ORION

Orion WHITEPAPER

BEST PLACE IN THE CRYPTO WORLD FOR MONEY MAKING DECISIONS

ORION

This whitepaper constitutes a technical report of the business purpose, project functionality and so cial value of Orion.

This document does not imply a prospectus of any sort

Let's explore the future of the crypto world together

TABLE OF CONTENT

Summary

Orion will continue to develop and improve its unique ecosystem, including but not limited to professional analysis tools in many fields such as encrypted transactions, community interaction, payment systems, advertising services and Orion Academy. Not only that, but the platform continues to develop more areas, and strives to bring powerful tools such as user sentiment index in the encrypted market, Orion price warning, private chat integration, Orion trading robot and AI price prediction to the market.

In the near future, Orion will also launch business segments such as shadow trading, Messenger price warning and Orion blockchain incubation to provide better services for users in the encryption market.

Orion is also a high-quality service platform, which relies on its blockchain infrastructure to build a highly loyal community and a well-defined ecosystem.

The economic attributes of the Orion platform will enable PMC tokens to become a multifunctional tool for payment, remuneration and accumulation. The token can be used as a payment and bonus tool within the system. Thanks to the PMC token, it is possible for the Orion team to quickly develop the internal system ecology.

Due to the increasing demand for PMC tokens in the market and their limited supply, PMC tokens have become one of the most attractive tokens in the cryptocurrency market with stable growth.

Blockchain and Finance

Blockchain is a new technology that promises to increase the transparency and efficiency of the financial system. Bitcoin is the groundbreaking cryptocurrency that grew out of an initiative to create a new global "people's currency" that would not be governed or controlled by any privileged organization. As technology advances, including smart contracts, zero-knowledge transactions, multi-signature wallets, and many other new features, the industry is beginning to realize the far-reaching potential applications beyond anarchist (decentralized) currencies

protocol standard

In many ways, the current state of financial infrastructure is a lot like the internet before the widespread

adoption of internet standard protocols like TCP/IP, TLS, HTTP, and SMTP. The most basic requirement for a network to function without centralized coordination is a common language so that independent systems can seamlessly communicate with each other and share information. For email, SMTP provides a standard data transfer protocol so that email can be sent between different mail clients and servers. In financial systems, there are additional constraints on the transfer of interdependent information. For example, double bank transfers where the same electronic funds are transferred from one bank to two other banks will be problematic.

The recent explosive growth of the blockchain and cryptocurrency industry presents an opportunity for a long-awaited overhaul of the global financial system. In a short period of time, it has facilitated the development of new open-source infrastructure for distributed databases, peer-to-peer broadcast protocols, and Byzantine consensus algorithms, as well as the implementation of new libraries of cryptographic tools that improve data integrity and privacy, such as multi-signature technology and Zero knowledge proof.

financial identity

In the context of financial systems, proof of identity has traditionally been required for asset ownership. In addition to physical assets, establishing ownership relies on legal documents corresponding to real-world identities. This approach to establishing ownership can be equally applied to more diverse assets. Company shares can legally be issued to a public key so that only those who know the corresponding secret key can claim ownership.

However, ownership of various assets in the global financial system typically has stricter identification and account verification requirements than in other areas. For example, banking and brokerage services must comply with know-your-customer (KYC) and anti-money laundering (AML) rules before accepting new clients.

The blockchain behind the cryptocurrency does not solve the identity authentication of participants in such detail. The public key alone does not contain any information about the user. Importantly, though, users can easily add additional information about their identity to the public keys they have access to. This identity can enable the enforcement of rich rules around KYC, AML, and other qualified certifications. These rules can determine the requirements for participating in different types of

financial transactions. However, existing blockchains do not propose comprehensive and comprehensive standards for real-world identity management and authentication.

Privacy and Compliance

Transparency and open participation are the cornerstones of blockchain-based finance. However, full transparency comes at the cost of privacy; and privacy is an absolute requirement for the vast majority of financial services. Therefore, although full transparency provides auditability, this feature also prevents most blockchain platforms from deploying most financial applications. On the other hand, cryptocurrencies such as Zcash and Monero utilize cryptography to protect the anonymity of token transfers. However, the limitation of these systems is that confidentiality is all or nothing. Transactions only prove that simple transfers of native cryptocurrency are valid, but not more nuanced statements (with the loss of auditability). Therefore, anonymous blockchains cannot provide the compliance requirements required to deploy financial applications.

Traditional finance provides users with privacy from the public, but the transparency provided is close to zero; moreover, it does not protect users' privacy from financial institutions. The first generation of blockchain-based finance offers complete transparency or complete confidentiality. Orion aims to provide the best of both worlds through what we call cryptographic transparency.

Cryptographic transparency provides better privacy protection than traditional finance, and even detailed user data is kept secret from the operating nodes of the infrastructure, while still allowing operating nodes to verify the validity of all transactions. It also successfully retains the transparency and auditability offered by first-generation blockchains, enabling users to prove complex statements about the details of private transactions. Orion provides privacy-centric tools for asset tokenization, identity proof/KYC integration, public and regulatory auditing, asset tracking, and many other special-purpose zero-knowledge proof functions to prove that transactions are compliant: e.g., proving that an exchange has Solvency and funds invest in whitelisted assets.

Transparency and Synchronization

Whether managed by a single server, a consortium, or a large-scale distributed network of operational nodes, all blockchain networks have one thing in common: the blockchain data structure. Blockchain is a simple Authenticated

Data Structure: Multiple records are cryptographically linked together to form an append-only list, so that the records stored in Consensus is reached on the history of transactions in a shared open database. The verified data structure allows the network of operating nodes, users and auditors to easily open access to public financial databases without relying on a central server to honestly provide access to the data. The history of transactions is immutable, and anyone can verify that all transactions are valid.
Orion's advanced proven data structure is based on the latest technologies such as encrypted accumulator (RSA Accumulator) and vector commitment (Vector Commitments).

consensus mechanism

One of the biggest misconceptions about blockchains is that they can simply replace the fiduciary role of financial institutions. In fact, the network that operates the blockchain is itself the new financial institution. The consensus protocol it operates on determines how influence is distributed among network participants.

Introduce

our mission

The vision of the project Orion is to develop a new global analysis ecosystem and create a simple and efficient financial environment for cryptocurrency transactions.

At present, although the trading income of cryptocurrencies is very rich, it is still difficult to conduct normal cryptocurrency transactions in the financial market, and mastering powerful information tools is the only way to solve these difficulties.

Orion came into being. We can help users find and analyze the correct information and data at the right time, so that users can make reasonable investment decisions.

Choose Orion, a platform that brings together the present and future of the cryptocurrency market, and you will open the door to the cryptocurrency world from now on.

Background of the project

Orion is the ultimate choice for making money-making decisions in the cryptocurrency world.

Unlike most newly developed crypto projects, the Orion platform was born with a proven track record. As early as 2015, the founding team had germinated the concept of this platform during the process of encrypted transactions.

Since then, the founding team has discovered various defects in the cryptocurrency trading industry, such as the lack of reliable market information that seriously affects the development of the encryption industry structure and ecosystem. These problems have brought irreversible damage to the cryptocurrency trading industry.

In order to solve these problems, in April 2020, the Orion platform was finally born.

Orion is not an ICO entity, and unlike most new projects, Orion does not set a ridiculously high soft cap, nor does it seek any external equity financing. Everything Orion has come from self-funding, and the project goes directly to the exchange market, all these represent its growth potential.

The Orion team is composed of top trading users and consultants in the world, and all the benefits and rewards they get will be distributed in the form of PMC tokens. This shows that the success of the project itself is closely related to the value the platform provides to the community. The same is true, everyone in the team will work hard to make the project continue to grow.

Project Description

The Orion platform consists of three sections: Beginner, Intermediate and Advanced.

New users after registering an account will automatically become novice users, and novice users enjoy the basic tools and reference indexes provided by Orion for free.

To use the tools or related reference data developed by the Orion technical team, users need to pay the corresponding fees for different tools or services on a monthly or annual basis.

In addition, our academy courses are free and open to everyone, because for us, it is also our interest to attract more potential users to join the entire field by popularizing the knowledge of the cryptocurrency world.

And our community prediction section allows trading users to share their market predictions, while users who make predictions can get weekly rewards in the form of PMC tokens.

The Orion platform can obtain the highest quality price analysis reports and customized market warnings, and with the continuous development of the platform, various functions of PMC tokens will also be connected to the platform simultaneously. The PMC team will

implement the team's plans step by step. With the establishment of the air classroom and the provision of real-time courses on encrypted transactions, these plans will also include content outside the platform.

In addition, an incubator is included in the team's development plan, which can help Orion members to incubate their own projects with the support of the Orion team.

system structure

The Orion platform can support high-load real-time data transmission, and read the information and data of blockchain network participants from the preset rules.

The platform's architecture allows the platform to update data within milliseconds in different environments (including those outside the blockchain).

Our system can collect thousands of data less than 100 bytes per batch. Since the data processed in each batch may contain different data from multiple environments, the amount of data that the platform needs to process every day can be measured in terabytes. In order to improve computing power, POrion has also specially created a custom software that integrates blockchain and distributed storage systems.

challenge

Cryptocurrencies are spreading at an unprecedented rate, and countless people have expressed a strong interest in this type of asset. However, these investors who are not yet familiar with cryptocurrencies also face two problems, which make them have to think twice about this market.

- Many people believe that the economic performance of encrypted assets is not yet stable, and market fluctuations may cause them to lose assets.
- Due to the lack of basic knowledge related to the blockchain, many potential investors neither know how to buy encrypted assets nor where to buy encrypted assets.

In addition, the amount of manipulated information on the Internet has also increased significantly, which can mislead investors and trading users in the market. In January 2018, the collapse of the cryptocurrency market brought great panic to investors in the market, and people's confidence in cryptocurrency was also declining, while traditional financial services were overpriced due to many risk factors, which also led to Many people cannot afford traditional financial services.

The threshold for using encrypted asset exchanges is relatively high.

When users lack proper guidance, it will be difficult for users to understand the operating mechanism of important tools including charts. Therefore, many users have made many blind investments, and the results of the income have to rely on luck. These users swim in the sea very cautiously like a small fish, and there are all kinds of big fish waiting around them, ready to devour them at any time.

solution

Orion is the most advanced crypto platform to date, containing everything a trader needs; information, knowledge and confidence all rolled into one. The platform was created for those who want to master the cryptocurrency market and reach new financial heights.

Orion's specially programmed indicators can identify any volatile market reaction and show its trend, thus keeping you on top of everything. The platform will monitor deposits and withdrawals on major fiat channels, large fund movements on exchanges, etc. to control whale behavior and more.

First, we need to raise the knowledge level of new members and get them started. The Orion Academy section is taught by the most experienced industry experts the necessary knowledge of the industry. The entire Academy section is designed to meet the learning needs of all traders, from beginner to expert, in preparation for real trading.

The content and information involved in Orion are richer and deeper than any other platform. At the same time, the entry threshold of the Orion platform is also very low.

Product

mobile application

The mobile application is a key part of the Orion ecosystem, conveniently integrating everything needed by both novice and experienced traders. It includes the latest market and portfolio tracking features, allowing users to fully customize the display of their favorite tokens and various portfolios (including the ability to display the value of tokens and portfolios in different fiat currency units).

This data tracking feature has made it an industry-leading app, far beyond what is offered by any other encryption app on the market today. The app is designed to create a comprehensive ecosystem of edutainment and entertainment. In other words, there are community interaction and encrypted game sections in the app,

and users can earn points through various activities in the app and exchange them for PMC tokens.

The community board is designed to reward users for voting on bullish/bearish sentiment. If the prediction is correct, the user can get more rewards, and can also participate in the weekly quiz leaderboard with friends, and can also create a personalized quiz, establish a bonus pool, and distribute rewards to the best prediction players.

Crypto games offer users another way to earn in-app credits while competing with friends. The app will have two very attractive games coming soon, and it will also be able to display weekly and monthly leaderboards.

Besides the community section, another focus of the app is the educational section, that's why it contains all the interactive educational information available on the platform as well as a personalized newsfeed, so every user is constantly updated with the latest coin news. In the future, Orion plans to cooperate with major exchanges, thus making it a truly comprehensive application.

platform

The Orion platform is the nerve center for making money in the cryptocurrency world and is very friendly to both newcomers and professional traders. Orion is committed to solving the problem of user information asymmetry and guiding investors to avoid blindly investing in encrypted assets. It is the first platform in the market to provide reliable knowledge and analysis.

The platform provides detailed information on buy and sell order data, best exchange rates, smart currency movements, displays fundamental and technical analysis and in-depth market insights into price movements. By having key information at your fingertips, the platform is able to save you time and effort in all aspects of the crypto world.

The Orion trading section is divided into three levels: primary, intermediate and advanced, which can meet the needs of different user groups.

The primary page is accessible after the user registers for an account. It contains the essential tools and features every cryptocurrency trader needs: from filtered breaking news, charts, currency watchlists, portfolios, performance indicators, and other bitcoin-oriented indicators.

Intermediate pages include advanced features with detailed market insights. Users can experience the arbitrage

function (the price difference between multiple markets for the same token). Additional features include investment sentiment indicators, stock-to-flow models, trading indicators such as Genesis, Bitcoin vs. Gold Comparison, Relative Strength Index, Options Trading, and more. In advanced functions, users are allowed to achieve more professional transactions.

The Advanced page unlocks state-of-the-art programming indicators that can outperform other traders in the cryptocurrency trading world. You can track every big transaction in the market through whale alerts, analyze the correlation between assets, view the inflow and outflow of fiat currency in encrypted transactions, in-depth bitcoin cycle analysis, historical price trend framework, relative changes in bitcoin, etc. . You can access all professional indicators and monitor all the action in the crypto world.

Of course, new indicators and tools are constantly being added to the advanced page. The roadmap for the project lays out necessary features that will continue to be updated.

Confidential Asset Transfer

A confidential asset transfer is a transaction that transfers the ownership of an asset from one address to another, but hides the details of the transferred asset. In the case of basic asset transfers, this includes the amount and asset_type fields in the input and output asset records consumed and created during the transaction.

To explain how confidential transfers in Orion work, let’ s take a closer look at the anatomy of a Orion asset transfer transaction. 5 Assets are transferred simply by posting a transfer note to the PoPMaxcrypto ledger (referred to as XfrNote).

[5]Technically, PoPMaxCrypto transaction bundle operation and asset transfer in PoPMaxCrypto are one operation

```
pub struct XfrNote
  {            pub(crate)
  body: XfrBody,
  pub(crate) multisign: XfrMultiSig,
}

pub struct XfrBody{
  pub(crate) inputs: Vec<BlindAssetRecord>,
  pub(crate) outputs: Vec<Blind
  AssetRecord>, pub(crate) proofs:
```

XfrBody contains a list of input asset records and output asset records. For confidentiality, these asset records are blinded, using encrypted commitments. These are implemented using Pedersen commitments on an elliptic curve group called 'Ristretto'. We call the blind record data structure a BlindAssetRecord to distinguish it from a normal AssetRecord.

```
pub struct
  AssetRecord{ pub
  (crate) amount: 64,
  pub(crate) asset_type: Option<[u8;16]>,
  pub(crate) public_key: XfrPublicKey, // ownership addre
}

pub struct BlindAssetRecord{
  pub(crate) asset_type: Option<[u8;16]>,
  pub(crate) amount_commitment: CompressedRistretto,
  pub(crate) asset_type_commitment: Compressed
  Ristretto, pub(crate) blind_share:CompressedEdwardsY,
  pub(crate) lock_amount: ZeiCipher,
  pub(crate) lock_type: ZeiCipher,
  pub(crate) public_key:
```

lock_amount and lock_type are the encrypted values of the asset record fields amount and type respectively. They are encrypted under the public key public_key of the asset record owner (ie receiver address). Cryptography promises to hide information perfectly, which makes them different from encryption. They do not contain any information that can be decrypted by someone with the key. Instead, they can be used as hidden fingerprints of committed information, similar to how a server sends a hash of a file before sharing it. A hash value is a unique fingerprint that can be measured from a file, but the file cannot be obtained from the hash value. Encrypted commitments can only be "unwrapped" or "unblinded" by obtaining that unique information being submitted and a secret value called the blinding factor. If C is a cryptographic commitment to message m using a blinding factor r, then C can be uniquely computed by obtaining m and r, r being a proof that C is a cryptographic commitment to m. In Orion's blinded asset record, the blinding factor is shared with the new asset owner (i.e. transfer recipient) using a method similar to Difi e-Hellman key exchange. This user gets the blinding factor from blind_share and its private key corresponding to public_key. Users need these blinding factors to check that the recorded decrypted content is correct (i.e., approved by validator nodes), and they are also required to use them (blinding factors) to transfer ownership of assets in future transactions.

```
pub struct OpenAssetRecord{
  pub(crate) asset_record: Blind
  AssetRecord, pub(crate) amount: u64,
  pub(crate) amount_blind: Scalar,
  pub(crate) asset_type: AssetType, //type AssetType =
  [u8;16] pub(crate) type_blind: Scalar,
}
```

XfrProofs contains a zero-knowledge proof that blinded output records are valid for blinded input records. Specifically, it proves that the sum of the output amounts for each asset type in the output records is equal to the sum of the input amounts for the same asset type in the input records. More precisely, if there are n input records and m output records, and the following variables are defined:

- αi is the amount in the ith input record
- βj is the amount in the jth output record
- In[t] is the set of input indices with asset type matching t
- Out[t] is the set of output indices with asset type matching t
- T is the complete set of types among the output records

We will take a closer look at the anatomy of XfrProofs when we next explain cryptographic commitments,

range proofs (Bulletproofs), and Pedersen equation proofs.
Finally, XfrNote only works if each input BlindAssetRecord correctly references an existing valid record created on the ledger by a previous transaction. Therefore, the transaction wrapping the XfrNote must also include a reference to the asset transfer (led) note from the previous transaction. These references are called Transaction Output Sequence IDs (TxoSIDs)

```
pub struct
  AssetTransferBody { pub
  inputs: Vec<TxoSID>,
  pub transfer: Box<XfrNote>,
```

A fully functional validator node with access to the entire ledger uses each ith TxoSID to look up the BlindAssetRecord in the previous XfrNote output and checks if it matches the ithBlindAssetRecord in the current transaction's XfrNote. Validator nodes also check that the TxoSID is still valid. Once a TxoSID has been used in a transaction, it becomes invalid (i.e. recorded as being "consumed").

mathematics background

finite group The encryption protocol used for secure transmission in Orion requires a finite group of prime order as a tool, some of which computational problems are difficult to solve. A finite group G is a finite set with predefined group operations on the elements in the set. We use the "+" symbol to denote operations between a pair of grouped elements. An operation on any two elements in the set gives the other element in the set. There is a unique "0" element such that for any g ∈ G, 0 + g = g. Every element g has an inverse element, denoted (−g), such that g + (−g) = 0. The order of a group is the number of elements in the set. Adding integers modulo n is a simple example of a group of order n. This group, denoted Zn, contains all integers less than n. The coprime integers of n are a group under integer multiplication, denoted Z∗ n. The set of integers {0, ..., p − 1} of primes p is the array Zp under addition, and if we exclude 0, the array Z∗ p under multiplication. Groups with this property are called finite fields, and this field is denoted Fp.

Elliptic Curve Group More advanced number groups can be constructed by looking at points on curves defined over finite fields. The elliptic curve E over p is defined by an equation of the form y2 = x3 + ax + b mod p, where a, b ∈ Fp. The elliptic curve group G = E(Fp) consists of all points (x, y) ∈ Fp satisfying this equation, and there is a group operation that interpolates any two points to find a third point on the curve. PoPMaxCrypto uses a curve named Curve25519, which uses the prime number p = 2255 − 19 and the curve equation y2 = x3 + 486662x2 + x.

business group Another type of group, called a quotient group, can be built on top of an existing group G, which has a special type of subgroup N $\subset$ G called a normal subgroup. Subgroup N is a subset of G and is also a group under the same operation. N is normal if the element g + h + (−g) is contained in N for all g $\in$ G and h $\in$ N . In a commutative group, the order of operations does not matter, each subgroup is normal. Given normal subgroups N and G, the quotient group G/N is constructed by forming partitions of G resulting in subsets called equivalence classes. Here two elements a, b $\in$ G are placed in the same equivalence class iff a − b $\in$ N . These equivalence classes are new elements of the G/N group, represented by picking an element from each equivalence class to "represent" that class. If a¯ and ¯b are two representative elements, the group operation finds a representative element c¯ for c $\in$ G, where c == a¯ + ¯b. If G has degree m and N has degree n, then G/N has degree m/n, which is always an integer.

Ristretto group Orion uses the Ristretto group, a quotient group built from groups of elliptic curves on Curve25519. The prime order of the elliptic curve group on Curve25519 is

8p:p = 2252 + 27742317777372353535851937790883648493

Ristretto quotient groups are constructed from normal subgroups of order 8 and thus have prime order p6.

abstract symbol For the purpose of describing the cryptographic protocol, we will operate in the Ristretto group using the following notation. We use Gp to denote the Ristretto group. Elements in Gp (represented by points on Curve25519) are denoted by capital letters, such as A, B $\in$ Gp. Lowercase letters are used to denote elements in Fp, also known as "scalars".

- Group addition: C ← A + B is a group operation in Gp that takes two representative curve points A B and returns the third representative curve point C.
- Scalar multiplication: aC denotes an element of Gp obtained by adding a C's together using the group addition operation, where a $\in$ Fp is interpreted as a positive integer less than p.

Discrete Logarithm Problem (DLP) An algorithm for solving DLP in the Gp group is given a nonzero element in tt $\in$ Gp and a random element H ←R Gp and proceeds to output a $\in$ Fp, so that att = H with non-negligible probability. It is generally believed that DLP is computationally difficult in the

Ristretto group, i.e. no efficient algorithm for DLP exists with current computing power.

Decisional Diffe Hellman (DDH)

If it is computationally difficult to distinguish the tuple (aC, bC, abC) from the tuple (aC, bC, rC) by randomly choosing a, b, r ∈ Fp and an arbitrary element C0, then the group of prime order has DDH security attributes. It is well known that the Ristretto group has DDH properties under current computing power. The DDH property is a stronger security assumption than DLP because solving DLP in Gp breaks the DDH property.

Orion - PMC

economic model

Orion's economic model is based on selling access to premium services, which is similar to that of traditional IT companies.

Orion makes money by providing professional technical and operational support to paying users.

Orion's economic model is based on a long-term campaign plan and a well-structured business approach for the continuous development of the service.

This can generate cash flow and quickly scale the platform, increasing the company's market share.

Another stabilizing factor is that Orion targets the largest trading market in the blockchain industry. Cryptocurrency trading is a huge and relatively predictable market, with thousands of people entering it every day.

This market is huge, and at the same time Orion's growth potential is unlimited.

Orion mechanism

PMC tokens are the basis of Orion's internal economic system and are equivalent to all services implemented on the platform. They are a special unit of account used to pay platform fees. By purchasing PMC tokens, users gain access to the functionality of the Orion platform as well as highly liquid instruments of increasing value.

PMC token is a general-purpose cryptocurrency that can be used as a circulation medium in Orion's internal ecosystem, and can be freely exchanged for legal tender and other cryptocurrencies.

Users can freely buy and sell PMC tokens, while the price of tokens is still

determined by supply and demand in the open market.

When building the Orion economic model, a deflation model will be used to regulate the token rate, which can ensure a stable supply balance to balance the platform's internal processes.

token mechanism

Orion-PMC

The PMC token is an internal unit of value created by the Orion platform to manage its business model. It is a bridge for the user to interact with the terminal. As the number of users and communities continues to grow, the success of the PoPMaxcrypto platform will be reflected in the price of PMC tokens.

Token Name: Orion
Abbreviation: PMC Total Supply:
Starting from 280.000.000, reduced by automatic token burn (more info in the ecosystem)

token burn

The number of tokens offered by Orion is limited. The token burn is at the heart of the token development system.

This means that Orion will automatically burn 20% of the PMC tokens it gets from membership fees. The process of token burning reduces the total supply of PMC tokens, which leads to a healthy increase in token prices and benefits investors and token holders.

Orion is committed to providing transparent and valuable services to the community. Therefore, the team is obliged to burn the same amount of tokens received from members. Orion strictly prohibits any form of token abuse and price manipulation, which will violate the mission of the team.

When the goal of 1 million members is reached, the company will dispose of all remaining tokens, if any. The total supply of tokens is 280,000,000, with a projected 5-year circulating supply of 90,000,000. Through the process of burning PMC tokens, Orion can keep the demand and price of the tokens as high as possible.

Advantage

Reasons and factors for Oriontobe abl e to dynamically develop and expand in complex markets:

1. The platform generates revenue for its users.

Today, Orion is a market-proven high-tech terminal with powerful analysis tools. By offering better services at lower prices, and offering basic tools and educational courses for free, Orion has built a community of over 110,000 certified traders.

2. The profit model of the platform on the blockchain can bring stable income.
The cryptocurrency trading market is huge with unlimited potential for growth.

3. Orion has established an effective business model and a transparent mechanism to increase the value of PMC tokens.
The mechanism of Orion's steady growth is the measure of Orion's effectiveness.

4.Orion has a fully transparent revenue stream, making it independent of external funds.
The project does not collect money from users, but relies on the project's own hematopoietic function, which allows it to quickly expand the platform and increase its market share.

5. Strong hematopoietic function.
The project fully follows its strategic plan. Orion creates tools that generate revenue for users.

6. Has a transparent and relevant success story.
Orion has been live since the mass adoption of blockchain technology. During all this time, it has continued to improve and build its user base.

7. The item is recommended by an independent expert.
Some well-known expert platforms have objectively emphasized the trust, experience and ecosystem of the Orion platform.

8. Active investing as a planning strategy.
The main goal of active investing is to achieve rapid growth in the market share of Orion and to create a structure capable of significantly influencing the market in order to obtain the most favorable conditions for traders.

9. Projects quickly transition to new levels.
The cumulative effect caused by the introduction of new services and the expansion of the user base has brought Orion into a phase of exponential growth.

10. Steady increase in PMC value.
The main task of the Orion team is to ensure that the value of PMC tokens increases every day. So far, they have been able to achieve this goal.

compliance

By utilizing zero-knowledge proofs, selective identity proof disclosure, and privacy-preserving computation, Orionis able to provide both privacy and transparency. These cryptographic techniques open new possibilities for more efficient regulation that was previously unattainable without compromising user privacy. Functionally, this means that funds can cryptographically prove to regulators that they are operating compliantly (for example through the use of proofs of solvency) without disclosing details of their actions or investments.

Privacy Shield Compliance Tools

One of the cornerstone values of Orion's design is to allow various levels of transparency while maintaining confidentiality. For example, Orion empowers smart investment funds to provide regulators with visibility into general fund information (assets, holdings, investor credentials) while keeping other selected fund-related data (investment activity, investors, terms, etc.) private . Advanced encryption techniques precisely accomplish the task of simultaneously achieving transparency and confidentiality.

The two most relevant cryptographic techniques we use are zero-knowledge proofs and multi-party computation. A zero-knowledge (ZK) proof is a technique used to show that a statement is true without revealing any other information other than the validity of the statement. ZK proofs can also be used to prove knowledge of a secret, such as the password to unlock an account, without revealing the password itself. Similar to ZK proofs, secure multi-party computation (MPC) enables a group of parties to jointly learn the output of an input computation without revealing to each other any additional information about the private input. For example, MPC can be used to conduct secret-bid auctions without relying on a trusted party to collect bids.

Typically, MPC either requires multiple rounds of interaction, or requires expensive computations such as fully homomorphic encryption, and is therefore impractical for smart contract implementations. However, SIF will use a dedicated efficient MPC protocol that is sufficient for Orion use cases (e.g. keeping a fund's balance sheet private).

Confidential payment Basic confidential payment is in a transaction denominated in some token unit, which transfers a hidden amount from one address/account to another

address/account, but the entire system can still publicly verify the validity of the transaction.

Confidential asset transfers
Confidential asset transfers use cryptographic commitments to hide details of assets held in sending and receiving accounts (such as types and balances), and use zero-knowledge proofs to prove that these commitments were correctly updated according to the asset transfer rules, such as new balances The sum of is equal to the sum of the old balances, neither of which has a negative balance. When the asset type is kept secret, the proof must also demonstrate that balances were updated in both accounts under the same asset type identifier without revealing this identifier. Our implementation uses a combination of Pedersen commitments, ElGamal encryption, Bulletproofs[11], and Σ-Bullets[12]. These cryptographic proofs are generated and verified in milliseconds under the implementation of Orion technology.

Proof of Solvency A proof of solvency[13] indicates that the value of asset-backed tokens owned by an entity such as a fund or exchange exceeds its liabilities (eg, total liabilities to investors). When the assets held by the entity producing the evidence are confidential, that is:

[11]B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell.Bulletproofs: Short Proofs for Confidential Transactions and More. https://eprint.iacr.org/2017/1066.pdf.
[12]B. Bünz, S. Agrawal, M. Zamani, and D. Boneh. Zether: Towards Privacy In a Smart Contract World. 2018.
[13]Dagher, Bünz, Bonneau, Clark, and Boneh. Provisions: Privacy-Preserving Proofs of Solvency for Bitcoin Exchanges, 2015. http://www.jbonneau.com/doc/DBBCB15-CCS-provisions.pdf.
This tool is especially important when hiding in a cryptographically committed manner. The general technique behind proofs of solvency takes a set of accounts or transactions labeled as liabilities and a set of accounts labeled as assets, and generates zero-knowledge proofs of the keys that know the accounts that control the assets, as well as proving the sum of those asset balances (by type weighted) over the sum of the liability balances.

Proof of Whitelisted Assets This proves that the identifiers of the confidential assets involved in the transaction are included in the whitelist set without revealing the identifiers themselves. For example, a whitelist can be kept in a Merkle tree, and there is a zero-knowledge proof that the identifier is included in the tree.

Balance Range Proof This tool uses Bulletproofs to prove the range of balances contained in an account or transaction, such as a minimum balance for an investment account or an upper range for the amount transferred in a transaction.

Permission-specific viewing keys Regulators can be granted keys to decrypt user accounts or transaction content that cannot be used to issue transactions on behalf of users (i.e. read-only keys rather than write-enabled signing keys). View keys can also be attached to proofs of compliance, such as proofs of solvency or proofs of whitelisted assets. These keys can disclose more detailed information to authorized regulators than the results of zero-knowledge proofs, but still not reveal all the details of individual accounts. If a trusted hardware execution environment is available, these tools can also be used to achieve highly granular function-specific view keys.

Confidential Multi-Source Payments While Confidential Transfers hide the amount transferred in a transaction from the public, this amount is always revealed to the recipient. Consider multiple payments to recipients from multiple independent sources. Hiding the amount transferred from each source from the recipient and showing only the total amount can be achieved via linear secret sharing[12]. This is a two-round protocol, in the first round, each source splits its input into linear secret shares, one for each source. In the second round, sources compute the sum of the shares they have received from other sources and publicly publish the results of their local computations. A final sum can be derived from these inputs. To keep the final sum secret from the public, recipients can also participate in a secret sharing scheme so that only the recipient can reveal the final sum. Furthermore, if the underlying confidential payment uses a homomorphic commitment scheme (such as a Pedersen commitment), the MPC can be effectively modified so that the recipient knows whether the final sum it learns is correct.

Privacy Preserving Computations Other examples of privacy preserving computations that can be implemented using MPC include sealed bid auctions and order book matching, where the values of bid and ask prices are hidden until a match to prevent front running. These computations require more than the extremely lightweight two-round secret sharing technique described above.

State-of-the-art MPC protocols for general functions employ several approaches to reduce computational

cost and round interactions that limit practical deployment. One approach is to advance most of the computation and interaction to a "preprocessing phase" that distributes setup information among the parties involved in preparation for an "online phase" in which parties repeatedly The input performs an efficient privacy-preserving computation. Another approach is to shift the responsibility for maintaining privacy to distributed "third-party" servers, which can maintain privacy as long as there is at least one "honest" non-colluding server.

Confidential Transactions

Transactions submitted to the ledger protocol generally execute one or more account operations in batches of atomic transactions. The signature required for each operation in a transaction must also sign a digest of the entire transaction. This guarantees that individual operations within a transaction cannot be replayed individually (non-atomically).

Transactions can also include preconditions, a logical expression whose inputs depend on the state of the ledger. For example, a precondition can evaluate whether a certain amount of time has passed between transactions. The precondition must resolve to true for the transaction to be valid. The same transaction can be broadcast multiple times until the precondition is met. This enables mutually distrusting users to atomically chain their transactions.

Basic Confidential Transactions hide the value exchanged in the transaction. Confidentiality is a very different privacy goal than anonymity, which also hides the identities of the accounts involved in transactions. Confidential payments are introduced into the Bitcoin ledger model using a combination of Pedersen commitments and zero-knowledge proofs. Orion implements a scalable solution for privacy goals (confidentiality and anonymity). Importantly, Orion integrates identity proofs with confidential transactions so that even anonymous addresses can be uniquely tied to identity/credentials, which can be selectively revealed. In this way, auditors of the ledger (e.g., regulators versus public users) can have varying degrees of visibility into the identities of transacting parties based on the access keys they have obtained.

multi-signature account

A multi-signature account is an account controlled by a distributed set of owners. Every account update, whether deposit or withdrawal, requires a threshold multi-signature

(TMS) from the owner. TMS is a technology commonly used in blockchain smart contracts. If there are n agents managing accounts, each agent holds a secret key and can be a contributing part of the TMS without revealing the secret. Basic k-of-n TMS works if and only if at least k of n agents contribute to the signature. More complex TMS validation logic is also possible. Weighted TMS assigns weights to each agent's signature and requires the weighted sum of the signatures to exceed a threshold. More generally, any logical predicate can be used to define signature validity. While most TMS signatures scale proportionally to the number of agents in the group, some TMS signatures (for example, BLS-based signatures) can be made compact even when the group of agents has a large value n

Future development

The Orion platform plans to build an air classroom where the Orion team will provide live courses to top cryptocurrency consultants and professionals. This service will help all those who want to learn about the crypto industry to learn more about crypto and provide an edge to those who want to take it a step further and start their crypto entrepreneurial journey.

Orion will establish an incubator, which will provide community users with the opportunity to start their own blockchain projects, and these users will also receive all the support needed for incubating projects. The Orion team will provide them with development guidance, marketing support, and all the know-how needed to create a successful project. Through the team's on-site support, users can obtain fast-response support services, making project incubation more efficient. The team is focused on building the most innovative incubator to date and expanding the entire Orion community through successful business alliances.

In conclusion

Cryptocurrencies are gradually being accepted by traditional markets, and compared to other traditional financial instruments, cryptocurrencies have more potential for development. It is expected that the blockchain industry will explode in the future, and many investors hope to participate in the dividends of growth. One thing is for sure, Orion will be a great place to make investment decisions in the cryptocurrency world.

Orion has proven that it can support and provide everything traders need to make a profit, and the

community membership is expected to explode. Orion strives to be the go-to place for every trader and investor.
Orion overcomes the common negative misconceptions about crypto products in the financial market (that is, the misconception that cryptocurrencies are not safe investment products). The Orion platform provides the best user experience in the crypto trading world by providing members with ways to find reliable information, tools and analytical data. We're making ourselves the Google of cryptocurrencies, and we're going to shape the industry the right way.

Through practice and feedback in the market, PMC tokens will eventually become mainstream tokens in the cryptocurrency world.

Legal Disclaimer

This document does not contain or constitute a sale, subscription, prospectus of any kind, nor does it constitute any warranty of subscription in jurisdictions where this document is unlawful. All statements, forecasts, financial data and other relevant information and data contained in this article may have known and unknown risks and uncertainties that may cause significant differences between expected results and actual results.

The information contained in this article may be used in written or oral communications with existing or potential community members and partners. The information and content of this document may be modified or adjusted with the development of Orion.
The content contained in this white paper may not be exhaustive and does not imply any elements that constitute a contract or agreed conduct. The sole purpose of this document is to provide token holders with relevant and reasonable information so that they can conduct a comprehensive analysis and consideration of the company before acquiring PMC tokens.

Final terms

This white paper is available in multiple languages and the information contained herein may from time to time be translated into other languages or used in the course of written or oral communications with potential PMC Token holders. During such translation or editing, some information contained in this document may be lost, damaged or distorted.

Therefore, the accuracy of other translated versions of the white paper cannot be guaranteed. In case of any disagreement, the content of the English version shall prevail

Thank you for reading

Orion is here to shape the future of crypto trading