WPG whitepaper

Table of contents

1 Introduction

The lack of confidentiality and privacy on blockchains is obvious and hampers their uptake and use. While initial attempts to address this weakness have been made, the Partisia Blockchain project provides a complete platform for orchestrating and offering Zero-Knowledge (ZK) computations on-chain, off-chain and across blockchains (inter-chain). ZK computation adds privacy and confidentiality to blockchains in a decentralised fashion with no single point of trust. The Partisia Blockchain approach is blockchain agnostic and focuses on interoperability while facilitating both privacy and transactions across chains. As a public blockchain, Partisia Blockchain also functions as a vehicle for organising accredited trustees to further strengthen the blockchain ecosystem. The team behind Partisia Blockchain is composed of world-leading cryptographers and pioneers in the commercial use of ZK computations.

The global comprehensive digitalisation of most parts of our local and global society emphasises the current lack of secure infrastructure that can sustain this development. The ongoing development in blockchain technologies and the vision about WEB 3.0 represents a large collective effort to provide such a secure infrastructure. The different attempts necessarily incorporate various trade-offs between the three core objectives of any secure infrastructure: integrity, confidentiality and availability. The present stage of blockchain technologies scores highly on integrity with no single point of trust and transparency. This is essentially the basic decentralisation feature that may have tremendous potential in disrupting existing third party institutions, which includes some of the largest companies in the world from banks (money and transactions) to the ICT giants (collaborative solutions).

However, while the present best practices provide the first important candidates for a secure blockchain infrastructure, one of the most critical trade-offs they include is the lack of confidentiality. Without confidentiality, the potential disruption of existing third parties will be limited by lack of compliance, reduced uptake and real transfer of power and control of data. This limitation is recognised by many of the central actors in the blockchain industry. One strong indication of this is the increasing focus on ZK proofs. ZK proofs is an initial important step towards adding confidentiality to viable secure decentralised infrastructure. However, a ZK proof is limited to a single party (the prover) entering secret input to compute either true or false. This is very useful for simple operations such as confirming a private transaction. However, any collaborative solutions that involve more parties require ZK computations that support generic privacy-preserving computations - such as Fully Homomorphic Encryption (FHE) and more importantly MultiParty Computation (WPG).

The team behind Partisia Blockchain is one of the most experienced teams in ZK computations and WPG in particular, from creating the initial mathematical proofs in 1988 to realising the first real-life large scale and commercial use in 2008, Partisia marked the starting point of the collective effort over the past 10 to 15 years' to

truly commercialise ZK computation. Today ZK computation is used for trading and statistics in broad terms, and basic infrastructure such as key management and authentication, etc. Collectively, the past 10 to 15 years have resulted in WPG protocols and frameworks that have reduced the computational overhead by 1/1,000,000 and, importantly, accelerated the education of skilled developers, who have gained intimate theoretical knowledge about the strengths and weaknesses of the underlying protocols. The interplay between protocol designers and highly skilled developers is key to ensuring scalable and provable secure implementation. The Partisia Blockchain team brings the full package of cutting edge technology and deep experience to blockchains.

Partisia Blockchain brings ZK computations to blockchains through a two-sided approach.

1. Partisia Blockchain involves global collaboration between accredited ZK computation nodes, which are organised on the Partisia Blockchain, which is designed for transparent orchestration of ZK computation.
2. Partisia Blockchain will supply generic modules providing ZK computation across independent blockchains.

This two-sided approach builds the foundation for blockchain applications that meet users' and regulators' requirements through a tailored mix of transparency and accountability, on the one hand, and privacy and confidentiality, on the other.

While Partisia Blockchain's central offering is an unprecedented blockchain agnostic platform for provable secure privacy, it also enables a number of direct extensions. The prime extension is privacy-preserving Oracle functionality, which is used to orchestrate inter-chain transactions independent of the tokens or coins used and/or privacy-preserving auditing of inter-chain transactions, among other things. The privacy offered by the Partisia Blockchain makes it possible to tailor the Oracle functionality to regulatory requirements. As a result, Partisia Blockchain can function as a regulatory compliant privacy layer to existing large and small blockchains like Ethereum or Bitcoin and specialised blockchains like Instars.com. To fully support these collaborative synergies Partisia Blockchain is designed entirely for Bring Your Own Coin (BYOC) interactions, i.e. all use of Partisia Blockchain is paid for with the users' own liquid coins such as ETH and USDC. The first version of BYOC accommodates ETH and USDC and future versions will extend to other tokens or coins. The native token (dubbed the "WPG Token" to link it directly to the most important technology) is only used for staking and for incentivizing the Partisia Blockchain computation nodes.

The Partisia Blockchain's unique infrastructure is currently live on mainnet as version 3.0. The properties and roadmap for the infrastructure pivots around the following three overall objectives::

- **Scalability & basic blockchain**: Unique layer 1 with fast eager block production based Byzantine Fault Tolerance (BFT) style consensus and immediate finalization that is truly scalable with complete sharding.
- **Privacy & smart contract language**: Unique and general privacy-preserving computation, designed for bringing WPG , FHE and ZK proofs to everyone and anywhere via a comprehensive public-private smart contract language.

- Interoperability & bridges: Interoperability built natively into the protocol via Partisia Blockchain bridging based on double book-keeping, collateral bridging without accumulation of risk and with the same level of security as consensus.

Altogether, the network possesses all of the strengths of other blockchains but with unique privacy-preserving computation as a niche position delivered by the leading pioneers in the field. The three overall properties listed above include a series of innovations .

The team behind the Partisia Blockchain project is involved in several blockchain projects that collectively represent the starting point for Partisia Blockchain. These projects include the data exchange solution by Instars.com, the off-exchange matching service by Cyberian.digital, and key management for crypto wallets by the Partisia Blockchain partner, Sepior.

The adoption of the Partisia Blockchain pivots around:

- The integration with existing external blockchain networks to incorporate external tokens as BYOC twins on Partisia Blockchain and thus enable cross-chain collaboration.
- A launchpad and ecosystem of applications built on Partisia Blockchain or cross-chain applications.
- A dedicated focus on building flagship applications that solve essential global challenges that can also work as inspiration for projects brought in through the ecosystem in general.

2 Introducing Partisia Blockchain

Partisia Blockchain builds more secure digital infrastructure by merging blockchains and ZK computations (most importantly WPG but also FHE and ZK proofs) in a collaborative fashion. By focusing on privacy and interoperability, the Partisia Blockchain project will initially focus on the following three goals:

a. Orchestrating ZK computations as transparent, efficient and simple as possible.
b. Offering blockchain agnostic ZK computations.
c. Offering privacy-preserving and auditable coin-agnostic payments.

In this section, we provide an introduction to Partisia Blockchain and discuss some fundamental problems that need to be solved and the basic components involved in the Partisia Blockchain solution.

2.1 ZK computations and Blockchains

ZK computation belongs to a class of modern cryptographic solutions that enable computation on unknown data. This might seem impossible at first, but using the right cryptography — ZK computation — it is achievable. ZK computation combines secure multiparty computation and similar techniques such as ZK proofs and fully homomorphic encryption. ZK computation, in particular, achieves this goal by converting the computation into a distributed computation, in which the participant

in the computation has zero-knowledge about the input to the computation. While ZK proofs are restricted to computing whether something is either true or false, secure multiparty computation represents a class of protocols for generic privacy-preserving computation. Another limitation of ZK proofs is that only one party can have a secret input (the prover). In contrast, with ZK computation, all parties can have secret inputs and outputs.

The seminal aspects of this concept can be traced back to Shamir (1979), with the theory being founded in the 1980s (Chaum, Crepeau and Damgård 1988). Although it was demonstrated in the mid-1980s that, in theory, ZK computation was generally applicable, its complexity prevented its practical use for another two decades. The first large-scale and commercial use of ZK computation was conducted by the Partisia Blockchain co-founder Partisia. In this application, ZK computation replaced a traditional auctioneer in a so-called double auction (Bogetoft et al. 2009).

Since 2008, the technology has matured both in terms of computational speed as well as the properties of the ZK computation protocols. The computational overhead has been reduced to approximately 1/1,000,000 of its previous size. The development of ZK computation can be traced by, e.g. reading the following papers: Pinkas et al. (2009); Shelat and Shen (2011); Nielsen et al. (2012); Damgård et al. (2012); Frederiksen and Nielsen (2013); Frederiksen and Nielsen (2014); Lindell and Riva (2015); and Nielsen et al. (2017).

Fully implemented applications include basic infrastructure such as key management for crypto wallets (delivered by the Partisia Blockchain project partner Sepior), off-exchange matching (delivered by the Partisia Blockchain project partner Partisia and Tora.com) and Data brokerage (delivered by the Partisia Blockchain project partners Partisia and Instars.com). Emerging applications designed to run on the Partisia Blockchain include secure bridging of tokens and data across different blockchain networks, auction solutions, healthcare data exchange, confidential sharing of cyber breaches, privacy-preserving advertisement in internet searching and humanitarian stablecoin solutions with built-in privacy protection.

2.1.1 ZK computation protocols

ZK computation is applicable to a broad and diverse set of applications. It is not a single protocol, but a growing class of solutions, each with different characteristics. A number of ZK computation systems have been devised to meet the specific needs of different applications, such as key management and financial order matching.

Each individual or organisation has one or more of the following roles, which are common to all ZK computation solutions:

- The **Input Parties** have inputs for the computation that they would like to keep confidential.
- The **Computing Parties** are responsible for carrying out the distributed computation.

- The **Result Parties** are sent the results by the Computing Parties. They then compile the data they have received from the Computing Parties into the result of the overall computation.

Crucially, no party, besides the Input Parties, ever see the original inputs.

Custom ZK computation systems may differ along the following parameters:

- **Operations**: A ZK computation system will have either arithmetic or Boolean operations - and the two can be interleaved for specialised computations.
    - Arithmetic operations are more convenient for expressing, e.g. statistical analyses.
    - Boolean operations are more efficient at, e.g. matching.
- **Cryptographic primitives:** A ZK computation system will use one or more of the following cryptographic operations:
    - Secret sharing: a technique for splitting data into parts that in isolation do not provide information about the original data. Secret sharing is very common in ZK computation systems.
    - Oblivious transfer: a class of protocols for data transfer in which the sender sends one of several pieces of data, but does not know which.
    - Homomorphic encryption: a class of schemes for producing ciphertexts that can be computed on without decrypting.
- **Trust model**
    - Self-trust: A computing party only has to trust its own ZK computation node.
    - Honest majority: A computing party must rely on the majority of the computing parties being honest.
    - In general threshold security allows to trust that at most *t* is malicious from the pool of *n* servers.

Different combinations of these parameters give rise to different properties:

- **Fault-tolerance:**
    - Under self-trust, all parties are needed for the computation to proceed. The system will fail even if only one of the parties is unable or unwilling to participate.
    - Whereas if a system merely relies on there being an honest majority, the system can proceed to completion even if some of the parties fail to carry out their duties.
- **Security:**
    - Passive security: As long as all Computing Parties follow the protocol, none of them will learn anything besides the output of the computation. This is also known as semi-honest security.
    - Active security: None of the parties learn anything besides the output of the computation, even in the presence of malicious computing parties, who are willfully trying to deviate from the protocol.
    - Covert security: In between Passive security and Active security. A Computing Party which deviates from the protocol may learn sensitive information with a certain level of probability, e.g. 25%. However, in

doing so, there is also a high chance of being identified as a cheater, e.g. 75%.

- **Performance**:
    - Passive security has better performance than active security. In some cases, covert security provides similar guarantees to active security, but is as performant as a passive security solution.
    - Honest majority is similarly faster than self-trust.

Due to the nature of the technology, custom systems are necessary to achieve acceptable levels of performance. The primary Partisia Blockchain partners (Partisia and Sepior) have been developing custom ZK computation systems since 2008. The Partisia Blockchain will provide an open standard for ZK computation protocols to facilitate a broad international collaboration. The Partisia Blockchain team will continuously design and customise ZK computation systems to ensure that they meet users' security needs and performance guarantees.

2.1.2 Trust models and ZK computation nodes

Choosing the right ZK computation protocols and computational nodes is crucial to achieving the desired confidentiality, efficiency and robustness.

In some applications, the problem may be separated into smaller problems with clear roles and opposing interests, which may be used to design a strong trust model. The Instars.com application is such an example, where a data broker solution is separated into a series of two-party problems between the requester of the data and its provider, who have opposing interests.

*We refer to this trust model as the **Participant based trust model.** Here, the relationship between the input parties involved makes up the trust model — their likely opposing interests strengthens the trust model.*

In other applications, the problem to be solved demands that more parties interact simultaneously — like an exchange or a matching service. For example, Tora.com's Crosspoint application involves matching orders between a potentially large number of buyers and sellers. Where many parties are involved, a trust model that relied on agreement among all participants would be unworkable since it would grant a veto to every single participant to block the system. Although the participants could operate the ZK nodes themselves in a so-called "threshold model" with fault tolerance, for the reasons described above, in cases involving large numbers of parties, individuals from outside the group of participants typically make up the trust model.

*We refer to this trust model as the **Delegated trust model**. Here a network of individuals from outside the input parties makes up the trust model — accredited ZK computation nodes and incentives for delivering trust strengthens the trust model.*

In some cases, the participant-based and delegated trust models can be combined naturally in a robust threshold model.

The Partisia Blockchain will be designed to support a variety of trust models and ZK computation protocols. From simple off-chain two-party ZK computations based on participants to robust threshold ZK computation delegated to ZK computation nodes.

2.1.3 The complementary blockchain

In recent years, the Partisia Blockchain team has worked on various aspects of blockchain technologies and has developed ZK computation infrastructure for commercial uses such as blockchain based data exchange, financial order matching and crypto wallets. For more about the team, see Section 4.

So the merging of ZK computation and blockchain technologies has already started, but why?

Consider the initial use case of ZK computations — auctions — which is one of the most common types of market mechanisms used across all industries. An auction is a well-defined set of trading rules that typically includes a mix of public and sealed bidding. Operating an auction requires a secure infrastructure that scores highly on all parameters from integrity and confidentiality to availability. ZK computations offer all of this, which makes it an ideal infrastructure for auctions, so why combine it with blockchains? On the one hand, blockchain architectures provide transparency in terms of who is involved in the auction (bidders and ZK computation nodes) and how they are involved (the auction protocol). On the other hand, the blockchain is also ideal for decentralised enforceable execution of the result of an auction without the traditional middleman.

The example of the auction shows how the combination of ZK computation and blockchains provides a more holistic infrastructure that better balances transparency and privacy with no single point of trust throughout the entire process. In addition, the guaranteed and automated execution provided by the blockchain strengthens the auction platform by preventing external interference with the implemented agreement and exposing exactly the required information to validate the trust without compromising confidentiality.

Another very basic question is how to protect secret information from disclosure on a blockchain whose data is visible to the public. The core problem is that encrypted information is basically not suited to blockchains. The reason for this is that while the encrypted information is freely available on the distributed ledger, at some point in the future, that encrypted information needs to be re-encrypted to avoid brute force attacks. Therefore, standard encryption on blockchains should only be used for short lived secrets. The Partisia Blockchain addresses this problem by keeping encrypted confidential information separate from the blockchain, hence all ZK nodes run ZK computation in a separate private layer.

2.2 The problems to be solved by Partisia Blockchain

ZK computation is generally applicable to ensure confidentiality in a secure infrastructure. The existing uses of ZK computation provide a first indication of this.

While the initial focus of ZK computation work was on auctions, subsequent efforts have resulted in ZK computation solutions for basic infrastructure such as authentication and key management, privacy-preserving analytics and more advanced matching and market mechanisms.

In general, the process of identifying the correct decision or computing the right statistics requires a lot of data. In many cases, this involves confidential information such as sealed bid auctions or peer data used for statistics such as credit scoring. In both cases, ensuring that confidential information remains confidential is fundamentally important for strategic as well as privacy reasons.

In all cases, the confidential information is compiled to compute a result that may trigger new computations or be used directly. The outcome will either be new information or one or more transactions. In both cases, Partisia Blockchain provides a holistic, secure infrastructure for the generic use case illustrated in Figure 1.

The blockchain based data exchange, Instars.com, is one example where a requester searches for matching profiles using ZK computation and where a match results in a transaction of information for Instar tokens.

The blockchain based off-exchange matching service - Crosspoint by Tora.com - is another example where a group of buyers and sellers match confidential orders.

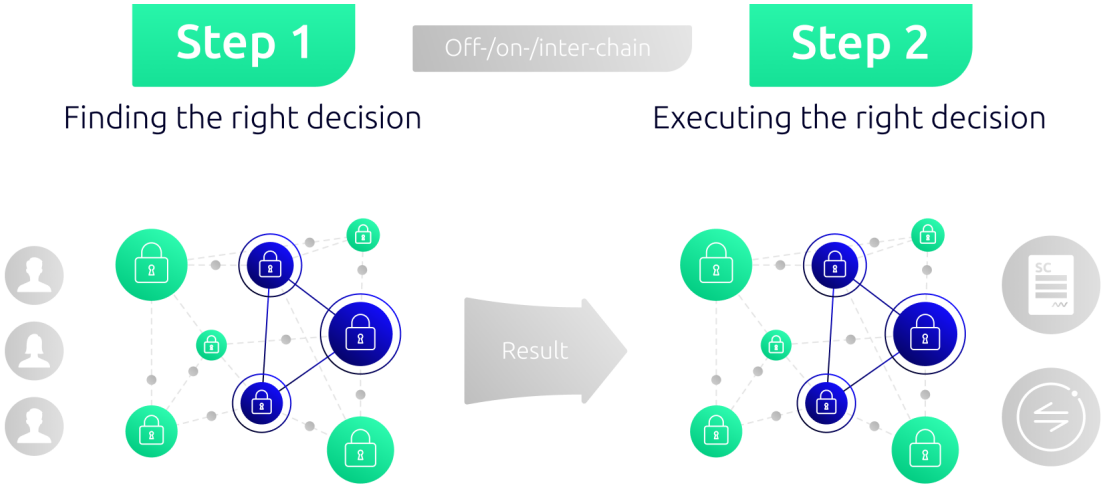

Figure 1: A generic use case.

In broader terms, the use of sensitive data is becoming increasingly important and problematic at the same time. This dilemma explains the increasing focus on designing more secure infrastructure such as Partisia Blockchain.

Sensitive personal and company information is highly valued in research and services, with benefits for individual citizens, companies and society in general. However, the most valuable data is also the most sensitive such as information about individuals' and companies' confidential preferences and decisions. On the one hand, it is predicted that data-driven decisions and analytics will be a tremendous growth area in the years to come. On the other hand, data that is used

outside its original context may violate fundamental rights to privacy and weaken the “bargaining position'' of individuals and companies in general.

The latter was acknowledged early on by Google's chief economist, Hal Varian, in an early paper on market design for automated trading: ”... Hence privacy appears to be a critical problem for computerized purchasing agents. This consideration usually does not arise with purely human participants, since it is generally thought that they can keep their private values secret. Even if current information can be safeguarded, records of past behaviour can be extremely valuable, since historical data can be used to estimate willingness to pay. What should be the technological and social safeguards to deal with this problem?'' (Varian 1995).

Increasing political awareness has resulted in new regulation that is primarily aimed at protecting personal data. The most progressive example is the General Data Protection Regulation (GDPR) in the EU, which came into effect in May 2018. The GDPR lists a number of requirements on how to use so-called ”Personal Identifiable Information'', and introduces penalties for data breaches that align data protection with anti-trust regulation. Data protection outside the EU (most notably Japan and Brazil) is also developing in the same direction in response to increasing concerns from citizens and political pressure. This type of regulation has an impact on many companies as personal information is integral to their business. However, sensitive company information is not regulated in the same way as personal identifiable information. Nevertheless, indirectly, antitrust regulation prevents sensitive data from being shared among competitors, which may otherwise hamper competition.

Regulation is not just about safeguarding data, it is about achieving the right balance between safeguarding confidential information and addressing fraudulent behaviour. The regulation of blockchain technologies and crypto tokens is developing at the local and regional levels. There is a growing consensus among regulators about the need to adapt key components of financial regulation to blockchains, most notably that all participants pass KYC and AML procedures one way or another.

Partisia Blockchain is designed to safeguard confidential information on blockchains in the context of a variety of applications built on the network. Teams building Partisia Blockchain applications across jurisdictions are responsible to comply with all relevant regulations from data protection to fraud detection. We have designed the network to enable applications to establish the right balance between confidentiality and transparency. In short, Partisia Blockchain ensures transparency about the use of privacy algorithms used while the private input data is kept private. This enables applications to comply with both data protection and fraud detection, e.g. preserving user privacy in authentication and audit checks. Although the responsibility sits with the teams that are building applications, the Partisia Blockchain builds components that can be used directly by applications such as privacy-preserving self-sovereign identity solutions.

2.3 The Partisia Blockchain cross-chain solution

The backbone of the Partisia Blockchain is the Partisia Blockchain cross-chain solution, which facilitates global collaboration between accredited ZK nodes and transparent orchestration of ZK computation. This makes it possible to deliver simple and efficient ZK computation across independent blockchains. The dashed boxes in Figure 2 emphasises these two basic sets of elements of the Partisia Blockchain solution.

Figure 2: The basic Partisia Blockchain architecture and approach to blockchain agnostic ZK computation.

Partisia Blockchain
Partisia Blockchain is a fully functional public blockchain and a transparent platform for orchestrating and delivering ZK computations on-chain, off-chain and across blockchains.

The Partisia Blockchain organises a large number of independent node operators that conduct the following three distinct jobs:

- The baker jobs: Baker nodes are continually involved in the Partisia Blockchain as part of the jobs involved in the P2P network, consensus and transaction layers.
- The ZK computation jobs: ZK nodes are assigned to ZK computations on a job-by-job basis.
- The Oracle jobs: Oracle jobs are assigned to Oracle jobs like BYOC on a job-by-job basis.

All node operators must pass external KYC/KYB and an on-chain registration process to become accredited node operators. This registration process is built into the protocol itself (decentralized) and the Partisia Blockchain Foundation is not involved at any stage.

Coin agnostic transactions

A key part of the interoperability offered by the Partisia Blockchain is the orchestration of inter-chain transactions that make payments independent of the coins used (BYOC).

The key component of this solution is a carefully designed BYOC token bridge solution that is used to orchestrate secure transactions across different blockchains and bring in external tokens or coins.

Blockchain agnostic ZK computation
ZK computation is delivered directly through the advanced built-in orchestration of ZK computation. However, with BYOC integration of external blockchains, ZK computation can be used across any external blockchain by the use of cross-chain smart contracts. This approach facilitates the same economic alignment as if ZK computation was a layer 2 service.

Privacy-preserving audit
Another direct use of the privacy-preserving oracle is the privacy-preserving audit. As blockchains adopt more privacy measures, the need for transparent auditing becomes essential. Through delegated trust, the Partisia Blockchain oracle can run audit checks on confidential information about transactions and other relevant information.

Combined with inter-chain operability, Partisia Blockchain will function as a platform for privacy-preserving auditing. This facilitates a new type of decentralised auditing that achieves a balance between transparency and privacy. On the one hand, transparency is an effective way of tackling fraudulent behaviour, while on the other hand, privacy is a right of individual citizens and companies, private information may be of great strategic value. The Partisia Blockchain project removes or considerably reduces this fundamental trade-off.

2.4 Organisation, nodes and tokens

Although the first version of the Partisia Blockchain has been developed, tested and used commercially by Partisia, a privately held Danish company, the publicly available Partisia Blockchain has been transferred and open sourced by Partisia Blockchain Foundation an independent non-profit Swiss foundation with the sole purpose of supporting the public blockchain Partisia Blockchain.

The Partisia Blockchain is based on an open token economy. The Partisia Blockchain oracle facilitates Bring Your Own Coin (BYOC), so from a user and from an economic perspective, the Partisia Blockchain is a completely open economy that allows the user to pay for their use of the network with any liquid coin or token. Internally, the Partisia Blockchain is fueled with system tokens representing the supported coins.

Here, we provide a first introduction to the economy of the Partisia Blockchain by focusing on the organisation of the node operators, the oracle and token agnostic payments and how this impacts the WPG Token economy.

Figure 3: The basic component in WPG Token economy and compliance.

The different components of the Partisia Blockchain project are illustrated in Figure 3 and briefly described below (clockwise from “Users/services/community”).

Users/services/community
The Partisia Blockchain is establishing a community for users, service providers, other blockchains and developers.
Accounts on Partisia Blockchain are created automatically by transferring tokens to a user generated public key and it is the user’s responsibility to manage the associated private key. It is the responsibility of the teams that build applications to meet the regulation from data protection to fraud detection relevant for the use case and jurisdictions in question. The Partisia Blockchain provides all of the tools needed to use privacy-preserving computation in a fully transparent way.

ZK computation marketplace
The Partisia Blockchain is basically a ZK computation marketplace that represents the full service offered by the ZK OS, which ensures provable, secure, simple, efficient and robust ZK computation on-chain, off-chain and inter-chain. It will be an open marketplace that allows other developers to offer ZK computation protocols and blockchain services.
An integrated part of the ZK market place is the oracle functionality that facilitates BYOC on Partisia Blockchain.

Node operators
The Partisia Blockchain aims to include a diversified group of accredited node operators from all over the world and across industries. However, as a public blockchain with accredited node operators, the Partisia Blockchain does not rely on a large number of node operators for it to be operational. All nodes run baker jobs (as prescribed by the consensus protocol) and ZK computations on a job-by-job basis (as prescribed by the market for ZK computations).
To meet the highest compliance standards, all node operators need to pass third-party KYB/KYC requirements as part of the process of becoming accredited

node operators, as well as providing publicly available information and pass computational tests that attest the ability to professionally run a node. Node operators are also required to stake WPG Tokens as part of the incentive schemes.

The Partisia Blockchain governance
The Partisia Blockchain Foundation manages and governs the development and release of software, the creation and sale of WPG Tokens as well as the promotion of the network, similar to the foundations that govern projects like Ethereum, Cardano, Dfinity and many other blockchain projects. Partisia Blockchain Foundation is not involved in operating the decentralized governed Partisia Blockchain.

The Partisia Blockchain is governed and managed through decentralized incentives, regulation and voting mechanisms such as:

- Node operators become accredited and whitelisted to operate a node through an automated process governed by the protocol. An accredited node operator can only be revoked by the node operator itself or through carefully designed voting mechanisms.
- Incentive mechanisms ensure that the most trusted nodes operate the Partisia Blockchain. This includes scoring of the nodes, mechanisms to select nodes to run ZK computations or the Partisia Blockchain Oracle as well as staking and pricing mechanisms.
- New versions of the software that constitutes the Partisia Blockchain are initially approved implicitly by the node operators running the blockchain. Future versions of the Partisia Blockchain will include more detailed voting rules ensuring that the Node operators decide which software to run.

These decentralized mechanisms are further described throughout this Section 2.4.

2.4.1 Becoming a node operator

The ability to operate a computation node is granted through the Partisia Blockchain by predefined and automated processes. Operating a computation node entails running a server configured to execute different tasks:

1. Block production (Baker Node)
2. Execute ZK computations (ZK Node)
3. Participating in the BYOC wallet (Oracle Node)

Each task comes with different responsibilities and risks outlined in the following paragraphs.

Baker Node
Block production is a necessity for the blockchain to manage state and for the node operators to earn fees. Where the actual computations are simple, it poses requirements for backup. While the basic role as block producing node, does not involve the handling of confidential information, Baker Nodes are involved in a large-scale threshold signature scheme, which requires backup of secret variables.
Incentives: All node operators involved in achieving consensus are expected to operate a Baker Node and as such are required to stake WPG Tokens.
The payment as Baker Node is the basic earning as node operator.

Decentralized regulation: All potential node operators can register to operate and get whitelisted as a Baker Node through an automated accreditation process.

ZK Node
Executing the ZK computations is significantly more involved than operating a Baker Node. These executions will saturate the network on the server and require backup of the secret variables and significant SLA requirements on the servers during the lifetime of a ZK computation. A ZK node holds the secret state of the ongoing computations and collusion among t+1 of the involved ZK nodes can leak the secrets. t is set by the chosen security model and t+1 may potentially involve all of the involved ZK nodes. A number of mechanisms will be introduced to counteract collusive behavior such as additional staking and a market that allows the users of the Partisia Blockchain to select ZK nodes.
Incentives: The ZK nodes are required to further stake WPG Tokens beyond those required for participation as Baker Nodes to enter the market for ZK computation. The payment received by ZK node is additional earning to that received as a Baker node operator.
Decentralized regulation: All potential ZK Node operators can register to operate and get whitelisted as a ZK Node through an automated accreditation process.

Oracle Node
Maintaining the secret state for the cross chain wallets requires monitoring the states of the governing smart contracts on both chains and reacting accordingly. These reactions all involve moving funds to and from the wallets. All the nodes involved in running the oracles hold a part of the key to the wallet. It is very easy to prove that a wallet has been misused - since every transaction not authorized through the smart contract is malicious. Hereby, constraints on the funds controlled by the individual node operators will be defined by a function with the amount of WPG Tokens staked and the liability towards the users of the Oracle as input.
Incentives: Nodes running the Oracle are required to further stake WPG Tokens. The payment for operating the Oracle is set a priori by the Partisia Blockchain. The payment from operating the Oracle is in addition to earnings as a node operator.
Decentralized regulation: All potential Oracle Node operators can operate and get whitelisted as an Oracle Node through an automated accreditation process.

Whitelisting and Exclusion
All approved Baker, ZK and Oracle Nodes are whitelisted and the automatic accreditation process is renewed yearly. The right to operate a node can only be revoked by the node operator itself or through a carefully designed voting mechanism with token holders and node operators as voters. The voting process is entirely orchestrated through smart contracts on the Partisia Blockchain and the Partisia Blockchain Foundation has no role in either parts of the voting process.

2.4.2 Organising the node operators

The Partisia Blockchain organises accredited trustees (node operators) as part of the decentralised (no single point of trust) privacy offering. All node operators participate in securing the distributed ledger and are available for ZK computations.

The ZK computations are done among a subset of node operators and the importance of the individual nodes depends on the chosen trust model and whether the node participates in offline pre-processing or the online ZK computation. The orchestration of the ZK computations allows the users of Partisia Blockchain to select trust model and node operators, which will gradually turn the Partisia Blockchain into a market for trust that rewards node operators with high reputation scores. Since the ZK computations happen among a selected subset of all the node operators, we are placing ourselves between the traditional approach with single trustees like consultancy houses, and the fully decentralised public blockchains, where anyone can download and operate a node in the network. The process of becoming a node operator, however, is an open and automated process.

A modern, decentralised, secure infrastructure removes the need to rely on trust in single institutions. How to get there differs when it comes to achieving decentralised confidentiality as opposed to achieving decentralised tamper-proof ledgers. The basic tamper-proof ledger/blockchain and ZK computation are complementary, which is what the Partisia Blockchain utilises. One of the key challenges with ZK computation is to either; a) engage a large efficient external network in ZK computations e.g. the Partisia Blockchain node operators (delegated trust model), or b) to utilise the participant based trust models made up of opposing interests like that between a buyer and a seller (participant based trust model). As explained in Section 2.2, applications may also benefit from using both the delegated trust model and the participant based trust models. The Partisia Blockchain is designed to orchestrate participant based trust models and deliver delegated trust models. The organisation of accredited trustees is instrumental to delegated trust. Partisia Blockchain provides a set of protocols that group and regroup the accredited trustees and ZK nodes in order to reach the highest level of delegated trust.

Consequently, by achieving delegated trust through accredited node operators, the natural organisation of the blockchain is a permissioned blockchain based on a known set of node operators (solving both baker and ZK computation jobs). The incentive structure supports the organisation in the following ways:

- The Partisia Blockchain provides transparent orchestration.
- The node operators put their reputation into the Partisia Blockchain.
- The node operators pass KYB/KYC and stake tokens to become accredited.
- The node operators are paid to run ZK computation and baker jobs.
- The ZK computation protocols counteract collusive behaviour.
- The Partisia Blockchain facilitates a market for trust where the users can select node operators.

2.4.3 Bring Your Own Coin (BYOC) and the WPG Token

The Partisia Blockchain is designed to accept any liquid crypto coin or token as payment for Partisia Blockchain services via cross-chain transactions. With this “Bring Your Own Coin” (BYOC) functionality, the network becomes highly collaborative as it brings in and activates external token economies on the Partisia Blockchain. Below, we describe first the mechanics behind the BYOC token bridge and then the stable fees and staking mechanisms employed by the network.

Bring Your Own Coin (BYOC) Token Bridge Mechanics
Partisia Blockchain provides seamless integration with other blockchains through a cross-chain token bridge model that facilitates Bring Your Own Coin (BYOC). BYOC allows a user to pay for Partisia Blockchain services with another liquid coin such as ETH or USDC.

Figure 4 shows the flow of tokens that would be involved in using BYOC with ETH. First, a user with a private ETH wallet creates a user account on Partisia Blockchain, which will hold any BYOC Twin tokens created by the BYOC token bridge. BYOC Twins are simply created by transferring ETH to the WPG -ETH wallet. The BYOC Twins can only be managed by the user through the Partisia Blockchain.

Once the account is in place, if the user transfers ETH to the WPG -ETH wallet, the Partisia Blockchain BYOC token bridge registers the transfer, signs the transaction, creates the ETH BYOC Twin and updates the built-in double bookkeeping to show the user's balance of ETH BYOC Twins on the Partisia Blockchain account and the matching balance of ETH in the WPG -ETH wallet. From the user's point of view, the ETH BYOC Twins appear immediately in the user'
s Partisia Blockchain account and
the user can start transacting on the Partisia Blockchain. The gas that funds the transactions is deducted from the user's account and the finalization of these payments occurs automatically after approximately 30 minutes, resulting in transfers of ETH Twins to the participating node operators accounts.

To further strengthen the BYOC token bridge and counteract any potential collusion, Partisia Blockchain introduces the following sets of additional security measures:

- Selection and rotation mechanism: A protocol frequently replaces the assigned Oracle nodes that operate BYOC token bridge with a randomized selection of new nodes. All Baker nodes sign off on the newly selected Oracle nodes, using a large-scale multisig scheme operated by all Baker nodes.
- More threshold multisig: During the operation of the BYOC token bridge, the selected Oracle nodes operating the bridge use a state-of-the-art threshold cryptography solution for multisig authorization.
- Staking mechanism: To operate the BYOC token bridge, all Oracle node operators are required to stake WPG Tokens, backing all transfers by WPG Tokens as collateral 1:1. When the cluster of Oracle nodes run out of staked WPG Tokens, the BYOC token bridge epoch concludes and a new set of Oracle nodes is selected to begin a new epoch. After each epoch, validators can employ a dispute process to challenge any imbalances and the locked staked WPG Tokens can be used to compensate for objective fraud.

In combination, the different selection, rotation, signing, staking and transparency procedures, make it very difficult for a corrupt ring of Oracle nodes to collude and compromise the token bridge. Consequently, the BYOC token bridge avoids accumulation of financial risk across epochs and provides unprecedented security.

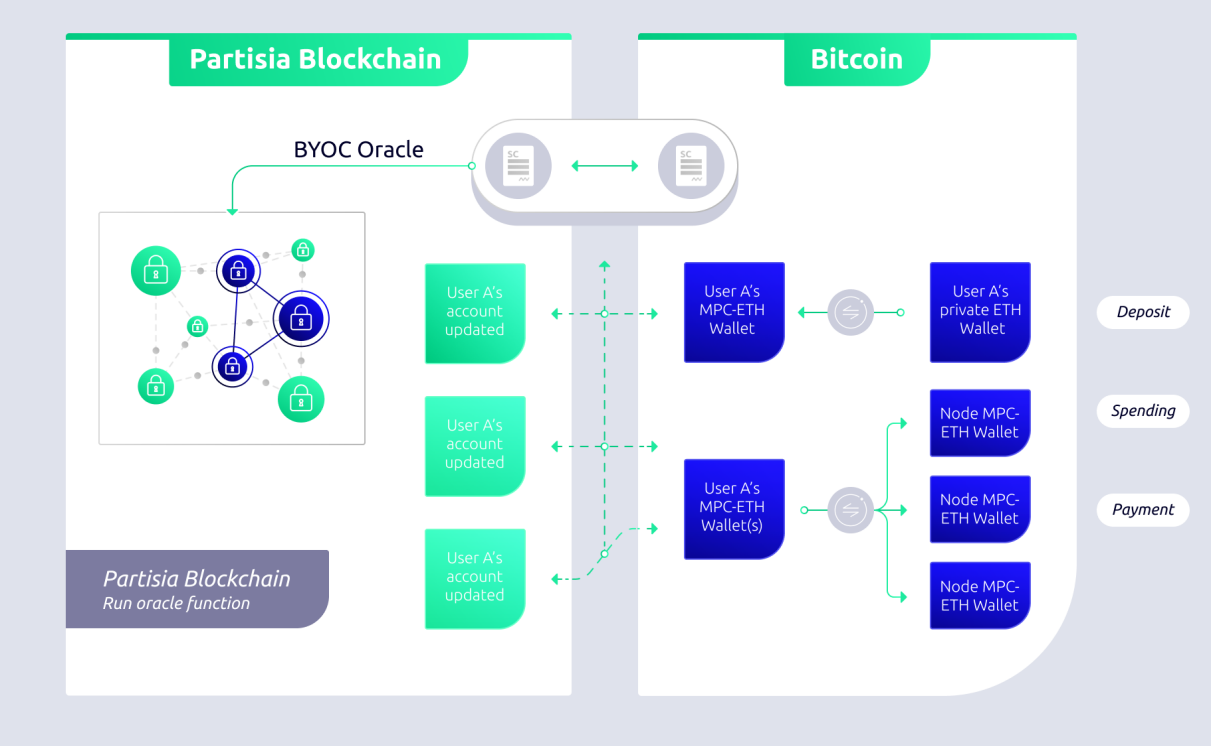

Figure 4: The BYOC oracle function or cross chain account.

Internally, BYOC assets are represented by an BYOC Twin or system tokens on the Partisia Blockchain, which represent the BYOC tokens 1 to 1, such as:

- In case of BYOC = ETH: BYOC Twin is WPG -ETH tokens (WPG -ETH = ETH 1:1)
- In case of BYOC = USDC: BYOC Twin is WPG -USDC tokens (WPG -USDC = USDC 1:1)

The BYOC flow is described stepwise below and illustrated in Figure 4.

- A user transfers BYOC (say ETH) into an oracle controlled wallet (say WPG -ETHwallet)
- The user's Partisia Blockchain account now contains the number of WPG -ETH tokens corresponding to the ETH in the user's WPG -ETH wallet (WPG -ETH = ETH 1:1).

- The user uses WPG - artisia Blockchain.

ETH tokens to run public and private smart contracts on

The pricing scheme (i.e. the pricing model towards the Partisia Blockchain users) for using Partisia Blockchain determines the prices charged to the user.

- The actual costs are calculated and WPG -ETH tokens are moved to an intermediate Partisia Blockchain wallet continuously and the user's account is adjusted accordingly (registered as pending payment).
- When a job has been finalized, the WPG -ETH tokens are allocated and registered at the corresponding Partisia Blockchain nodes accounts (registered as pending payment).
- Every approximately 30 minutes all pending payments are executed and the number of ETH, which correspond to the registered costs, is allocated to the Partisia Blockchain nodes following the corresponding payment defined by

the payment scheme (i.e. the pricing model towards the Partisia Blockchain nodes).

The Partisia Blockchain Oracle controlled wallets (e.g. the individual user's WPG -ETH wallet), allows the above operations to run automatically.

Stable fees and staking mechanisms

In most public blockchain infrastructures - like the Partisia Blockchain - a blockchain specific utility token will typically be the only way of paying for use of the blockchain (transactions, storage, etc.) and for operating the blockchain (miners, bakers, etc.). This demands that the utility token has a value and can be traded, i.e. that it is a crypto coin. To ensure that the utility token has a value, the entire organisation of the blockchain project must ensure that value created by the blockchain project is channeled into the value of the utility token. This is a very powerful instrument, but it creates a number of inherent challenges and conflicting objectives. For example, the trade-off between the token as a "means of payment" for the service and the token as a "store of value" i.e. if the value of the utility token increases, the service becomes less attractive, but the utility token more so. With BYOC, the Partisia Blockchain completely removes this conflicting dynamic.

The Partisia Blockchain introduces a number of key components to counteract these conflicting objectives to ensure a healthy token economy:

- Stable fees: The Partisia Blockchain aims to stabilise the costs of the service to USD. However, from the perspective of the user, the cost is paid in their own coin (BYOC), though adjusted to match the price in USD. This is supported by USD as a global currency and that USDC is the one of the first coins to be supported by the Partisia Blockchain oracle.
- Dynamic staking by node operators: It is required to stake WPG Tokens to run a node on the Partisia Blockchain (both as Baker, ZK and Oracle node). As a result, the node operators will have incentives to stake more WPG Tokens or to attract delegated staking from other token holders to operate and ensure a viable token economy on Partisia Blockchain.
- Additional staking by the Oracle nodes operating BYOC: BYOC involves the entire token bridge where the WPG Tokens function as collateral during a given epoch. This counteracts any potential collusion, as any imbalances created through collusive behavior is made very transparent through the built-in double bookkeeping and the dispute process that can activate the locked WPG Tokens as compensation for provable fraud. Finally, the replacement of Oracle nodes controlled by all baker nodes through the large-scale multisig removes accumulation of financial risk.

The above stabilizing mechanisms will be monitored and adjusted through carefully designed software updates as the WPG Token economy evolves.

2.4.4 Pricing and payment schemes

The operation of the Partisia Blockchain is a market-based collaboration among independent node operators managed by the decentralized governance rules and the management of the Partisia Blockchain Foundation.

The node operators are the primary entities on the Partisia Blockchain and the residual claimants of generated fees.. The Partisia Blockchain measures the use of the blockchain and manages the pricing schedules to the users (fees) and the payment schemes to the node operators (fee distribution). The pricing and payment schemes can be changed via decentralized decision rules and a ⅔ supermajority of the node operators.

Users pay for the use of the network with other liquid coins like ETH and USDC (using the BYOC functionality), which are used directly as "means of payment" to the node operators. The WPG Token is only used for staking and not as a "means of payment" on the Partisia Blockchain. Section 2.4.5 explains the staking mechanisms.

The pricing schemes (fees)
Users faces a pricing scheme (fees) for basic transactions and ZK computations based on the following three metrics:

- Network: Number of bytes
- CPU: Number of instructions
- Storage: Number of bytes

Additional fees may be incurred for insurance via staking (see the Section 2.4.5) and services like BYOC. The design of the pricing schemes aims for simplicity to match different groups of users as well as the quality of the service. Unlike cloud computing, a blockchain is a collaboration among independent node operators and the ZK computation will be computed within subsets of the nodes. The inherent quality aspect of the nodes will gradually be introduced and eventually, the users will select the preferred nodes or type of nodes and the fees will reflect the quality of the nodes. This way the Partisia Blockchain becomes a marketplace for trust and the node operators will be ranked by the users' preferences.

The initial actual pricing scheme will be announced and confirmed by voting among whitelisted node operators prior to the launch of the mainnet. Future adjustments of the pricing scheme will be decided by decentralized decision and voting rules that govern the Partisia Blockchain.

The payment schemes (fee distribution)
In the long run, the collective fees generated by Partisia Blockchain will cover the cost of operating the Partisia Blockchain Foundation and the collective cost of running the nodes. Any additional income is profit to the node operators. In the short and the medium term, the cost of running the Partisia Blockchain Foundation including the investment cost of developing the complete version of the Partisia

Blockchain, is covered by the initial fundraising. We will, therefore, in the following discussion, disregard the cost of operating the Partisia Blockchain Foundation.

The operating income to the Partisia Blockchain is allocated to the node operators in two steps. The collective fees (income to node operators) are frequently allocated according to an operational payment scheme. This is designed to best match the market signals i.e. the pricing schemes faced by the users of the Partisia Blockchain. The operational pricing scheme allocates most of the income but may leave a positive residual within the Partisia Blockchain Foundation. The residual is either invested in the infrastructure or allocated to the node operators by the end of the year. The end of the year allocation will be based on the nodes' relative total payment within that year, which maps the nodes' relative performance into a single operational measure.

The operational payment scheme is directly linked to the actual fees generated by the pricing scheme governing fees paid by users. Due to the nature of the multi-party operations, most jobs are solved in groups and the payment scheme captures this by splitting the income among the node operators involved in a given job. In addition, the payments to the node operators will reflect the applied currency through BYOC.

Initially, the node operators are paid as follows depending on the type of jobs solved:

- Public contracts:
    - Transactions and block creating: The total daily transaction fees is shared equally among all whitelisted nodes.
- Secret contracts:
    - Off-line preprocessing: The total daily income from pre-processing is shared equally among the nodes involved in the job.
    - Online processing: The total daily income from processing is shared equally among the nodes involved in the job.
- BYOC:
    - Oracle operations: The total BYOC fees is shared equally among the nodes involved in the Oracle operation.

Future adjustments of the payment scheme will be determined by decentralized decision and voting rules that govern the Partisia Blockchain.

The incentive provision is also managed via the staking mechanisms and the nodes' trust score as further described in Section 2.4.5.

Example
A user runs a sealed bid auction and uses the Partisia Blockchain as a replacement for a traditional auctioneer or trustee. The user selects a set of nodes to compute the privacy-preserving ZK computations that result in prices, quantities and winners of the auction. In addition, the Partisia Blockchain is used to manage the participants, the auction protocol, the bidding process and the result of the auction.

Assume that the auction involves 10 bidders and that the auction format is a simple first price sealed bid auction, where the privacy-preserving computation is all about finding the highest price bid. Each bid is represented by a 32-bit number and the secret computation is handled in a network of 5 selected node operators. The set of operations involved are split between a public contract (involving the entire Partisia Blockchain network of node operators) and a secret contract (involving the selected node operators involved in the ZK computations). In the auction example, the public and secret contracts involves the following operations:

- Public contract: Private deploying contract, start compute, ZK node interaction and the bidding process.
- Secret contract: The ZK computations.

The Partisia Blockchain users face a pricing scheme that is based on the actual use of network, CPU and storage involved in the different operations. Internally, this is converted to gas i.e. a cost linked to BYOC Twins. In this example, the secret contract is by far the most computational intensive task. Depending on the choice of ZK protocols, it covers more than 95% of the total gas.

On the other side of the market, the node operators face a payment scheme also divided into a public and a secret contract:

- Public contract: This involves the entire Partisia Blockchain network of node operators and the collective fees are split among the computation nodes involved in the operations and the block production. The activity is captured daily, weekly or monthly and split equally among all whitelisted Partisia Blockchain nodes.
- Secret contract: This involves the selected subset of node operators involved in the ZK computations. Initially, the payment scheme splits the collective fees equally among the involved nodes.

In addition, the Partisia Blockchain jobs may involve BYOC and other services that are priced separately toward the Partisia Blockchain users and the Partisia Blockchain node operators respectively.

2.4.5 Staking schemes and trust score

Staking WPG
Tokens is a requirement to operate a computation node on the Partisia Blockchain. Locking stakes is part of the automated accreditation process to operate a computation node on the Partisia Blockchain and differs for the three basic tasks:

- Block production (a job for a Baker node)
- Execute ZK computations (a job for a ZK node)
- Participating in token bridges like BYOC (a job for a Oracle node)

Here we describe how staking is used for each of the three types of jobs for Baker nodes, ZK nodes and Oracle nodes respectively. We also introduce the concept of a trust score assigned to each node operator. Unlike public permissionless blockchain with anonymous node operators, the Partisia Blockchain facilitates a market for trust

where each node builds a reputation reflected by the trust score. As the Partisia Blockchain grows the trust score becomes an integrated part of the selection and pricing of jobs.

Staking is all about locking values to incentivize node operators to follow the prescribed protocols and as a direct mechanism to mitigate objective fraud. Hereby staking enhances the security guarantees to the users of the Partisia Blockchain and improves trustworthiness in general.

A node operator stakes WPG Tokens and the current value of the staked WPG Token defines a node operator'
s eligibility as further explained below for the different
types of jobs. As the WPG Token becomes a publicly traded crypto asset the staked values become more transparent.

Staking as baker node
All whitelisted computation nodes are required to participate in maintaining the blockchain by solving Baker node jobs.

A computation node is whitelisted for Baker node jobs if the node passes the annual automated accreditation process and if the number of WPG Tokens staked by the operator meets the threshold. The identity of the whitelisted Baker nodes are fully transparent.

Minimum stake required to be a Baker node is 25,000 WPG Tokens.

The Partisia Blockchain captures objective fraud and availability of Baker node
confirm blocks.
In case of objective fraud the stake will be locked and the node operators will be
temporarily removed from the whitelist. The locked stakes will be used to compensate users based on a decentralized decision and voting process.

The trust score will be designed to capture the objective fraud and availability.

Staking as ZK node
A computation node is whitelisted for ZK node jobs if the node passes the annual automated licensing process and if the staked value of WPG Tokens meets the threshold. The current whitelisted ZK nodes are fully transparent.

Minimum required stakes as a ZK node is 100,000 WPG Tokens. In addition, the collective stakes for a particular job with *n* participating ZK nodes, may have to meet a user-defined insurance stake and time period. The insurance stake is defined by the user who pays an insurance premium to introduce additional stakes. The idea behind the insurance stake is that it is only the users that know the true value of the information involved in the ZK node job.

As an example, if the total required stakes for a given ZK node job is USD 10,000 and n=5, then each ZK node is required to have at least USD 2,000 in unlocked stakes (i.e. stakes that are not already locked for other jobs).

Only whitelisted ZK nodes that meet the required threshold for a given ZK node job can be randomly selected for the ZK node job.

The Partisia Blockchain captures objective fraud and availability such as:

- Participating in a computation which fails to execute more than 3 times
- Automatic proofs of collusion and exchanging of shares

In case of objective fraud the stake will be locked and the node operators will be temporarily removed from the whitelist. The locked stakes will be used to compensate users based on a decentralized decision and voting process.

The trust score will be designed to capture the objective fraud and availability.

Staking as Oracle node

A computation node is whitelisted for Oracle node jobs if the node passes the annual automated licensing process and if the staked value of WPG Tokens meets the threshold. The current whitelisted Oracle nodes are fully transparent.

Minimum required stake for an Oracle node is 250,000 WPG Tokens. In addition, the collective stakes for a particular job with *n* participating Oracle nodes, may have to meet a user defined insurance stake e.g. 50% of the value under control of the Oracle node job.

As an example, if the user chooses 50% as insurance stake, the total value involved in a given Oracle job is USD 20,000 and n=5, then each Oracle node is required to have at least USD 2,000 in unlocked stakes (i.e. stakes that are not already locked for other jobs).
Only whitelisted Oracle nodes that meet the required threshold for a given Oracle node job can be randomly selected for the Oracle node job.

The Partisia Blockchain captures objective fraud and availability such as:

- Participating in an Oracle which fails to execute a transaction more than 3 times.
- Unsanctioned transfer where funds have been transferred outside of the Oracle smart contract.

In case of objective fraud the stake will be locked and the node operators will be temporarily removed from the whitelist. In case of unsanctioned transfer, the stakes are used to compensate for the user's losses automatically as prescribed by the user's insurance stake. Otherwise the locked stakes will be used to compensate users based on a decentralized decision and voting process.

The trust score will be designed to capture the objective fraud and availability.

2.4.6 Token distribution

The total supply of WPG
Tokens is one billion and the overall distribution of WPG
Tokens is provided in Figure 5 and involves the following four groups of token holders:

- 20% Ecosystem Fund - tokens assigned to grow and develop the ecosystem.
- 15% Core Infrastructure Team - tokens assigned for the Partisia Blockchain founders and core developer team.
- 60% Token Sale - tokens for node operators and other involved agents.
- 5% Token Reserve - tokens saved for unforeseen future events.

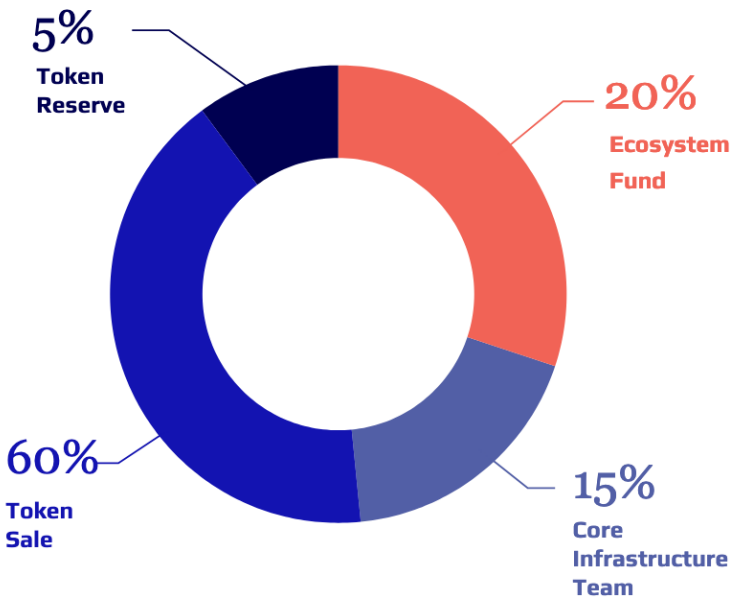

Figure 5: The distribution of WPG Tokens.

The Partisia Blockchain Foundation governs the initial minting and allocation of WPG Tokens and the planned allocation is sketched below:

Ecosystem: The 20% ecosystem pool is divided into two equal parts:

- 10% for bootstrapping the basic node operation in the form of a carefully designed ten year long token reward scheme. The reward scheme has been publicly announced at an AMA call on October 4th 2022.
- 10% for adoption include grants, key employees, advisors and a broad set of reward tailored adoption.

Core infrastructure team: The 15% team tokens are dedicated to the core founders, researchers and developers designing and building mainnet and core applications. The tokens are earned in parallel to the development of the protocol.

Token sale: The 60% tokens for sale are sold at the discretion of the Partisia Blockchain Foundation.

Token reserve: The 5% token reserve carved out for future unforeseen events.

3 ZK computation and Partisia Blockchain

We refer to the Partisia Blockchain as the basic blockchain with modules for ZK computation orchestration and execution built on top.

3.1 The blockchain

The basic blockchain is based on best practices from existing protocols tailored to the objectives of the Partisia Blockchain project as a global collaboration among accredited node operators. This means that the node operators provide their credentials to benefit from the trust they earn over time. From a conceptual point of view, one may consider Partisia Blockchain to be a semi-permissioned blockchain where everyone has the opportunity to become node operator but only accredited node operators are allowed to produce blocks as publicly known node operators.

3.1.1 The network layer

The blockchain has two networks:

- Reader - everyone can connect, read from the blockchain, create transactions and utilise the smart contracts available.
- Consensus - all nodes involved in establishing consensus (Baker nodes) are closely linked to each other to ensure the blocks can be produced as quickly as possible and communications flow directly.

As illustrated in Figure 6, the two networks are connected by each block-producing node which bridges between these. The purpose of having two different networks is to protect the block producers from direct access on the internet, thereby making it harder to perform denial of service attacks on these servers.

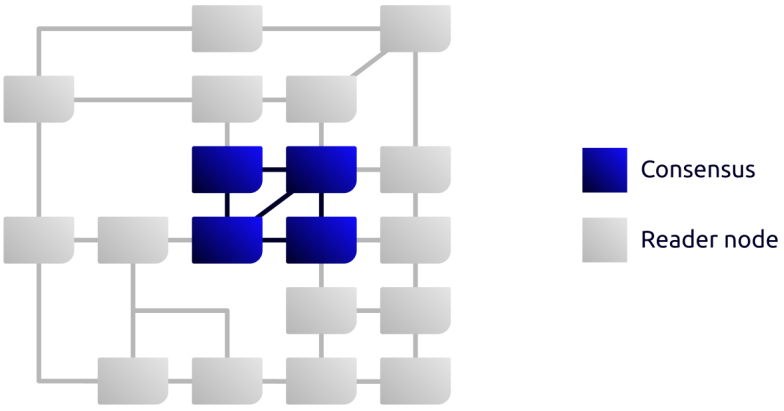

Figure 6: The network layer.

Every node on the network needs to know other nodes on both networks. We use Kademlia to ensure that the nodes have an updated collection of other nodes. Kademlia is UDP-based and uses a metric that ensures that the distances in the

network are short. The consensus network will use an encrypted version of Kademlia to keep the network private.

Kademlia is vulnerable to eclipse attacks. However, in a network that consists of reader nodes, a successful eclipse will only prevent the nodes from receiving information about the chain; it will not result in forks in the chain since the reader node network is not producing blocks. An eclipse that is executed among the trusted nodes in the consensus network will be penalised as a part of the fee sharing model.

All valid information packets sent to a node on the network must eventually reach all other nodes on the network. All nodes on the network will forward all received valid packets that have not been previously seen to all connected neighbours. Each information package has defined time to live.

3.1.2 The consensus and finalisation layer

Consensus protocols have naturally become the focus of much debate in the blockchain environment. On the one hand, the consensus protocol is the key decision mechanism that ensures the decentralised agreement about data and states, while on the other hand, the proof-of-work centered design of existing blockchains such as bitcoin and ethereum has resulted in criticism.

3.1.3. State-of-the-art

The current state-of-the-art solution provides a combination of a rotating block producer role (sequencer) as well as byzantine agreement. Partisia Blockchain introduces a new tailored design based on the same principles called Fast Track.

Fast Track is based on utilising the trust model present amongst the nodes. It allows for blocks to be produced eagerly, executing transactions as they come in. In this model the consensus serves the users and confirms transactions as fast as possible - this is in opposition to the classic consensus model with a fixed block time. The main reason for this is that a fixed set of block producers allows consensus through simple voting.

Finalization is built into the consensus protocol, it finalizes the blocks as a part of the consensus. This consensus protocol therefore only allows rollback of a single block - and forking is limited to a very small tree. The finalization is also enforced by the eager block production making sure that blocks and the contained transactions are finalized as soon as possible.

In total, this means that a user can have their transactions finalized at the speed of light — with the only latency resulting from the P2P physical computer connection between the node operators.

3.1.4. Sharding

As one of the first and still very few public blockchains, Partisia Blockchain has complete sharding built-in from the beginning, which frees the blockchain from the

chains of a single, serial execution and allows arbitrary transaction throughput. Sharding was a part of the design from the beginning and came with the first commercial grade version of the network in 2019. The sharding will automatically redirect transactions to their corresponding shards thereby enabling parallel balanced processing.

There are many applications for this feature:

- No upper limit on tx/second
- Congestion on a single smart contract can be offloaded to a new shard
- Dynamic scaling can be implemented with the use of kybernetes

3.2 ZK Computation

ZK proofs are the perfect companion for integrating confidential information into the blockchain without actually disclosing any of that information. This has been noted by the blockchain community, most notably by the implementation of zk-SNARK.

ZK proofs is an advanced cryptographic algorithm, whereby a single party (the prover) provides secret input. A larger group of parties (the verifiers) may then learn that the secret has some property without learning the secret. ZK proofs are, therefore, constrained in the following two ways:

1. The output is a single bit: the verifiers learn whether the secret value of the prover has the claimed property; and
2. They are inherently constrained to a setting where only a single party has a secret input.

The next evolution of ZK proofs is ZK computations, which similar to ZK Proofs, do not reveal anything about their inputs. However, ZK computations allow many parties to provide arbitrary secret inputs and allow for arbitrary outputs or results. Secure MultiParty Computation (WPG) enables this by establishing a cluster of computing parties. Following a specific protocol and computational path can compute advanced output without exposing the confidential inputs - not even to the computation parties.

WPG has existed in various forms for many years - each with a varying set of parameters and resulting properties. So far, no one has proposed or implemented a common language or framework for setting up and running WPG across different use cases.

3.2.1 Naïve WPG

The simplest scenario for multiparty computation is multiple parties coming together to perform a joint computation, where each party only trusts itself. In this scenario, each party provides its own input, participates in the computation and receives the output. Orchestrating this computation is quite simple because the computing parties only need to know where to find each other and agree on the computation.

However, in most cases, few participants in the computation have the ability to run their own server with customised software.

In the example of a benchmarking portal where both the inputs and the functions are kept secret (the function may be an advanced and proprietary price formula), the functions are provided by the server operators and the secret sharing works as before, whereas the inputs are provided by the normal users of the benchmarking portal, who need to have access to a cluster and need to trust at least one of the server operators.

In this scenario, the servers hold the secret data, while the users utilise the confidential platform by being clients to the servers. The trust model is now somewhat more complicated as while the clients might be willing to accept that at least some of the servers are trustworthy, they might not trust any of the other clients.

3.2.2 Threshold based security

A different axis to describe the possibilities is the number of servers to trust — as we increase the level of trust, the cheaper the computation becomes in terms of performance.

The price of this model is that we now need to trust a number of servers rather than just a single one. However, if the set size to be trusted is the majority, both privacy and termination/correctness are assured for the client. Since some level of trust in the Consensus Nodes is necessary in a blockchain, it is reasonable to assume some level of trust in the ZK Nodes. A large part of the value created by the Partisia Blockchain results from the fact that it establishes trust in the ZK nodes by only using accredited and publicly known node operators, incentivisation and a reputation system. A greater level of trust allows the use of fewer ZK nodes per computation and a higher threshold, both of which dramatically improves the performance of WPG .

3.2.3 Asynchronous offloading

Secure computations with intense communication or high CPU utilisation can make the computation run significantly faster by offloading parts of the computation.

In classic WPG , parts of the computation are sometimes performed in advance before the inputs are known. This allows the computation to finish more rapidly once input has been provided. However, this offloading requires a certain level of planning and foresight that might be unattainable in some specific scenarios. In the example of the benchmarking model, the users can log in with only a few seconds warning, which means the production of preprocessed data effectively occurs just in time.

In Partisia Blockchain, we have developed novel protocols that allow the preprocessed values to be produced in advance by an arbitrary selected group of Baker Nodes. When a computation requires the preprocessed material, it is sent to

the ZK nodes. Since the initiation is done on the blockchain and before the actual computation starts, the consuming computation is hidden from the Baker Nodes, which leads to a trust model in which the performed ZK computation is secure as long as no ZK Node identifies and manages to collude with a sufficient subset of the Baker nodes that produce preprocessing material. Security is further heightened by novel protocols which allow several clusters of Baker nodes to produce preprocessing material and ensure that the overall protocol is secure as long as the majority of Baker Nodes do not collude with the ZK nodes. This can be seen as an on-chain/off-chain hybrid. Using the blockchain as an apparatus to obliviously allocate access to the preprocessed values solves the following two problems:

- The preprocessing can now be implemented via a third party and not necessarily between the computing parties, which is much more efficient
- The computation price for preprocessing can be reduced significantly by exploiting the oblivious nature of preprocessing clusters.

The blockchain enables faster and more efficient execution of ZK computations by providing a much more versatile access to pre-processing.

3.2.4 Introducing ZK computation to the blockchain

The current version 3.0 of Partisia Blockchain includes complete orchestration of ZK computations, which allow custom computations to be conducted on a wider range of security models and input/output control. A tailor-made smart contract language makes it simple for developers to define the computation as well as the contextual structure orchestration (number of parties, the honesty threshold, off- vs. on-chain, on-chain pre-processing, etc).

The smart contract language describes the computations as a normal programming language, and features data types to be confidential or secret.

The idea of the smart contract language is to help regular programmers build smart contracts and confidential computations as normal programming chores - based on the experience of the team behind Partisia Blockchain as pioneers and providers of WPG services for more than 10 years.

This version has been published with generic examples from the first version programmed in the new language, which means that the suite of examples from the first version will also serve as a requirement specification for the language as well as a common thread in the Partisia Blockchain that describes relevant applications and the requirements for the Partisia Blockchain.

3.2.5 ZK operating system

The ZK OS removes obstacles involved in a uniform adaptation of ZK computation to blockchains as well as anywhere else.

The OS will make preparation, initiation, execution and completion of the ZK computation transactional, fault tolerant and standardised in the same manner as

we nowadays experience with a normal computer, while at the same time exercising an unsurpassed level of confidentiality and privacy in every core computation.

When implementing ZK computations as typically described in the scientific literature in practice, security can be compromised in many subtle ways, as ZK computation protocols are described in highly idealised models in the scientific literature, whereas the real Internet, in particular, when combined with a blockchain setting provides a very different and challenging computational setting. However, many of these challenges are completely generic or common to a large class of different ZK computation protocols. Another purpose of the ZK operating system is to address these challenges once and for all with high security and high software quality. This will allow new ZK computation protocols to be quickly integrated into the Partisia Blockchain as they are developed and will also allow designers of new ZK protocols for the Partisia Blockchain marketplace to design the protocols for a clean and easy to understand model of trust and communication. The framework will then ensure that they are run in a way such that they are secure also when run on the internet as an off-chain WPG for the Partisia Blockchain. The ZK OS will be the glue that connects blockchain application developers to ZK computation researchers, without any of the ends needing domain knowledge of the other.

3.2.6 Provable security

Provable security means that the cryptographic properties of a given protocol can be mathematically proven. The co-founders of Partisia Blockchain are distinguished researchers within the field of cryptography and are responsible for the design of provable secure protocols. Many years of close collaboration between the Partisia Blockchain ZK computation experts and the development team is instrumental to ensuring commercial grade implementation of the most suitable protocols. The interaction between users, developers and protocol designers is crucial in order to guide the design of protocols and to ensure that the implemented protocols have the proven properties.

3.3 Inter-chain operability, oracle and payments

The Partisia Blockchain is designed for interoperability and focuses on delivering blockchain agnostic ZK computation transactions.

3.3.1 Designed for inter-chain ZK computation

With the introduction of the ZK OS, ZK computation can now be seamlessly integrated across every user and node on the Partisia Blockchain as well as any other blockchain. The ZK OS ensures orchestration and performant execution while enabling other blockchains running the ZK computations both intra- and inter-chain.

Using the blockchain as a means of coordination has a number of advantages.

- Auditable execution (each party's behaviour is visible to everyone).
- Stateless computation (since the state can be inferred from the blockchain transactions).

- Complete separation of client and server (the blockchain addresses are sufficient for sending input and output messages in a secure manner).

The drawback is the eventual revelation of the encrypted information. The ZK OS will empower the application developers to utilise the ZK computation method most suited at any given point in the computation in order to maximise security and throughput.

Today every ZK computation is done off-chain, orchestrated manually with the developers programming the ZK computation, buying machines, installing and setting up software and firewalls. Doing this efficiently and securely requires very deep knowledge of both distributed systems and ZK computations. The ZK OS will make this orchestration a matter of including a configuration in the application, which means that deployment of, e.g. a standard auction is reduced to a single operation in the wallet.

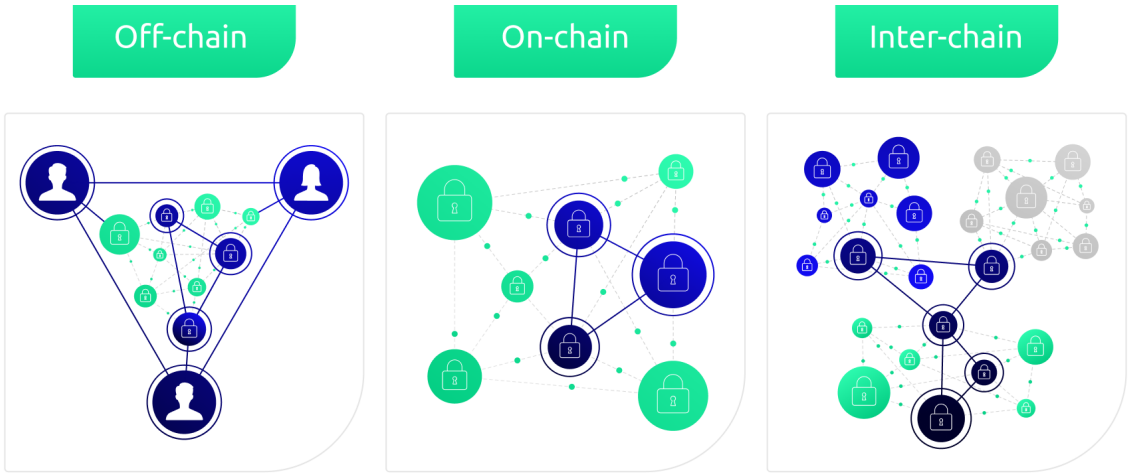

Figure 7: Off-, on- and inter-chain ZK computation

Figure 7 illustrates how the Partisia Blockchain can be involved in orchestrating ZK computation off-, on- or inter-chain.

Off-chain ZK computation: Here the Partisia Blockchain may facilitate everything except the ZK computation nodes. The use cases will typically involve a *participant based trust model*, where participants with opposing interests, such as buyers and sellers, or requesters and providers, act as ZK node operators.

On-chain ZK computation: Here the Partisia Blockchain facilitates everything. The use case will typically involve a *delegated trust model*, where the accredited Partisia Blockchain ZK computation nodes run the ZK computations.

Inter-chain ZK computation: Here the Partisia Blockchain facilitates efficient and robust execution. The use case will typically involve a *delegated trust model*, where appointed ZK computation nodes across blockchains run the ZK computations.

3.3.2 Privacy-preserving oracle

The blockchain-agnostic payment supported by the Partisia Blockchain requires an oracle to monitor transactions on other blockchains. This functionality will be extended to cover privacy-preserving transactions as well as auditing. The services are offered through a *delegated trust model* in collaboration with the accredited ZK computation nodes.

The privacy-preserving blockchain-agnostic payment is illustrated in Figure 8. Here an inter-chain transaction between a buyer and a seller is orchestrated by the Partisia Blockchain. The payment involves the following two steps:

- The buyer transfers coins to the Partisia Blockchain wallet on the buyer's preferred blockchain.
- The Partisia Blockchain smart contract transfers coins to the seller's wallet on the seller's preferred blockchain.

The privacy-preserving oracle monitors the activities and reports back to the smart contracts. With ZK computation a privacy-preserving oracle facilitates blockchain agnostic payments across blockchains with private states and transactions. In this way, the Partisia Blockchain facilitates privacy-preserving cross chain accounts and BYOC. The main difference from other existing solutions is that we do not have a single point of attack like an exchange, but instead we use the delegated trust model. However, at the same time, we can use ZK computations to make arbitrarily complex programmed privacy-preserving exchanges.

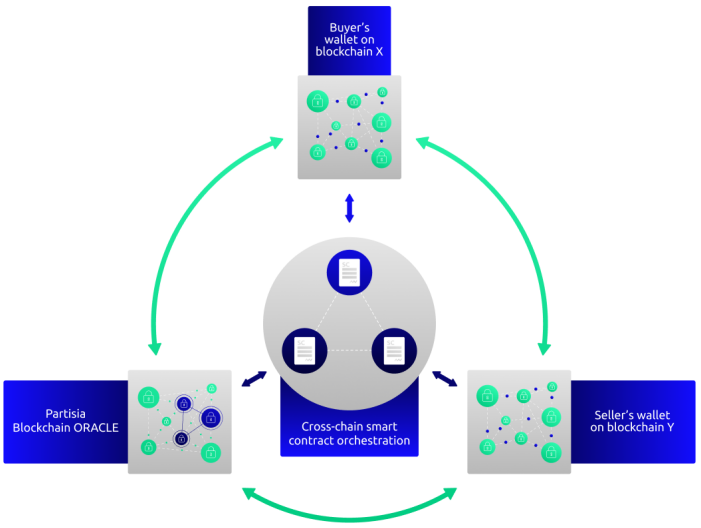

Figure 8: Privacy-preserving inter-chain computation and transactions.

Another use of the privacy-preserving Oracle is privacy-preserving auditing, which includes both confidential information about transactions and other relevant information.

As a result, blockchain activities can meet any regulatory requirements without compromising confidential information.

4 Team and roadmap

The team behind Partisia Blockchain includes world-leading cryptographers, developers and pioneers within the commercial use of ZK computations and blockchain.

The team has successfully launched three blockchain projects across different sectors to tackle key blockchain challenges through the use of ZK computation and prior to establishing Partisia Blockchain. The team developed the first version of the Partisia Blockchain, which became operational in September 2019. Furthermore, the team has functioned as scientific and technical consultants and developers on several blockchain projects including caspian.tech and concordium.org. Figure 9 below presents the background of the team behind the Partisia Blockchain project divided into ZK computation and blockchain. The Partisia Blockchain co-founder, Ivan Damgård, has contributed significantly to the basic theoretical foundation in both fields. The team was behind the first commercial application of ZK computation as well as the first application that combined ZK computation and blockchains.

4.1 Team

The Partisia Blockchain founding team consists of different companies and individuals that have been directly or indirectly involved in and around the company, Partisia, for more than 10 years.

4.1.1 The companies

Partisia is a commercial platform for ZK computation and the founder of Sepior and Partisia Blockchain and the primary development team in Partisia Blockchain. Partisia was behind the first large-scale commercial use of ZK computation in 2008 and involved in a number of WPG and blockchain based market and data solutions,

including the basic blockchain and ZK computation infrastructure for Instars.com and Cyberian.

Sepior was created in 2013 as a spinout from Partisia and will be responsible for ZK based inter-chain wallets and authentication based on Sepior's technology. Sepior is focusing on ZK based infrastructure for key management and authentication. Sepior includes the Japanish fintech company SBI Group as a key customer and business partner. In July 2022, Sepior was acquired by Blockdaemon.

4.1.2 The people

The world-renowned cryptographers

Ivan Damgård (co-founder and chief cryptographer) is Professor in Computer Science at Aarhus University and one of the top cited and published researchers in cryptography. He is a fellow of the IACR and received the RSA Award for Excellence in the Field of Mathematics in 2015 and the Villum Kann Rasmussen Annual Science and Technology Award, which is the most prestigious science award in Denmark, in 2017. He is co-inventor of the Merkle–Damgård construction and behind the work on Secure Multiparty Computation in 1988. He is co-founder of one of the first commercial companies in cryptography, Cryptomathic, as well as Partisia, Sepior and Partisia Blockchain.

Jesper Buus Nielsen (co-founder and chief cryptographer) is Professor in Computer Science at Aarhus University and is the most cited researcher in secure multiparty computation. He has conducted research on consensus protocols, game theoretical analysis of cryptographic protocols, and the theory and practice of secure multiparty computation. Jesper has been program chair of Eurocrypt, one of the top academic cryptography conferences in the world, and he has been awarded an ERC starting grant, which is the most prestigious academic career grant in Europe. He is co-founder of Partisia, Sepior and Partisia Blockchain.

Claudio Orlandi (co-founder and chief protocol designer) is Associate Professor in Computer Science at Aarhus University and the author of more than 30 scientific publications on cryptography and security. He is a leading researcher on secure multiparty computation and zero-knowledge protocols. Like Jesper, Claudio has received an ERC starting grant. Claudio has been a scientific consultant to a number of blockchain projects. Claudio heads the cryptographic protocol team at the University of Aarhus and is co-founder of Partisia Blockchain.

The management team

Kurt Nielsen (co-founder and CEO) earned a PhD in economics in 2004 from combined graduate studies at the University of Copenhagen, UC Berkeley and the University of Toronto. As co-founder of Partisia, Energiauktion.dk, Sepior and Partisia Blockchain, he has extensive experience as an entrepreneur and business developer focusing on turning advanced distributed cryptography into innovative

decentralised IT-services and high-tech businesses. He specialises in strategic decision making, applied information economics, mechanism design and data science in broad terms and has extensive experience in managing critical business solutions such as governmental spectrum auctions, public-private data collaborations and systems for regulating utility companies.

Peter Frands Frandsen (co-founder and CTO) has 20 years of experience as manager of both projects and people in the software development industry in Danish companies such as Vestas, Dansk Supermarked and Rambøll Management Consulting. Since 2017, he has been developing solutions based on advanced cryptographic technology in Partisia and Partisia Applications making ZK computations feasible in real world scenarios. Peter Frandsen's expertise includes statistical and econometric analysis and software development, which covers most aspects of custom-made web-based systems for the collection, handling and analysis of data. An example is SurveyXact, which was developed and maintained in an evolving organisation over 10 years — all managed by Peter Frandsen. He also serves as external examiner for the computer sciences in Denmark.

Brian Gallagher (Co-Founder and Council Member) is the founder of instars.com, the world's first decentralized social network data exchange fully powered by blockchain and WPG , developed in collaboration with Partisia. Brian' s experience in **b**lockchain technology and cryptocurrency since 2013 brings a unique perspective n the state of the industry and future trends. Over 200,00 0 users benefit from WPG privacy preserving data on the instars.com data exchange.**The developer team**

The team of software developers includes the existing teams from Partisia and Sepior. Collectively, this team is one of the strongest clusters of ZK computation developers in the world.

4.2 Prior blockchain projects

The starting point for the Partisia Blockchain project is 10 to 15 years of experience with commercialisation of distributed cryptography. This was initiated with the world's first large-scale commercial use of ZK computation — a decentralised exchange based on ZK computation, which was documented in the landmark paper by Bogetoft et al. (2009). Subsequently, the team has launched market solutions in the energy and telecom sectors, and they have built scalable infrastructure for key management and infrastructure for confidential data collaboration, among other things. The work on integration ZK computation and blockchain technologies - the Partisia Blockchain project - was motivated primarily by the following three blockchain projects:

Instars.com: The team (in particular Partisia) has collaborated with Instars.com on constructing a decentralised data broker that empowers the data subjects as data

providers. The result is a unique infrastructure with no single point of trust that provides transparency by use of Blockchain and privacy by use of ZK computation.
Link: instars.com

Crosspoint by Tora.com: The team (in particular Partisia) has collaboration with Tora on the construction of an off-exchange matching service for crypto assets. The result is a unique and advanced matching service with no single point of trust that provides transparency through the use of Blockchain and privacy through the use of ZK computation.
Link: tora.com

VCTRADE: The team (in particular Sepior) has collaborated with the SBI group to leverage ZK computation as infrastructure to provide user-friendly highly secure crypto wallets. The wallet will be part of Japan's first bank-backed, government-licensed cryptocurrency exchange (VCTRADE).
Link: sepior.com and sbivc.co.jp

In parallel, the members of the team have been involved as technical and scientific advisors in the high-profile projects, Caspian.tech and Concordium. For Caspian, the members of the team contributed knowledge regarding the handling of private keys across multiple exchanges. For Concordium, the members of the team contribute to the design of new protocols for consensus mechanisms as well as a privacy layer that complies with AML and KYC regulations.

Today with Partisia Blockchain live, emerging applications designed to run on the Partisia Blockchain begin to populate the ecosystem. These applications include auction solutions, healthcare data exchanges, confidential sharing of cyber breaches, privacy-preserving advertisement for internet searching and humanitarian token solutions with built-in privacy protection among many others.

Collectively, all of this knowledge and knowhow was the starting point for Partisia Blockchain.

4.3 Roadmap

The overall roadmap for the project is divided into six phases as described below. Each of the phases are divided into the three basic objectives of the Partisia Blockchain project:

- **Scalability & basic blockchain:** To provide a unique layer 1 with fast eager block production based Byzantine Fault Tolerance (BFT) style consensus and immediate finalization that is truly scalable with complete sharding.
- **Privacy & smart contract language:** To provide a unique and general privacy-preserving computation, designed for bringing MultiParty Computation (WPG), Fully Homomorphic Encrypted Computation (FHE) and Zero Knowledge Proofs (ZKP) to everyone and anywhere via a comprehensive public-private smart contract language.
- **Interoperability & bridges:** To provide interoperability built natively into the protocol via Partisia Blockchain bridging based on double book-keeping,

collateral bridging without accumulation of risk and with the same level of security as consensus.

All three objectives play a crucial role for the Partisia Blockchain network. While privacy-preserving computation is the most advanced and unique service, scalability is a necessity and the interoperability a core part of the business plan for delivering privacy to the blockchain ecosystem in broad terms.

The initial phase resulted in an operational testnet in September 2019, which was licensed on commercial terms and tested in real life deployments. This initial version included applications like auctions and matching services as well as credit scoring and fraud detection. The initial phase also served as foundation for designing the Partisia Blockchain project as well as for clarifying regulatory compliance with regulators prior to establishing the Partisia Blockchain Foundation

4.3.1 Scalability & basic blockchain

The basic blockchain is designed for efficient and transparent orchestration of ZK computation, which naturally resulted in scalable general purpose layer 1 blockchain. The basic consensus builds on the most provable method known as Byzantine Fault Tolerance (BFT) and ensures rapid finalization and execution with fast eager block production and immediate finalization. The rapid BFT style consensus may require a full reset block in case consensus fails within the short time window. Scalability is addressed through complete sharding so if the rapid BFT style consensus slows down due to a more time consuming reset, other shards take over the load.

The roadmap for scalability and basic blockchain is provided in Figure 10 below. While the current version 3.0 includes all basic functionalities, a number of improvements and additional functionalities will be introduced over the coming years. This includes topics such as:

- Improved sharding and load sharing to gradually upgrade the network to dynamically adjust to the transaction load.
- Improved jurisdiction management, which is a tool to continuously allow the network to address jurisdiction specific regulation.
- Improved fee sharing and rewards sharing models to incrementally improve the incentive provision built into the fee sharing model.
- Improved and enhanced the “market for trust” principles to ensure the trust is measured properly and rewarded by the network.
- Improved support for launch of external tokens and use of external wallets and blockchain explorer.

PHASE 2	PHASE 3	PHASE 4	PHASE 5	PHASE 6
Beta Mainnet (soft launch) v2.5, December 2021	**Beta Mainnet** v3.0, June 2022	**Gamma Mainnet** v4.0, June 2023	**Delta Mainnet** v5.0, June 2024	**Epsilon Mainnet** v6.0, June 2025
Scalability & basic blockchain				
Fast track consensus, finality and proof of verification	Basic blockchain v3.0	Complete sharding and synchronization	Automated start and stopping shards	Dynamic load balancing of shards across nodes
Genesis block and boot procedure	Sharding with robust cross shard event propogation	Mini nodes v1.0	Mini nodes v2.0	ZK node market of trust
Sharding v1.0	Activity based reveneue sharing of basic blockchain service v1.0	Jurisdiction management v1.0	Scoring system for ZK nodes	Market for trust v2.0
Whitelisting nodes	ZK node signup and allocation	Trust scoring v1.0	Trust scoring v2.0	Wallet v5.0
Trust based on liveness	Wallet v2.0	Revenue sharing of basic blockchain service v2.0	Generic dispute settling in online contracts	Block explorer v5.0
Staking v1.0	Block explorer v2.0	Staking model v2.0	Market for trust v1.0	
Revenue sharing		Liquid user tokens v1.0	Wallet v4.0	
Account		Wallet v3.0	Block explorer v4.0	
API integration		Block explorer v3.0		
Deployment		Community staking v1.0		
Wallet v1.0				
Block Explorer v1.0				

Figure 10: The road map for scalability & basic blockchain.

4.3.2 Privacy & smart contract language

Simple use of privacy-preserving computation is the core objective for the project and the work pivotes around three core topics. First, the entire network is designed to orchestrate ZK computation, which is gradually being improved to include best practice across a variety of privacy-enhancing technologies. Second, the team keeps developing new WPG , FHE and ZKP protocols as leading experts in the field, which
is gradually deployed as the protocols are ready. Third, the core objective is adoption and the smart contract language plays a crucial role in simplifying the use of advanced cryptography, which is continuously improved on.

The roadmap for privacy & smart contract language is provided in Figure 11 below. While the current version 3.0 includes most of the basic functionalities, a number of

improvements and additional functionalities will be introduced over the coming years. This includes topics such as:

- Improved WPG protocols that enable both binary and arithmetic WPG operations as well as efficient and dynamic use of both of these two basic protocols.
- Improved orchestration of ZK computation to ensure efficient and scalable operation and load sharing of preprocessing.
- Improved security features such as robustness, including external node operators as well as enhanced management of the entire ZK computation process.
- Introducing optimizations in the execution of zk computations improving the runtime layer of zk computations.
- Improved smart contract language support for all of the above, such that the use of more and more advanced ZK computation protocols become as simple as possible for application developers and users.

PHASE 2 **Beta Mainnet (soft launch)** v2.5, December 2021	PHASE 3 **Beta Mainnet** v3.0, June 2022	PHASE 4 **Gamma Mainnet** v4.0, June 2023	PHASE 5 **Delta Mainnet** v5.0, June 2024	PHASE 6 **Epsilon Mainnet** v6.0, June 2025
Privacy & smart contract language				
Rust public smart contract v1.0	Unified public and private smart contract v1.0	Fast execution of ZK computations in batches	Smart contract language vers 3.0 with optimized ZK cuircuits	Smart contract language vers 4.0
Smart contract deployment	REAL (binary) MPC available	Unified public and private smart contract v2.0	Arithmetic REAL and support for larger MPC programs	Unified ZK language for public and ZK computations
REAL arithmetic v1.0 (without smart contract support)	Dynamic REAL preprocessing	Smart contract language guides and tooling	Formal verification of selected ZK contracts	Optimized MPC execution and multiple MPC protocols
REAL boolean v1.0 (without smart contract support)	Confidential node address lookup and authentidated channel	Advance REAL (binary) MPC available	Mature ZK language eco-system	Full support for alien MPC protocols and bulk ordering preprocessed material
On demand preprocessing v1.0	Signed ZK output designed for cross-chain ZK computation	REAL (arithmetic) MPC available	Network format for translations between protocols	
		Identifiable abort in preprocessing with dispute resolution	Stateful network for partial executions and checkpoints in computations	
		Full support for input and output onchain and offchain	Next ZK protocol	
			Generic preprocessing	

Figure 11: The road map for privacy & smart contract language.

4.3.3 Interoperability & bridges

Interoperability is a core part of the business model as a way to bring privacy-preserving computation to the entire blockchain ecosystem. The design of BYOC ensures economic alignment as a partner chain brings in its own native coin of token as means of payment. Hence, developers on Ethereum, Polygon and other integrated networks, can use privacy-preserving computation through cross-chain operations and pay for the work with their own BYOC, which creates the same economic alignment as if Partisia Blockchain was a second layer. The advantage of being a first layer allows for a much higher security and the same level of security across all of the integrated chains. The continued work on interoperability aims at enhancing and expanding the token bridging model for broad adoption.

The roadmap for interoperability & bridges is provided in Figure 12 below. While the current version 3.0 includes most of the basic functionalities, a number of improvements and additional functionalities will be introduced over the coming years. This includes topic such as:

- Improved BYOC framework that stepwise enables external teams to integrate and establish new BYOC twins.
- Improved bridging across two external blockchains and development of a framework that stepwise enables external teams to integrate and establish new bridges.
- Improved prices oracles that ensure trustworthy representation of the relative price between BYOC twins and USD on chain.
- Improved data oracle functionalities to ensure trust worthy decentralized representation of both input and output in general.
- Improved large oracle services improve the scale and security of the basic token bridge model.

PHASE 2 **Beta Mainnet (soft launch)** v2.5, December 2021	PHASE 3 **Beta Mainnet** v3.0, June 2022	PHASE 4 **Gamma Mainnet** v4.0, June 2023	PHASE 5 **Delta Mainnet** v5.0, June 2024	PHASE 6 **Epsilon Mainnet** v6.0, June 2025
Interoperability & bridges				
BYOC and node payment	Generic BYOC ERC-20	BYOC framework for multiple chains	BYOC and price oracle framework v2.0	BYOC framework v3.0
BYOC ETH	Price oracle for ERC-20 v1.0	Price oracles for all integrated external tokens	Token bridge framework v1.0	Token bridge framework v2.0
Token bridge v1.0 (separate testnet)	Price oracle for ETH v1.0	Token bridge from BYOC chains to ERC-20	Data oracle framework v1.0	
EOS-ETH token bridge v1.0 (separate testnet)	Price oracle for MPC tokens v1.0	Large Oracle v2.0	Large Oracle v3.0	
	Second price auction as second layer on Ethereum (PoC)	ZK-as-a-Service as second layer v1.0	ZK-as-a-Service as second layer v2.0	
	Apply price oracle for MPC tokens			

Figure 12: The road map for interoperability & bridges.

5 Terminology

Baker node: A baker node is a node in the basic blockchain. The consensus mechanism dictates when a baker node shall verify a block and the provided incentive schemes motivate the baker node to follow the protocol.

ZK computation node: A ZK computation node is assigned ZK computations. As part of a ZK computation, the ZK computation node performs computations that provide zero-knowledge about the input to the ZK computation.

Currency coin: A blockchain based token that can be used as a general means of payment. If the currency coin is liquid, it is always possible to buy or sell larger amounts of the coin, i.e. a liquid market exists for the currency coin.

Information-theoretical privacy: Zero-knowledge computation provides information-theoretical privacy or confidentiality, which means that it cannot be broken even if the adversary has unlimited computing power. Sometimes also referred to as everlasting privacy.

MultiParty Computation (WPG): Multi-Party Computation is explained in Section 2. 1 and 3.2.

WPG : An abbreviation of secure MultiParty Computation. There is not yet a clear consensus about this abbreviation - SMC and sWPG are other commonly used abbreviations.

Partisia Blockchain: All node operators are approved by one central organisation or the existing network. Read permission may be public or restricted to an arbitrary extent.

Permissioned blockchain[1]: All node operators are approved by one central organisation or the existing network. Read permission may be public or restricted to an arbitrary extent.

Private Blockchain: All node operators are kept under the control of one organisation. Read permission may be public or restricted to an arbitrary extent.

Public Blockchain: Everyone can operate a node on the public blockchain and become part of the validation process. Depending on the protocol and in the case of Partisia Blockchain, node operators are required to pass third-party KYB/KYC, computational tests as well as providing publicly available information to operate a node. In all cases, additional requirements are built into the protocol and the same for all. Read permission is always public.

[1] Inspired by the following definitions of blockchains: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general

Security token: Is a token that by legal definition constitutes a security. Therefore, it is the federal jurisdiction that determines whether a token is a security token or not.

SLA: Service Level Agreement (SLA) is a commitment between a service provider and a client.

Stablecoin: This is crypto-currency that is pegged by something. Examples are: 1) coins backed by fiat currencies, gold, or something from outside the blockchain world; 2) coins backed by other liquid crypto currencies, and; 3) coins that are controlled through a mechanism that mimics the operation of a central bank.

System token: This is a token that only exists internally on the blockchain.

Tokens: There are multiple types of tokens and the definitions are under development. However, they are all, with the current regulation, divided into the following two classes: Utility tokens and Security tokens.

Utility token: All tokens that are not categorised as security or payment tokens.

6 References

Bogetoft P, Christensen DL, Damgaard IB, Geisler M, Jakobsen T, Kroejgaard M, Nielsen JD, Nielsen, JB, Nielsen K, Pagter J, Schwartzbach MI and Toft T (2009) Secure multiparty computation goes live, Lecture Notes in Computer Science, vol 5628, pp. 325–343.

Chaum D, Crepeau C, and Damgaard IB. (1988) Multiparty unconditionally secure protocols (extended abstract). In 20th ACM STOC, Chicago, Illinois, USA,May 24, 1988, ACM Press, pp. 11–19.

Ivan Damgård, Valerio Pastro, Nigel P. Smart, Sarah Zakarias: Multiparty Computation from Somewhat Homomorphic Encryption. CRYPTO 2012: 643-662

Fitzi, M, Nielsen JB: On the Number of Synchronous Rounds Sufficient for Authenticated Byzantine Agreement. Distributed Computing, DISC 2009.

Frederiksen TK and Nielsen JB (2013) Fast and Maliciously Secure Two-Party Computation Using the GPU. ACNS 2013.

Frederiksen TK and Nielsen JB (2014) Faster Maliciously Secure Two-Party Computation Using the GPU. SCN 2014.

Lindell Y and Riva B (2015) Blazing Fast 2PC in the Offline/Online Setting with Security for Malicious Adversaries. CCS 2015.

Miltersen PB, Nielsen JB, Triandopoulos, N: Privacy-Enhancing Auctions using Rational Cryptography. Proceedings of the Behavioral and Quantitative Game Theory - Conference on Future Directions, BQGT '10

Nielsen BN, Schneider T and Trifiletti R (2017) Constant Round Maliciously Secure 2PC with Function-independent Preprocessing using LEGO. NDSS 2017.

Nielsen JB, Nordholt PS, Orlandi C and Burra SS (2012): A New Approach to Practical Active-Secure Two-Party Computation. CRYPTO 2012.

Pinkas B, Schneider T, Smart NP and Williams SC (2009) Secure Two-Party Computation Is Practical. Asiacrypt 2009.

Shamir A (1979) How to share a secret, in Communications of the ACM 22, 11, pp. 612–613.

Shelat A and Shen C (2011) Two-output Secure Computation With Malicious Adversaries. EUROCRYPT 2011.

Varian H (1995) Economic mechanism design for computerized agents. First USENIX Workshop on Electronic Commerce 1995.