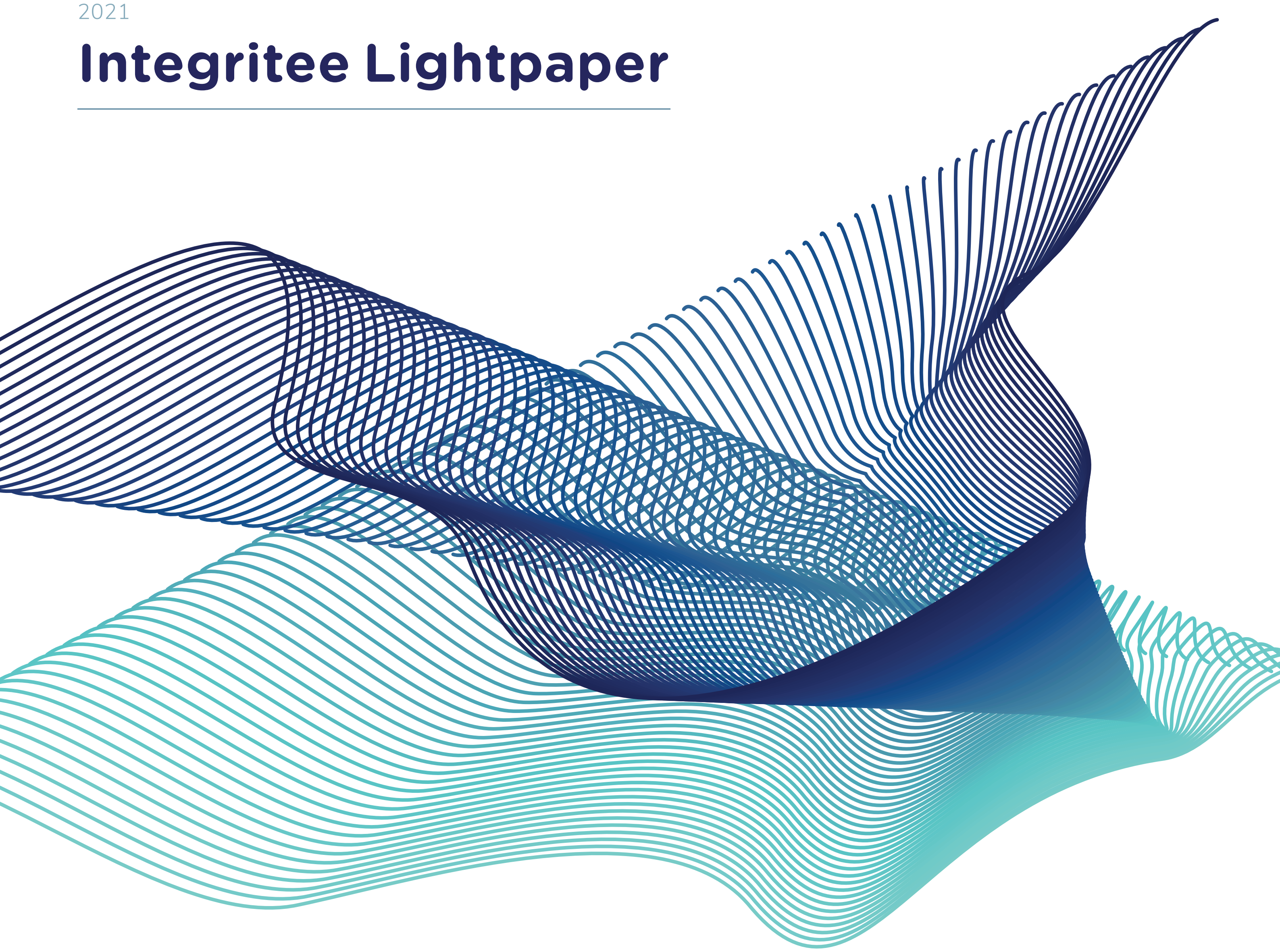
2021

Integritee Lightpaper

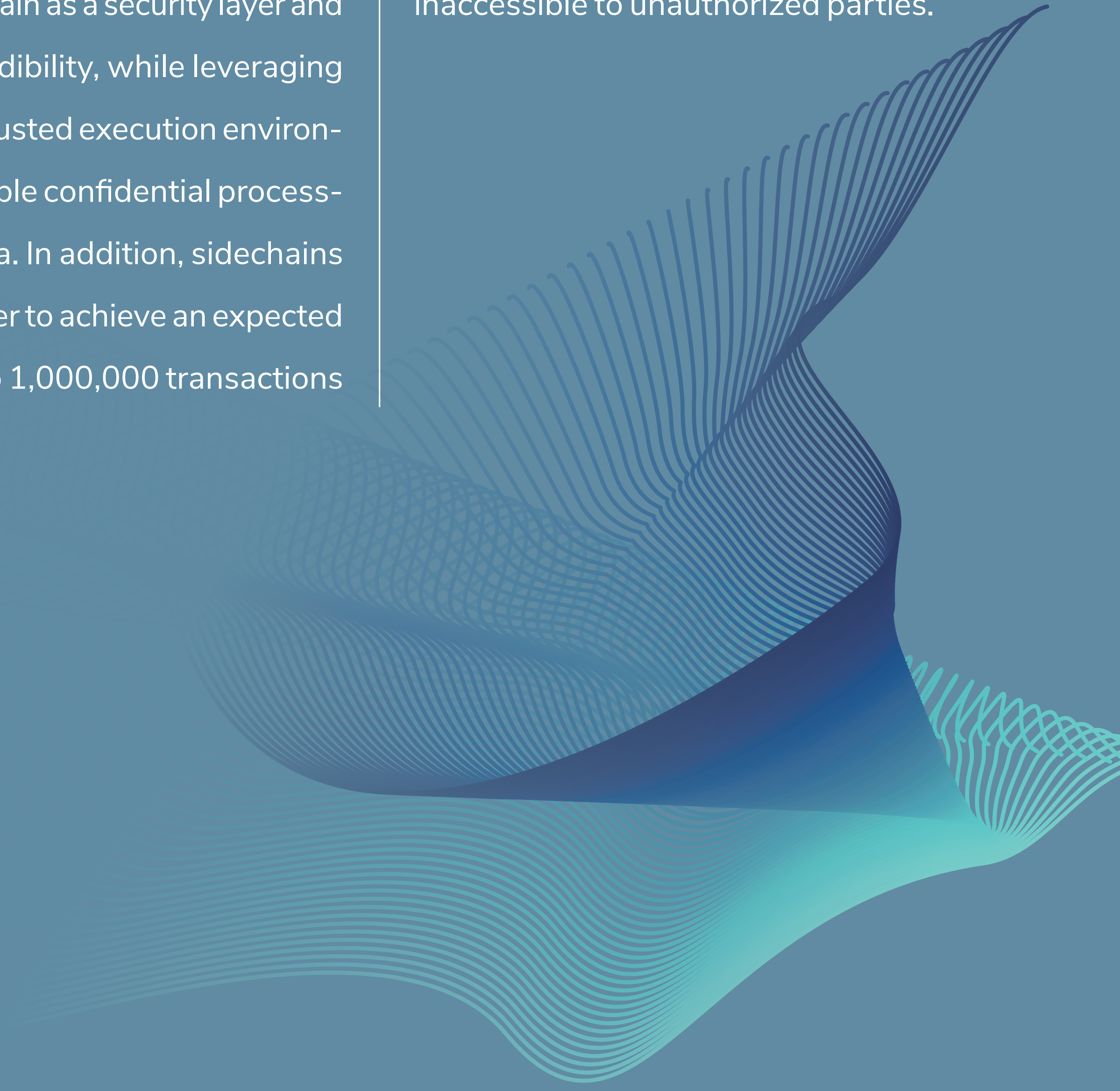


INTEGRITEE

Integritee AG | Technoparkstrasse 1 | CH-8005 Zurich | hello@integritee.network | integritee.network

Abstract

The Integritee network is a second-layer solution built on a parachain on Polkadot's Substrate blockchain framework. Integritee aims to solve the three main challenges facing most blockchain solutions to date — namely scalability, interoperability, and confidentiality. To achieve this, Integritee uses Polkadot's Relay Chain as a security layer and to ensure public audibility, while leveraging hardware-based trusted execution environments (TEE) to enable confidential processing of sensitive data. In addition, sidechains are deployed in order to achieve an expected throughput of up to 1,000,000 transactions per second. These technical achievements combined open the door to a new era of applications focused on confidentiality. Integritee can be deployed wherever sensitive information needs to be securely processed while providing verifiable proof that the underlying raw data remains confidential and inaccessible to unauthorized parties.



GO STRAIGHT TO

Table of Contents

1. INTRODUCTION 4

2. TODAY'S CHALLENGES 6

2.1. IT Security

2.2. Technology

2.3. Regulation on Data Protection

2.4. Customer Trust

3. THE SOLUTION 12

3.1. Forging A Real Blockchain Ecosystem

3.2. What We Do

3.3. How We Do It

3.4. The Value Proposition

4. THE POLKADOT BLOCKCHAIN ECOSYSTEM 15

4.1. Polkadot's Blockchain Concept

4.2. Parachains

5. THE INTEGRITEE NETWORK 17

5.1. Introduction

5.2. Integritee Off-chain Workers

5.3. Integritee Sidechain

5.4. Substrate Runtime Compatibility

5.5. Sharding

5.6. Deployment Options

5.7. Remote Attestation

6. TEER TOKEN ECONOMICS 24

6.1. Token Quick Facts

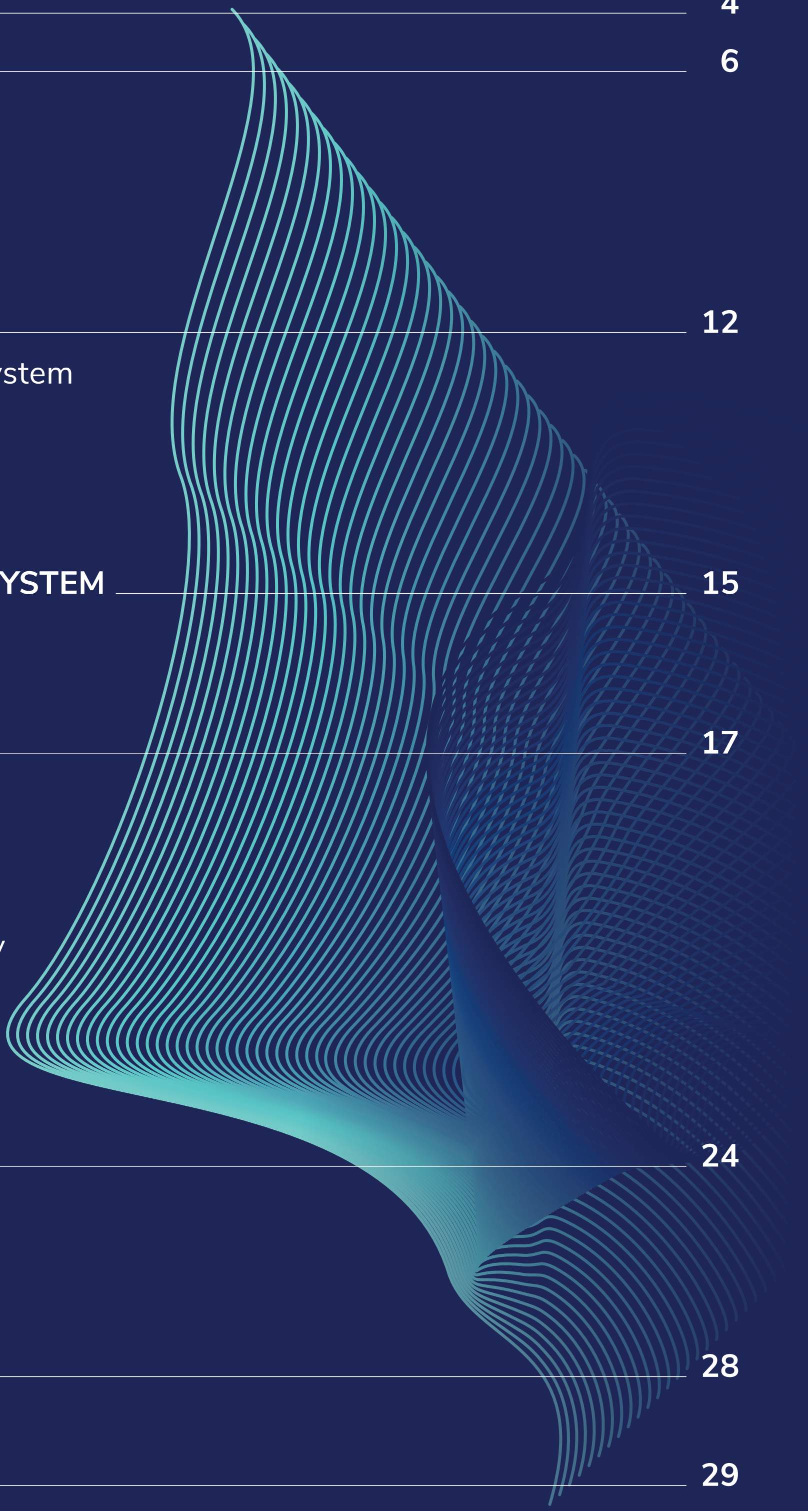
6.2. Token Use

6.3. Token Distribution

7. USE CASES 28

7.1. General Fields of Application

8. ROADMAP 29



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 subsequently monetize that base by handing user data over to third parties.

By collecting huge amounts of sensitive data and storing it centrally, this trend has made cybercrime and cybertheft more lucrative and attractive. As a result, the number of cyberattacks has significantly increased, resulting in major leaks of sensitive user and business data. Billions of people and millions of businesses are affected by cybercrime. According to the 2019 Official Annual Cybercrime Report by Cybersecurity Ventures, cybercrime represents the single greatest threat to companies worldwide, and by extension, to individuals' personal data.

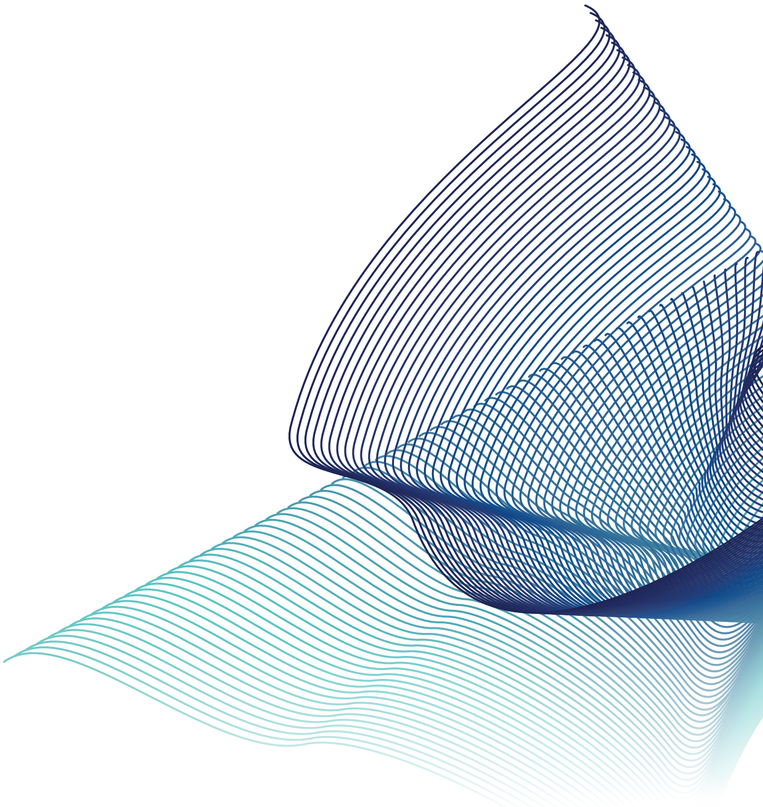
Cybercrime is predicted to inflict damages totaling $6 trillion globally in 2021. If concentrated in one country, this would be the world’s third-largest economy after the US and China. Global spending on cybersecurity products and services is projected to exceed

$1 trillion cumulatively over the five-year period from 2017 to 2021.[1]

In the past few years, regulators have introduced new regulations governing how businesses can handle sensitive user data. The objective is to make firms implement new processes and technology to counteract both data misuse and data leaks. The General Data Protection Regulation (GDPR) enacted by the EU in 2018 requires organizations to safeguard personal data and uphold the privacy rights of everyone within EU territory. Organizations found to be in breach of these regulations can be fined up to €20 million or 4% of their global annual revenue, whichever is higher.[2]

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-knowledge 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.

Integritee provides a scalable, interoperable and confidential network layer that can be used by companies and developers to establish new, user-centric privacy solutions that leverage the combined benefits of blockchain and trusted execution environments (TEEs).



[1] Cybercrime To Cost The World $10.5 Trillion Annually By 2025.
[2] What are the GDPR Fines?

2. Today's Challenges

When it comes to cybersecurity, 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.

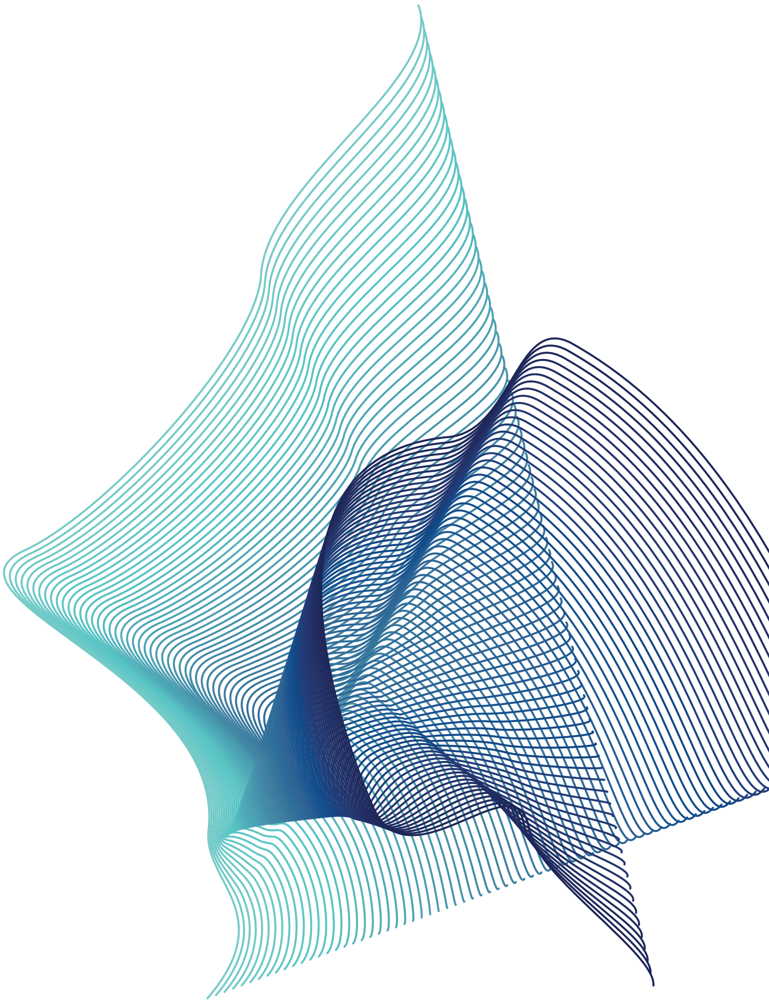
Data in transit, or data in motion, is data in the process of moving from one device to another, either across untrusted public networks, or within a private network. When data is moving, it poses some specific security risks, which need to be mitigated through targeted security measures. Conversely, 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.[3]

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 computation on cyphertext,

[3] Data Protection: Data In transit vs. Data At Rest.

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 (TEE) 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 IT service providers 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 data is used and managed, and whether the solution is scalable.

Whenever services are moved 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 move sensitive data to the cloud. Indeed, many companies remain wary of migrating parts of their infrastructure.

In the blockchain space, one approach to interfacing with sensitive 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.[4]

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:

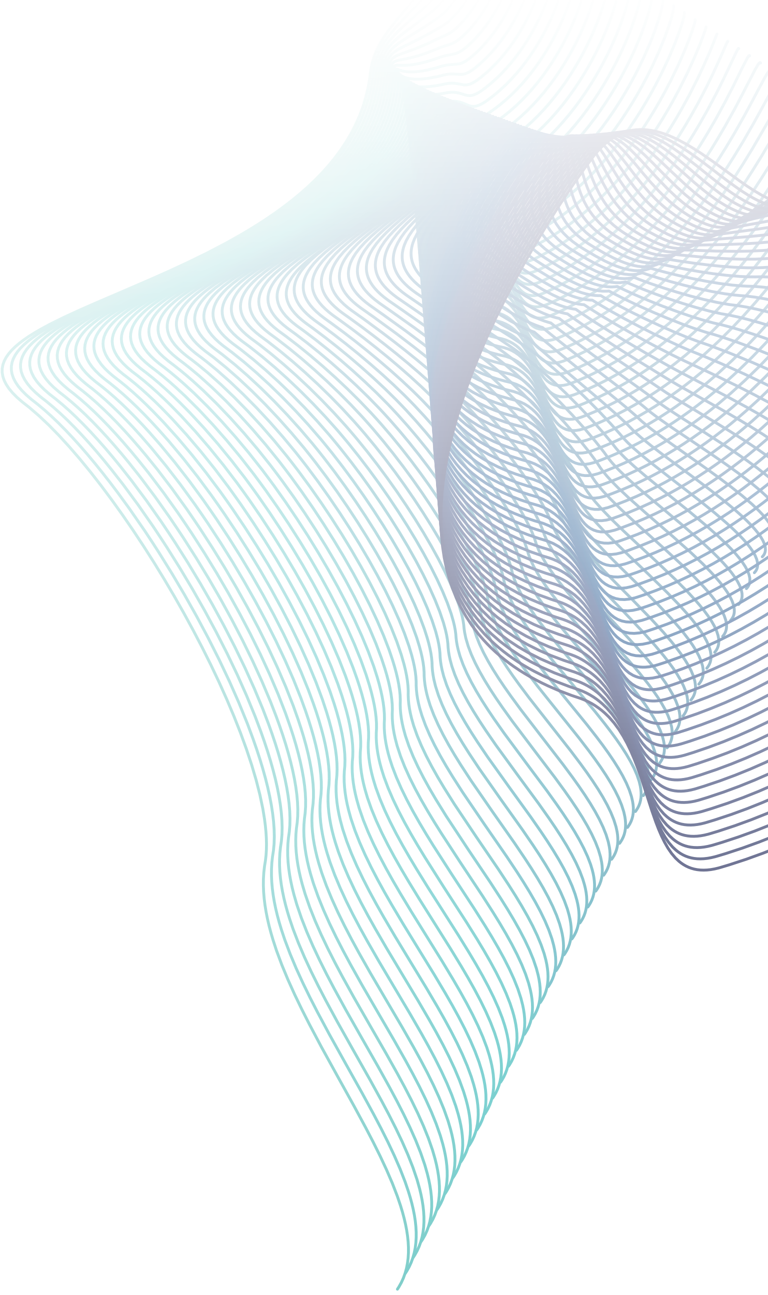
1. Secure Multiparty Computation (MPC):
MPC provides cryptographic methods for parties to compute data jointly, without it being revealed to any single one of those parties. Data is computed in a distributed manner, such that each party securely and privately handles different parts of the computation 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.

[4] Zero-knowledge proof.

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, TEEs 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, TEEs 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 Integritee'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 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.[5] Meanwhile, influenced by GDPR, Australian regulators have also proposed widespread changes to the Privacy Act 1988.[6] In the US, several states including Nevada, New York, Texas, and Washington are considering enacting data privacy regulations similar to those in California.[7]

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. [8, 9]

Why GDPR alone is not the solution:

The volume and size of fines issued to companies so far only amount to a drop in

[5] How the GDPR could change in 2020.

[6] House of Commons of Canada BILL C-11.

[7] This Privacy Awareness Week looks at possible reforms that could come out of the Privacy Act review.

[8] Facebook earmarks €302M for privacy fines.

[9] EU hits Amazon with record-breaking $887M GDPR fine over data misuse.

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

Cybercrime and large-scale data leaks from big platforms and even government services are becoming increasingly common. There has been an almost constant stream of big data leaks in recent years, with millions of users affected. Personal data is collected and sold in a multitude of ways and an individual's private details, behavior, and trends become easily accessible online. People are becoming increasingly privacy-conscious and are questioning their growing lack of data privacy and control. This leads to a social shift in the long term. For instance, the 2021 Edelman Trust Barometer revealed that trust in the tech sector is at an all-time low in 17 of the 27 markets surveyed, including the US, UK and China.[10] In 2019, Forbes stated that "Data Privacy Will Be The Most Important Issue in the Next Decade".[11]

One of the best recent examples of this phenomenon was provided by the reaction to changes to WhatsApp's privacy policy. The updated policy, which would allow the sharing of data with Facebook, led to millions of users signing up with competitors like Telegram and Signal.[12]

[10] Tech Loses Its Halo.

[11] Data Privacy Will Be The Most Important Issue In The Next Decade.

[12] Signal and Telegram downloads surge, passing Facebook chat tools.

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 without unpredictable 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

Integritee provides insights without access to sensitive 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 (TEE) is a highly secure, isolated area within a computer processor that is separated from the system's main operating system. It ensures that data is stored, processed, and protected in a secure environment. Integritee combines the confidentiality of TEEs with the trust of blockchain. This enables multiple firms to process data in pre-agreed ways, without having direct access to the underlying dataset.

PROTECT

Create applications that reap the benefits of consumer data, without compromising on privacy.

COLLABORATE

Collaborate on data, without ceding control of sensitive business information.

BUILD

Securely process sensitive data with an interoperable second-layer blockchain solution.

3.3. How We Do It

Existing centralized approaches to data-driven services tend to be fast and convenient, but involve big compromises in terms of user privacy and data security. Many blockchain solutions deliver increased trust and security but involve unacceptable trade-offs in performance.

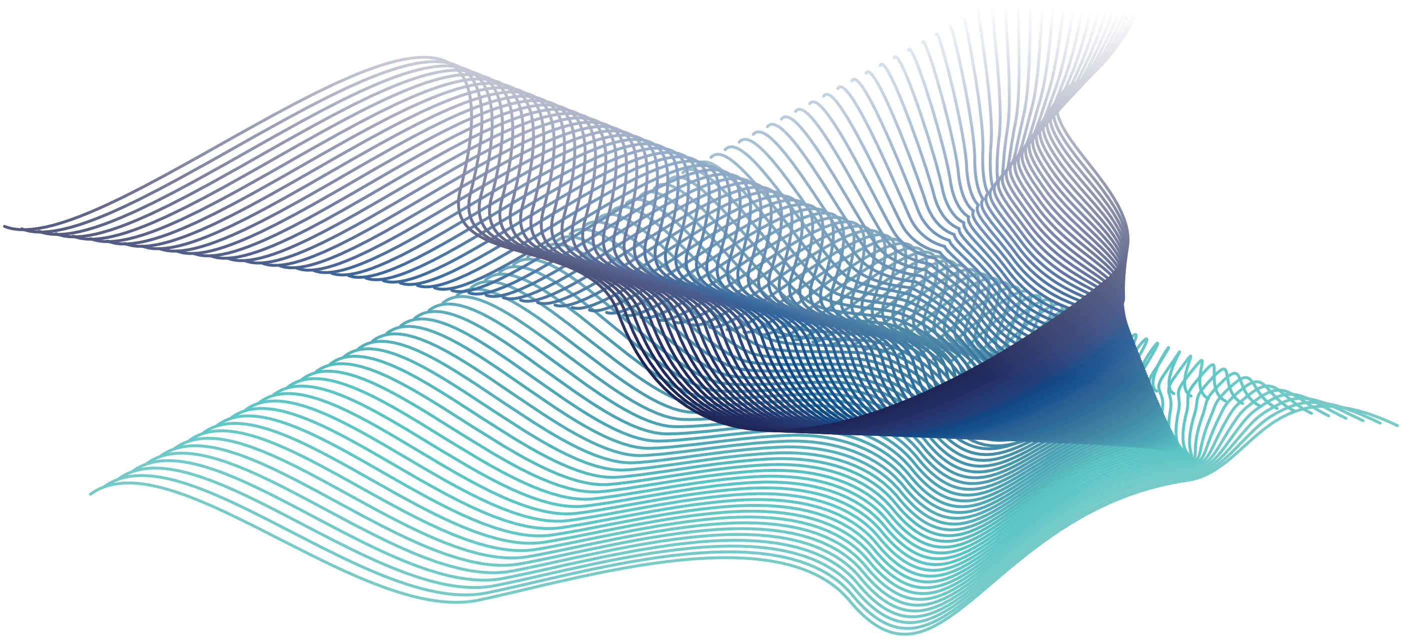
Integritee is poised to become one of the foundational parachains on Polkadot and Kusama, an interoperable ecosystem of blockchain-based networks. Through collaboration with third-party blockchain developers and enterprise clients, the Integritee parachain will serve as a versatile planting ground for a vibrant array of scalable, interoperable blockchain dApps, services, and platforms.

SMART & SAFE

By combining the security of Polkadot, the scalability of second-layer technology, and the speed and privacy of enterprise-grade trusted execution hardware, we provide the smartest and safest way to build data-driven dApps and services.

PRIVACY & PERFORMANCE

By separating attestation from computation, we let blockchain do what it does best, and modern hardware handle the rest. In this way, our solution combines the security and trust of blockchain with the speed and power of enterprise hardware.

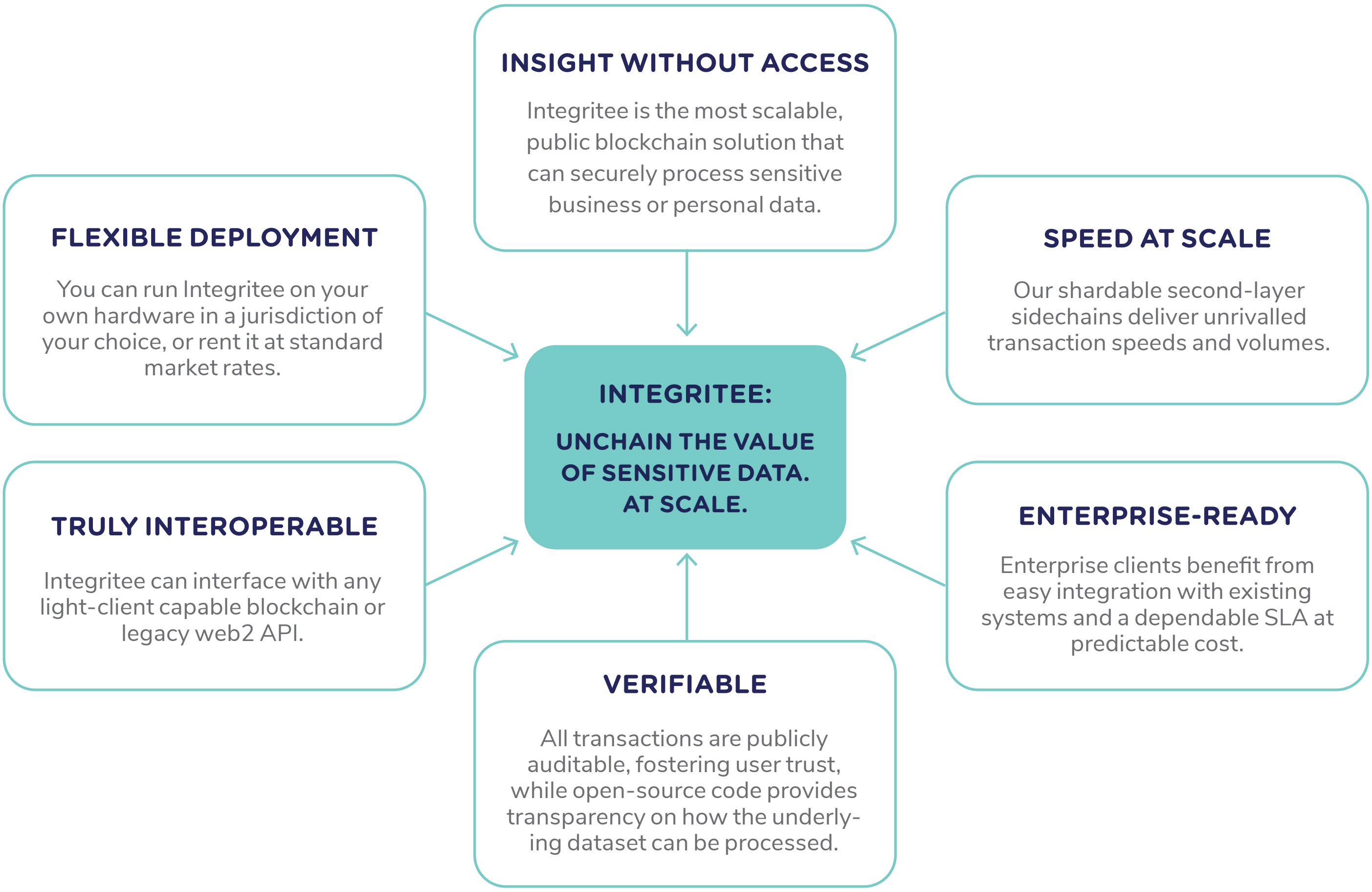


3.4. The Value Proposition

Through a powerful hybrid of the public blockchain and hardware-enabled confidential computing, Integritee provides insight without access to sensitive data.

All sensitive data is stored securely, separately, and encrypted. It can only be processed in an isolated, trusted execution environment that is accessible to no one, not even a system administrator with physical access to the device.

This enables multiple firms to query or process data in pre-agreed ways, without having direct access to the underlying dataset. Integritee is both smart and safe, unlocking all the benefits of data-driven platforms, in a secure, decentralized ecosystem.



INSIGHT WITHOUT ACCESS

Integritee is the most scalable, public blockchain solution that can securely process sensitive business or personal data.

FLEXIBLE DEPLOYMENT

You can run Integritee on your own hardware in a jurisdiction of your choice, or rent it at standard market rates.

SPEED AT SCALE

Our shardable second-layer sidechains deliver unrivalled transaction speeds and volumes.

INTEGRITEE:

UNCHAIN THE VALUE OF SENSITIVE DATA. AT SCALE.

TRULY INTEROPERABLE

Integritee can interface with any light-client capable blockchain or legacy web2 API.

ENTERPRISE-READY

Enterprise clients benefit from easy integration with existing systems and a dependable SLA at predictable cost.

VERIFIABLE

All transactions are publicly auditable, fostering user trust, while open-source code provides transparency on how the underlying dataset can be processed.

4. The Polkadot Blockchain Ecosystem

4.1. Polkadot's Blockchain Concept

Polkadot is not a standalone smart contract platform. Instead, it provides a heterogeneous, multi-chain network that connects a diverse array of different blockchains together. Polkadot is built on Substrate, a modular framework that facilitates the creation of purpose-built blockchains from both pre-built and customizable components. According to the Polkadot lightpaper, the network "connects several chains together in a single network, allowing them to process transactions in parallel and exchange data between chains with security guarantees."

In essence, this means that data in any format can move throughout all applications and chains on Polkadot, just like assets in the real world. Any existing blockchain can join Polkadot and benefit from the pooled security that it provides by aggregating validators.

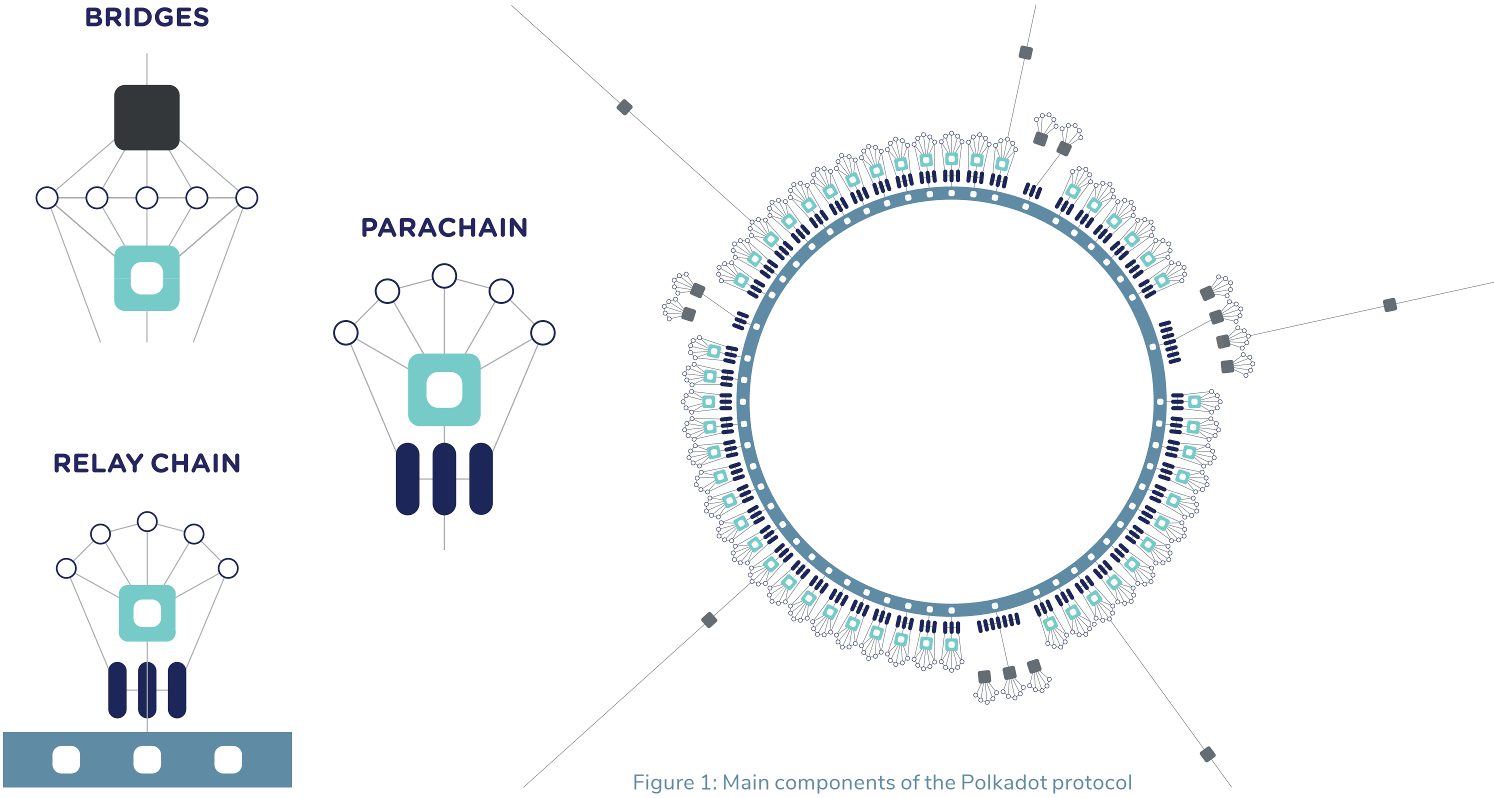


Figure 1: Main components of the Polkadot protocol

Polkadot leverages an architectural design known as heterogeneous sharding. Sharding operates on the principle of dividing up the overall workload that nodes need to handle into smaller, more manageable chunks. This means the network's transaction volume can be managed more efficiently through multiple "lanes" of traffic.

Just like with conventional sharding techniques, Polkadot's chains are interoperable with each other. However, heterogeneous sharding brings the added benefit that chains can be different to one another and thus optimized to fulfill specific requirements.

The core components of Polkadot are the Relay Chain, parachains and bridges. The Relay Chain provides pooled security and consensus for all network participants and interoperability among chains. Each parachain is essentially a heterogeneous blockchain shard that connects to the Relay Chain. Parachains can be tailored to specific use cases and can mint both their own native tokens and transfer tokens. Finally, bridges allow parachains to connect externally to other major blockchain networks, such as Ethereum or Bitcoin, for example. [13]

4.2. Parachains

As discussed above, the Relay Chain can be considered to be one of the key innovations of Polkadot — providing pooled security, consensus and cross-chain interoperability for a multi-(para)chain system. As they are heterogeneous, parachains can be considered to be individual blockchains in their own right, with specific features and native tokens. Due to the fact that parachains 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 parachains communicate with the same Relay Chain, they are mutually interoperable. Each Relay Chain is expected to be able to accommodate a finite number of parachains, however, with current projections placing that limit at around 100.[14]

[13] A Deep Dive Into Polkadot and How DOT Became a Top Ten Crypto Contender.

[14] Polkadot 101.

5. The Integritee Network

5.1. Introduction

The public blockchain: The Polkadot network

On Polkadot, 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 Polkadot's key benefits is that it provides strength in numbers by enabling many blockchain networks to pool their security resources.

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

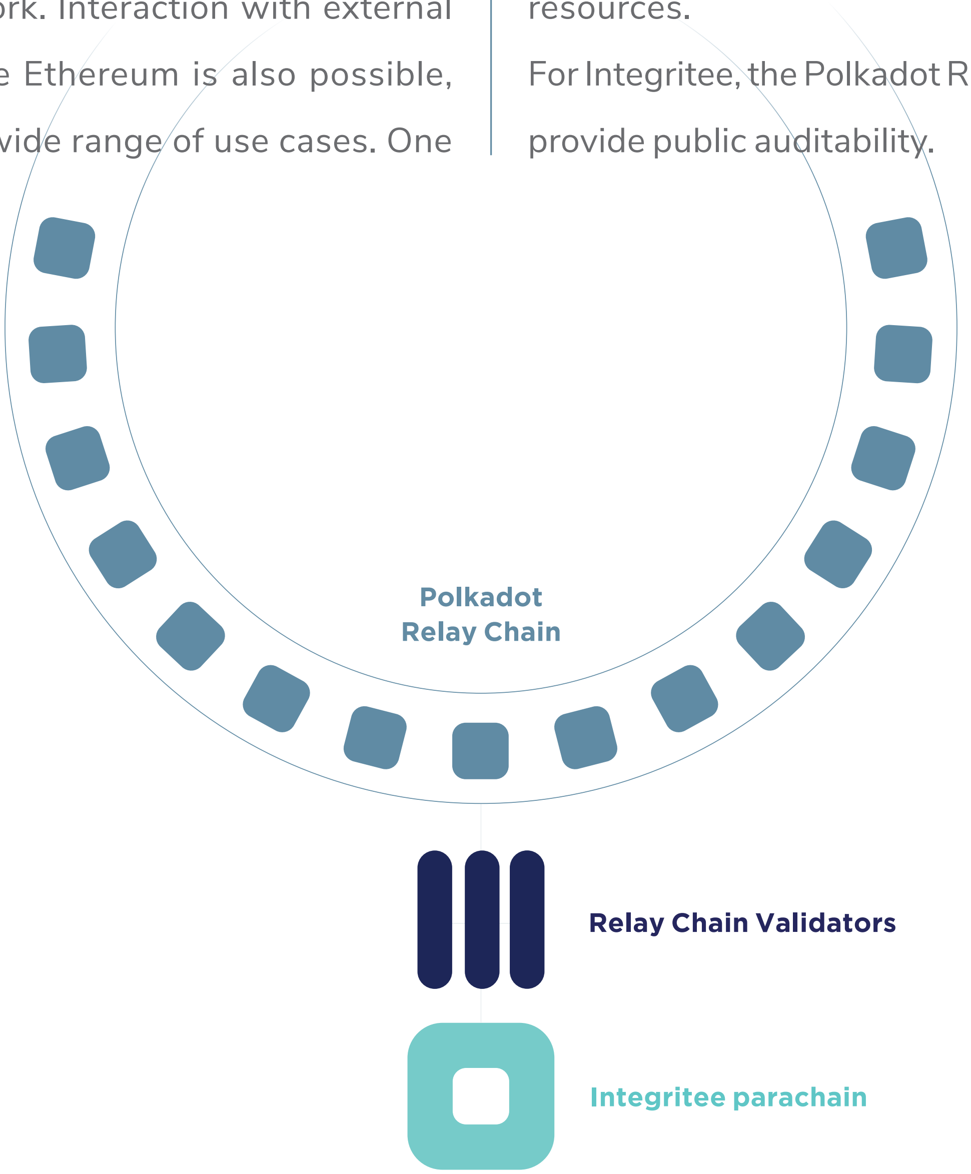


Figure 2: The Polkadot Relay Chain and Integritee parachain.

The hardware: Trusted execution environment (TEEs)

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. Integritee will use its Polkadot parachain 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 Polkadot with the confidentiality and speed of TEEs, Integritee delivers verifiable privacy at scale.

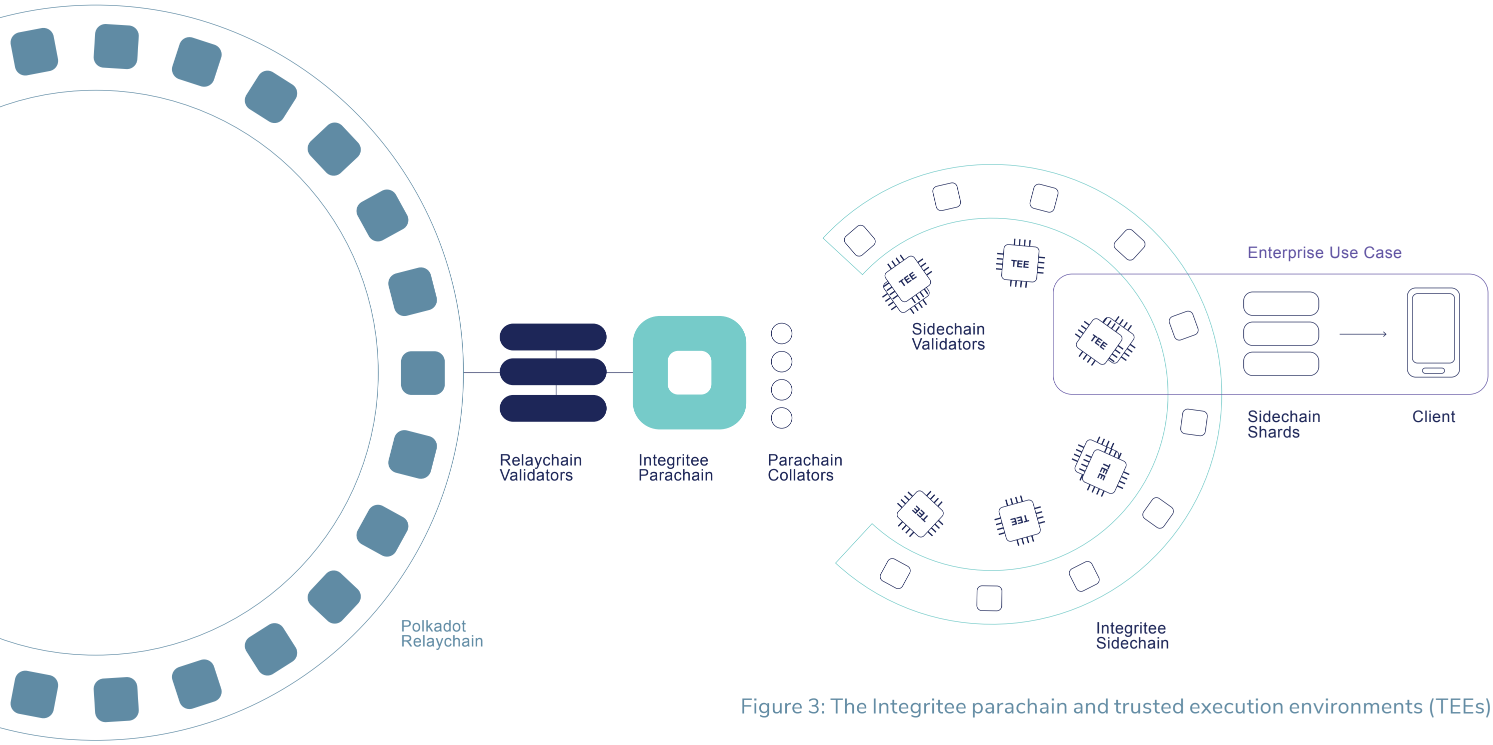


Figure 3: The Integritee parachain and trusted execution environments (TEEs)

The software: Off-chain worker and sidechain validator templates

Integritee 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 Integritee parachain. 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 is invoked indirectly via an extrinsic on the Integritee parachain.

5.2. Integritee 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 in a TEE. 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.

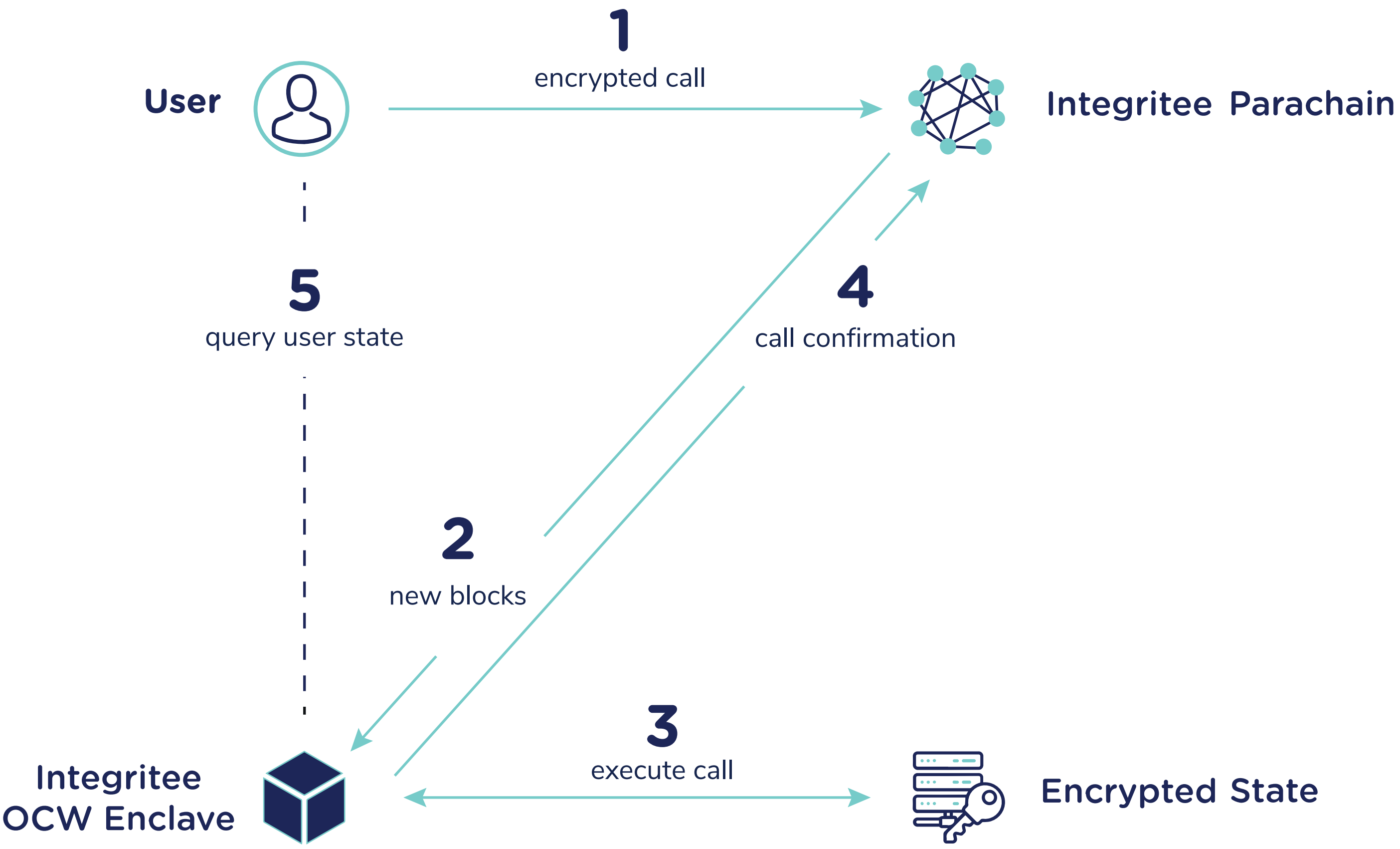


Figure 4: Indirect Invocation

5.3. Integritee Sidechains

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 directly, this gives rise to the problem of transaction ordering consensus. This is why a second-layer solution is needed.

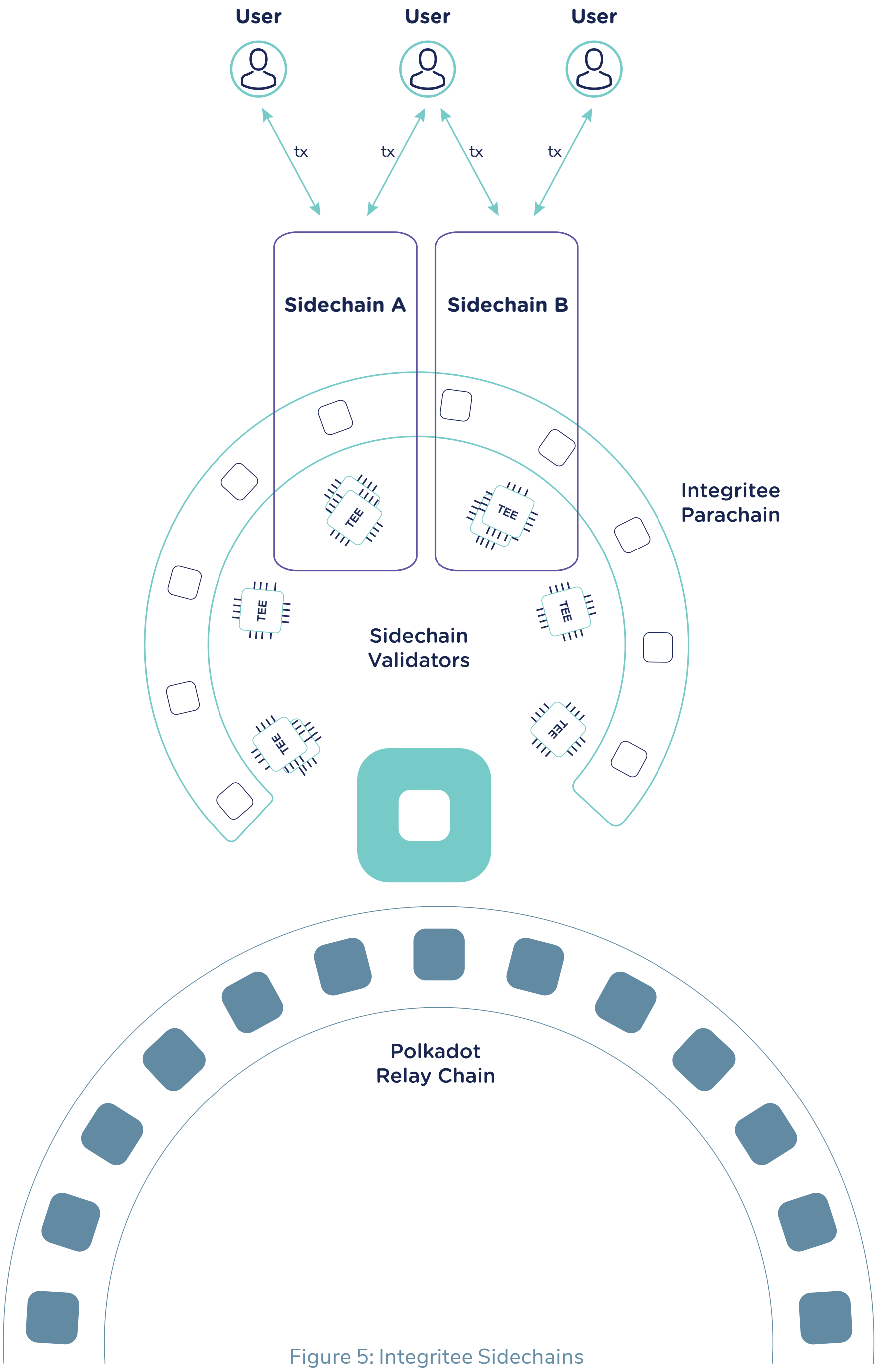


Figure 5: Integritee Sidechains

Develop TEE-validated sidechains

The Integritee SDK empowers you to develop TEE-validated sidechains with sub-second blocktimes. Because sidechain validators are running in TEEs, 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 Integritee parachain 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 TEEs' 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.

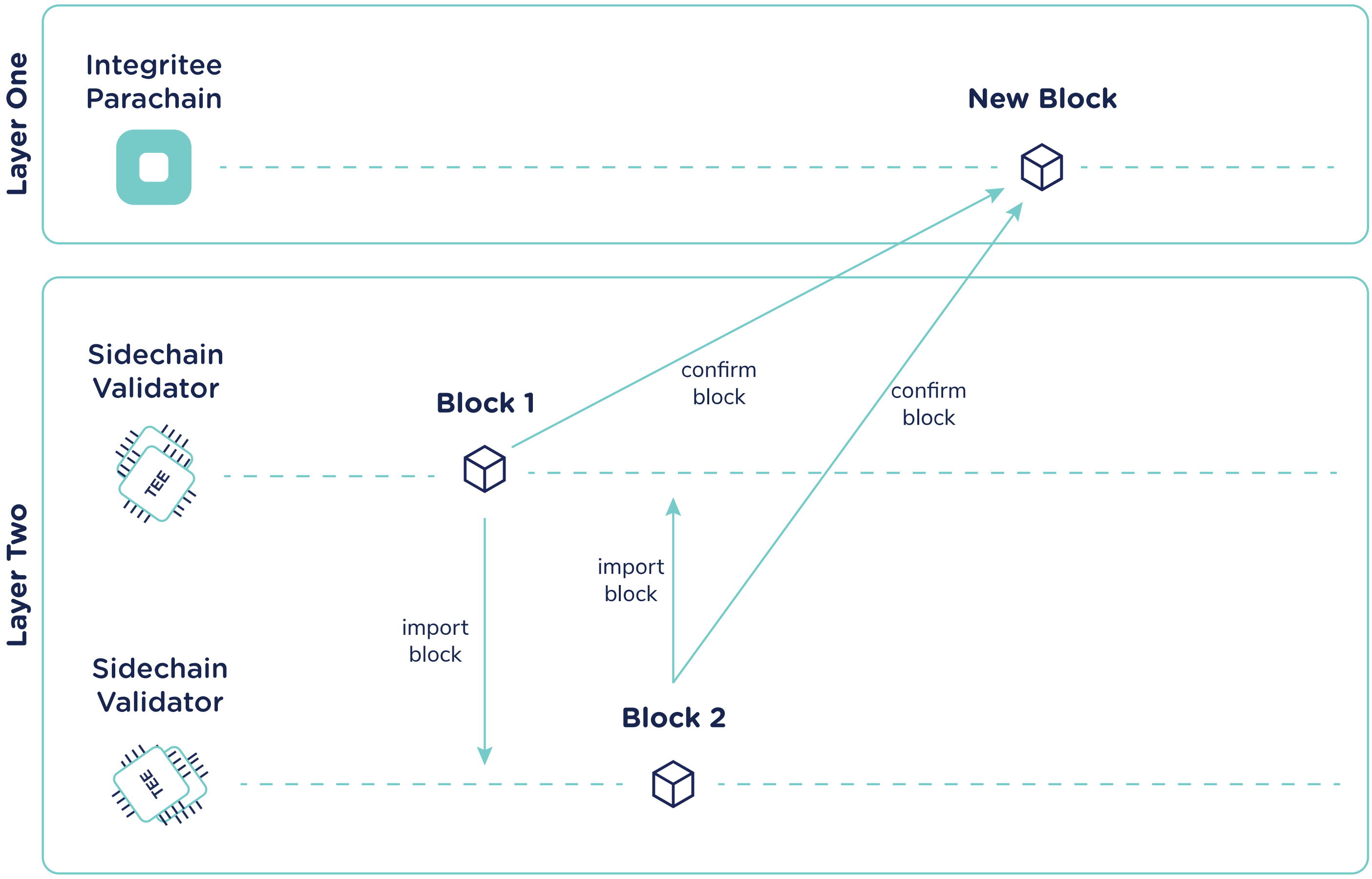


Figure 6: Direct Invocation

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 Integritee 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 Integritee off-chain worker or sidechain. It is even possible to trustlessly interact between on- and off-chain runtimes.

5.5. Sharding

Integritee 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

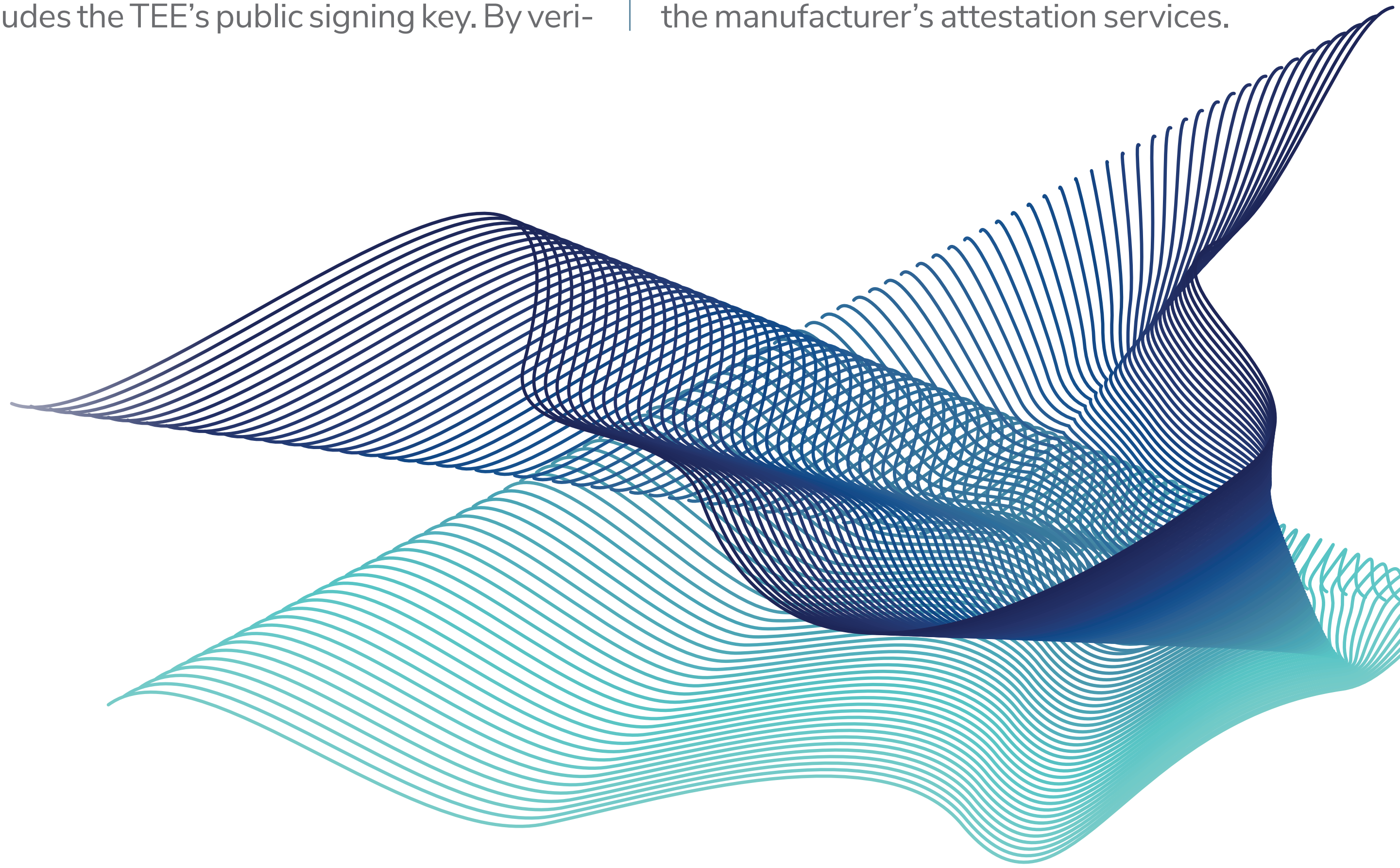
Even if we trust the TEE manufacturer's ability and integrity, a decentralized application (dApp) should be operated by an unpermissioned set of infrastructure providers. Integritee enables you to allow unpermissioned operation of your off-chain workers or sidechain validators, while still ensuring integrity and confidentiality through remote attestation. It is important to note, however, that allowing unpermissioned operation opens more attack vectors on SGX, 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 Integritee parachain 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 verifying this signature, the user can rest assured that they are communicating with the correct TEE. Integritee 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

6.1. Token Quick Facts

- ➔ Hard-cap token supply at genesis: 10M TEER
- ➔ Token nature: Utility and governance
- ➔ Token generation event (TGE): Planned in Q3 - Q4 2021

Find the Integritee token paper here.

6.2. Token Use

Given the growing consumer and regulatory pressure for data services that protect user privacy, Integritee's powerful hybrid of TEEs and blockchain is ideally positioned. Firms intending to use Integritee 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 parachain fees on their behalf. This automatically caters to a broader market of potential adopters and creates a direct relationship between the value of Integritee's Network and demand for the token.

From a technical perspective, the Integritee parachain ecosystem will need collators, off-chain workers and sidechain validators.

Collators produce parachain 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 TEE 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 TEEs. Therefore, the validators can trust each other and the consensus protocol is greatly simplified.

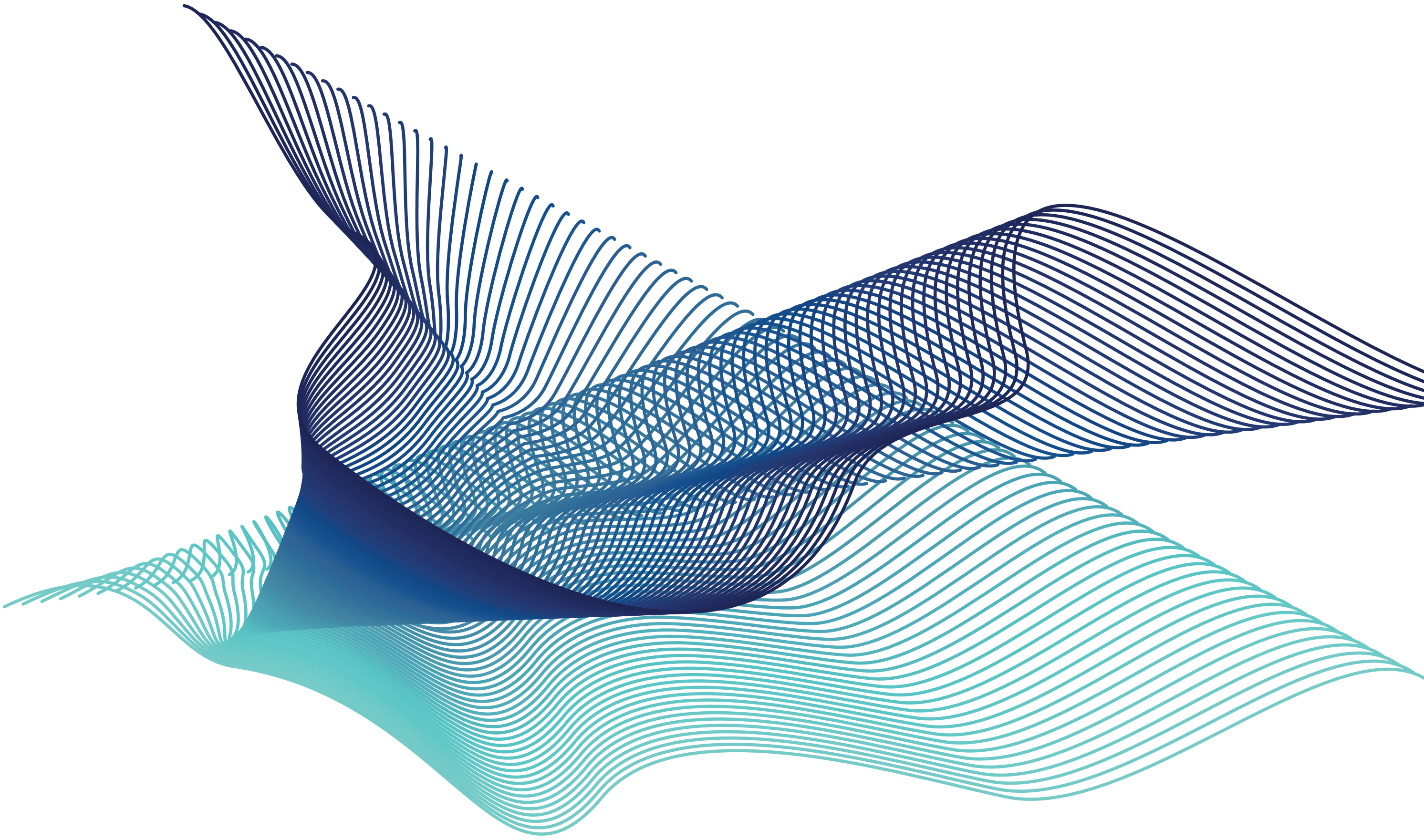
Integritee does not incentivize OCWs or SCVs because they are dApp-specific. It is up to the stakeholders of each dApp project that deploys on Integritee to incentivize infrastructure providers. This gives projects deploying on Integritee a great deal of independence. To drive the value of the TEER token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

BURNING FUNCTION

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

LOCKDROPS FOR FEE DISCOUNTS

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



Integritee Parachain Fees

The following Interactions with the Integritee parachain cost fees that are charged in TEER token exclusively and are paid to the network. More precisely, they are transfered to the parachain treasury, after burning a fraction of the fees (see burning mechanism).

Actor	Action	Goal
SCV, OCW	Register remote attestation for own SGX machine.	Obtain and renew membership in the set of attested TEE providers.
SCV	Confirm new sidechain block.	Obtain finality for sidechain
OCW	Confirm execution of a call.	Convince a requester that her call has been executed correctly.

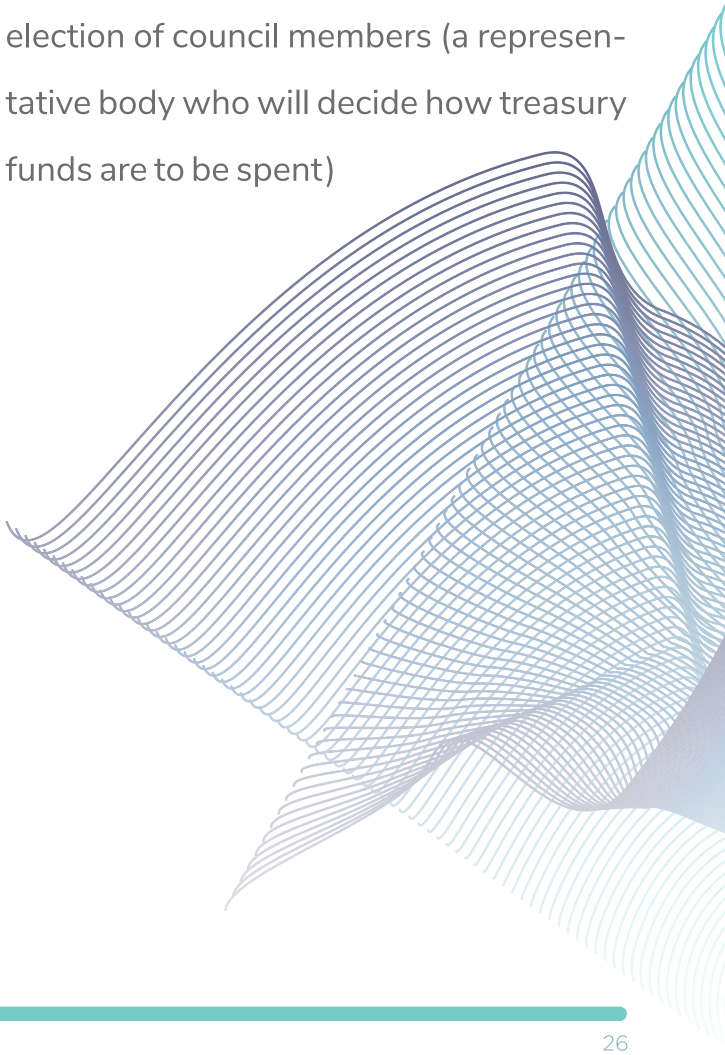
Governance

All TEER token holders can participate in the parachain governance process. Decision making is based on coin-voting. Voters will lock a freely-choosable fraction of their TEER for a certain amount of time and declare their desired outcome. Their vote will be weighted with the amount of TEER they have locked.

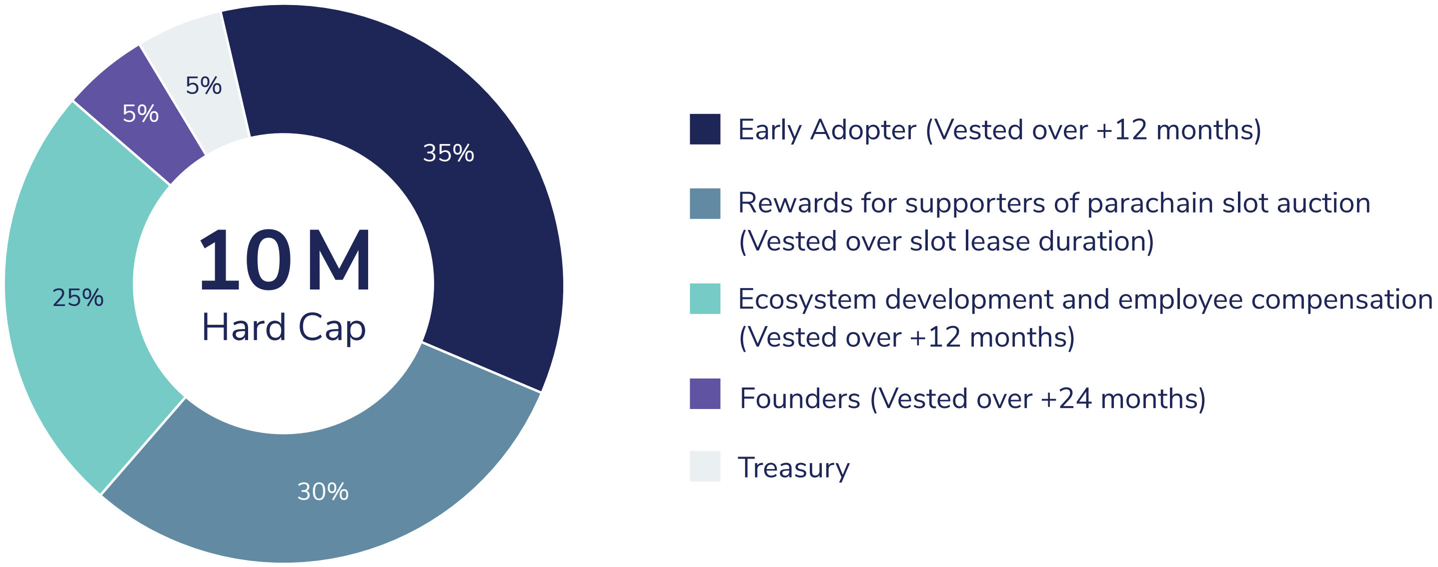
During the lock period, the TEER holder is still in custody of her funds but the lock prevents transferring tokens or using them to pay fees.

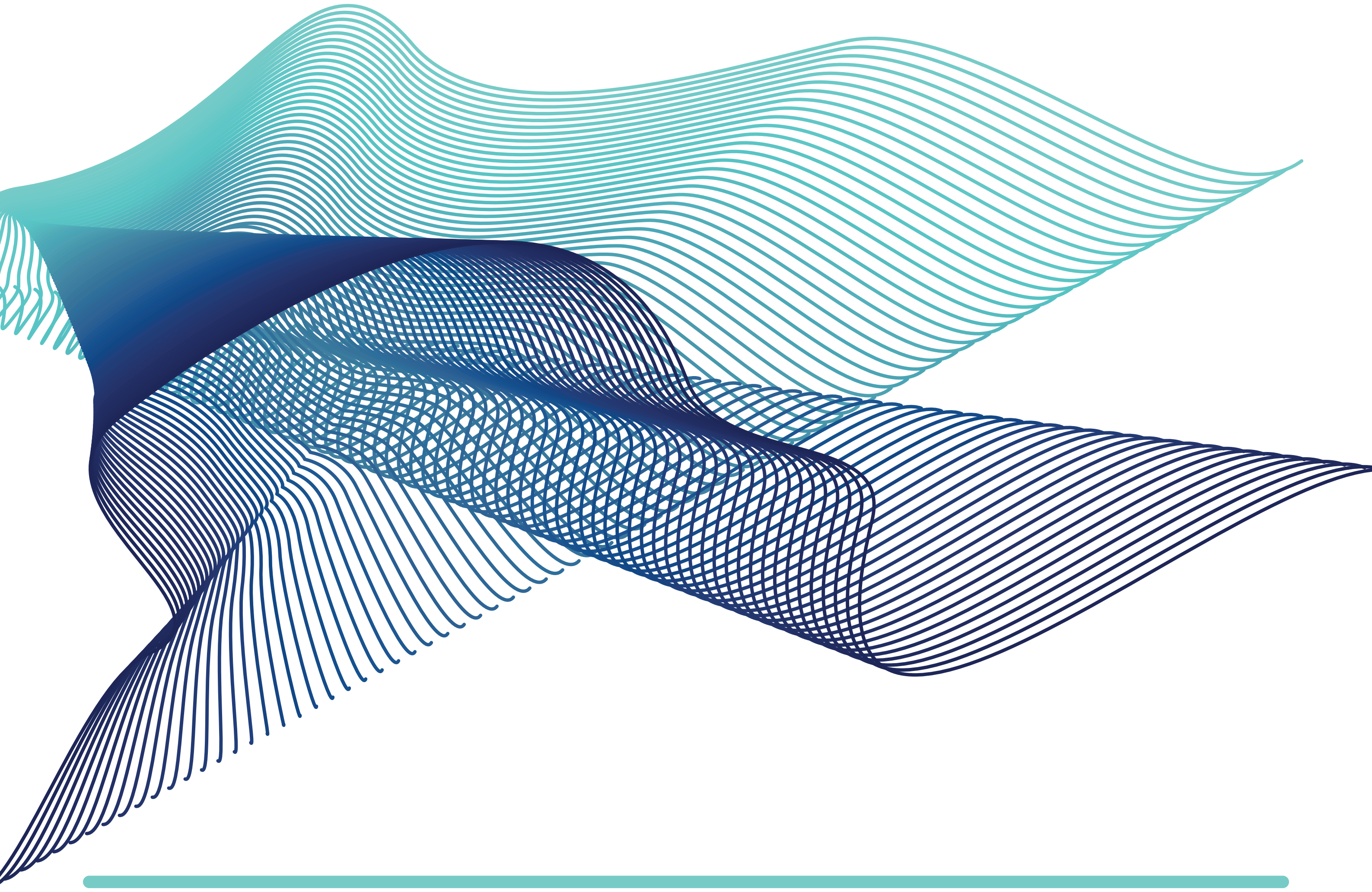
The following is a non-exhaustive list of governance actions that TEER holders can vote on

- parachain runtime code upgrades
- adjusting fees
- election of council members (a representative body who will decide how treasury funds are to be spent)



6.3. Token Distribution





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, Integritee provides a trusted technical foundation. There are far too many potential applications to list, but here are three possibilities:

HEALTH & WEARABLES

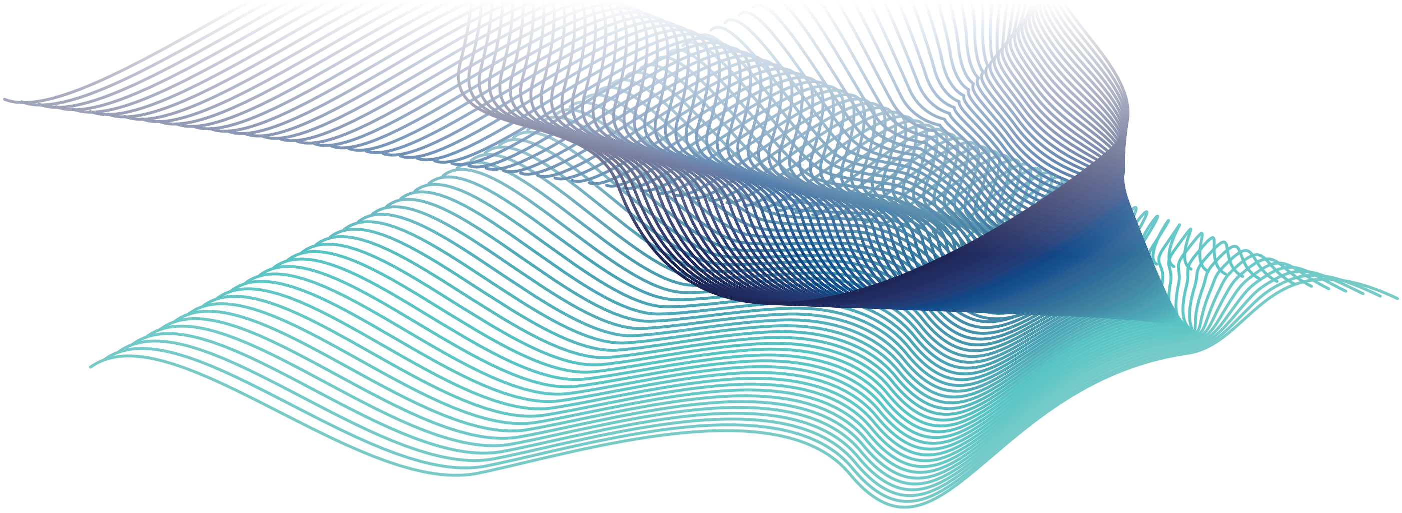
Integritee allows multiple manufacturers of wearable devices to securely pool data insights, while protecting user privacy.

CRYPTO EXCHANGES

Integritee enables a hybrid design that delivers the speed of a centralized exchange, while minimizing counterparty risk and the threat of frontrunning.

PRIVACY MESSENGER BRIDGE

Integritee can facilitate interoperability between private messaging apps, without exposing unencrypted data to an intermediary.



8. Roadmap

2018

Q4

- Release of the Encointer Whitepaper - "Local Community Cryptocurrencies with Universal Basic Income" and start of the SubstraTEE journey

2019

Q1

- 1st Web3 Grant for: Substrate Transaction Privacy using Intel SGX

Q3

- 2nd Web3 Grant for: Substrate Rust API client

Q4

- First SubstraTEE Meetup to demonstrate private token transactions

2020

Q1

- 3rd Web3 Grant for: SubstraTEE extension pack

Q2-Q3

- Development Prototype Platform based on SubstraTEE
- First deployed and running use case with Encointer on the Platform

Q4

- Polkadot Treasury Grant "SubstraTEE scalability"

2021

Q1

- Launch Rococo test-net parachain
- Conceptualize and preparation of spin-off

Q2

- Spin-off from SCS and birth of Integritee AG
- Seed round close

Q3

- New brand and website relaunch
- Move from SubstraTEE to Integritee
- Release lightpaper and tokenomics
- Participation in public slot auctions on Kusama
- Main-net & token launch
- Release of sidechains with smart contracts

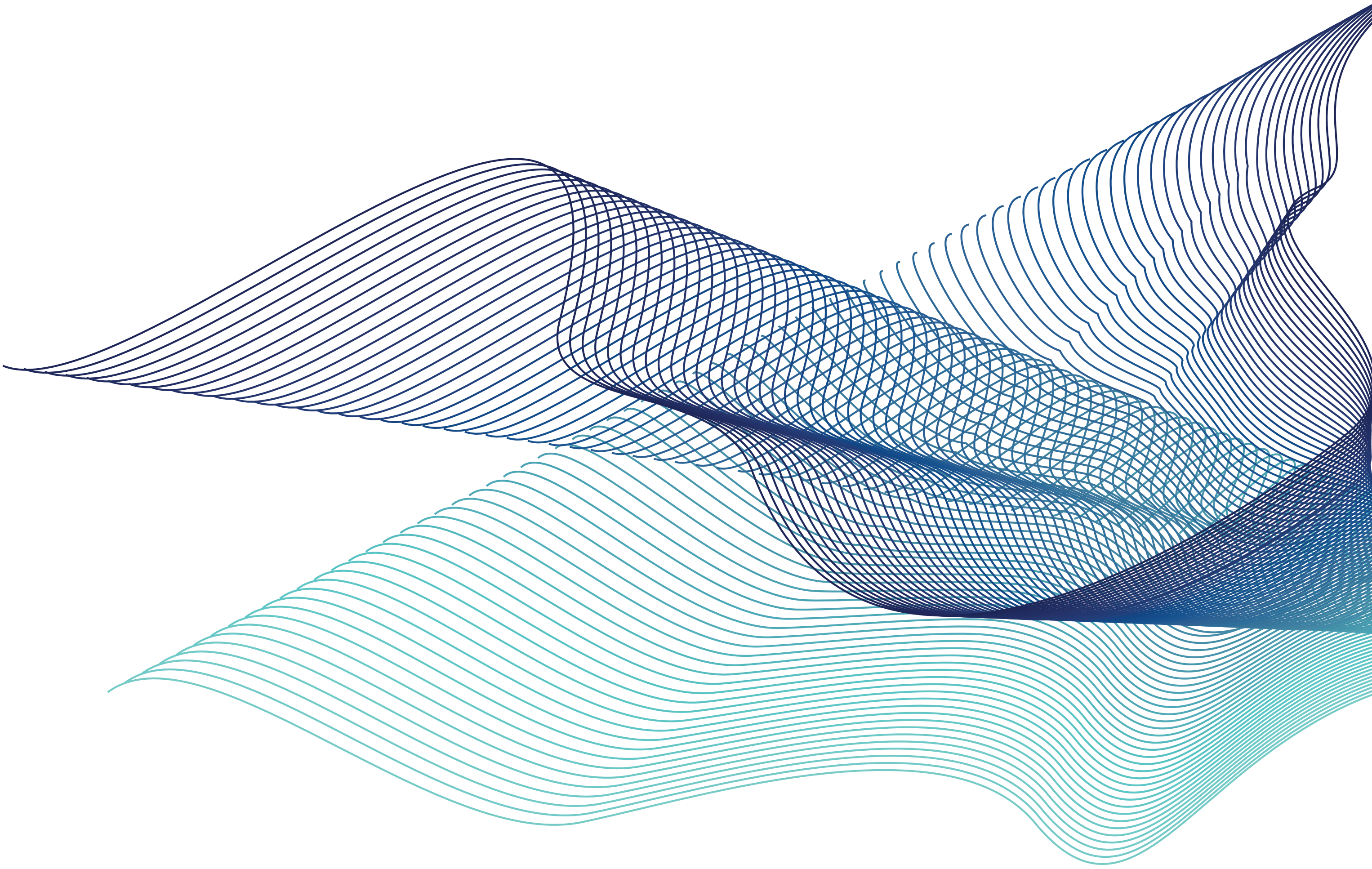
Q4

- Participation in public slot auctions on Polkadot
- Listing on first major exchange
- Release of a bridge between Kusama and Polkadot
- Release of new products for enterprise clients

2022 onwards

THE PATH TO ADOPTION

- Decentralize and establish the Governance Council
- First PoCs with enterprises
- Establish Integritee as the leading Polkadot Privacy Solution
- Run a multi environment TEER 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



INTEGRITEE