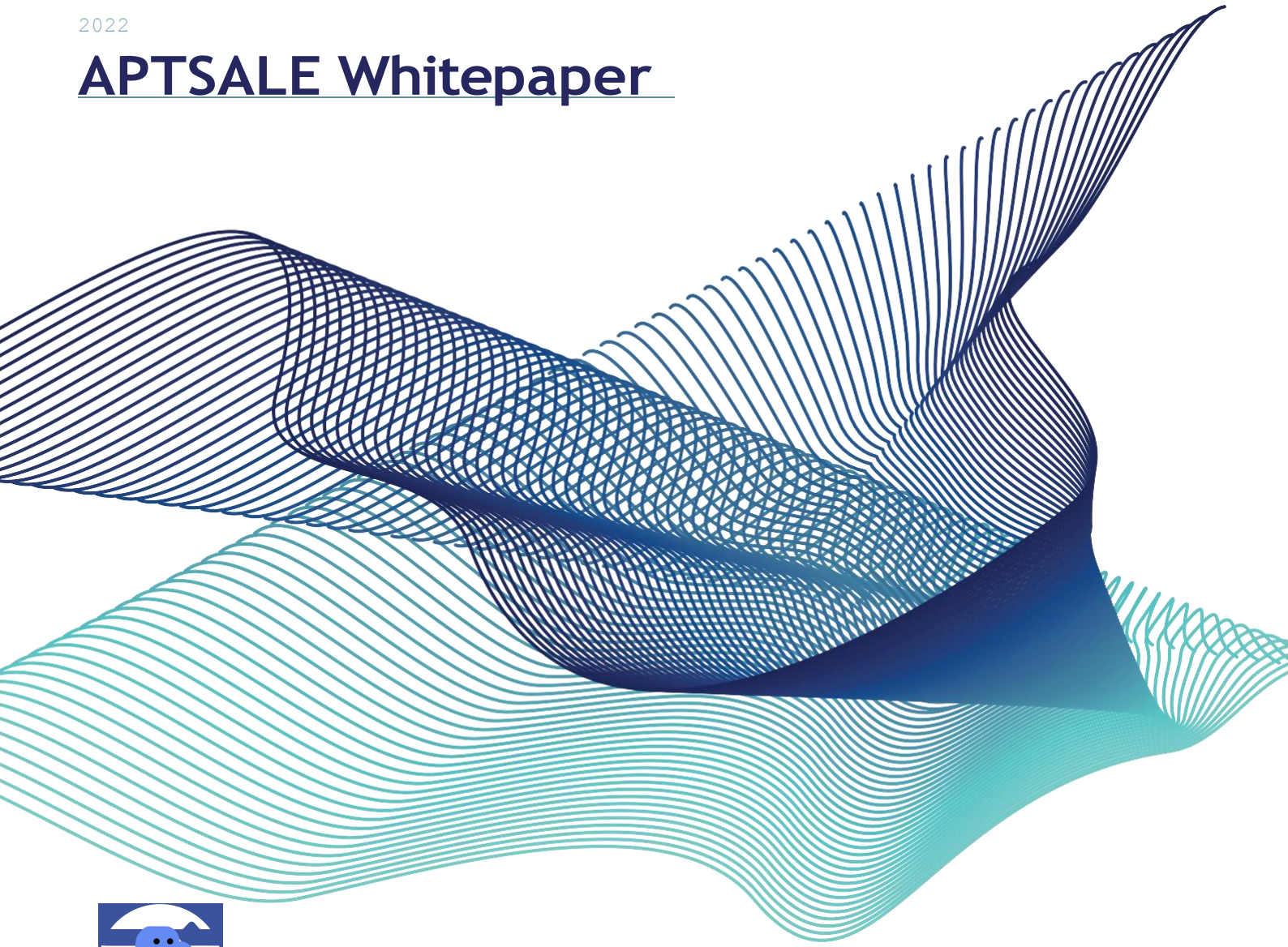
2022

APTSALE Whitepaper



APTSALE

APSALE.IO | https://t.me/APTS_EN | discord.gg/sDYABadMjg | @Aptoslabsale

Abstract

The full name of APTS is Aptoslabsale, which is the first diversified comprehensive service platform on Aptos, including token creation, pre-sale, Swap, NFT market, etc.

APTSALE is a decentralized launchpad that allows users to launch their own token and NFT, users can create their own initial token and NFT sale. No coding knowledge is required, just simply navigate through to our terminal and design your own token and NFT in just a few clicks.

APTSALE offers multiple other features to help you with the overall token launch, such as: Automatic listing of your token on APTSALE Swap and automatic listing of your token on APTSALE Platform, all whilst giving you the ability to lock your LP and and adding an optional vesting period for your tokens.

On top of being a premier token sale and NFT sale creator, APTSALE aims to incentivize users to continue use our platform. Our goal is to provide a safe environment for all of our investors that use our APTSALE ecosystem.

Contents

1. Introduction

In the past 30 years, since the internet became publicly accessible to a broad market in the early 1990s, and with the rapid development of hardware technologies that leverage processing capacity more efficiently, a lot of new business models have emerged. Early businesses focused on IT infrastructure, online advertisements and marketing, and e-commerce. With rising internet user numbers, an increasing number of cloud applications, marketplaces and social media platforms arose during the internet boom of the 2000s. This led to a vast amount of user and business data being generated, which is now referred to as big data. Businesses started to analyze data more efficiently to improve their business processes and products with insights derived from their user base.

Today, these business practices have become extremely prevalent. Indeed, the sole purpose of some businesses is to generate a big user base with a “free” to use service and subse-uently monetize that base by handing user data over to third parties.

In the web2 version of the Internet, services such as messaging, social media, finance, gaming, shopping, and audio/video streaming, are provided by centralized companies that control direct access to user data (e.g., Google, Amazon, Apple, and Meta). These companies develop infrastructure using

application-specific software optimized for targeted use cases and leverage cloud infrastructures to deploy these applications to users. Cloud infrastructure provides access to virtualized and/or physical infrastructure services, such as rented virtual machines (VMs) and bare metal hardware operating inside data centers worldwide (e.g., AWS, Azure, and Google Cloud). As a result, building web2 Internet services that can scale to billions of users has never been easier than it is today.

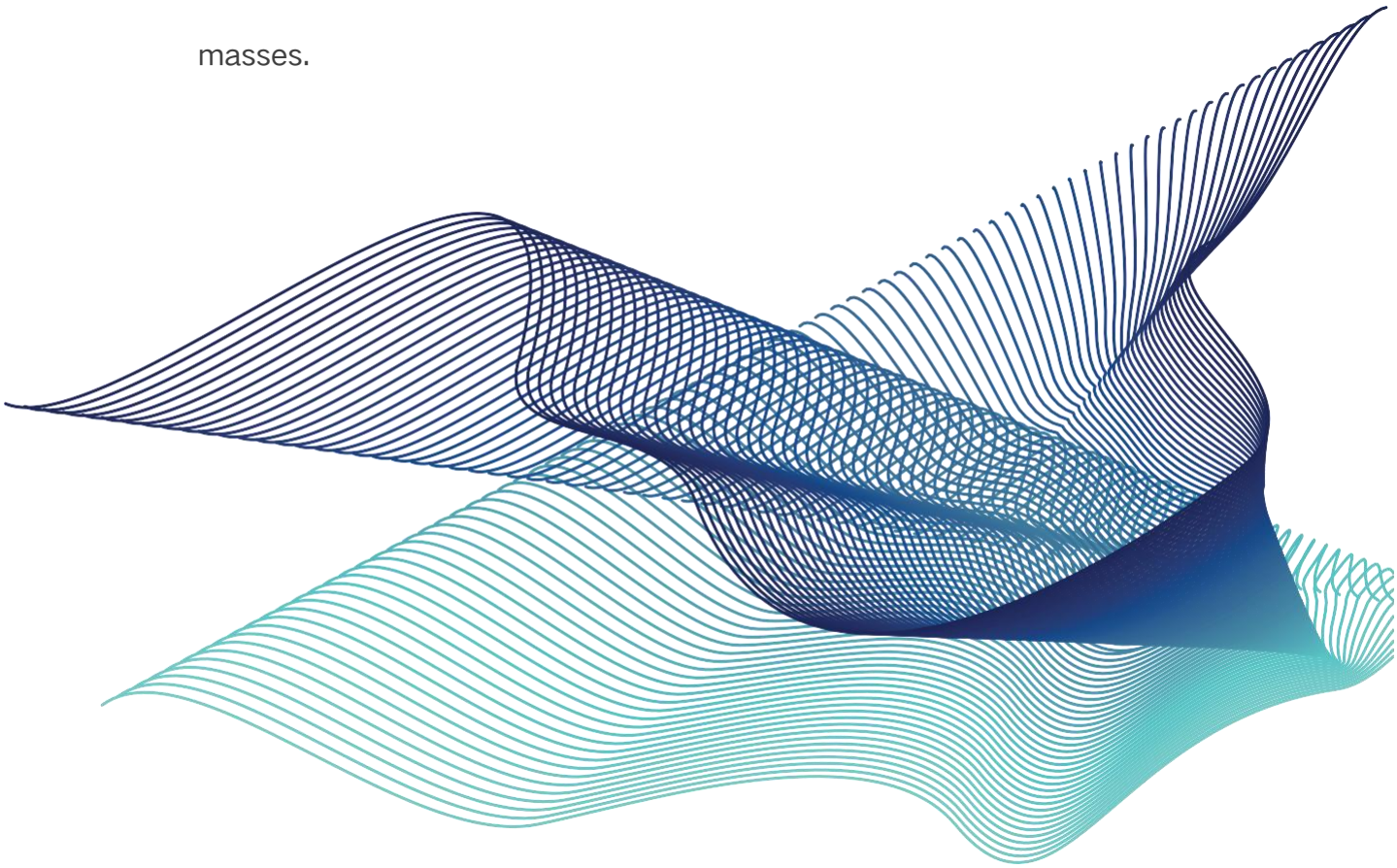
However, web2 requires that users place explicit trust in centralized entities, a requirement that has become increasingly concerning to society.

To combat this concern, a new Internet age has begun: web3. In the web3 version of the Internet, blockchains have emerged to provide decentralized, immutable ledgers that enable users to interact with one another securely and reliably, all without requiring trust in controlling intermediaries or centralized entities.

Blockchain was designed with the intention of solving some of the issues caused by centralized information systems. By decentralizing computation in an encrypted form, the risks posed by single sources of failure are minimized. However, most current blockchain solutions lack either scalability or confidentiality. With regard to the latter, most public chains are completely

transparent and are pseudonymous rather than anonymous. While interesting approaches like zero-proof or multiparty-computation have been proposed, they come at the cost of lower scalability, remain largely academic and can be effectively implemented only for a very narrow range of use cases, like transferring tokens.

APTSALE provides a scalable, interoperable and confidential network layer and offers new and novel innovations in consensus, smart contract design, system security, performance, and decentralization. The combination of these technologies will provide a fundamental building block to bring web3 to the masses.



2. Today's Challenges

When it comes to Web 3.0, companies are confronted with myriad challenges across many different areas. As a result, instead of focusing solely on their core business they need to simultaneously manage processes related to security, technology, regulation and customer trust.

2.1 IT Security

Today, the security strategy of most companies is to build an impenetrable wall around their IT infrastructure to protect sensitive user and business data. Within those systems, data can be secured by setting access privileges and restrictions on data use.

Data in transit, or data in motion, is data in the process of moving from one device to another, either across untrusted public networks, or within a private network. When data is moving, it poses some specific security risks, which need to be mitigated through targeted security measures. Conversely, data at rest is data that is not currently moving between devices and is archived or stored on a hard disk, flash drive, or other storage medium. While it is sometimes considered to be slightly less challenging to secure data at rest, it is regarded by

hackers as more valuable than data in motion.

While protection layers exist for both data in transit and data at rest, the most critical situation is when data is in use. Data in use refers to active data which is stored in a non-persistent digital state, typically in a computer's random access memory (RAM), CPU caches, or CPU registers. Data is actively processed in plaintext and thus readable at least by the operating system and anyone with administrator privileges. While fully homomorphic encryption allows generic avoiding decryption, this approach is still very academic and not practical in most use cases. However, it is possible to protect data in use at the hardware level by using trusted execution environment technology.
Large companies have heterogeneous IT systems with hundreds of solutions where subsets of sensitive data are processed. Typically, they try to secure these systems by implementing extensive cybersecurity frameworks like ISO27001, NIST, or NCSC. In contrast, small companies have to rely on their chosen Safe Web3 Infrastructure to keep their data safe and secure.

2.2 Technology

Companies use a wide range of technologies to run their business processes, secure their systems, and protect sensitive data. Technologies such as cloud computing, blockchain, and software-based privacy technologies like

zero-knowledge proof are becoming increasingly popular, but their requirements put an increased workload on staff. In addition to the fundamental business knowledge required, every IT solution also requires a skilled workforce to operate, maintain and secure the system from both internal and external intrusion. The key challenges such technologies pose relate to how encrypted data is used and managed.

Whenever services are TEEd to the cloud, the customer needs to transfer data and information to a third-party service provider. Furthermore, it is impossible for the customer to verify how their data will be secured or managed by this third party. This is why it took so long for companies to TEE encrypted data to the cloud. Indeed, many companies remain wary of migrating parts of their infrastructure.

In the blockchain space, one approach to interfacing with encrypted data is to use zero-knowledge proofs. This involves a cryptographic method through which an actor can prove to another actor that they know a specific value, without actually revealing the information itself. This approach is only applicable to a very narrow range of use cases, like transferring tokens or proving isolated, specific details. In addition, this approach requires a lot of computational overhead and increases blockchain bloat, due to larger transaction sizes, and is therefore not scalable enough to be widely adopted.

In the context of privacy-preserving technologies, four specific technologies have emerged, which are tailored to cover different use cases and have different strengths and weaknesses:

1. **Secure Multiparty Computation (MPC):**

MPC provides cryptographic methods for parties to compute data jointly, without it being revealed to any single one of those parties. Data is computed in a distributed manner, such that each party securely and privately handles different parts of the computation process. Although MPC has some clear benefits, it is vulnerable to collusion of malicious participants and also has very high computational costs and network bandwidth requirements.

2.Homomorphic Encryption (HE):

HE is an encryption method that allows data to be computed in encrypted cyphertext form, without needing to be decrypted first. In theory, therefore, HE can protect data in use, similarly to how AES encryption protects data in rest and how data in transit is protected by encrypted connections (HTTPS, SSL, TLS). However, one of the most significant disadvantages of HE is that applications need to be modified, or dedicated and specialized client-server applications need to be deployed, for it to work.

3.Differential Privacy (DP):

DP essentially limits the amount of information or data points on each individual record in a database by releasing the result of an aggregate computation on that database. However, this method has significant drawbacks. It only works for interactive scenarios, but does not work with complex queries, and it is also computationally very expensive. The biggest drawback is that when there is little diversity in the data, it includes too much noise, which ultimately reduces the utility of the data and the quality of the analytical output.

4.Trusted Execution Environments (TEEs):

The best of the mix, TEE provide a simple and currently unrivaled way to securely and confidentially process sensitive data. A TEE is an isolated environment that uses both special-purpose hardware and software to protect data. In general, TEE provide a “trusted environment” inside which computations and analysis can run while remaining invisible to any other process on the processor, the operating system, or any other privileged access. Unlike HE, computations inside the TEE are performed on the decrypted cleartext data with comparatively

good performance. These clear advantages drove APTSALE’s decision to leverage TEE technology. There is, however, a downside. We have to trust the TEE manufacturer in several ways: to provide sound hardware and microcode

design, swift and effective patches for newly discovered vulnerabilities and honest remote attestation.

2.3 Regulation on web3 data protection

The GDPR requires organizations to safeguard personal data and uphold the privacy rights of users in all EU territory. As mentioned in the introduction, firms found to have violated these regulations can be fined up to €20 million, or 4% of their global annual revenue, whichever amount is higher. Since GDPR was enacted in 2018, lawmakers in other jurisdictions have passed similar legislation, such as LGPD in Brazil and CCPA in California. Although broadly similar in terms of their overall aims, each of these regulations requires differing implementation measures.

These regulations are just the beginning of an even wider regulatory realignment. In November 2020, for example, the Canadian government tabled the Consumer Privacy Protection Act before parliament. Meanwhile, influenced by GDPR, Australian computation on cyphertext,regulators have also proposed widespread changes to the Privacy Act 1988. In the US, several states including Nevada, New York, Texas, and Washington are considering enacting data privacy regulations similar to those in California.

GDPR regulations have been actively enforced since 2018. In the first 20 months after it was enacted, regulators issued more than €114 million of GDPR fines to hundreds of companies, including Google and Facebook. Since then, the fines have continued to mount. Facebook has set aside a budget of €302 million to pay European regulatory fines, while Amazon was hit with a record $887 million GDPR fine in July 2021.

Why GDPR alone is not the solution:

The volume and size of fines issued to companies so far only amount to a drop in the ocean. Big data giants like Facebook and Google can easily pay such fines and it makes sense for them to do so, as their business model is built mainly on generating and monetizing user data, which generates billions in revenue annually. Thus, they can simply budget for such fines and continue with the same practices.

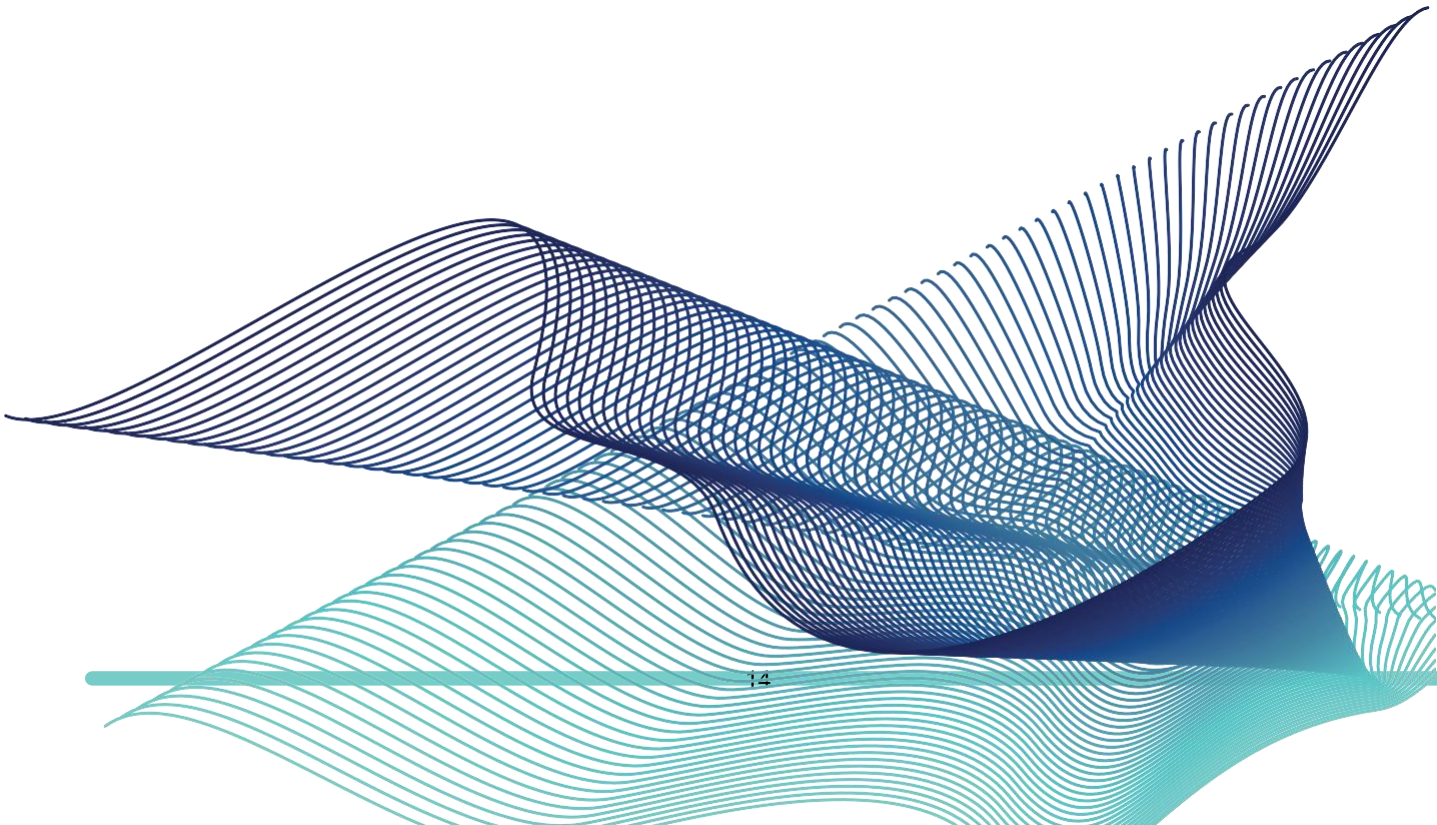
While big players are not hugely affected, small and medium-sized businesses are struggling to cope with increasing regulatory requirements that necessitate the implementation of new processes and security systems. In addition, collaboration between businesses is hampered as it becomes cumbersome to share data while ensuring compliance with data protection regulations.

2.4 Customer Trust

Web2 requires that users place explicit trust in centralized entities, a requirement that has become increasingly concerning to society. However, despite the existence of many blockchains today, widespread adoption of web3 has not yet taken place. While technology continues to advance the industry, existing blockchains are unreliable, impose high transaction fees for users, have low throughput limitations, suffer regular asset losses due to security issues.

In comparison to how cloud infrastructure has enabled web2 services to reach billions, blockchains have not yet enabled web3 applications to do the same.

APTSALE have made a series of radical improvements to the technology stack, In particular, we highlight novel methods of transaction processing and new approaches to decentralization and network governance.



3.The Solution

3.1 Forging A Real Blockchain Ecosystem

For blockchain to become a viable alternative to centralized data solutions, a diverse ecosphere is required to serve as the basis.

Such a system needs to be:

• scalable and fast enough to allow decentralized applications and services to achieve widespread adoption withoutunpredictable transaction costs.

• able to securely refer to private data, without it being stored on-chain or being directly accessible to anyone other than the data owner.

interoperable with many other blockchain architectures and consensus mechanisms as well as cloud-based centralized services

3.2 What We Do

APTSALE provides insights without access to encryption data and empowers firms and developers to build broader, fairer, and more secure data platforms. What if you could unlock the value of data, without access to the data itself? A trusted execution environment is a highly secure, isolated area within a computer Encryption.

APTSALE combines the confidentiality of it with the trust of blockchain. This enables multiple firms to process data in preagreed ways, without having direct access to the underlying data set.

3.3 How We Do It

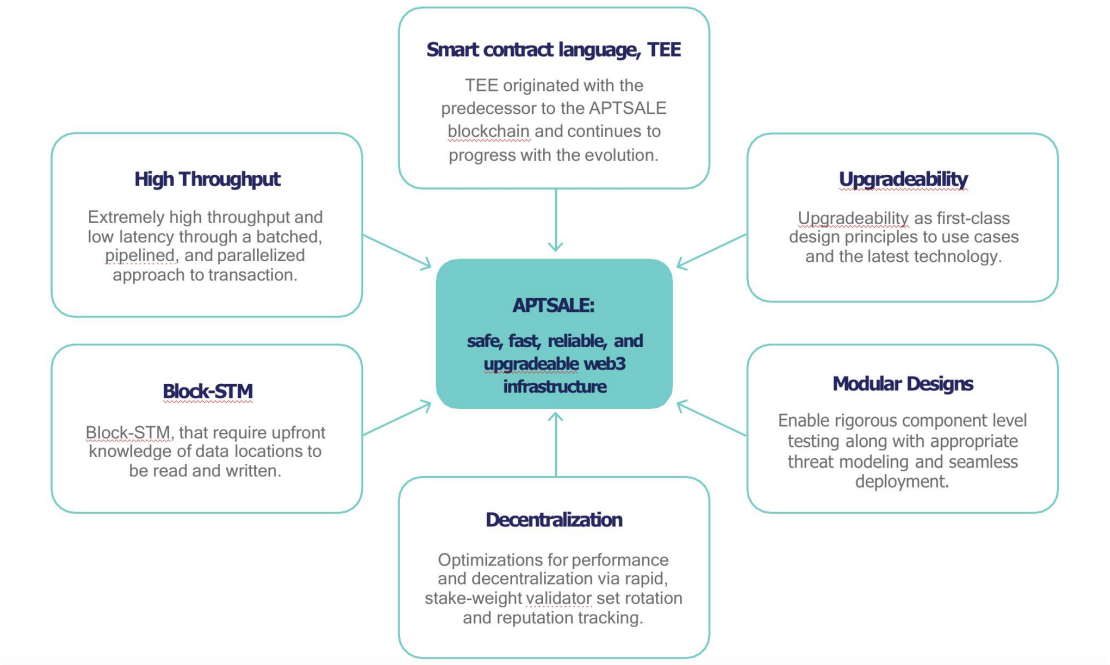
The Aptosale is comprised of a set of validators that jointly receive and process transactions from users using a byzantine fault-tolerant (BFT), proof-of-stake consensus mechanism. Token holders lock up, or stake, tokens in their selected validators. Each validator’s consensus voting weight is proportionate to the amount staked into it.

A validator can be active and participate in consensus. Likewise, a validator may also be inactive if it does not have enough stake to participate, rotates out of the validator set, elects to be offline as it synchronizes blockchain state, or is deemed not participating by the consensus protocol due to poor historical performance.

3.4 The Value Proposition

Aptosale have made a series of radical improvements to the technology stack while also incorporating safe, transparent, and frequent upgrades as a core feature, as inspired by the Diem blockchain. In particular, we highlight novel methods of transaction processing and new approaches to decentralization and network governance.

Full Node they may elect to prune transaction history and blockchain state as desired to reclaim storage. Light clients only maintain the current set of validators and can query partial blockchain state securely, typically from full nodes. Wallets are a common example of a light client.



4. The APTSALE Ecosystem

4.1 The TEE Language

TEE is a new smart contract programming language with an emphasis on safety and flexibility. The Aptsale blockchain uses TEE’s object model to represent its ledger state and uses TEE code (modules) to encode rules of state transitions. Users submit transactions that can publish new modules, upgrade existing modules, execute entry functions defined within a module. Or contain scripts that can directly interact with the public interfaces of modules.

The TEE ecosystem contains a compiler, a virtual machine, and many other developer tools.TEE is inspired by the Rust programming language, which makes the ownership of data explicit in the language via concepts like linear types.

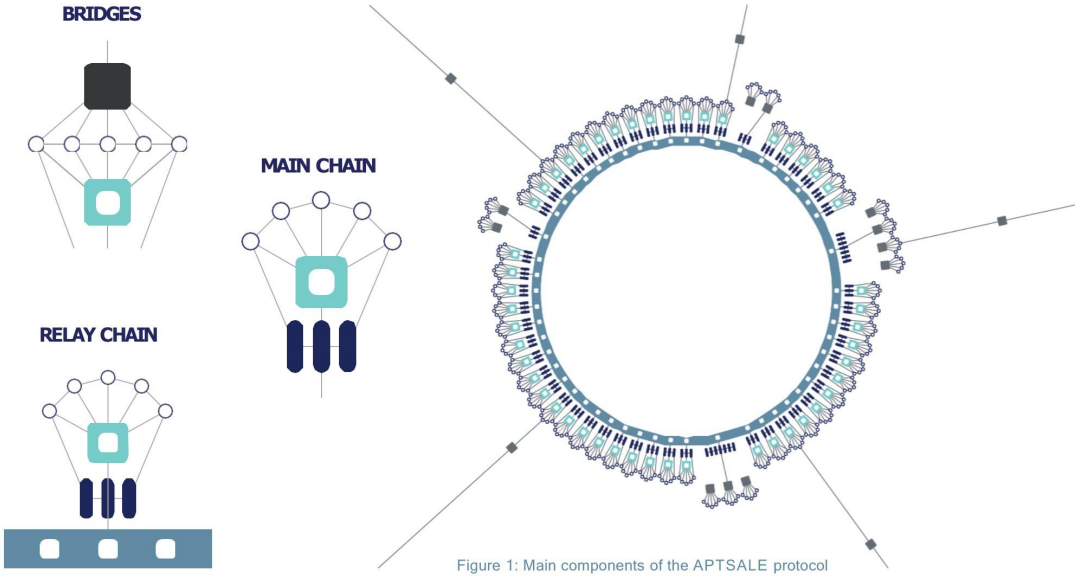


Figure 1: Main components of the APTSALE protocol

TEE emphasizes resource scarcity, preservation, and access control. TEE modules define the lifetime, storage, and access pattern of every resource. This ensures that resources like Coin are not produced without appropriate credentials, cannot be double spent, and do not disappear.

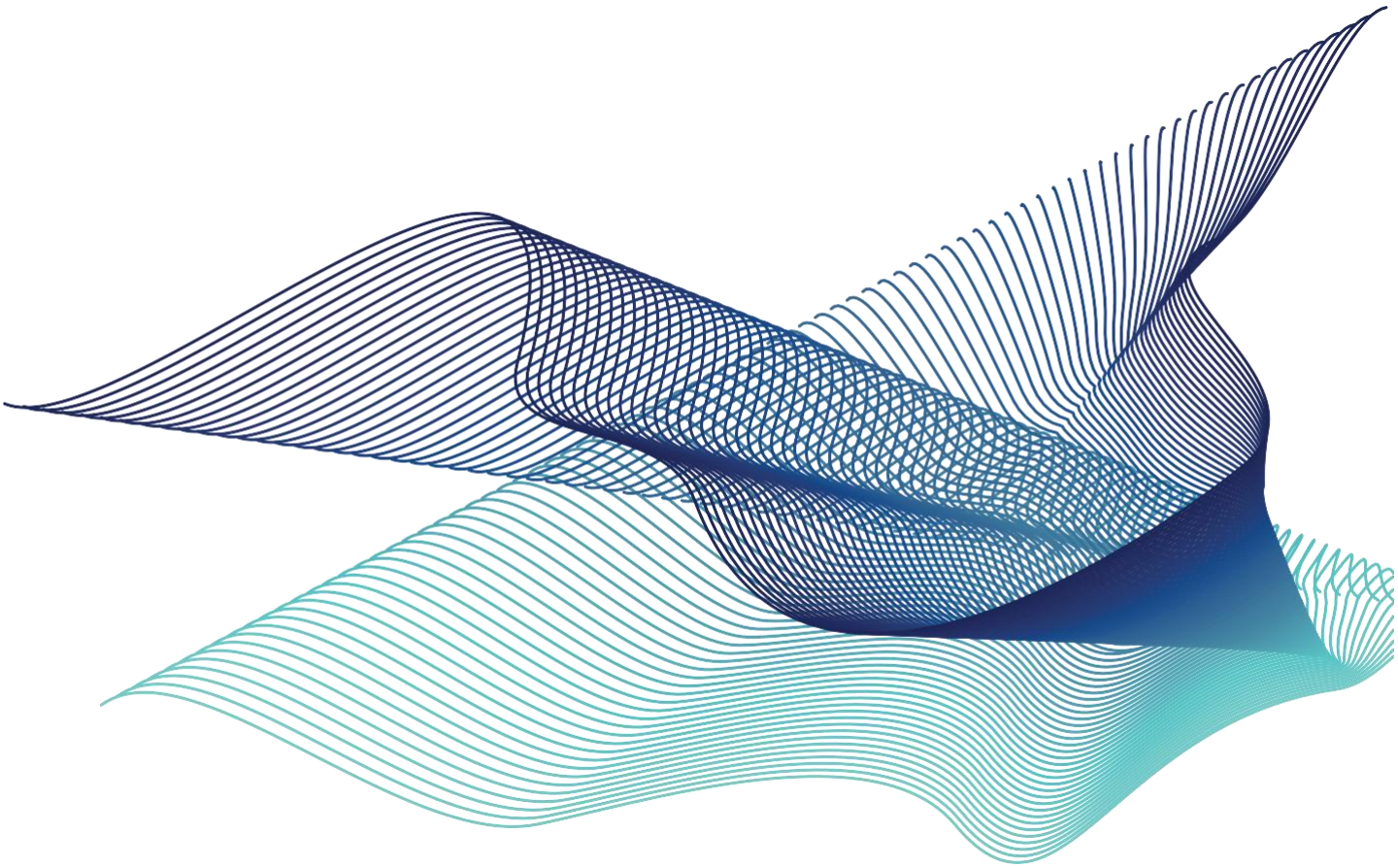
TEE leverages a bytecode verifier to guarantee type and memory safety even in the presence of untrusted code.To help write more trusted code, TEE includes a formal verifier, the TEE Prover, capable of verifying the functional formal verifier. The functional correctness of a TEE program against a given specification, formulated in the specification language integrated into TEE.

Beyond the user accounts and corresponding account content, the ledger state also contains the on-chain configuration of the blockchain. This network configuration includes the set of active validators, staking properties, and the configuration of various services within the blockchain.

4.2 TEE Network

As discussed above, the Relay Chain can be considered to be one of the key innovations of APTSALE— providing pooled security, consensus and cross-chain interoperability for a multi-(para)chain system. As they are heterogeneous, chains can be considered to be individual blockchains in their

own right, with specific features and native tokens. Due to the fact that Chains can rely on the Relay Chain for pooled security, more time and resources can be focused on innovating to build new functionality, targeted for specific uses. In addition, as all chains communicate with the same Relay Chain, they are mutually interoperable. Each Relay Chain is expected to be able to accommodate a finite number of chains, however, with current projections placing that limit at around 100.



5. The APTSALE Network

5.1 Introduction

The public blockchain: The APTOS network On Aptos, any type of data can be exchanged between any type of blockchains on the network. Interaction with external protocols like Ethereum is also possible, unlocking a wide range of use cases. One of key benefits is that it provides strength in numbers by enabling many blockchain networks to pool their security resources.

For APTSALE, the Polkadot Relay Chain will provide public auditability.

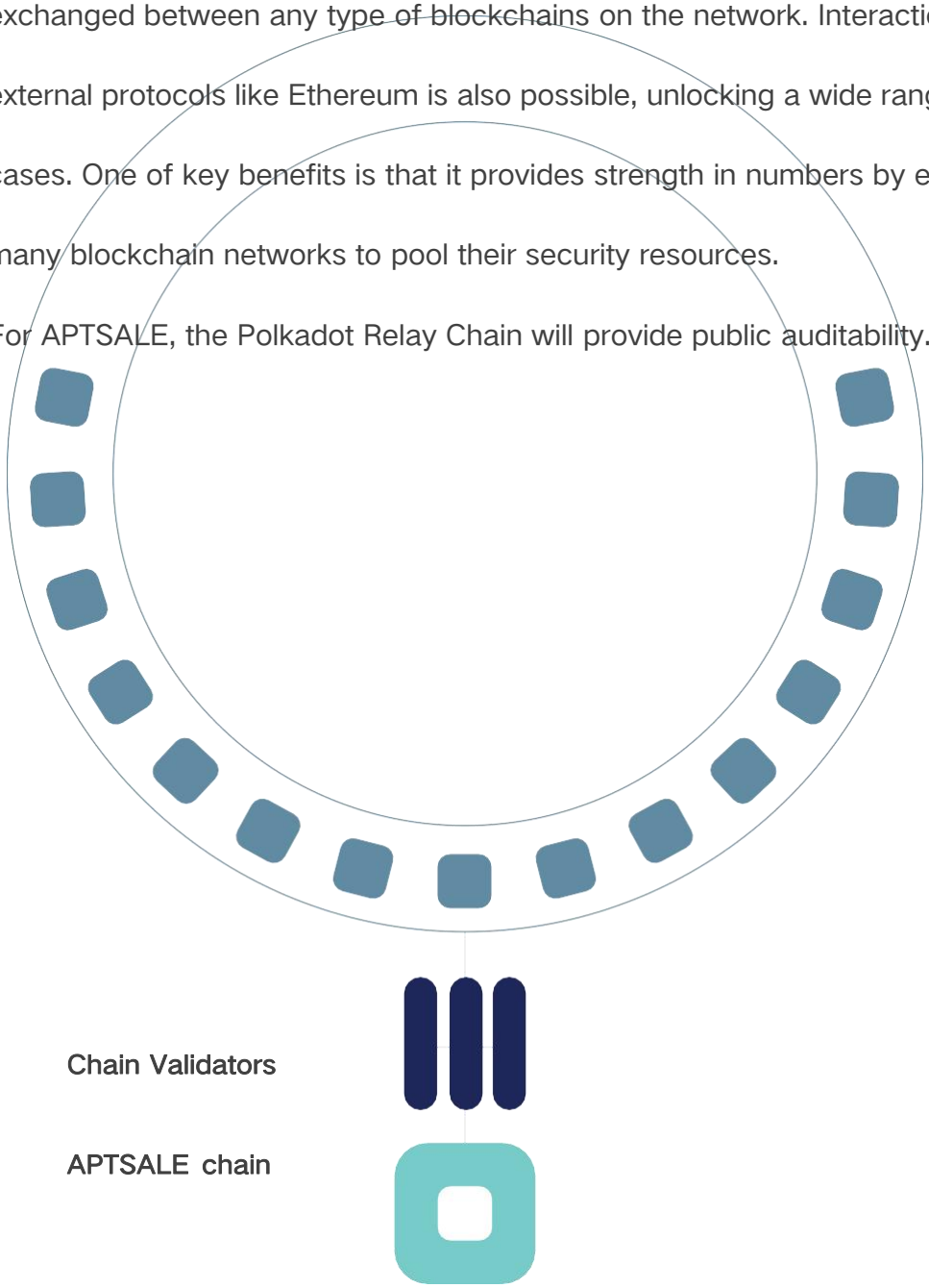


Figure 2: The APTOS Chain and APTSALE Chain.

The hardware:

Trusted execution environment

In order to trust that a remote party runs the agreed process in a genuine TEE, remote attestation using a digital signature from the TEE manufacturer is required. APTSALE will use its APTOS to verify remote attestation. This will provide all users with assurance that their data can only be processed in pre-agreed ways in an isolated and trustworthy hardware environment.

By combining the auditability of APTOS with the confidentiality and speed of TEEs, APTSALE delivers verifiable privacy at scale.

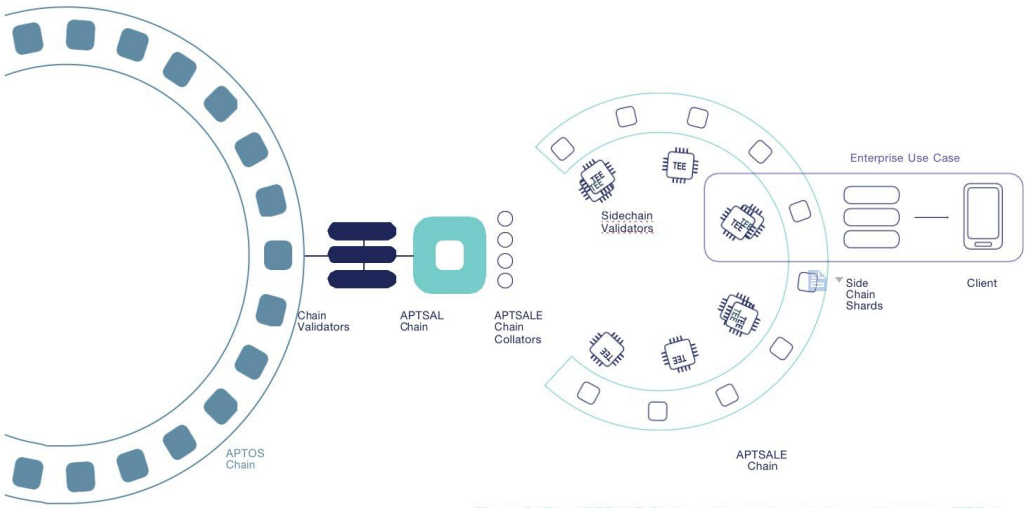


Figure 3: The APTSALE Chain and trusted execution environments (TEEs)

The software: Off-chain worker and sidechain validator templates

APTSALE offers an open-source framework with code templates for various scenarios. For use cases with a large number of rather simple state transitions where the ordering of invocations matters (like token transfers or smart contract

execution), a third party can develop. their own sidechain where state transitions are directly invoked without any interaction with the APTSALE chain. For use cases which focus on oracle or data storage services or a low number of high-complexity computations, developers should implement their own off-chain workers where every execution.

5.2 APTSALE Off-chain Workers

Off-chain workers (OCW) are not to be confused with Parity Substrate off-chain workers. They execute a custom state transition function or oracle service. State transitions are triggered through on-chain extrinsics with encrypted payloads (indirect invocation).

Indirect invocation: With indirect invocation, a requester calls (1) a confidential dispatchable function (state transition) by signing a trusted call and encrypting it with the worker-enclave’s shielding key. She then wraps the cyphertext into an extrinsic which she sends to the chain.

The worker forwards all new blocks to the light client (2) within the worker-enclave where the cyphertext gets decrypted and the trusted call is executed (3) on encrypted state. The call is then confirmed on the parachain (4). The user can query (5) their own state directly at the OCW enclave subject to

authentication.

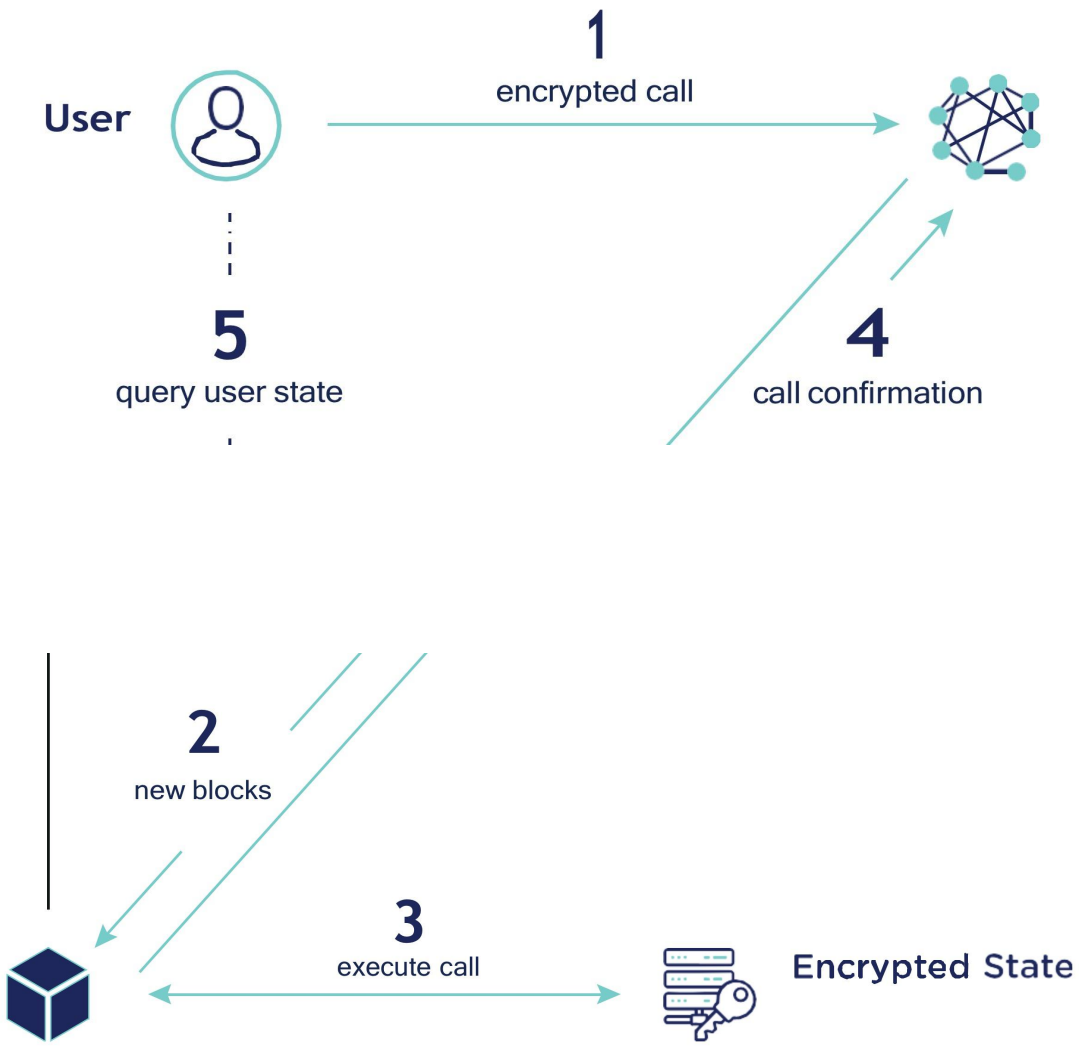


Figure 4: Indirect Invocation

5.3 APTSALE Chains

When using indirect invocation, all trusted calls need to pass through the chain. Thus, it is not a very scalable solution. While it would be preferable to interface with enclaves di-rectly, this gives rise to the problem of transaction ordering consensus. This is why a second-layer solution is needed.

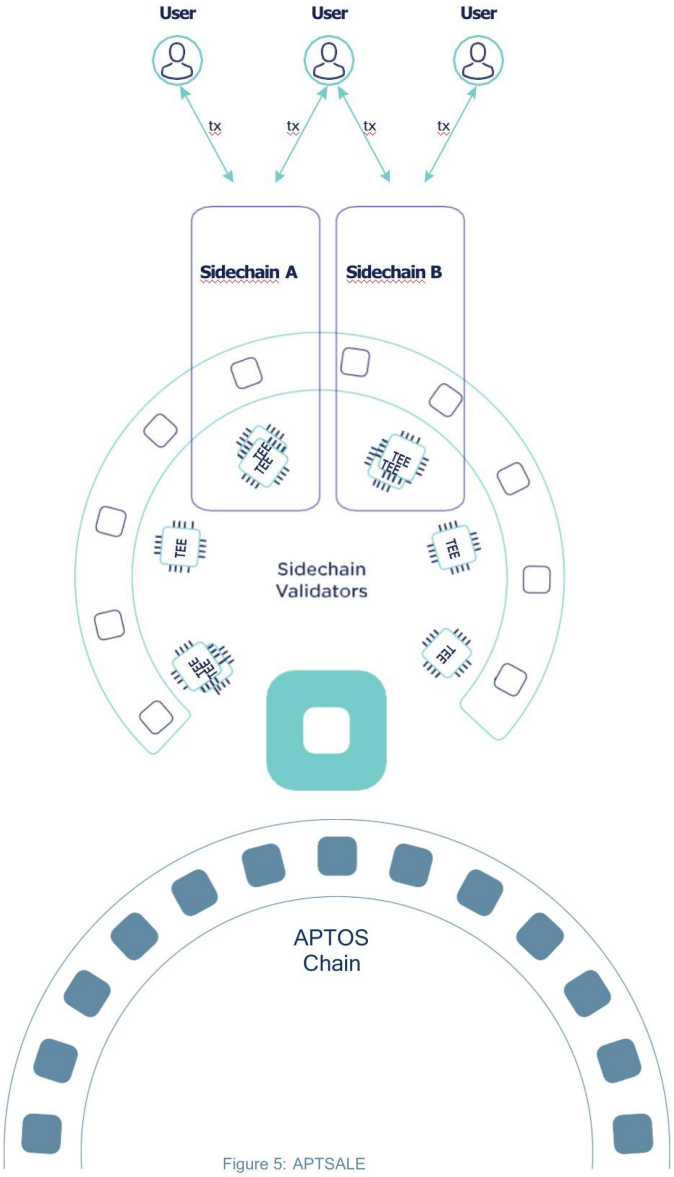


Figure 5: APTSALE

Develop TEE-validated Chains

The APTSALE SDK empowers you to develop TEE-validated sidechains with subsecond blocktimes. Because sidechain validators are running in TEE, all validators trust each other, greatly reducing the complexity of the consensus protocol.

Direct invocation

With direct invocation, a requester chooses one of the sidechain validators to which to send her trusted call. The next time that validator produces a block, that call will be executed. The block gets committed onto the APTSALE Chain and the state diff is broadcast to the other validators, who simply apply the diff to their copy of the state.

Finality Sidechain blocks are produced asynchronously to layer one at a higher block rate. Despite the TEE’ integrity guarantees, these blocks are not final because forks on the sidechain can still happen. Every sidechain block hash is anchored to the layer one blockchain and gets finalized on layer one with the block that includes its anchoring extrinsic.

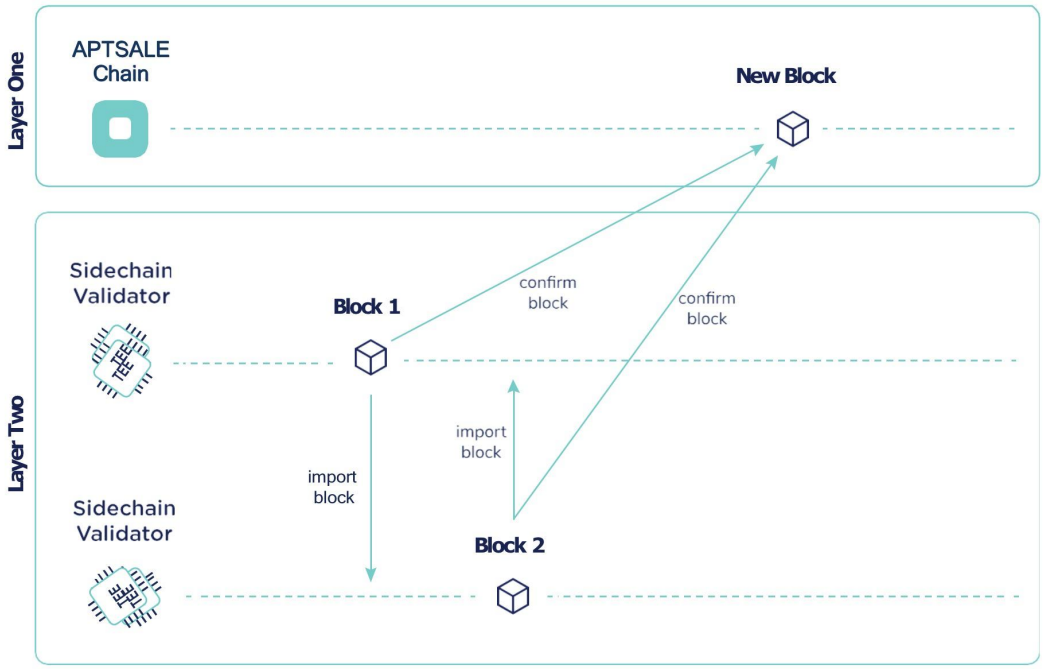


Figure 6: Direct Invocation

5.4 Substrate Runtime Compatibility

Have you already developed Substrate pallets for your (para-)chain but now you would like to add confidentiality and scalability? The APTSALE SDK is compatible with Substrate runtime pallets. With a few lines of glue-code you can re-use your pallets and instantiate them inside an APTSALE offchain worker or sidechain. It is even possible to trustlessly interact between onand offchain runtimes.

5.5 Sharding

APTSALE isolates confidential state from the blockchain by maintaining it off-chain and processing it in TEEs. This strategy allows application-specific sharding. Every use case can work on its own shard and even one use case could be divided over several shards. Sharding can be used with off-chain workers (OCS) and sidechain validators (SCV).

5.6 Deployment Options

Unpermissioned operation

Even if we trust the TEE manufacturer’ s ability and integrity, a decentralized application (dApp) should be operated by an unpermissioned set of infrastructure providers. APTSALE enables you to allow unpermissioned

operation of your off-chain workers or sidechain validators, while still ensuring integrity and confidentiality through remote attestation. It is important to note, however, that allowing unpermissioned operation opens more attack vectors, as untrusted operators have physical access to the hardware.

Permissioned operation

You may choose to operate all TEE hardware yourself or rent it through a service-level agreement in a jurisdiction of your choice. It is up to you to define who may validate your sidechain or run your off-chain workers. In any case, the APTSALE Chain provides a remote attestation registry for public auditability of your services.

5.7 Remote attestation

Remote attestation is the process of asking the TEE manufacturer to authenticate a TEE. The manufacturer signs a report to confirm that both the TEE itself, and the hash of the binary it is executing, are genuine. Such a report also includes the TEE’s public signing key. By veri-fying this signature, the user can rest assured that they are communicating with the correct TEE. APTSALE simplifies this process for users by storing remote attestations on-chain. This avoids the need for users to obtain a license for the manufacturer’s attestation services.

6. TEER Token Economics

The Aptsale blockchain will be owned, operated, and governed by a broad and diverse community. A native Apts token will be used for transaction and network fees, governance voting on protocol upgrades and on-chain/off-chain processes, and securing the blockchain via a proof-of-stake model. A complete description of Apts token economics will follow in a future publication.

6.1 Token Distribution

Given the growing consumer and regulatory pressure for data services that protect user privacy, APTSALE’s powerful hybrid of Apts and blockchain is ideally positioned. Firms intending to use APTSALE network need to acquire the token, either on the open market or through an intermediary who creates barrier-free access by accepting fiat payments and paying the Chain fees on their behalf. This automatically caters to a broader market of potential adopters and creates a direct re-lationship between the value of APTSALE’s Network and demand for the token.From a technical perspective, the APTSALE Chain ecosystem will need collators, off-chain workers and sidechain validators.

Collators produce Chain blocks and send them together with a proof-of-validity (PoV) to Relay Chain validators for validation and finalization.

Off-chain workers (OCWs) run a Apts to perform tasks with confidentiality and/or integrity, such as oracle services, operations on encrypted storage, and bridges to other blockchains.

Sidechain validators (SCVs) operate second-layer sidechains. Block production and validation happen in Apts. Therefore, the validators can trust each other and the consensus protocol is greatly simplified.

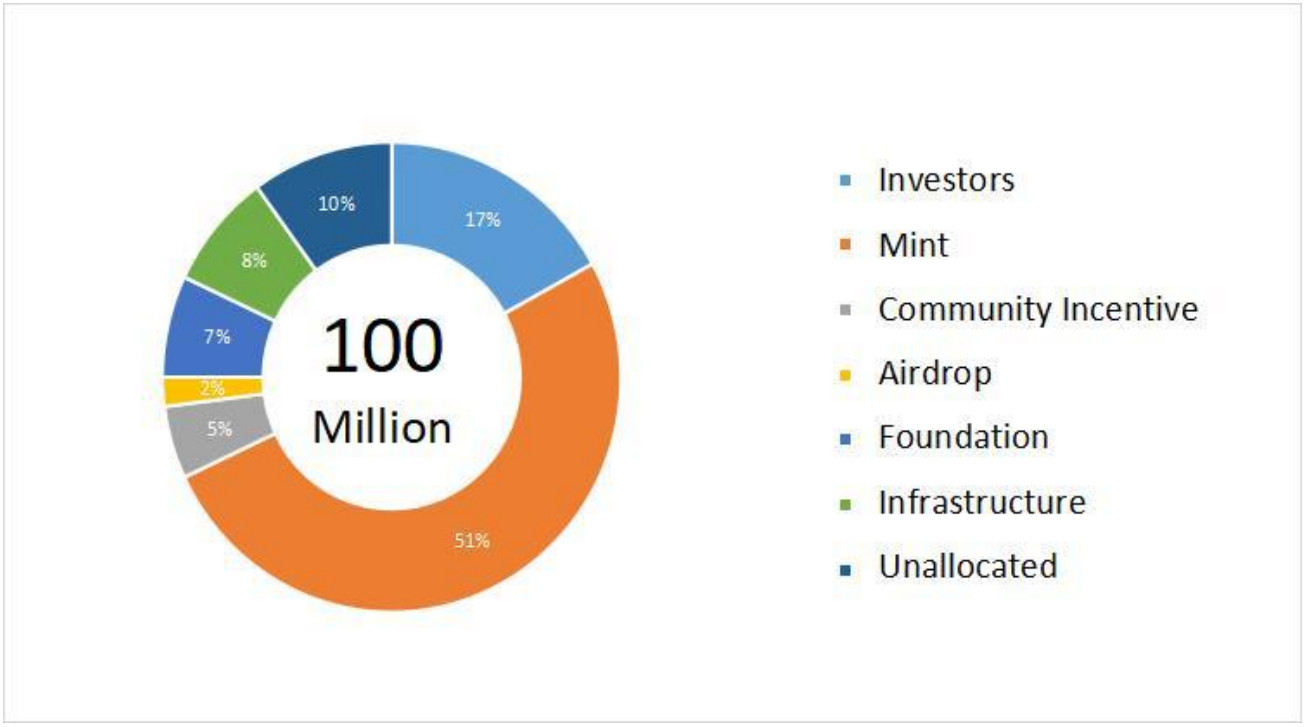
BURNING FUNCTION

APTSALE will implement a revenue burning function which burns a fraction of each fee paid to the treasury. This implies that the overall Apts token supply is deflationary, leading to an increase in the price of the Apts token as its supply decreases.

LOCKDROPS FOR FEE DISCOUNTS

APTSALE offers off-chain workers (OCWs) and sidechain validators (SCVs) discounted fees if they lock Apts tokens. Lockdrops have become increasingly popular for spreading tokens to a wide range of entities, slowing down the token velocity of Apts and therefore further increasing its value as adoption rises.

APTSALE does not incentivize OCWs or SCVs because they are dApp-specific. It is up to the stakeholders of each dApp project that deploys on APTSALE to incentivize infrastructure providers. This gives projects deploying on APTSALE a great deal of independence. To drive the value of the Apts token beyond its intrinsic utility, APTSALE is deploying further proven mechanisms.



6.2 Blue Flame Skull NFT

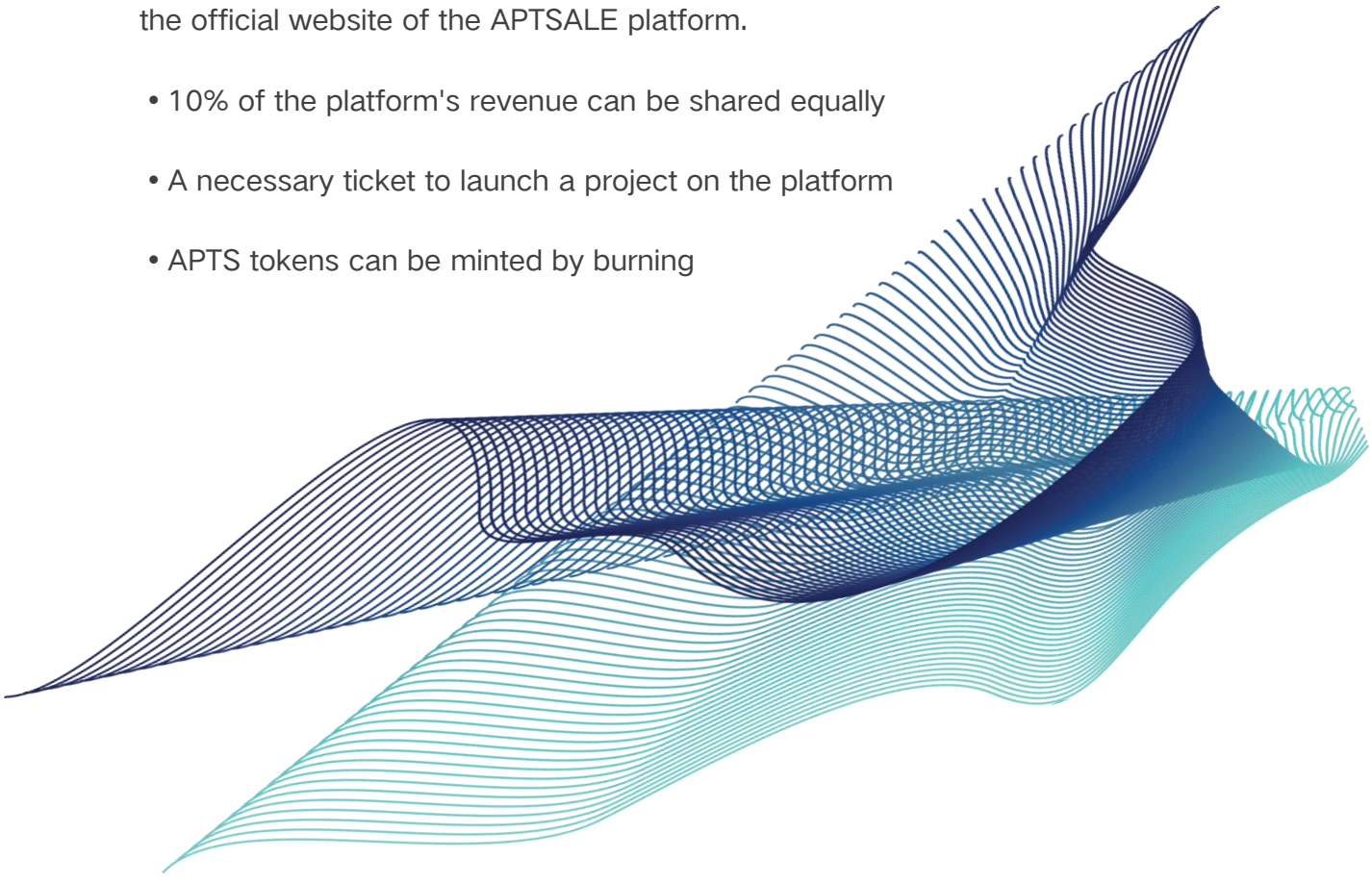
In the early stage, Blue Flame Skull NFT can only be obtained by participating in the official event airdrop. The obtained NFT is a primary NFT, which can be exchanged for advanced NFT through the website. Advanced NFT has the following three functions:

Dividend	Governance	Mint APTS
10% dividend	Community Governance	Destroy Burning
Profit and Dividend	Function Upgrade Management	Hold Appreciation
Other dividends	Ecological Governance	Participate in project voting

Blue Flame Skull NFT

The NFT on the APTSALE platform has important collection value. After the function upgrade of version 2.0, all users can publish their own NFT works on the platform with one click. The APTSALE platform has advanced NFT and primary NFT. All users can only obtain the primary NFT by participating in the official event airdrop, and then they can exchange it for the advanced NFT on the official website of the APTSALE platform.

- 10% of the platform's revenue can be shared equally
- A necessary ticket to launch a project on the platform
- APTS tokens can be minted by burning



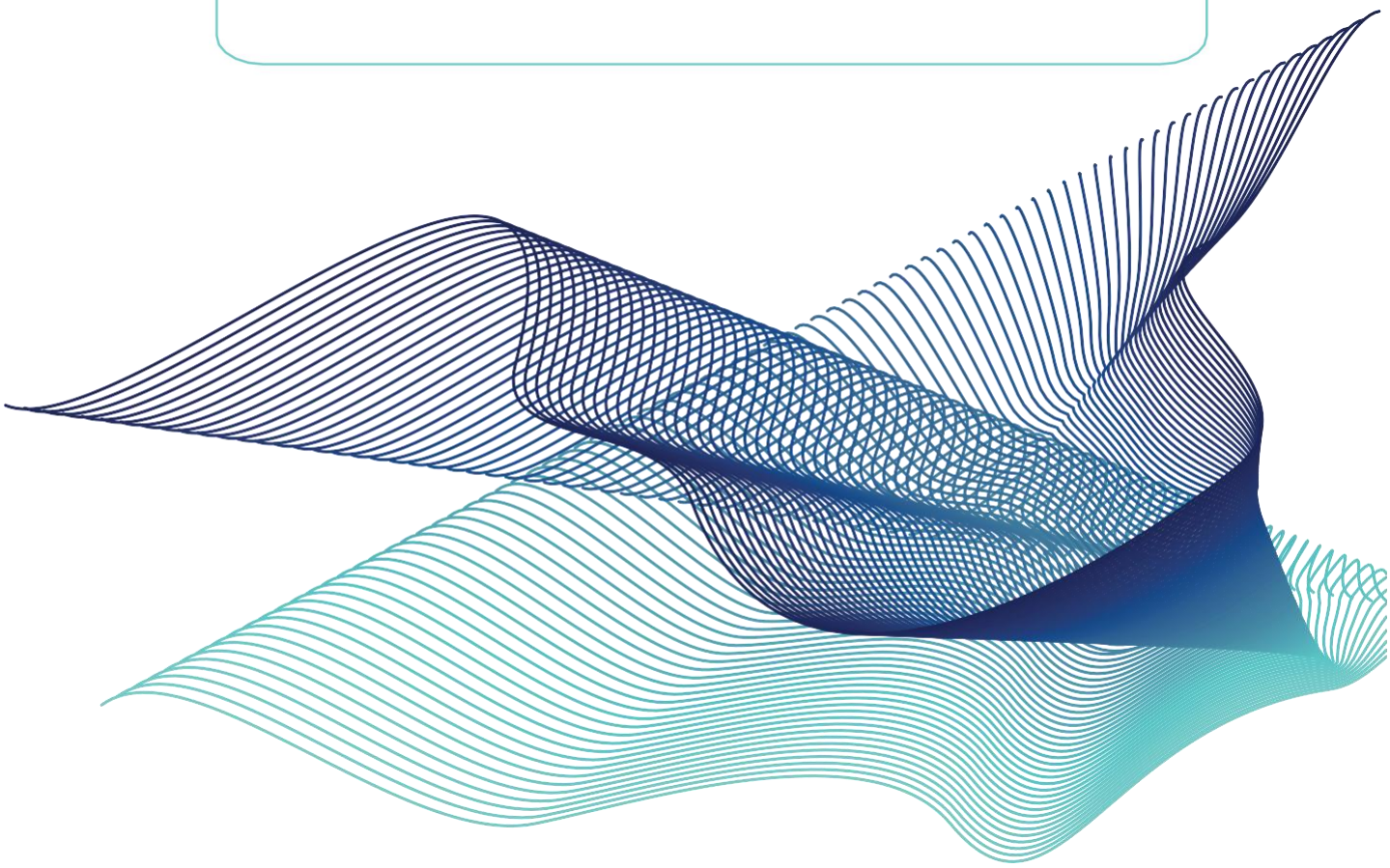
6.3 Launchpad

Decentralized Launchpad

APTSALE is a decentralized launchpad that allows users to launch their own token and NFT, users can create their own initial token and NFT sale. No coding knowledge is required, just simply navigate through to our terminal and design your own token and NFT in just a few clicks.

SWAP

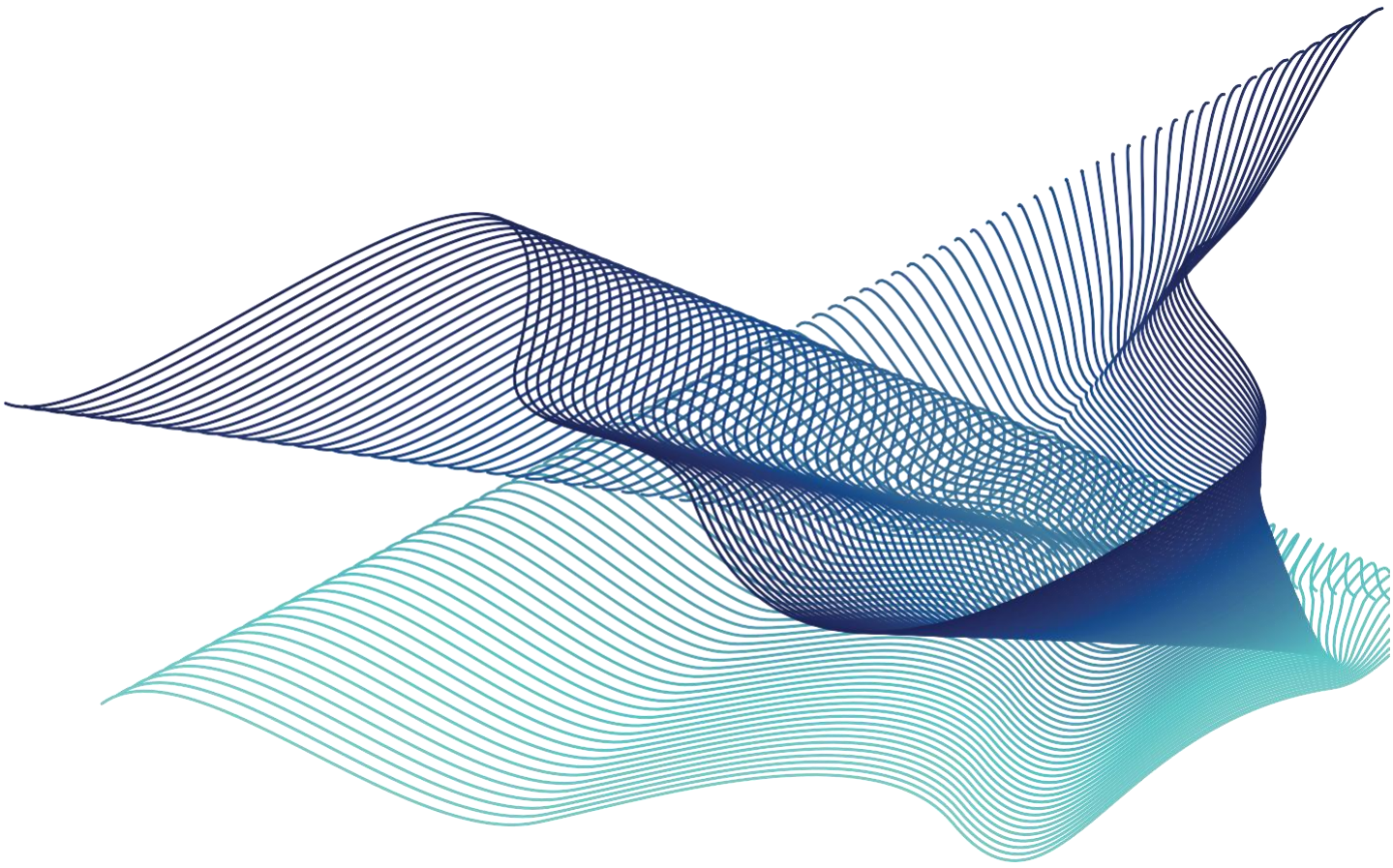
The decentralized currency issuance platform can help users quickly raise IDO funds for projects, and then launch NFT cards, and tokens can be traded on the Swap decentralized platform.



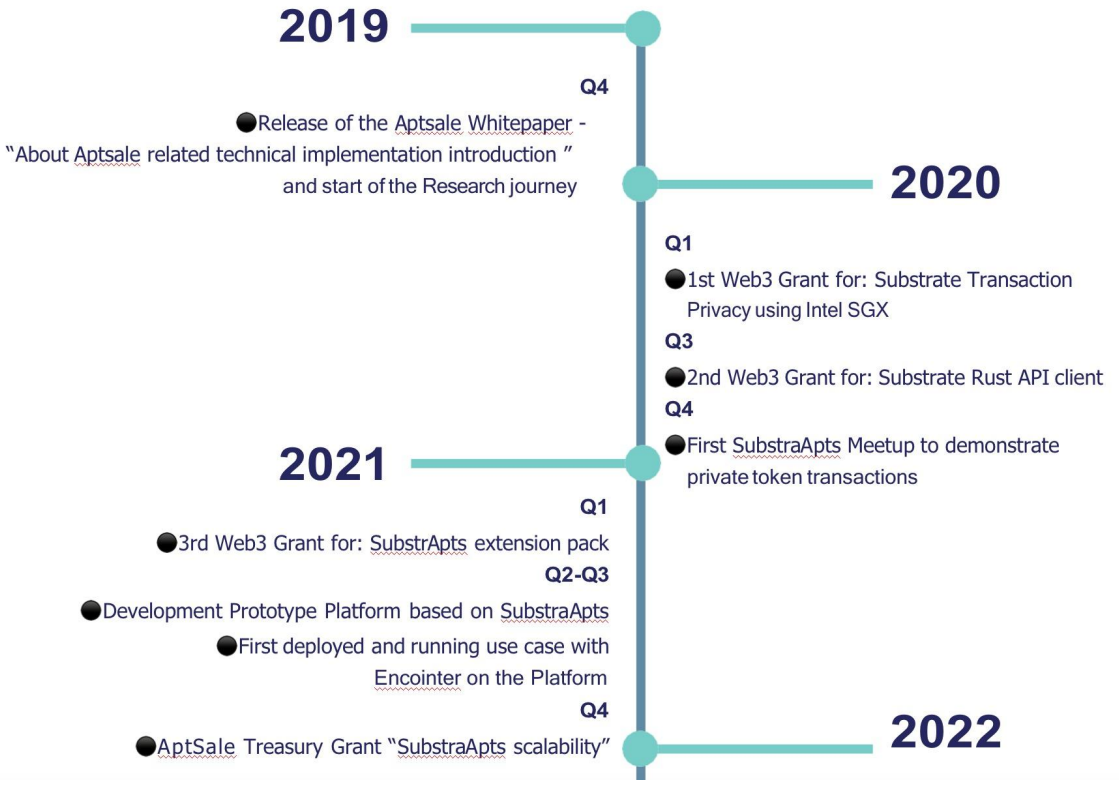
7. Use Cases

7.1 General Fields of Application

Our technology can be deployed in a wide range of industries for a broad set of use cases. From healthcare and decentralized finance to supply chain management, processing sensitive data is sometimes simply unavoidable. In any situation where multiple parties need to process potentially sensitive data, whether that is a B2B or B2C interaction, APTSALE provides a trusted technical foundation. There are far too many potential applications to list, but here are three possibilities:



8. Roadmap



2023 onwards

THE PATH TO ADOPTION

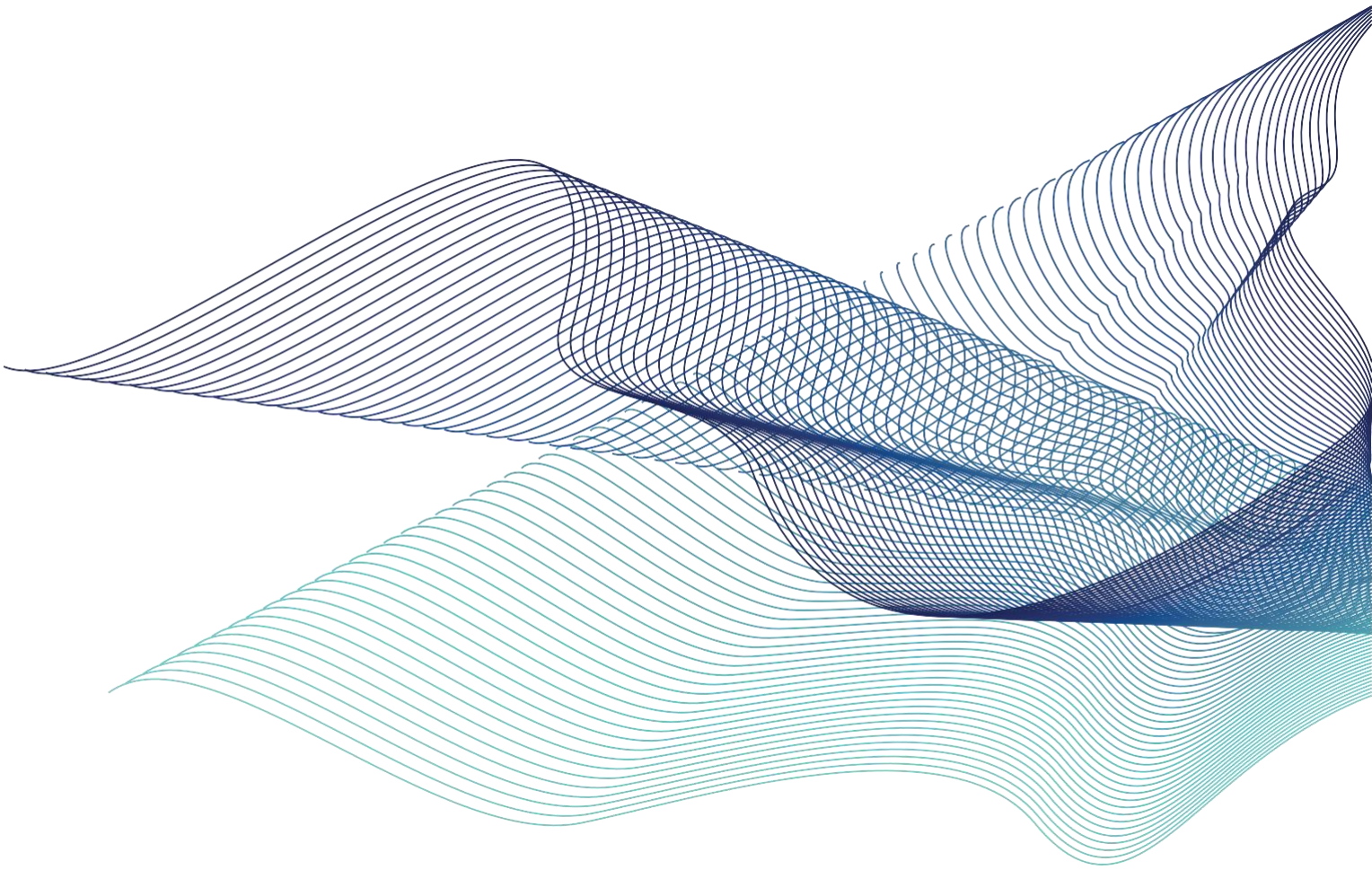
- Decentralize and establish the Governance Council
- First PoCs with enterprises
- Run a multi environment Apts token
- Establish a healthy token economy
- Establish a international footprint via partnerships and cooperate with institutions and universities
- Implementation of burning and lockdrop mechanisms
- Growth of community with events and treasury grants for enhancements

Q1
- Aptsale test-net Chain
- Conceptualize and preparation of spin-off

Q2
- Spin-off from SCS and birth of APTSALE AG
- NFT function development

Q3
- New brand and website relaunch
- Apts from Substra to APTSALE
- Release Whitepaper and tokenomics

Q4
- Officially launched the one-click coin issuance function and NFT card
- Preparing for go-live planning work
- SWAP function development and testing



APTSALE

APSALE.IO | t.me/APTS_EN | discord.gg/sDYABadMjg | @Aptoslabsale