Due to the flexibility of NEAR accounts, council members 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. It can be regarded as a type of liquid democracy. Task Force is a professionals group appointed by the council through approval of proposals. They're responsible for the daily maintenance of Octopus Network and receive salaries from the on-chain treasury. Task Force members who misbehaved or lacked 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, as well as the promise to create innovative governance mechanisms. The main criticism of on-chain governance, the inability to resist plutocracy, has been made up by forkability. With the emergence of Octopus appchain and Polkadot parachain 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.

What needs attention is that validators and service providers are the same groups for a base layer protocol where security is the service provided and distinctive groups for an appchain where security is a service needed. Providing the security level is high enough, an appchain as a whole would like to keep the security cost as low as possible. Appchains should never let validators gain control of governance since rational validators will keep on trying to maximize their gain from the appchain economy, which conflicts with other participants' interests and goes the opposite direction of cryptonetworks working as minimally extractive coordinators.

Although we think LPoS is more conducive to the long-term development of appchain than independent PoS. But more importantly, the right to choose always belongs to the appchain community. Octopus Network will provide tools to support appchain to stop using leased security and transform into an independent PoS blockchain. Once the appchain community makes such a decision, its connection with Octopus Network will downgrade to a standard IBC interoperability, and existing cross-chain assets will not be affected.

Due to the incentive structure, an independent PoS blockchain is very easy to be controlled by validators which is catastrophic for appchains. So appchains should use leased security or shared security to achieve a long-term economic balance. In Octopus Network, appchain validators are not involved in the appchain's governance. They are merely providers of security services through a free market.

Coda

Now you know 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 cryptonetwork.

Besides cryptocurrency and DeFi, it is still unclear in which area cryptonetworks can work well on a grand scale. But we do know we can try it with the most dominating force in the whole universe: evolution. By decreasing the total cost of cryptonetworks innovation and enlarging the incentive, absorbing the most creative minds into Web3.0 space, prompting an exuberant and highly diversified ecosystem, the market will filter out winners.

If you don't expect the one chain to fit all needs, you are like us. If you don't believe one chain can rule all the others, you are among us. And if you believe Web3.0 is more than DeFi, you are us. Let's deliver decentralization applications in every online business field that Web2.0 giant or traditional middleman has controlled and return value to its real creators. Gaming, NFT/digital collectible, DAO, Ad, creator economy (video, audio, blog, novel...), prediction market, 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 network after the fiercely smart marine benthos. Rather than a centralized nervous system as vertebrates have, two-thirds of an octopus's neurons are spread throughout its body, distributed between its arms. And now scientists have determined that those neurons can make decisions without input from the brain, essentially making octopus a [decentralized intelligence form](). From evolution's 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 work in an octopus' way. Each blockchain has its intelligence and decision-making mechanism, adapting to specific ever-changing environments efficiently. While connected as a whole, all members benefit from a much more significant network effect and economies of scale. Octopus is a successful alternative form of intelligence. We expect it is a successful alternative form of multichain network. Go, Octopus! Be a unique animal in the crypto sea, and enjoy your journey!