Partisia Blockchain

White Paper Version 1.06
18th March 2021

Partisia Blockchain

A WEB 3.0 public blockchain built with MPC for trust,transparency, privacy and *speed of light finalization*

Confidential © 2021 Partisia Blockchain™

Table of contents

1. Introduction 2

2. Introducing Partisia Blockchain 5

2.1. ZK computations and Blockchains 5
2.1.1. ZK computation protocols 6
2.1.2. Trust models and ZK computation nodes 9
2.1.3. The complementary blockchain 10
2.2. The problems to be solved by Partisia Blockchain 11
2.3. The Partisia Blockchain solution 13
2.4. Organisation, nodes and tokens 15
2.4.1. License to operate a computation node 18
2.4.2. Organising the node operators 20
2.4.3. Bring Your Own Coin (BYOC) and the MPC Token 21
2.4.4. Pricing and payment schemes 25
2.4.5. Staking schemes and trust score 30
2.4.6. Token distribution 33

3. ZK computation and Partisia Blockchain 34

3.1. The blockchain 34
3.1.1. The network layer 35
3.1.2. The consensus and finalisation layer 36
3.1.3. State-of-the-art 37
3.1.4. Sharding 37
3.2. ZK Computation 38
3.2.1. Naïve MPC 38
3.2.2. Threshold based security 39
3.2.3. Asynchronous offloading 40
3.2.4. Introducing ZK computation to the blockchain 41
3.2.5. ZK operating system 41
3.2.6. Provable security 42
3.3. Inter-chain operability, oracle and payments 43
3.3.1. Designed for inter-chain ZK computation 43
3.3.2. Privacy-preserving oracle 45

4. Team and roadmap 46

4.1. Team 47
4.1.1. The companies 48
4.1.2. The people 48
4.2. Existing blockchain projects 50
4.3. Roadmap 51

5. Terminology 56

6. References 58

Confidential © 2021 Partisia Blockchain™

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. The Partisia Blockchain is a public permissioned blockchain that functions as a transparent and structured platform for ZK computation and as a vehicle for organising accredited trustees to further strengthen the blockchain ecosystem. The team behind Partisia Blockchain represents world-leading cryptographers and pioneers within the commercial use of ZK computations.

The global comprehensive digitalisation of most parts of our local and global society emphasises the 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 encompass 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).

While the present best practices provide the first important candidates for a secure blockchain infrastructure, one of the most critical trade-offs 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 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.

Confidential © 2021 Partisia Blockchain™

1. Introduction

However, a ZK proof is limited to a single party (the prover) entering secret input to compute either true or false, which is very useful for simple operations such as confirming a private transaction. Any collaborative solutions that involve more parties require ZK computations thatsupport generic privacy-preserving computations.

The team behind Partisia Blockchain is one of the most experienced teams in ZK computations, from the initial mathematical proofs in 1988 to the first real-life large scale and commercial use in 2008, which marks the starting point for the past 10 years' collective effort 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 years have resulted in protocols and frameworks that have reduced the computational overhead by 1/1.000.000 and, not least, 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 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 the 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 the prime offering is an unprecedented blockchain agnostic platform for provable secure privacy, it also opens up for a number of direct extensions. The prime extension is privacy-preserving Oracle functionality, which is used to orchestrate inter-chain transactions independent of the coins used and/or privacy-preserving auditing of inter-chain transactions, among other things.

Confidential © 2021 Partisia Blockchain™

1. Introduction

The privacy offered by the Partisia Blockchain makes it possible to tailor the Oracle functionality to regulatory requirements. Hereby, Partisia Blockchain can function as a regulatory compliant privacy layer to existing large and small blockchains like Bitcoin and specialised blockchains like instars.com. To fully support these collaborative synergies Partisia Blockchain is designed entirely for Bring Your Own Coin (BYOC) i.e. all use of Partisia Blockchain is paid for with the users' own liquid coins such as BTC and ETH.

The Partisia Blockchain Oracle manages BYOC and internal system tokens represent BYOC. The first version of the Partisia Blockchain Oracle is tailored BTC and ETH and will gradually be extended to cover other tokens. The MPC Token is only used for staking and for incentivizing the Partisia Blockchain computation nodes.
The realisation of the Partisia Blockchain has unique infrastructure, which combines a number of key components such as:

- *A state-of-the-art high performance public permissioned blockchain with sharding, eager block producing and pure finality.*
- *Infrastructure for privacy preserving orchestration and auditing.*
- *Orchestrating working on a number of ZK computation protocols tailored to different use cases.*
- *A framework for efficient and robust communication and processing of ZK computations.*
- *A framework for tailored secure preprocessing material as fuel for efficient ZK computations.*

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. In parallel, a number of applications designed to run on the Partisia Blockchain are currently being developed, which include three auction solutions and a public-private healthcare data exchange.

Confidential © 2021 Partisia Blockchain™

2. Introducing Partisia Blockchain

Partisia Blockchain builds more secure digital infrastructure by merging blockchains and ZK computations in a collaborative fashion. By focusing on privacy and interoperability, the Partisia Blockchain project will initially focus on the following three goals:

- *Orchestrating ZK computations as transparent, efficient and simple as possible.*
- *Offering blockchain agnostic ZK computations.*
- *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 not. ZK computation is secure multiparty computation and similar techniques such as ZK proofs and 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 reduced 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).

Confidential © 2021 Partisia Blockchain™

2.1. ZK computations and Blockchains

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. 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).

Recent applications include basic infrastructure such as key management for crypto wallets (delivered by the Partisia Blockchain project partner Sepior and SBI Holding), off-exchange matching (delivered by the Partisia Blockchain project partner Partisia and Tora) and Data brokerage (delivered by the Partisia Blockchain project partners Partisia and Instars.com). Also, a number of applications designed to run on the Partisia Blockchain are currently being developed - including three auction solutions and a public-private healthcare data exchange.

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.

Confidential © 2021 Partisia Blockchain™

2.1.1. ZK computation protocols

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.*

Confidential © 2021 Partisia Blockchain™

2.1.1. ZK computation protocols

- *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 a 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 marketplace for ZK computation protocols as a broad international collaboration. The Partisia Blockchain team will continuously design and customise ZK computation systems to ensure that they meet customers' security needs and performance guarantees.

Confidential © 2021 Partisia Blockchain™

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 Insights Network 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 input parties involved make up the trust model - the likely opposing interest 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. The Crosspoint.io application is an example of this, where a potential large number of buyers and sellers match orders. This requires a trust model that does not rely on all participants as they all would be granted a veto to block the system. Although the participants could operate the ZK nodes themselves in a threshold model with fault tolerance, for practical reasons, 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.*

It may also be a mix of trust models that naturally involves the participants and trust models that are delegated to a network of trustees with, e.g. 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

Confidential © 2021 Partisia Blockchain™

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 applied types of market mechanisms used across all industries. An auction is a well-defined set of trading rules that typically include 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 ideal infrastructure for auctions, so why combine it with blockchains? On the one hand, blockchain provides 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 handle secret information on a blockchain that is accessible to the public. The core problem is that encrypted information is basically not suited to blockchains. The reason for this is that the encrypted information is freely available on the distributed ledger, but at some point in the future, the 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 at all times.

Confidential © 2021 Partisia Blockchain™

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 was on auctions, subsequent work has 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 - Insights Network - 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 - is another example where a group of buyers and sellers match confidential orders.

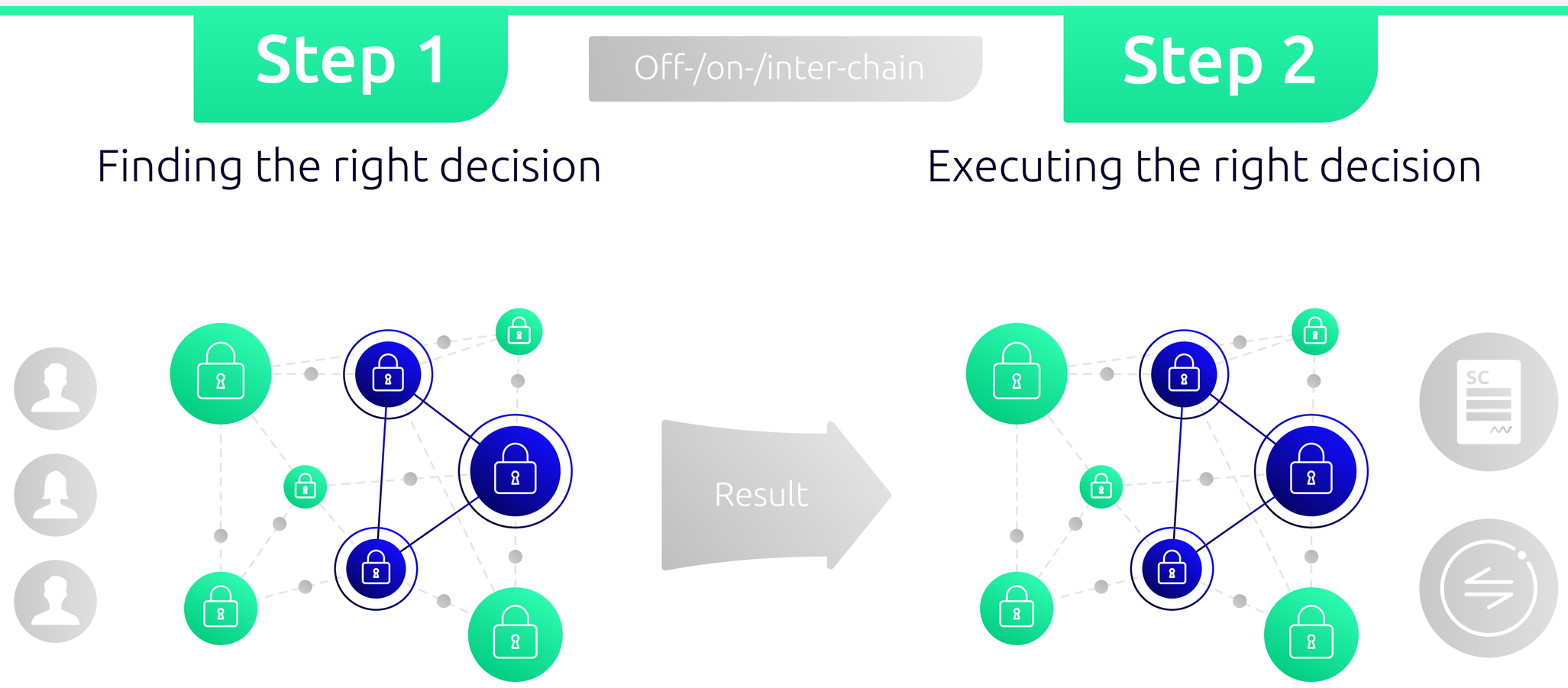

Figure 1: A generic use case

Confidential © 2021 Partisia Blockchain™

2.2. The problems to be solved by Partisia Blockchain

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 are used outside their 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.

Confidential © 2021 Partisia Blockchain™

2.2. The problems to be solved by Partisia Blockchain

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.

While Partisia Blockchain is designed to safeguard confidential information on blockchains, the infrastructure cannot be a vehicle for fraudulent behaviour and activities. To ensure this, every account on the blockchain will have a persona or other legal entity as counterpart and every transaction will be accountable and attributable to a real person or other legal entity.

2.3. The Partisia Blockchain solution

The backbone of the Partisia Blockchain solution is the Partisia Blockchain, which facilitates global collaboration between accredited ZK computation 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* emphasise these two basic sets of elements of the Partisia Blockchain solution.

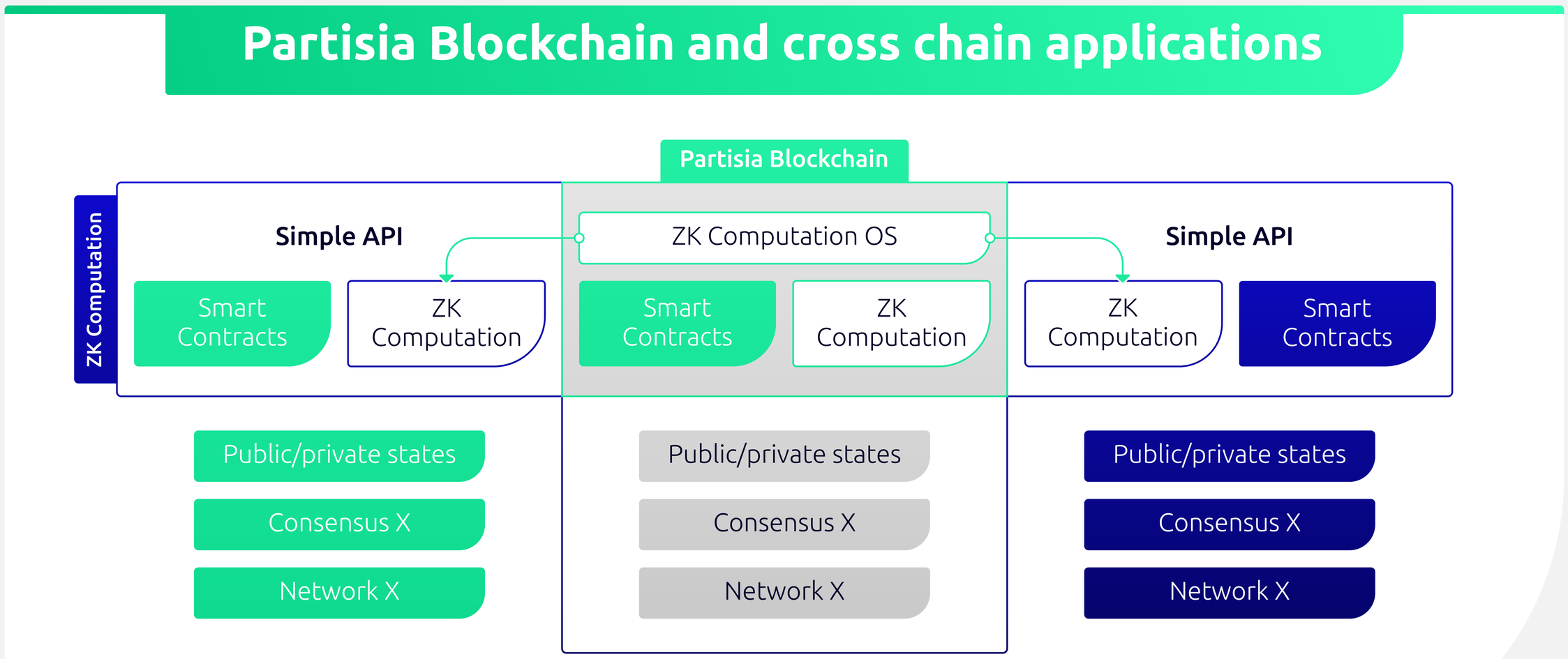

Figure 2: The basic Partisia Blockchain architecture and approach to blockchain agnostic ZK computation

Confidential © 2021 Partisia Blockchain™

2.3. The Partisia Blockchain solution

Partisia Blockchain

Partisia Blockchain is a fully functional permissioned 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 two distinct jobs:

- *The baker jobs: The ZK 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: The ZK nodes are assigned to ZK computations on a job-by-job basis.*

All node operators must pass rigorous due diligence to become accredited node operators and further motivated through carefully designed incentive contracts.

Blockchain agnostic ZK computation

ZK computation is delivered through ZK computation modules that are tailored to the partner blockchain. The partner blockchain can choose to run the ZK computations from its own blockchain or utilise the services offered by the Partisia Blockchain to make ZK computation simpler, more efficient and robust.

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 privacy-preserving oracle, which is used to orchestrate a transaction across different blockchains and coins.

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.

Confidential © 2021 Partisia Blockchain™

2.3. The Partisia Blockchain solution

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 will be transferred and governed exclusively by a Swiss foundation. The Partisia Blockchain Foundation will become the legal entity and basis for the decentralized organisation that will ensure the long term existence of the Partisia Blockchain. The Partisia Blockchain Foundation structure combines best practice from several existing blockchain projects and the decision rules and incentive provision of all stakeholders, from the users, node operators to developers, will gradually be developed.

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 the use with any liquid coin/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 MPC Token economy.

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

Confidential © 2021 Partisia Blockchain™

2.4. Organisation, nodes and tokens

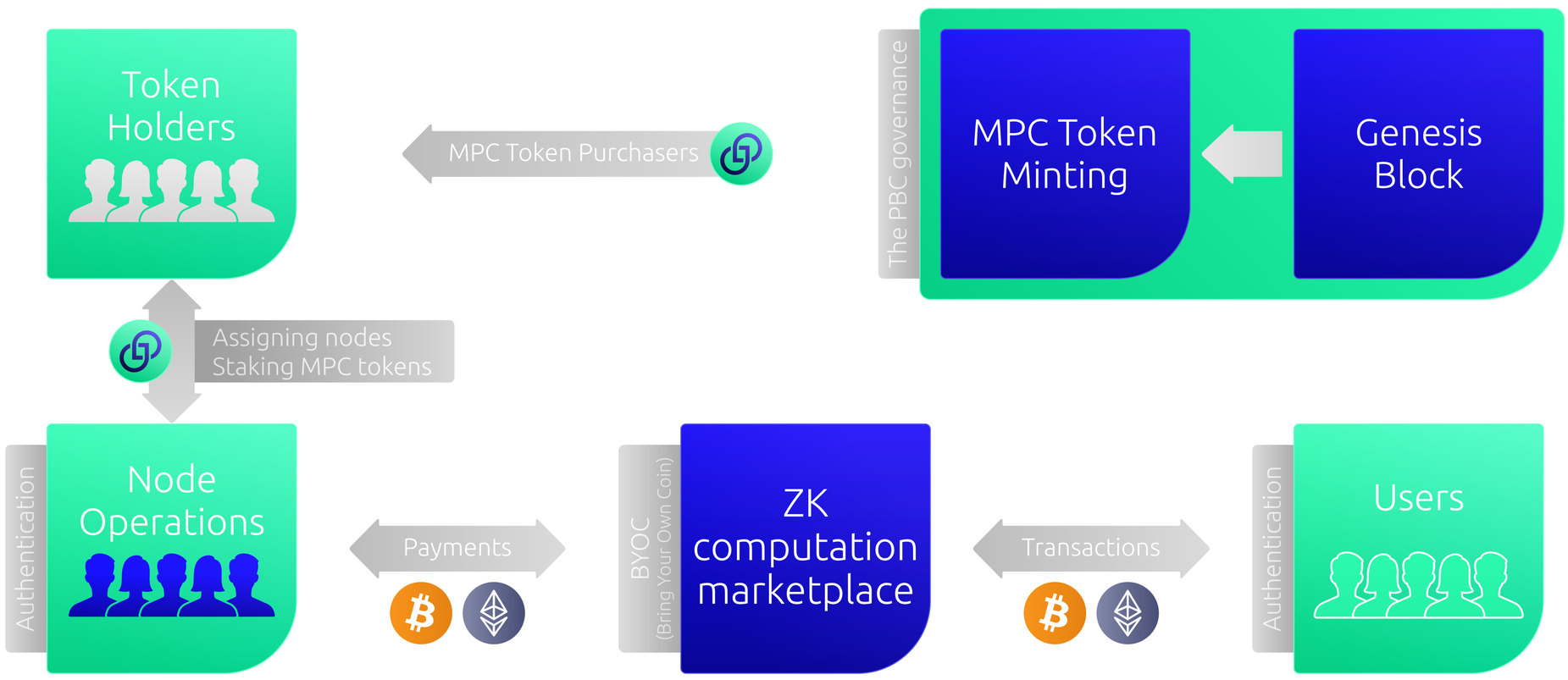

Figure 3: The basic component in MPC Token economy and compliance

Users/services/community

The Partisia Blockchain will establish a community for users, service providers, other blockchains and developers.

To meet the highest compliance standards, all users on the Partisia Blockchain need to pass KYC/AML requirements either on the Partisia Blockchain or through an accredited third party. The level of involvement in the Partisia Blockchain defines the requirements.

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.

Confidential © 2021 Partisia Blockchain™

2.4. Organisation, nodes and tokens

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 permissioned 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 the prescribed Partisia Blockchain KYC/AML requirements as part of the process of becoming accredited node operators, as well as attest the ability to professionally run IT-services (in this case the node). Node operators are also required to dynamically stake MPC Tokens as part of the incentive schemes.

The Partisia Blockchain governance

The Partisia Blockchain will be governed by the Partisia Blockchain Foundation similar to the foundations that govern projects like Ethereum, Cardano, Dfinity and many other blockchain projects as well as decentralized mechanisms.

The Partisia Blockchain Foundation manages the project including the development agreements, the creation of tokens, the sale of tokens.

The decentralized mechanisms manage the Partisia Blockchain through decentralized incentives, regulation and voting mechanisms such as:

- *Node operators are approved and whitelisted to operate a node through an automated vetting process. The license to operate 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.***

Confidential © 2021 Partisia Blockchain™

2.4.1. License to operate a computation node

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

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

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

Baker Node

Block production is a necessity for the blockchain to work and for the node operators to make an income. Where the actual computations are simple, it poses requirements for backup. The role as block producing node, does not involve the handling of confidential information on the Partisia Blockchain as such, Baker nodes do, however, play a central role by verifying the results from certain Oracle operations.

Incentives: All node operators are expected to operate as bakers and are required to stake MPC Tokens to become a baker. The payment as baker is the basic income as node operator.

Decentralized regulation: All potential node operators can apply for a license to operate and get whitelisted as a Baker Node through an automated vetting process.

ZK Node

Executing the ZK computations is significantly more involved. The executions will saturate the network on the server as well as requiring 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 MPC Tokens to enter the market for ZK computation. The payment as ZK node is additional income as node operator.

Confidential © 2021 Partisia Blockchain™

2.4.1. License to operate a computation node

Decentralized regulation: All potential ZK Node operators can apply for a license to operate and get whitelisted as a ZK Node through an automated vetting process. A successful vetting will also include a license to operate a Baker Node.

Oracle Node

Maintaining the secret state for the cross chain wallets requires monitoring the states of the governing smart contracts on both chains and react 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 MPC Tokens staked and the liability towards the users of the Oracle as input.

Incentives: Nodes running the Oracle are required to further stake MPC Tokens. The payment for operating the Oracle is set a priori by the Partisia Blockchain. The payment from operating the Oracle is additional income as node operator.

Decentralized regulation: All potential Oracle Node operators can apply for a license to operate and get whitelisted as a Oracle Node through an automated vetting process. A successful vetting will also include a license to operate a Baker Node.

Whitelisting and Exclusion

All approved Baker, ZK and Oracle Nodes are whitelisted and the automatic vetting process is renewed yearly. The license 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.

Confidential © 2021 Partisia Blockchain™

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 allow 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. 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 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.

Confidential © 2021 Partisia Blockchain™

2.4.2. Organising the node operators

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 KYC/AML 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 MPC Token

The Partisia Blockchain is designed to accept any liquid crypto coin as payment for the Partisia Blockchain services via inter-chain payments i.e. Bring Your Own Coin (BYOC). BYOC makes the Partisia Blockchain highly collaborative.

First we describe the mechanics behind BYOC and second we describe incentive provision through so-called staking mechanisms.

Bring Your Own Coin (BYOC)

Partisia Blockchain provides seamless integration with other blockchains through a cross chain account that facilitates Bring Your Own Coin (BYOC). The user experience is that BYOC allows a user to pay for Partisia Blockchain services with another liquid coin such as BTC.

Figure 4 shows the flow of tokens involved in using BYOC with BTC. A user with a private BTC wallet creates a user account on Partisia Blockchain. As part of the account creation the user chooses BYOC with BTC. Now the user automatically gets a new private BTC wallet managed by the Partisia Blockchain oracle and the Partisia Blockchain node operators.

Confidential © 2021 Partisia Blockchain™

2.4.3. Bring Your Own Coin (BYOC) and the MPC Token

This is called a MPC-BTC wallet and it can only be managed by the user through the Partisia Blockchain or automatically by the smart contracts that make up the cross chain account i.e. the Partisia Blockchain oracle. Apart from this, the MPC-BTC wallet is a standard BTC wallet.

Now if the user transfers BTC to the MPC-BTC wallet, the Partisia Blockchain oracle registers the transfer and updates the user's Partisia Blockchain account accordingly. With tokens in the user's MPC-BTC wallet the user can start using the Partisia Blockchain. The used gas is deducted from the user's account and registered on the node operators accounts according to the payment scheme. The finalization of these payments is automatically done periodically, e.g. daily, and transfer BTC to the node operators MPC-BTC wallets. This finalizes the payment and the collective user experience is limited to depositing BTC to the user's private MPC-BTC wallet.
For this to work the private key to the user's MPC-BTC wallet is managed by the Partisia Blockchain node operators using state-of-the-art threshold cryptography by Sepior.com. The configuration may require e.g. 7 node operators and at least 4 node operators to access the private key. This ensures a high degree of redundancy and at least 4 corrupt node operators to misuse the wallet.

To further strengthen BYOC and counteract any potential collusion, the following two set of addition mechanisms are introduced:

- *Selection and rotation mechanism: Based on a user's preferences, a protocol selects a subset of Partisia Blockchain nodes out of the total set of eligible Partisia Blockchain nodes. An example could be that a user deselect Partisia Blockchain nodes based on jurisdiction. The Selected Partisia Blockchain nodes are allocated BYOC jobs following a rotation scheme with random replacement. This makes it very difficult for a potential corrupt ring of Partisia Blockchain nodes to collude.*
- *Staking mechanism: To further counteract any potential collusion, the node operators are required to stake MPC Token to operate a node and participate in incentive schemes that reward BYOC and punish collusive behaviour. For instance, if a wallet controlled by the oracle has been compromised, then the involved nodes get their stakes frozen for the duration of the pending investigation.*

Confidential © 2021 Partisia Blockchain™

2.4.3. Bring Your Own Coin (BYOC) and the MPC Token

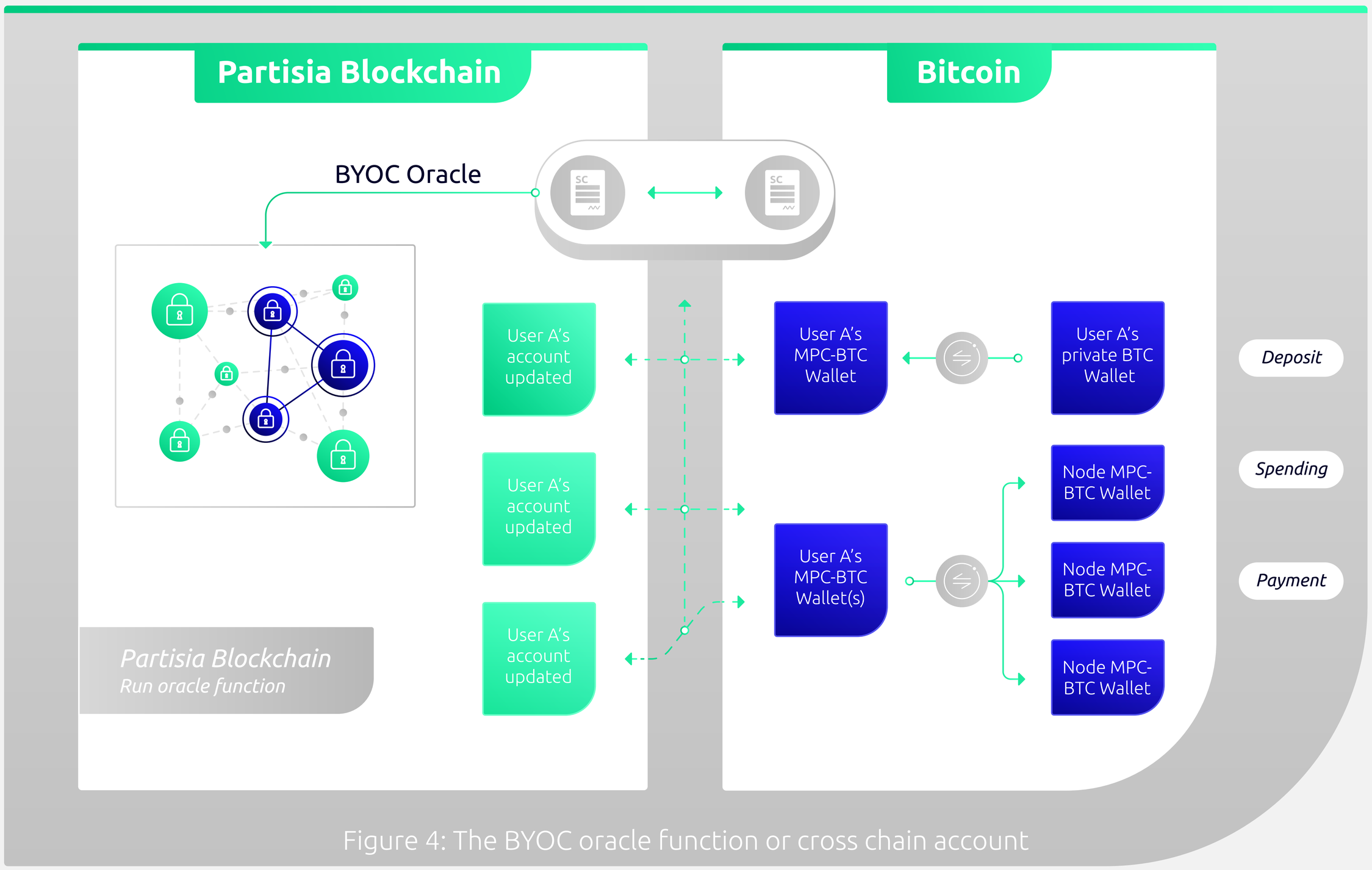

Figure 4: The BYOC oracle function or cross chain account

Internally, BYOC is represented by MPC gas or system tokens on the Partisia Blockchain, which represent the BYOC 1 to 1, such as:

- *In case of BYOC = BTC: MPC gas is MPC-BTC tokens (MPC-BTC = BTC 1:1)*
- *In case of BYOC = ETH: MPC gas is MPC-ETH tokens (MPC-ETH = ETH 1:1)*

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

- *A user transfer BYOC (say BTC) into an oracle controlled wallet (say MPC-BTC wallet)*
- *The user's Partisia Blockchain account now contains the number of MPC-BTC tokens corresponding to the BTC in the user's MPC-BTC wallet (MPC-BTC = BTC 1:1).*
- *The user uses MPC-BTC tokens to run public and private smart contracts.*
- *The pricing scheme (i.e. the pricing model towards the Partisia Blockchain users) for using Partisia Blockchain determines the prices towards the users.*

Confidential © 2021 Partisia Blockchain™

2.4.3. Bring Your Own Coin (BYOC) and the MPC Token

- *The actual costs are calculated and MPC-BTC 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 MPC-BTC tokens are allocated and registered at the corresponding Partisia Blockchain nodes accounts (registered as pending payment).*
- *Every fixed time period (e.g. daily or hourly) all pending payments are executed and the number of BTC, 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 MPC-BTC wallet), allows the above operations to run automatically.

Stabilizing 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 channelised into the value of the utility token. This is a very powerful instrument, but it involves 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.

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

- *Fixing the price of use: The Partisia Blockchain aims to stabilise the price of the service to the price of BTC. However, from the perspective of the user, the cost is paid in their own coin, though adjusted to match the price in BTC. This is supported by BTC as the most dominating crypto currency and that BTC is the first coin to be supported by the Partisia Blockchain oracle.*

Confidential © 2021 Partisia Blockchain™

2.4.3. Bring Your Own Coin (BYOC) and the MPC Token

- *Dynamic staking by node operators: It is required to stake MPC Tokens to run a node on the Partisia Blockchain (as Baker and as ZK node). Hereby, the node operators will have to invest in MPC Tokens to gain a license to operate and consequently assess economic viability of the Partisia Blockchain.*
- *Additional staking by node operators to operate BYOC: BYOC involves distributed handling of private keys for the cross chain wallets e.g. the MPC-BTC wallets. To counteract any potential collusion, the node operators engaged in running the BYOC jobs are required to further stake MPC Tokens as a limited guarantee for losses in case of unauthorized use of the cross chain wallet. This will punish collusive behavior but also introduce guarantees known from traditional banks in case of e.g. bankruptcy.*

The above stabilizing mechanisms will be governed and adjusted by the Partisia Blockchain Foundation as the MPC Token economy evolves and the introduction of MPC Tokens will be carefully managed.

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 the net operating income to the Partisia Blockchain. The Partisia Blockchain measures the use of the blockchain and manages the pricing schemes to the users (fees) and the payment schemes to the node operators (payments). The pricing and payment schemes can be changed via decentralized decision rules.

Users pay for the use with other liquide coins like BTC and ETH (using the BYOC functionality), which are used directly as means of payment to the node operators. The MPC Token is only used for staking and as a means of payment on the Partisia Blockchain. *Section 2.4.5* explains the staking mechanisms.

Confidential © 2021 Partisia Blockchain™

2.4.4. Pricing and payment schemes

The pricing schemes (fees)

The 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*

as well as fees 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 main net. Future adjustments of the pricing scheme will be decided by decision and voting rules that govern the Partisia Blockchain Foundation.

The payment schemes (payments)

In the long run, the operating income to the Partisia Blockchain should 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 run, 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 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. On a daily basis, the income is 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.

Confidential © 2021 Partisia Blockchain™

2.4.4. Pricing and payment schemes

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 income generated by the users' pricing scheme. 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 decided by decision and voting rules that govern the Partisia Blockchain Foundation.

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 results 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.

Confidential © 2021 Partisia Blockchain™

2.4.4. Pricing and payment schemes

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 income generated by the users' pricing scheme. 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 decided by decision and voting rules that govern the Partisia Blockchain Foundation.

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 results 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.

Confidential © 2021 Partisia Blockchain™

2.4.4. Pricing and payment schemes

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 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 MPC gas i.e. a cost linked to BTC. In the concrete 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 MPC 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 revenue is 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 revenue 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.

Confidential © 2021 Partisia Blockchain™

2.4.5. Staking schemes and trust score

Staking is a pre-requirement to operate a computation node on the Partisia Blockchain. Locking stakes is part of the automated process of getting a license 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 the 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 (coins) 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 MPC Tokens and the current value of the staked MPC Token defines a node operator's eligibility as further explained below for the different types of jobs. As the MPC 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 licensing process and if the staked value of MPC Tokens meet the threshold. The current whitelisted Baker nodes are fully transparent.

Minimum required stakes as Baker node is USD 10,000.

Confidential © 2021 Partisia Blockchain™

2.4.5. Staking schemes and trust score

The Partisia Blockchain captures objective fraud and availability such as:

- *Participating more than 5 times in a consensus committee which to 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 MPC Tokens meet the threshold. The current whitelisted ZK nodes are fully transparent.

Minimum required stakes as ZK node is USD 25,000. In addition, the collective stakes for a particular job with n participating ZK nodes, need 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.

Confidential © 2021 Partisia Blockchain™

2.4.5. Staking schemes and trust score

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 MPC Tokens meet the threshold. The current whitelisted Oracle nodes are fully transparent.

Minimum required stakes as Oracle node is USD 100,000. In addition, the collective stakes for a particular job with n participating Oracle nodes, need 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.

Confidential © 2021 Partisia Blockchain™

2.4.6. Token distribution

The overall distribution of MPC Tokens is provided in ***Figure 5*** and involve 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 stakeholders.*
- *5% Token Reserve - tokens saved for unforeseen future events.*

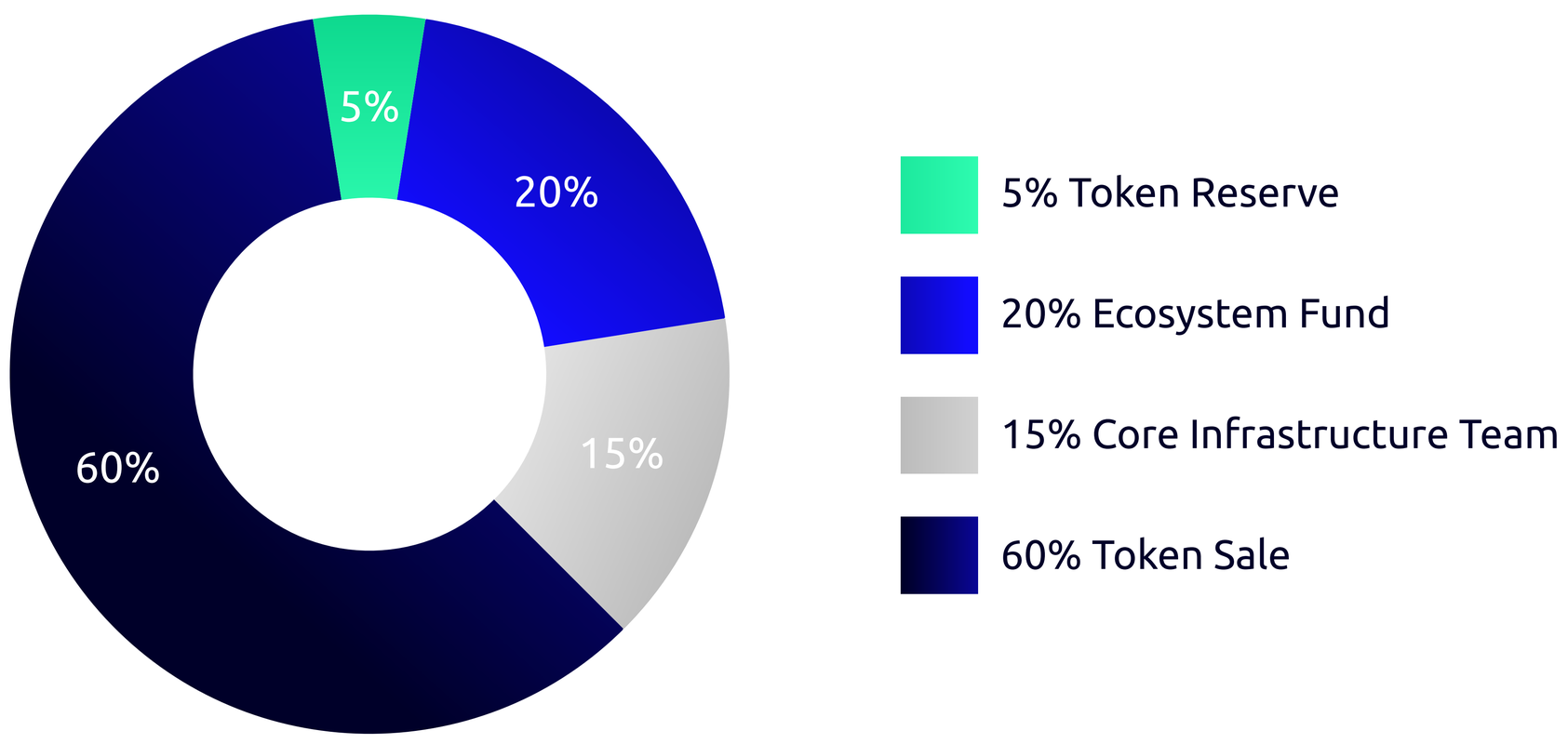

Figure 5: The distribution of MPC Tokens

The planned minting and allocation of MPC Tokens will occur in stages as sketched below:

Stage 1: *The first approximately 10% of the total token supply (as part of the Developer Ecosystem share) will be minted to motivate the initial node operators who assist in the bootstrap of the network. Each of the initial node operators will have the ability to claim reward of their share of the total token supply on a monthly basis, for up to four years. If the initial node operators stop operations during the first four years, the remaining unclaimed MPC Token rewards will be recycled back into the Developer Ecosystem pool or self destructed.*

Confidential © 2021 Partisia Blockchain™

2.4.6. Token distribution

Stage 2: *The next 10% of the total token supply (as part of the Token Sale share) will be minted and released to pre-sale token purchasers. The first use cases available to pre-sale purchasers include the ability to power and stake their own nodes and get rewarded as node operator. At* ***Stage 2****, the payment schemes sketch in* ***Section 2.4.4*** *will be introduced.*

Stage 3: *Following the pre-sale of 10% of the token supply in* ***Stage 2****, the remaining 35% of the total token supply will be available for sale orchestrated by the Partisia Blockchain Foundation. At this time the 15% of the token supply allocated to the core infrastructure team, will be minted and used to incentivize the core team development over the first 5 years at the discretion of the Partisia Blockchain Foundation. The remaining 20% of tokens in the Developer Ecosystem pool as well as the 10% token reserve will be minted over time at the discretion of the Partisia Blockchain Foundation.*

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. Since the node operators provide their credentials to profit from the entailed trust, the public blockchain is built on these parties as both baker nodes and participants in the ZK computations. This means that the Partisia Blockchain is a semi-permissioned blockchain and every node that is allowed to produce blocks is known at any given time.

Confidential © 2021 Partisia Blockchain™

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 (i.e. block producering 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 public access, thereby making it harder to perform denial of service attacks on these servers.*

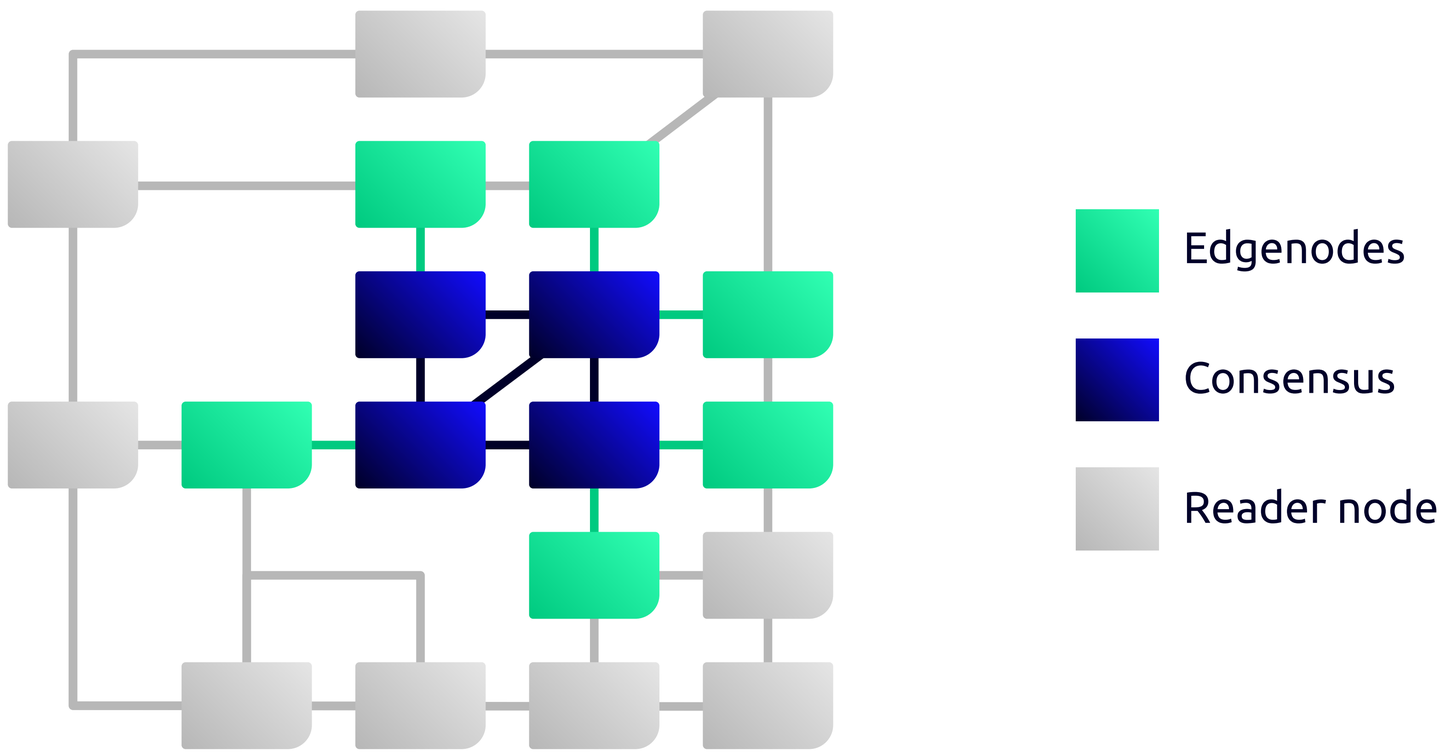

Figure 6: The network layer

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.

Confidential © 2021 Partisia Blockchain™

3.1.1. The network layer

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 only the block producing network is producing blocks. An eclipse that is executed among the trusted nodes in the consensus network will be penalised as a part of the revenue model.

All valid 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 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 decentralisation feature, while on the other hand, the proof of work aspect of the design of existing blockchains such as bitcoin and ethereum has resulted in criticism. We intend to allow multiple consensus protocols, while the consensus layer in the blockchain will be modular and interchangeable.

The two simplest protocols are probably Sequencer and Round-robin, which have already been implemented. Both of these protocols produce blocks that are final by definition.

Confidential © 2021 Partisia Blockchain™

3.1.3. State-of-the-art

The current state-of-the-art solution provides a combination of the sequencer as well as byzantine agreement, this protocol is designed tailored to this public blockchain and is called Fast Track

It 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 - being the latency from the users computer to the block producers.

3.1.4. Sharding

Current development entails support for sharding, this will free the blockchain from the chains of a single, serial execution and allow arbitrary transaction throughput. The sharding will automatic 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*

The first version of the mainnet will include sharding.

Confidential © 2021 Partisia Blockchain™

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:

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

The next level of ZK proofs is ZK computations, which are computations that in a somewhat similar way do not reveal anything about their inputs. However, ZK computations allow several parties to provide secret input, while the outputs can be larger values depending arbitrarily on all the secret inputs. Secure MultiParty Computation (MPC) 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.

MPC 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 MPC across different use cases.

3.2.1. Naïve MPC

The simplest scenario 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.

Confidential © 2021 Partisia Blockchain™

3.2.1. Naïve MPC

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 numbers 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 permissioned nodes, 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 MPC.

Confidential © 2021 Partisia Blockchain™

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 MPC, 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 then 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 acted as the Trusted Dealer.

Security is further heightened by novel protocols which allow several clusters of Baker nodes to act as Trusted Dealers 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 trusted dealer can now be implemented via a third party and not necessarily between the computing parties, which is much more efficient*
- *The computation price for the trusted dealer can be reduced significantly by exploiting the oblivious nature of the trusted dealer*

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

Confidential © 2021 Partisia Blockchain™

3.2.4. Introducing ZK computation to the blockchain

The first version will include a set of fixed zero knowledge computations which showcase the different aspects and potential of ZK computations on a blockchain, as described above. The computations will be examples based on the work already completed on actual blockchain projects.

The next version will most prominently feature, which will allow custom computations to be conducted on a wider range of security models and input/output control. This will be enabled through a tailormade language that describes 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 language will describe the computations as a normal programming language, although this programming language will feature new constructs of simple types being confidential or secret.

The idea of the programming 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 MPC services for more than 10 years.

This version will be 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

Confidential © 2021 Partisia Blockchain™

3.2.5. ZK operating system

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 MPC 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 customers, 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.

Confidential © 2021 Partisia Blockchain™

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.

Confidential © 2021 Partisia Blockchain™

3.3.1. Designed for inter-chain ZK computation

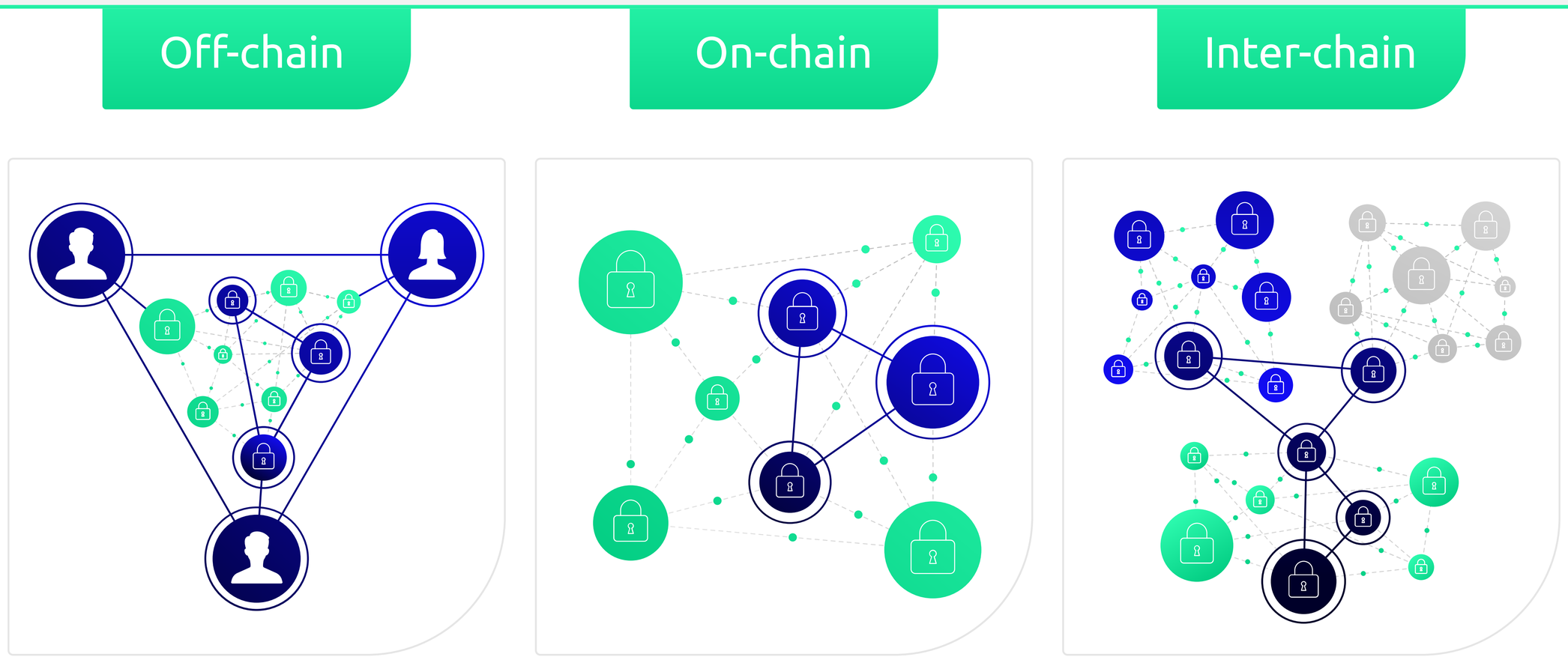

Figure 7: Off-. on-, and inter-chain ZK computation

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.

Confidential © 2021 Partisia Blockchain™

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 differences 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.

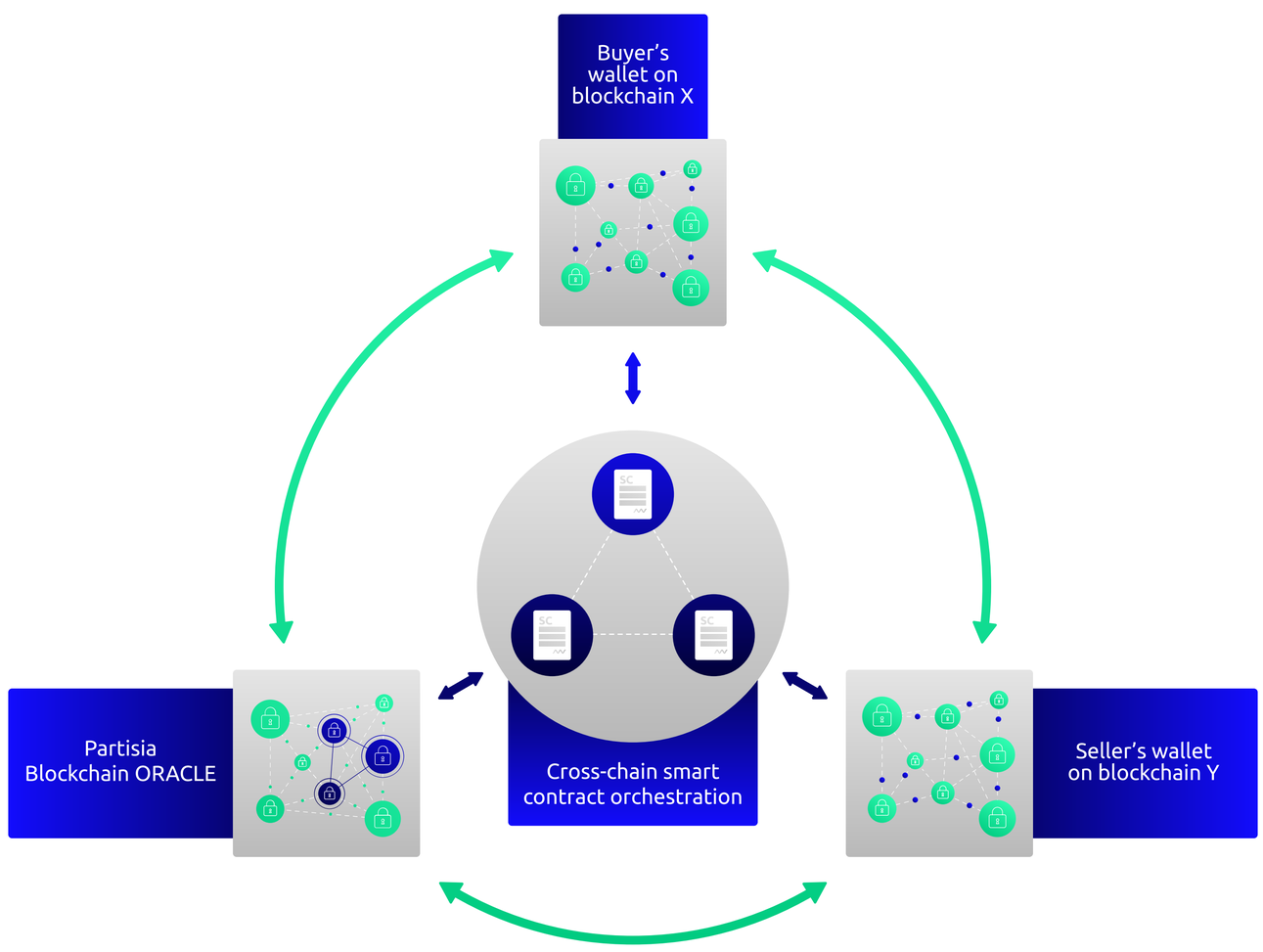

Figure 8: Privacy-preserving inter-chain computation and transactions

Confidential © 2021 Partisia Blockchain™

3.3.2. Privacy-preserving oracle

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 of experts is headed by **Ivan Damgård** and **Jesper Buus Nielsen**. Ivan is one of the founding fathers of the modern hash function as well as ZK computation. Jesper is one of the most quoted researchers within the field of ZK computations and also works on consensus protocols and the microeconomic analysis of distributed protocols. The team of experts also includes **Claudio Orlandi**, who has a similarly strong background in protocol design.

The management team is headed by **Kurt Nielsen** (CEO) and **Peter Frands Frandsen** (CTO). Kurt is the co-founder of Partisia and Sepior. Both companies are pioneers within the use of ZK computations, while Partisia was behind the first large scale commercial use of ZK computation in 2008. Peter is co-founder of Partisia Application and Partisia Infrastructure and has managed software development in complex IT projects for decades. The team includes developers from Partisia and Sepior, which probably makes it the most experienced team of ZK computation developers in the world.

The team has successfully launched three blockchain projects across different sectors to tackle key blockchain challenges through the use of ZK computation. The team developed the first version of the Partisia Blockchain, which is operational by August 2019.

Confidential © 2021 Partisia Blockchain™

4. Team and roadmap

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.

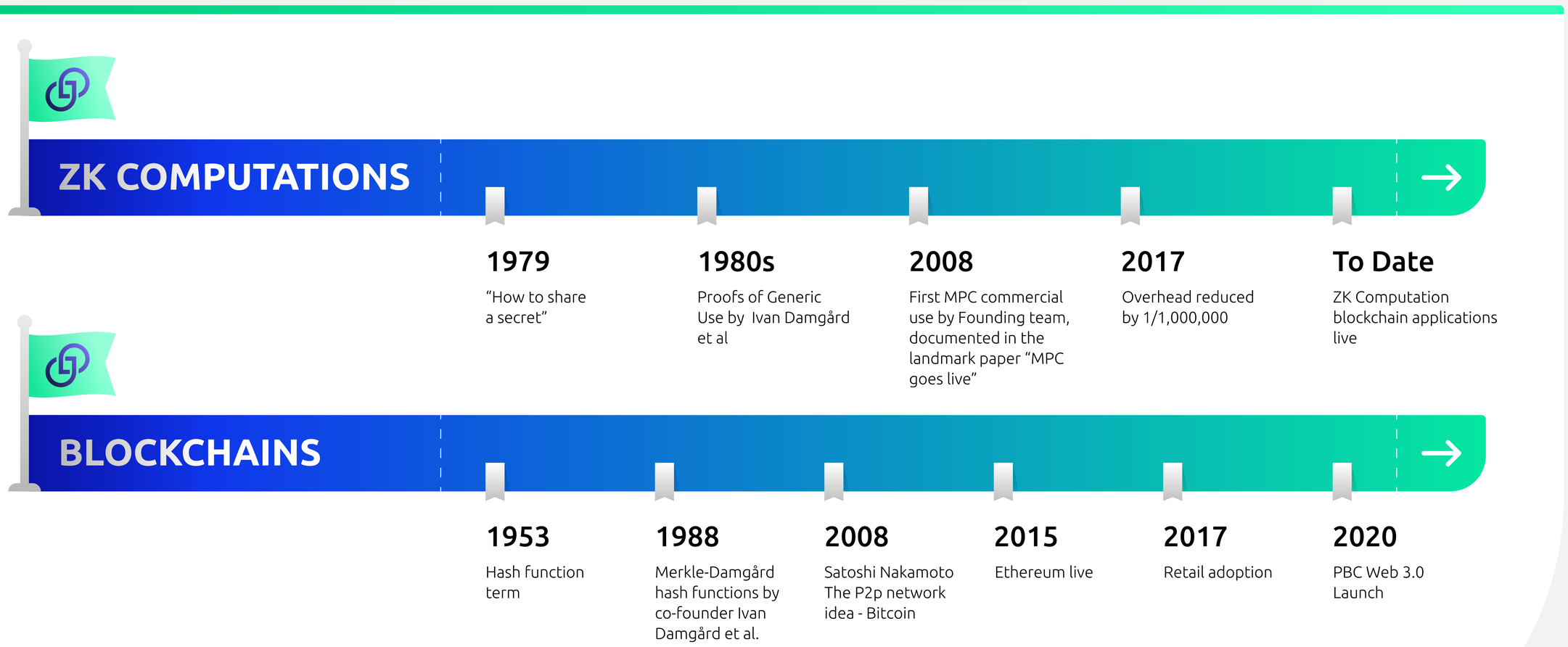

Figure 9: Illustration of the team from theory and practice.

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.

Confidential © 2021 Partisia Blockchain™

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 MPC and blockchain based market and data solutions. Including the basic blockchain and ZK computation infrastructure for Insights Network 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 Japanese fintech company SBI Holding as a key customer and business partner.

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.

Confidential © 2021 Partisia Blockchain™

4.1.2. The people

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 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) holds a PhD in economics from 2004. He did 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 is specialised 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.

Confidential © 2021 Partisia Blockchain™

4.1.2. The people

Brian Gallagher (Co-Founder and Council Member) Founder of instars.com, the world's first decentralized social network data exchange fully powered by blockchain and MPC, developed in collaboration with Partisia. Brian's experience in blockchain technology and cryptocurrency since 2013 brings a unique perspective on the state of the industry and future trends. Over 200,000 users benefit from MPC 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. Existing blockchain projects

The starting point for the Partisia Blockchain project is 10 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. Recently, work has focused on integrating ZK computation and blockchain.

Three of the most relevant public projects are:

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: ***https://instars.com***

Confidential © 2021 Partisia Blockchain™

4.2. Existing blockchain projects

Crosspoint: 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: *https://cyberian.digital*

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: *https://sepior.com/press-release-sbi-october-22-2018*

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.

4.3. Roadmap

The overall roadmap for the first four years is divided into four phases as described below. Each of the four phases are divided into the three basic components of the Partisia Blockchain business:

- *Partisia Blockchain - blockchain and platform for building smart contracts and orchestrating ZK computations and interoperability.*
- *ZK computation - ZK computation protocols and execution of ZK computations.*
- *Partisia Blockchain cross chain computation - cross chain operations such as BYOC functionality that allows integration of different blockchains into the execution framework of the smart contracts.*

Confidential © 2021 Partisia Blockchain™

4.3. Roadmap

The Partisia Blockchain and the ZK computation is the core and the Partisia Blockchain cross chain computation stepwise extends the collaboration with other blockchains. The initial phase has resulted in an operational testnet and was finalized by September 2019.

PHASE 1 (Version 1.0)

Partisia Blockchain

- Version 1.0 running on testnet with block producers and ZK nodes
- Smart contracts using ZK computation deployable and include among others:
  - Second price auction
  - Matching service
  - Credit scoring
  - Fraud detection
- First API for developing own smart contracts

ZK computation

- First version of the ZKC protocol tailored executing within blockchain
- ZK framework that provides orchestration of ZK computations without delegating trust

Partisia Blockchain cross chain computation

- Cross chain demonstrators allowing cross chain value transfer and moving INSTAR tokens to Ethereum

The planned future work is divided into three phases as illustrated in Figure 10 and described in more detail below.

Confidential © 2021 Partisia Blockchain™

4.3. Roadmap

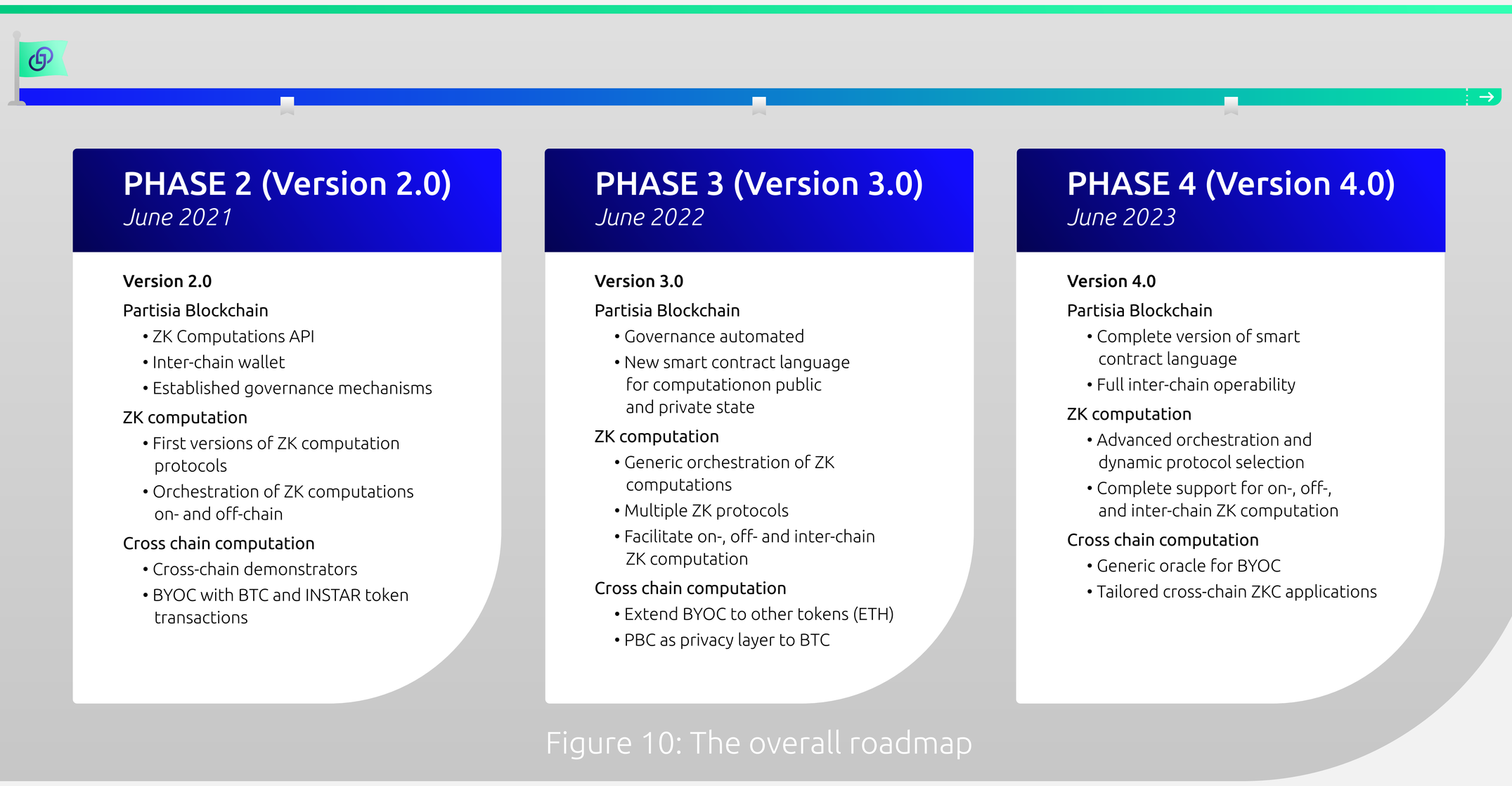

Figure 10: The overall roadmap

PHASE 2 (Version 2.0)

October 2019 - June 2021

Partisia Blockchain

- Version 2.0 will be deployed with block producers and ZK nodes
- Decentralized consensus
- Decentralized governance mechanism including among others:
  - Automatic process of becoming a node operator
  - Voting mechanisms for decisions among nodes operators and token holders
  - Staking mechanism for operating Oracle wallets and ZK computations
  - Scoring of node operators
- Inter-chain Oracle wallet
- Smart contracts with and without secret state deployable to Partisia Blockchain including among others:
  - Second price auction
  - Matching service
  - Credit scoring
  - Fraud detection

Confidential © 2021 Partisia Blockchain™

4.3. Roadmap

ZK computation

- ZK Computation API
- ZK framework that provide access to trust in a decentralized blockchain
    - First versions of multiple blockchain embeddable ZKC protocol
    - Seamless orchestration of ZK computations

Partisia Blockchain cross chain computation

- Cross chain demonstrators
- Oracle for BYOC tailored BTC and ETH
- Partnerships that utilizes the inclusion of BTC and ETH and the orchestration of ZK computations

PHASE 3 (Version 3.0)

June 2021 - June 2022

Partisia Blockchain

- Version 3.0 will be deployed with at least 20 computation nodes
- The ZK framework will be deployed on the Partisia Blockchain
- Active applications running on the chain based on the user base in Insights network
- Strategic partnership agreements supporting the uptake of blockchain applications
- New smart contract language for computation on public and private state

ZK computation

- Generic orchestration will facilitate user defined secure computations using well-defined primitives
- The ZK framework will facilitate simple on-, off- and inter-chain ZK computations that are provable secure and efficient through coordinated pre-processing

Partisia Blockchain cross chain computation

- Inter-chain wallet and generic oracle for most common, liquid tokens
- Oracle for BYOC tailored BTC and ETH
- Partnerships that utilizes the inclusion of BTC and ETH

Confidential © 2021 Partisia Blockchain™

4.3. Roadmap

PHASE 4 (Version 4.0)

June 2022 - June 2023

Partisia Blockchain

- Version 4.0 will be deployed with at least 50 computation nodes
- Complete version of new smart contract language supporting public and private state
- The full ZK computation operating system deployed on the Partisia Blockchain
- Full inter-chain operability based on Partisia Blockchain smart contracts with public and private state
- Strategic partnership agreements to further support the uptake of blockchain applications

ZK computation

- The ZK computation operating system will extend the orchestration by facilitating a wide range of node types and security models
- Developing a ZK computation operating system that fully supports independent selection of orchestration, execution of ZK computations as well as an independent definition of security model
- The ZK computation operating system will improve efficiency through dynamic protocol selection
- The ZK operating system will facilitate known types of on-, off- and inter-chain ZK computations

Partisia Blockchain cross chain computation

- Generic oracle for BYOC tailored liquid tokens
- User defined ZK computations done via ZK contracts operating on a number of chains
- Full inter-chain operability by inter-chain ZK computations and inter-chain wallet allowing direct payments to be made with liquid coins

Confidential © 2021 Partisia Blockchain™

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 (MPC): Multi-Party Computation is explained in *Section 2.1* and *3.2*.

MPC: An abbreviation of secure MultiParty Computation. There is not yet a clear consensus about this abbreviation - SMC and sMPC 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: All node operators are approved by one central organisation or the existing network. Read permission may be public or restricted to an arbitrary extent.
(Inspired by the following definitions of blockchains: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general)

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

Confidential © 2021 Partisia Blockchain™

5. Terminology

Public Blockchain: Everyone can operate a node on the public blockchain and become part of the validation process. Beyond standard KYC/AML, operating a node requires no approval. Read permission is always public.

Public permissioned blockchain: Our definition of the Partisia Blockchain as a public blockchain that everyone can read and where every approved entity can operate a baker and ZK computation node.

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.

Stable coin: 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 tokens.

Confidential © 2021 Partisia Blockchain™

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

Confidential © 2021 Partisia Blockchain™

6. References

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.

Confidential © 2021 Partisia Blockchain™