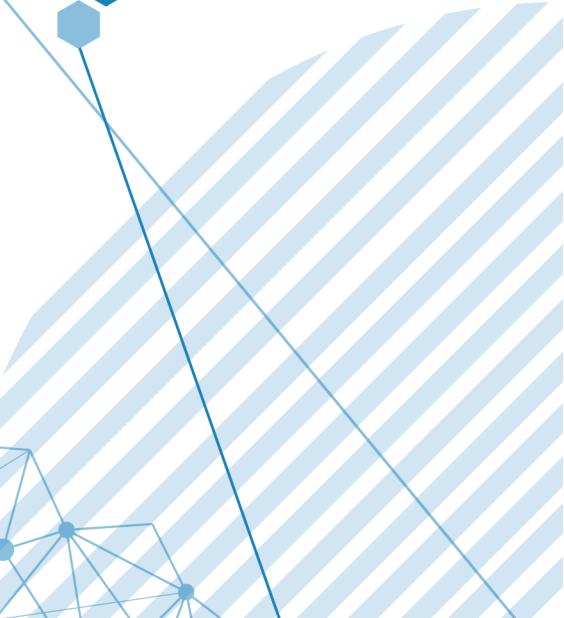




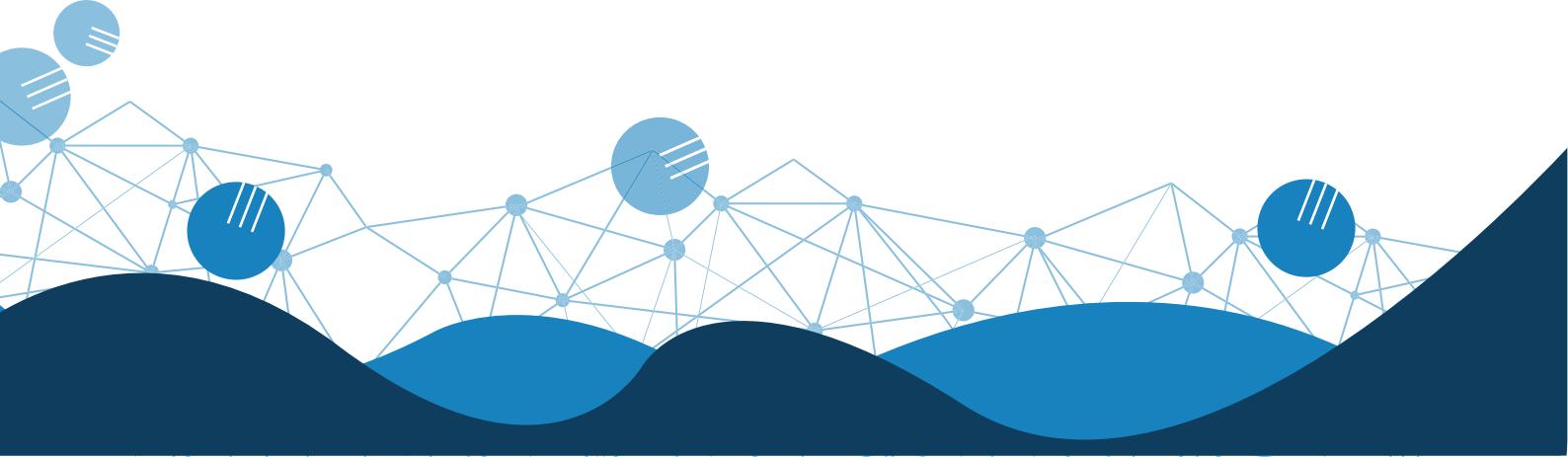
# Precium

**Hybrid Blockchain  
for peer-to-peer Smart Contracts**



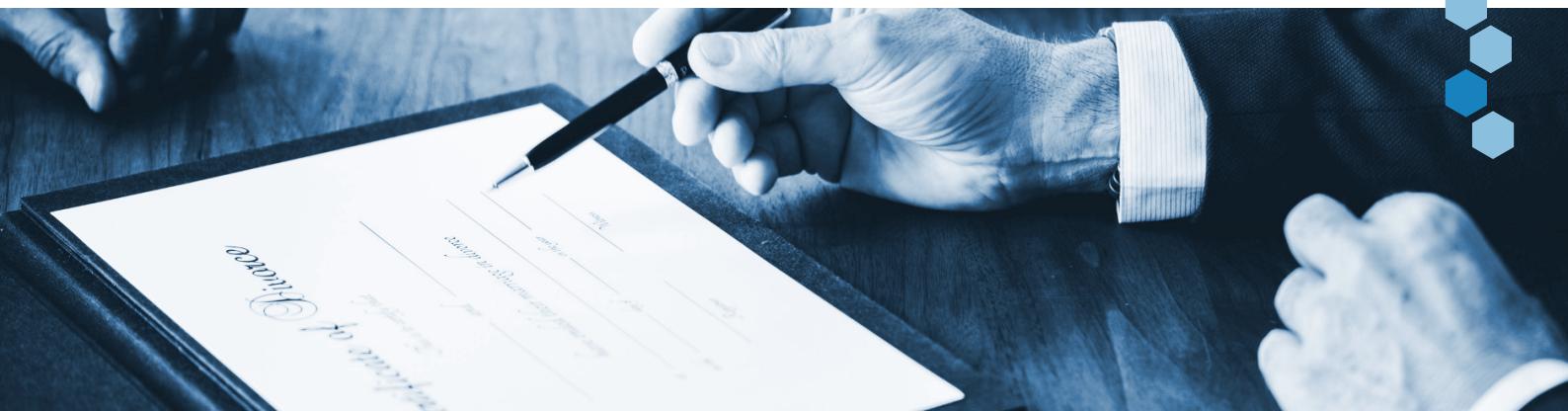
# Whitepaper

<b>Abstract</b>	3
<b>1. INTRODUCTION</b>	4
1.1 Issues of Blockchain	5
1.2 Issues of Smart Contract	8
1.3 Solution of Precium	9
<b>2. PRECIUM PLATFORM</b>	
2.1 Introduction	10
2.2 Architecture	11
2.3 Ecosystem	12
2.4 Applications	13
<b>3. ONYX CHAIN</b>	
3.1 Hybrid Blockchain	15
3.2 Technical Overview	16
3.3 Consensus Protocol for Onyx Chain	19
<b>4. TOKEN ECONOMY</b>	21
<b>5. ACTIVATION PLAN</b>	22
5.1 Roadmap	
5.2 Marketing strategy	
<b>6. TOKEN DISTRIBUTION</b>	23
6.1 Introduction	
6.2 Token sales and ICO fundraise managements	
<b>7. TEAM &amp; PARTNERS</b>	24
<b>8. REFERENCE</b>	27
<b>Disclaimer of Liability</b>	28





## Abstract



Unlike existing methods of data storage in which all data is stored in a centralized server, blockchain technology allows data to be linked together like a chain and shared among all participants, creating a distributed, immutable system. Smart contracts automatically execute according to contract terms set between the contracting parties, fundamentally eliminating the risk of contract failure without any additional administrative costs. These characteristics give smart contracts unlimited potential. However, smart contracts have many technical shortcomings to address for real-world applications. Blockchain, upon which smart contracts are based, is still technologically inadequate in regards to economic efficiency and the reliability of decentralization. Smart contracts are also difficult for normal users to write and use. Additionally, there is still no method to determine with certainty whether or not a smart contract has been fulfilled.

The Precium platform is a new smart contract platform for peer-to-peer (P2P) transactions that allows contracting parties to create and use smart contracts simply and securely. The Precium platform provides users with a template of code for various contract terms, allowing platform users to select and combine their preferred contract terms to create a complete smart contract. In addition, anyone can create and upload contract terms to the Precium platform. These contract terms go through a validation process to ensure users' safety.

Onyx chain, the core of the Precium platform, is a hybrid blockchain that combines public and private blockchains. Onyx chain employs the raft consensus protocol used by Quorum, a representative private blockchain based on go-Ethereum, and simultaneously preserves blockchain's transparency while enjoying a high transaction rate and high scalability. Onyx chain's unique structure combining both public and private blockchains gives it differentiated advantages over other blockchains. It can also use Oracle technology more efficiently, which is a technology that calls information from an off-chain network to an on-chain network on the blockchain.

Onyx chain can secure a competitive advantage over existing blockchains through Precium's unique and efficient hybrid blockchain structure. With this foundation, the Precium platform will contribute to the development of a robust smart contract ecosystem.

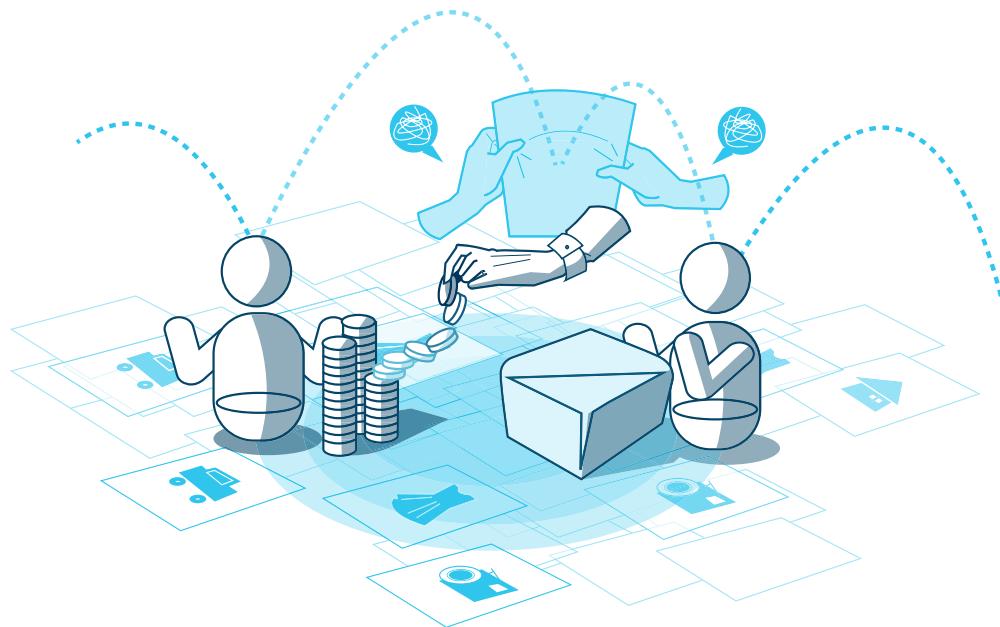




## 1. INTRODUCTION

Various industries recognize blockchain as one of the innovative technologies that will change the future. Enterprises in each industry are making various attempts to apply blockchain to their specific goals. Among these efforts is the active research and development of smart contracts, which can simplify contract procedures. A smart contract refers to a contract on a blockchain that automatically executes according to terms agreed upon by the contracting parties; in reality, they are executed according to the agreement of a number of parties. Depending on the purpose of the blockchain, the parties involved can be anyone who can participate in the blockchain or limited to a certain set of authorized users.

These blockchain-based smart contracts have various advantages. Most importantly, they reduce or completely eliminate the dependence on a middleman, a role necessary for traditional contracts. Smart contracts are well-suited for use in contract structures that require trust between the contracting parties, and have a decisive advantage over middleman systems in terms of productivity and cost savings. Additionally, compared to contracts administered manually, smart contracts are faster and much less prone to human error since they can be automatically managed and executed only through the network.

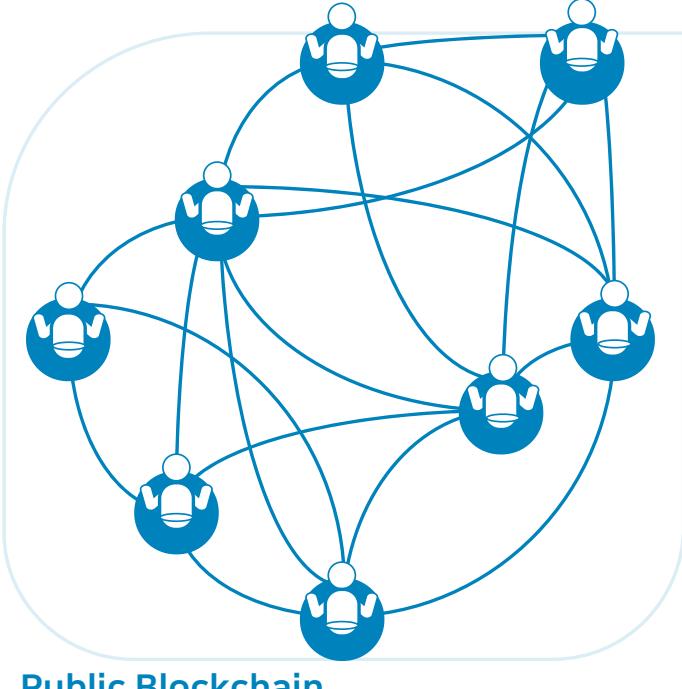


하지만, 블록체인과 스마트 계약이 실제 산업에 사용되기엔 많은 기술적 보완점들이 존재합니다. 스마트 계약의 근간이 되는 블록체인은 탈중앙화의 신뢰성과 경제적 효율성 사이에서 아직 기술적 미흡함이 존재하며, 스마트 계약은 일반 사용자들이 쉽게 작성하고 사용하기 어렵습니다. 또한, 스마트 계약의 계약 이행 여부에 대한 신뢰성 또한 아직 완벽하게 보장되지 못하고 있습니다.

## 1.1 Issues of Blockchain

블록체인은 정보를 기록한 장부를 특정 기관의 중앙 서버가 아닌 P2P(Peer-to-Peer) 네트워크에 분산하고, 참여자가 공동으로 기록하고 관리하는 새로운 분산형 데이터베이스 관리 시스템으로, 다른 말로 분산원장 기술이라고 불리기도 합니다. 따라서, 공동으로 사용되는 데이터들을 한 공간에서 통합적으로 관리하던 기존의 데이터베이스와 매우 차별된 형태를 갖으며, 합의 알고리즘을 통해 원장에 기록될 데이터를 선별하고 검증함으로써, 데이터의 완전성을 유지합니다.

블록체인은 읽기 권한과 쓰기 권한, 그리고 합의 참여 권한을 누가 갖느냐에 따라 크게 퍼블릭 블록체인(Public Blockchain)과 프라이빗 블록체인(Private Blockchain)으로 구분됩니다.

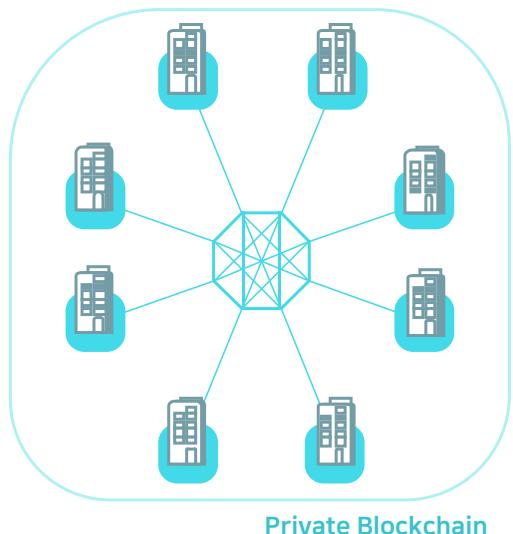


**퍼블릭 블록체인**이란, 거래의 모든 당사자가 거래 정보를 분산원장에 나눠 보관함으로써 거래의 투명성을 확보하는 분산형 데이터베이스 관리 시스템으로, 무허가형 원장(Permissionless Ledger)이라고도 불립니다. 따라서, 네트워크에 참여한 당사자라면 누구나 거래 검증, 생성 및 열람이 가능하며, 널리 알려진 비트코인(Bitcoin), 이더리움(Ethereum) 등이 이에 해당됩니다.

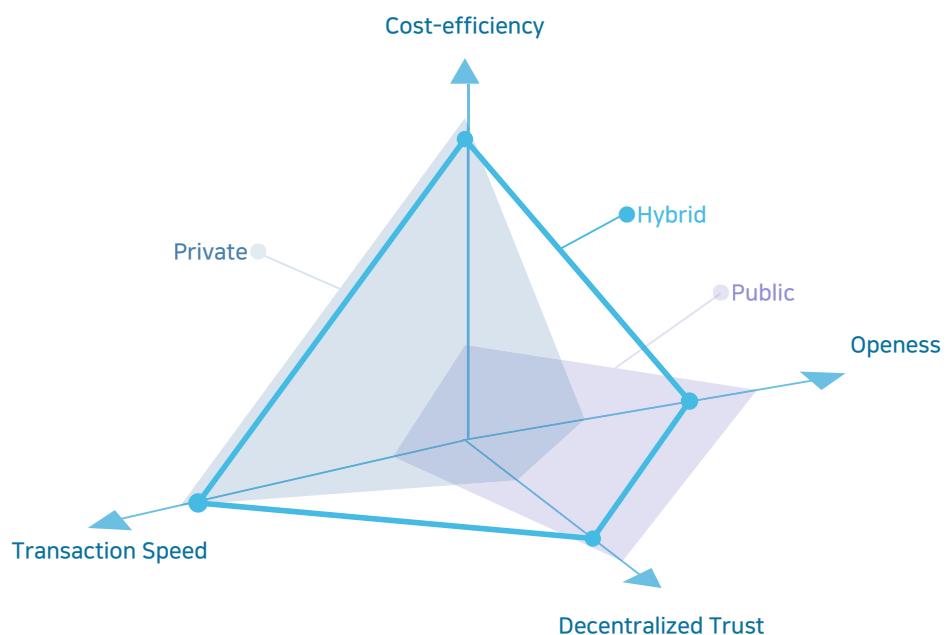
퍼블릭 블록체인은 중앙 관리 시스템에 비해 해킹으로부터의 보안 및 신뢰문제에서 강력한 힘을 발휘하지만, 느린 처리속도, 확장성의 한계와 같은 기술적 문제 및 가격 변동성으로 인해 실제 산업분야에 활용되는데 많은 어려움을 겪고 있습니다.

물론, 플라즈마(Plasma), 샤딩(Sharding), 라이덴(Raiden), DAG(Directed Acyclic Graph) 등 퍼블릭 블록체인의 기술적 한계를 극복하기 위한 많은 기술들이 연구 및 개발 중에 있지만, 블록체인의 트릴레마(Trilemma)로 꼽히는 탈중앙화(Decentralization), 보안(Security), 그리고 확장성(Scalability)을 동시에 해결할 수 있는 방안은 제시되지 못하고 있습니다.

허가형 원장(Permissioned Ledger)이라고도 불리는 **프라이빗 블록체인**은 특정 노드만 참여할 수 있는 블록체인으로, 최근들어 기업들의 큰 관심을 받고 있습니다. 기업의 입장에서, 프라이빗 체인은 신뢰할 만한 노드들을 직접 선발하기 때문에 관리가 수월하며, 이 노드들은 신뢰가 보장되기 때문에, 퍼블릭 블록체인과는 다른 개념의 합의를 통해 빠른 처리속도와 높은 확장성을 가질 수 있습니다. 하지만, 결국 참여하는 노드를 특정 기관 또는 기업으로 제한하는 프라이빗 블록체인은 서비스 제공자에 전적으로 의존해야 하기 때문에 신뢰성의 한계를 갖고 있습니다.



퍼블릭 블록체인과 프라이빗 블록체인은 투명성, 보안성, 확장성 및 비밀유지 측면에서 명확한 장단점을 갖습니다. 퍼블릭 블록체인은 누구나 참여가 가능하기 때문에 탈중앙화를 지향하며, 수많은 참여자들이 원장을 나누어 보관하기 때문에 강력한 보안성을 가집니다. 반면, 프라이빗 블록체인은 허가 받은 노드만 참여하기 때문에, 개인 정보 보호를 더 강화할 수 있고, 성능과 비용상에서 큰 이점을 갖습니다.



결국, 퍼블릭 블록체인과 프라이빗 블록체인은 신뢰와 속도에 대한 트레이드 오프(trade-off)의 관계를 갖는다고 볼 수 있으며, 많은 블록체인 전문가들은 이 두 블록체인의 범주 간의 경계가 모호해질 것이라고 예상하고 있습니다.

## 1.2 Issues of Smart Contract

스마트 계약이란, 1996년 Nick Szabo에 의해 처음 제안된 개념으로, 이더리움 가상머신의 튜링-완전성을 통해 빛을 발하게 되었는데, 그 중심에는 자동화된 계약 메커니즘이 있습니다.

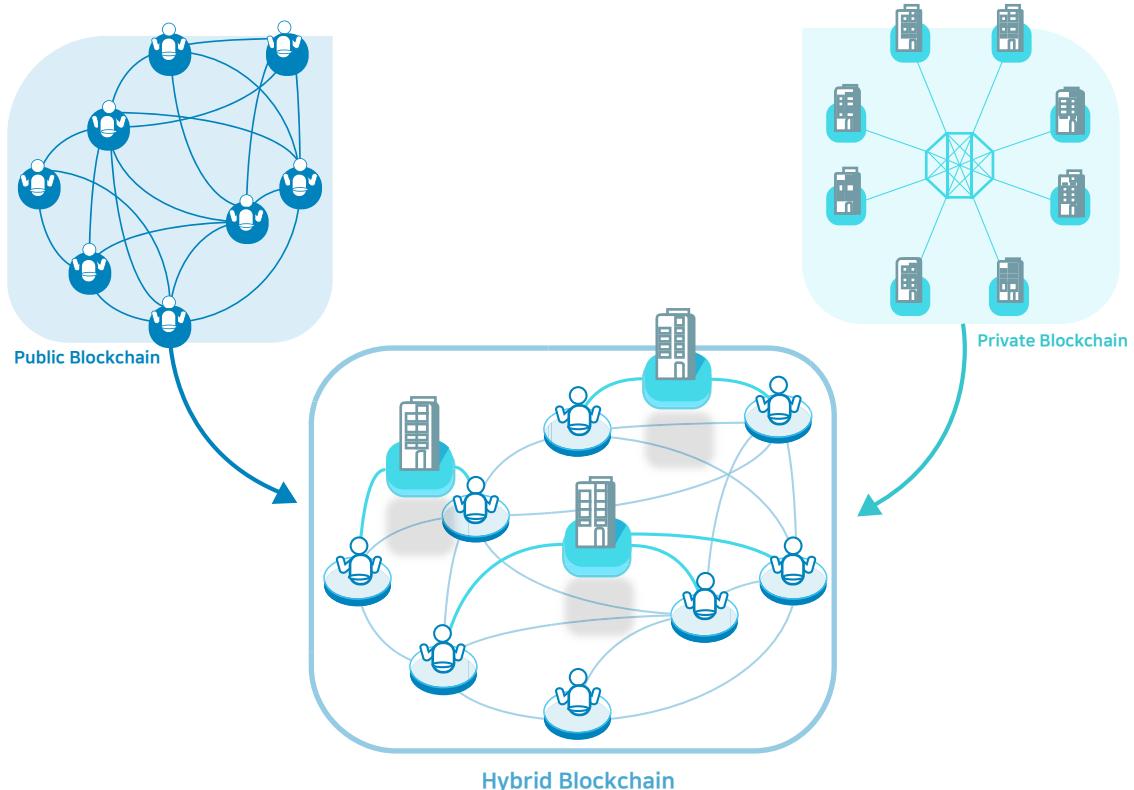
스마트 계약의 가장 큰 장점은, 중개인이 없이 신뢰도 높은 계약을 직접 체결할 수 있다는 것입니다.

이는 곧, 낮은 실행위험과 비용 절감으로 이어지기 때문에, 금융거래, 부동산 계약, 무역 등 다양한 분야의 기업들이 관심을 갖도록 하는 원동력이 되고 있습니다.

하지만, 스마트 계약이 실생활에서 자유롭게 사용되기 위해선 기술적으로 보완해야 할 많은 문제들이 존재합니다. 우선, 사람들이 자신이 원하는 스마트 계약을 만들기 위해선, 프로그래밍 언어를 기반으로 계약 조건과 내용을 코딩해야 하는데, 이는 일반인이 직접 다루기엔 어려운 부분이 존재합니다. 또한, 한번 만들어진 스마트 계약은 일부 조건을 수정하여 재사용 할 수 없기 때문에, 비효율적인 측면이 존재합니다. 특히 보안적 측면에서, 만약 코드의 오류 또는 취약점이 존재할 경우, 이는 사용자에게 막대한 손실을 입힐 수 있습니다.

스마트 계약 내의 조건들에 대한 이행 여부를 판단하는 블록체인의 합의 과정 또한 불완전한 부분이 존재합니다. 스마트 계약은 블록체인에 담겨 있기 때문에, 블록체인 외부의 정보를 사용할 경우, 스마트 계약의 신뢰도는 해당 정보의 신뢰도에 의존성을 갖게 됩니다. 따라서 블록체인 외부 네트워크(Off-chain) 상의 정보가 누락되거나 변조되어 블록체인 내부 네트워크(On-chain)로 들어올 경우, 이는 스마트 계약의 신뢰성에 큰 타격을 줄 수 있습니다. 또한, 온체인 상의 정보를 확인하기 위해, 많은 노드들이 계속해서 외부 정보를 가져와야 하는데, 이 과정에서도 많은 문제가 발생할 수 있습니다.

### 1.3 Solution of Precium



Precium은 퍼블릭 블록체인과 프라이빗 블록체인을 결합한 **하이브리드 블록체인(Hybrid Blockchain)**인 *Onyx Chain* 개발을 통해 현존하는 블록체인의 문제들을 해결하는 것을 목표로 합니다.

Onyx Chain은 퍼블릭 블록(Public Block)과 프라이빗 블록(Private Block)을 같이 사용할 수 있는 구조로 이루어져 있으며, go-Ethereum 기반의 프라이빗 블록체인인 Quorum이 사용하는 Raft 합의 프로토콜을 발전시켜, 블록체인의 투명성을 유지하면서 동시에 빠른 전송속도와 높은 확장성을 갖는 것을 목표로 하고 있습니다.

Onyx Chain은 퍼블릭 블록체인이 스마트 계약에서 갖는 문제점을 개선하여, 높은 신뢰도를 갖고 실생활에 적용되는 것을 지향합니다. 스마트 계약의 기본적인 정보는 퍼블릭 블록을 통해 공개되며, 계약에 대한 상세 내용은 프라이빗 블록을 통해 당사자들만 확인할 수 있도록 하여 계약 내의 비밀정보를 보호합니다. 또한, 블록체인 외부 네트워크 상의 정보를 블록체인 네트워크 내부로 들여오는 기술인 오라클(Oracle)을 퍼블릭 블록이 아닌 프라이빗 블록에서 사용함으로써, 퍼블릭 블록체인에 비해 높은 효율성을 갖습니다.

Precium 플랫폼은 Onyx Chain을 기반으로, 안전성이 보장된 스마트 계약을 보다 편리하게 사용할 수 있도록 하는데 목적이 있습니다. Precium 플랫폼 내에서, 사용자들은 프로그래밍 없이 자신이 원하는 계약 조항을 선택하고 조합하는 과정을 통해 P2P로 스마트 계약을 진행할 수 있습니다. 또한, 누구나 계약 조항들을 만들어 Precium 플랫폼에 올릴 수 있으며, 이 계약 조항은 검증과정을 거쳐 사용자들에게 제공되기 때문에, 안전성이 보장됩니다.

## 2. PRECIUM PLATFORM



### 2.1 Introduction

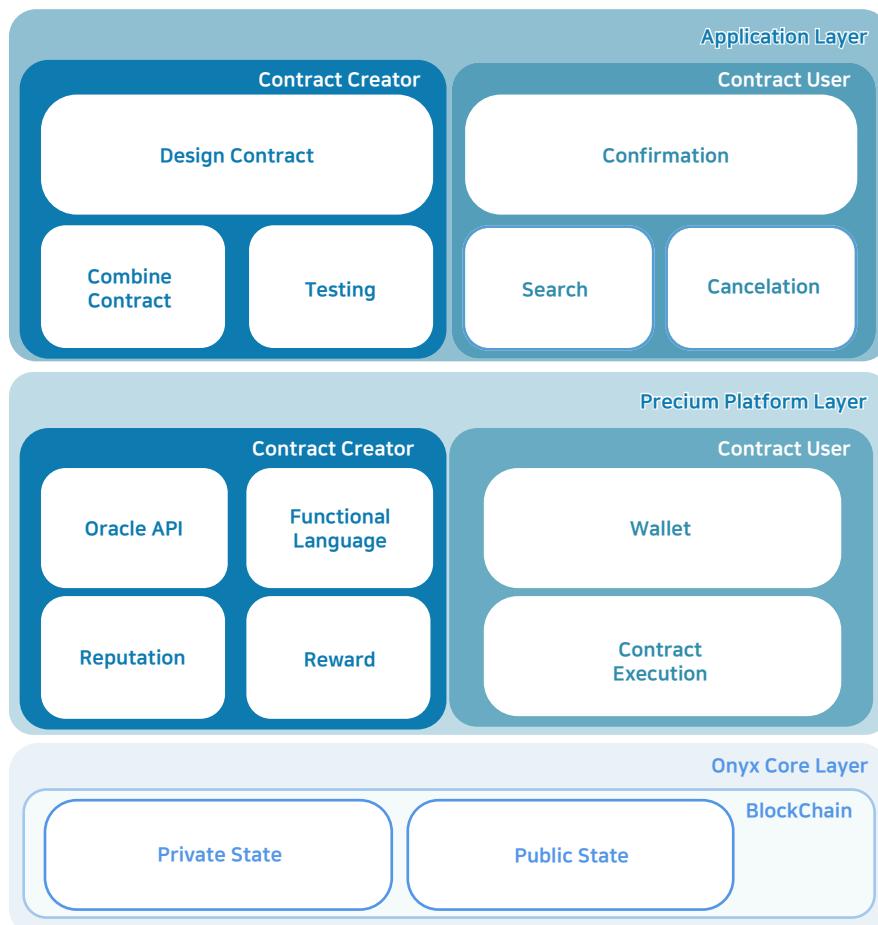
Precium 플랫폼은 P2P(peer-to-peer) 거래에 있어서, 사람들이 간단하면서도 안전하게 스마트 계약을 만들고 사용할 수 있도록 지원하는 **Onyx Chain 기반의 스마트 계약 플랫폼**입니다. 기존의 스마트 계약 플랫폼은, 개발자가 코딩을 통해 계약 조항들을 코드화 하여 하나의 스마트 계약서를 만들고, 이를 사용자들이 이용하는 방식으로 구성되어 있습니다. 하지만, 이 방식은 일반인들이 자신이 원하는 스마트 계약을 직접 구성하는데 큰 진입장벽으로 작용하고 있습니다.

Precium 플랫폼은 수많은 스마트 계약의 조항들을 템플릿화 하여 사용자에게 제공함으로써, 스마트 계약에 대한 사용자의 진입장벽을 낮추는데 뜻을 두고 있습니다.

Precium 플랫폼 사용자는 자신이 원하는 계약 조항들을 선택하고 조합하는 것 만으로 계약서를 완성할 수 있으며, 플랫폼은 템플릿화 되어있는 선택된 각 계약 조항 코드들을 조합하여 하나의 완성된 스마트 계약을 제공합니다. 따라서, 사용자는 별다른 프로그래밍 없이 스마트 계약을 사용하여 자신이 원하는 상대와 P2P로 거래할 수 있게 됩니다.

이러한 과정은 스마트 계약의 재사용에 있어서도 큰 효율성을 갖습니다. 실생활에 사람들 간에 체결되는 많은 계약들은 서로 다른 목적을 위해 존재하지만, 많은 공통적인 계약 조항을 포함하고 있습니다. 예를 들어, 계약 기간, 계약 내용을 수행해야 하는 횟수 및 시간 등이 이에 해당합니다. Precium 플랫폼에는, 위와 같은 공통적인 조항 뿐만 아니라, 일정 분야에 특화된 다양한 계약 조항들을 미리 검증된 코드로 보관하고, 이를 템플릿화 하여 제공합니다. 따라서, 계약 조항들의 재사용이 매우 용이하며, 검증된 코드를 반복해서 사용할 수 있기 때문에 코드 오류 등의 문제를 줄일 수 있습니다.

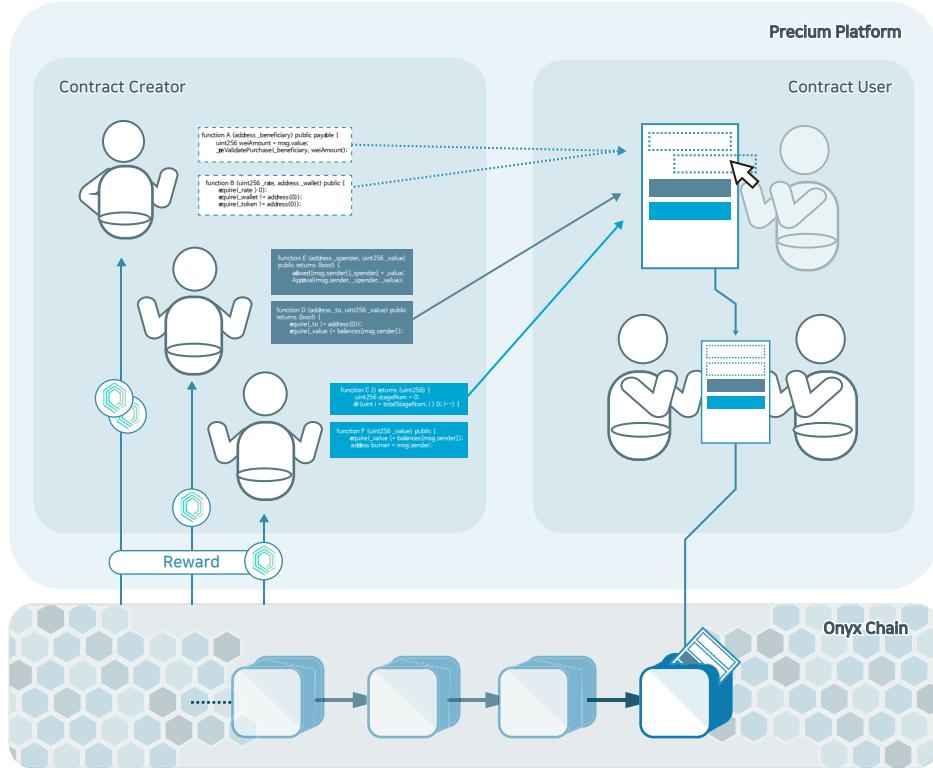
## 2.2 Architecture



Precium 아키텍처는 세 개의 Layer로로 구성되어 있습니다. 가장 기초가 되는 **Onyx Core Layer**는 Precium 플랫폼 상의 모든 계약이 생성되고 기록되는 Onyx Chain이 존재합니다. 나머지 두개의 Layer인 **Precium Platform Layer** 와 **Application Layer**는 계약생성자(Contract Creator)와 계약사용자(Contract User)를 구성원으로 갖습니다. **Precium Platform Layer**는 계약생성자와 계약사용자를 위한 기능을 담당하는 층으로, 계약생성을 위한 Oracle API, Functional Language, Reputation, Reward와 계약사를 위한 Wallet, Contract Execution의 기능으로 구성되어 있습니다. 최상위 Layer인 **Application Layer**는 Precium Platform Layer의 기능들을 이용하여 계약생성자와 계약사용자가 사용할 수 있는 다양한 어플리케이션들이 존재합니다.

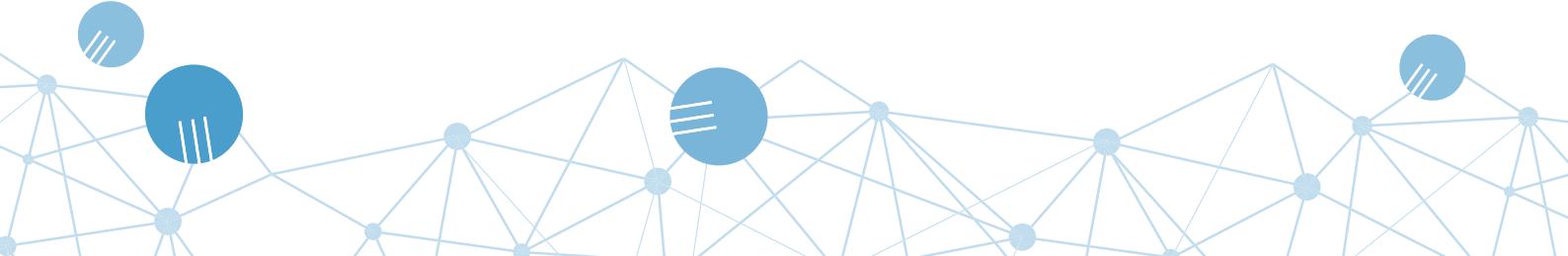
## 2.3 Ecosystem

Precium 플랫폼은 스마트 계약의 조건들을 템플릿화 하여 제공하는 **계약생성자**와 조건들을 사용하여 계약을 맺는 **계약사용자**를 구성원으로 하며, 플랫폼 상에서 누구나 계약생성자, 또는 계약사용자가 될 수 있습니다.



계약생성자는 Precium 플랫폼 상에 사용될 수 있는 다양한 계약 조건을 코드화 하여 계약사용자에게 제공하는 이들을 뜻합니다. 계약생성자는 자신이 구상한 계약 조건을 코드화 한 후, Onyx Chain 상에서 직접 시험할 수 있고, 플랫폼에 업로드할 수 있으며, 이 코드는 플랫폼 상에서 검증을 받게 됩니다. 이 검증을 통해 코드 내의 에러로 인해 발생할 수 있는 다양한 계약에서의 문제들을 미연에 방지할 수 있습니다. 검증을 통과한 코드는 템플릿화 되어 계약사용자들에게 제공되며, 계약사용자들이 해당 템플릿을 사용하여 계약을 맺으면, 해당 템플릿을 제공한 계약생성자들은 Onyx Coin을 보상으로 받을 수 있습니다.

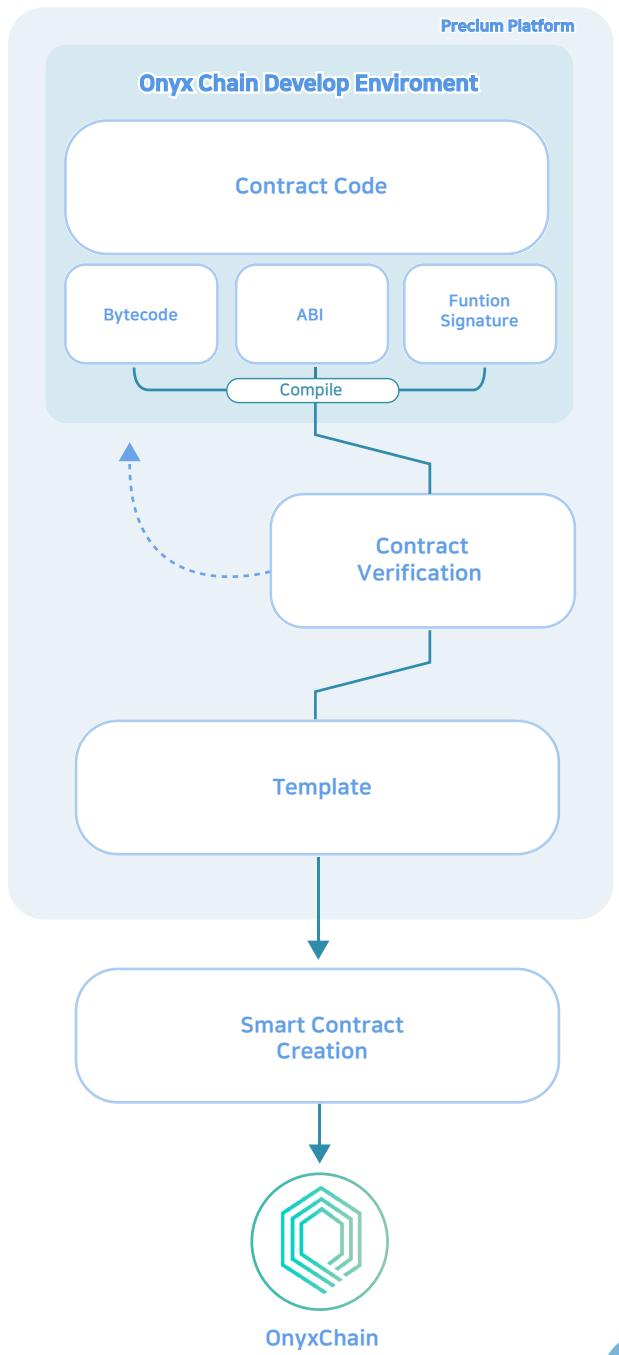
계약사용자는 Precium 플랫폼상이 제공하는 계약 템플릿 중, 자신이 필요로 하는 계약 조건들을 간단히 조합하여 하나의 완성된 스마트 계약을 구성할 수 있습니다. 이 스마트 계약은 Onyx Chain상에 저장되고 자동 이행되며, 앞에서 언급된 것처럼 스마트 계약의 기본적인 정보는 Onyx Chain의 퍼블릭 블록을 통해 공개하되, 계약에 대한 상세 내용은 Onyx Chain의 프라이빗 블록을 통해 당사자들만 확인할 수 있도록 하여 계약 내의 비밀정보를 보호합니다.

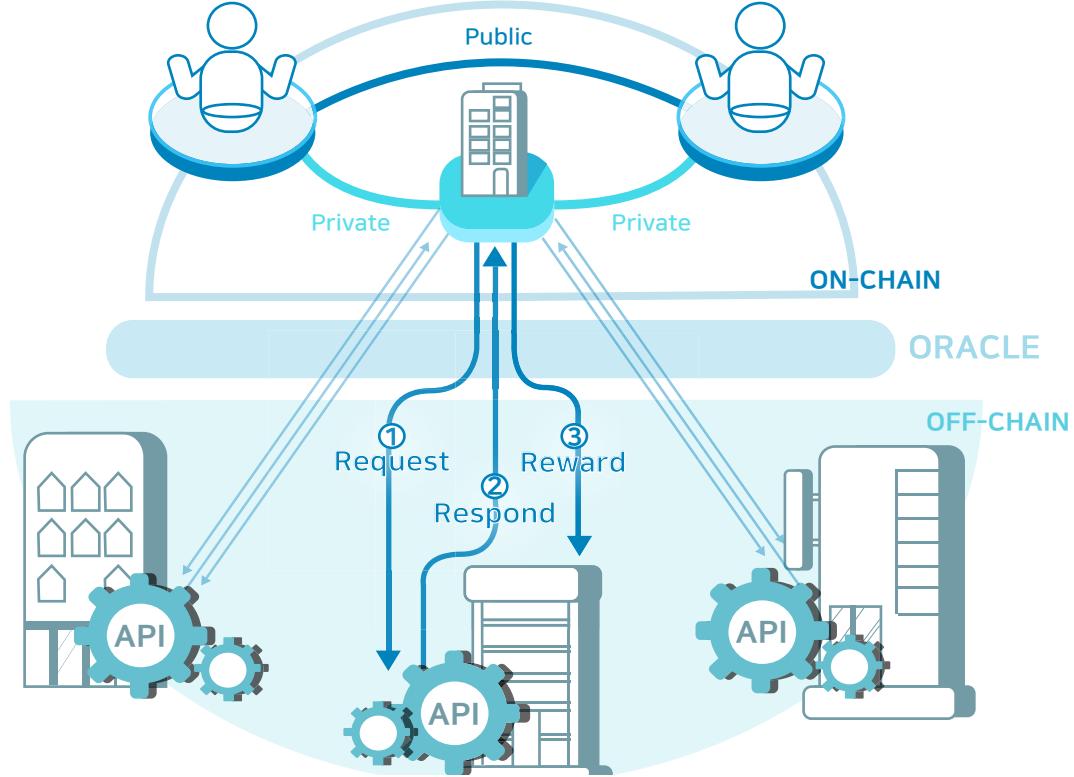


## 2.4 Applications

Precium 플랫폼은 Onyx Chain 상에서 계약생성자가 계약 템플릿을 구성할 수 있는 최적의 환경을 제공합니다. 계약생성자가 Precium Solidity를 사용하여 계약 조항을 프로그래밍 한 후 컴파일하게 되면, 컴파일러는 Bytecode 와 Function Signature, 그리고 ABI를 제공합니다. 여기서 Byte Code는 16진수로 표현된 스마트 계약 코드의 컴파일 결과이며, Function Signature 와 ABI는 스마트 계약 함수들과, Parameter에 대한 Metadata 를 포함하고 있습니다. 이는 이더리움의 Smart Contract 개발환경과 동일한데, Onyx Chain의 기반이 되는 Quorum이 이더리움을 기반으로 만들어진 블록체인입니다.

이는 곧, 이더리움의 스마트 계약만큼, Onyx Chain의 스마트 계약이 안정성을 보장함을 의미합니다. 컴파일이 완료된 계약 코드는 작성자의 의도, 목적과 함께 플랫폼으로 전달되며, Precium 플랫폼에서는 이 코드에 대한 검증을 진행합니다. 최종적으로 검증이 완료된 계약은 플랫폼의 템플릿에 추가되며, 계약사용자는 여러 계약 조항들을 조합하여 하나의 계약을 구성하고, 플랫폼은 저장된 템플릿의 코드를 조합하여 하나의 완전한 스마트 계약을 Onyx Chain을 통해 제공할 수 있습니다.



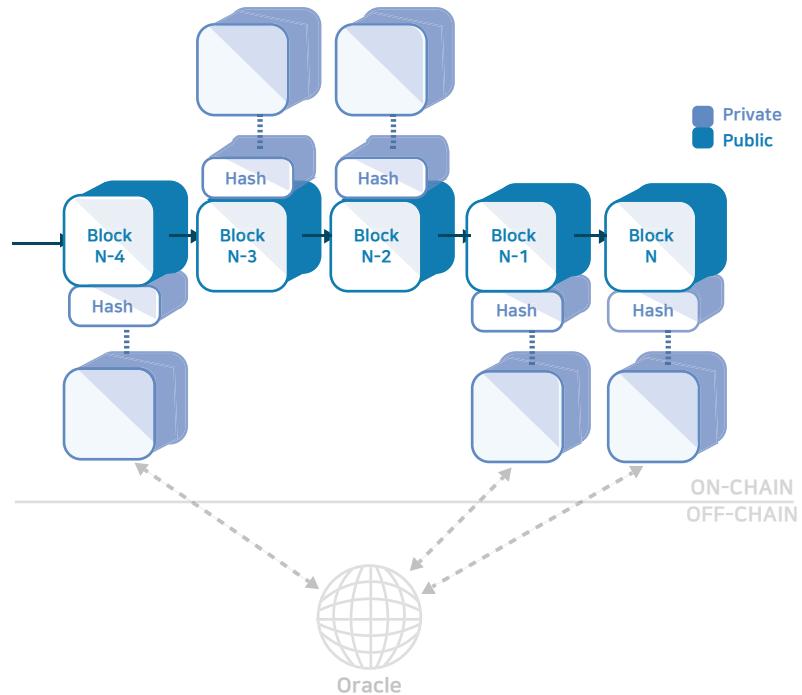


스마트 계약의 신뢰성을 극대화하기 위해선, 오라클 기술을 통해 블록체인 외부 네트워크로부터 블록체인 내부로 들어오는 정보에 대한 신뢰도가 매우 중요합니다. 이는 오라클로부터 들어온 블록체인 외부 정보를 토대로, 스마트 계약의 계약 조건에 대한 이행 여부를 판단하기 때문입니다. 이 신뢰도를 높이기 위해, Precium에서는 오라클에게 외부 정보를 제공하는 API를 구성하는 기관 및 연구소와 협력하여 개발자에게 최적화된 다양한 API를 제공하고자 합니다. 이를 통해, 계약생성자들은 신뢰도 높은 외부 정보를 갖고 계약 조항을 코드화 할 수 있습니다. 또한, API를 제공하는 기관 및 연구소는 스마트 계약에서 사용되는 API의 사용 빈도수에 비례하여 Onyx Coin을 보상으로 받을 수 있습니다. 이는 Precium 플랫폼이 신뢰도 높은 정보를 받는 차원을 넘어, 스마트 계약을 사용할 수 있는 다양한 시장들을 활성화하는 역할을 할 것으로 기대할 수 있습니다.



## 3. ONYX CHAIN

### 3.1 Hybrid Blockchain



Onyx Chain은 퍼블릭 블록체인과 프라이빗 블록체인을 결합한 하이브리드 블록체인의 구조를 갖고 있습니다. 위 그림과 같이, Onyx Chain의 각 퍼블릭 블록은 페어에 해당하는 프라이빗 블록의 해쉬값을 포함하는 형태로 두 블록의 연결성을 확보하고 있습니다. 따라서, Onyx Chain의 퍼블릭 블록은 누구나 자유롭게 열람할 수 있는 반면, 프라이빗 블록은 해당 블록의 당사자만이 열람할 수 있습니다. 또한, Onyx Chain은 오라클 기술을 통해 블록체인 외부 정보를 전달받을 때, 프라이빗 블록을 이용합니다. 따라서, 수많은 노드들이 오라클 API에 접속하여 계약 내용을 검증해야 하는 퍼블릭 블록체인에 비해 높은 효율성을 갖습니다.

결론적으로, Onyx Chain은 프라이빗 블록에 대한 해시를 공증하기 위해 퍼블릭 블록체인을 이용하는 하이브리드 블록체인의 구조적 성격을 지닌 블록체인이라 정의할 수 있습니다.

Onyx Chain은 스마트 계약을 사용하는데 있어 매우 효율적인 구조를 갖고 있습니다. 퍼블릭 블록체인의 스마트 계약의 경우, 계약 당사자의 의지와 상관없이 모든 계약 내용을 누구나 열람할 수 있지만, Onyx Chain은 프라이빗 블록에 계약의 상세 정보들을 담음으로써, 계약 당사자들만 열람이 가능하도록 합니다.

### 3.2 Technical Overview

Onyx Chain은 프라이빗 블록체인인 Quorum이 사용하는 Raft 합의 프로토콜을 발전시켜, 블록체인의 투명성을 유지하면서 동시에 빠른 전송속도와 높은 확장성을 갖습니다. Quorum은 J.P.Morgan Chase에서 개발한 Ethereum을 기반으로 한 분산원장 프로토콜로, Go Ethereum 클라이언트를 최소한으로 포킹하여 설계되었습니다.

*"Quorum is an Ethereum-based distributed ledger protocol that has been developed to provide the Financial Services Industry with a permissioned implementation of Ethereum that supports transaction and contract privacy." - J.P.Morgan*

Quorum은 트랜잭션과 계약의 프라이버시, 다중 투표 기반의 합의 메커니즘, 네트워크 및 피어 노드의 참여 권한 및 높은 퍼포먼스 등의 주요 특징을 가지고 있습니다. 특히, 모든 노드가 자유롭게 참여 가능한 Ethereum과 달리, Quorum에 노드로서 참여하기 위해선 권한을 부여 받아야 하기 때문에, 프라이빗 블록체인에 해당됩니다. Onyx Chain은 Quorum 고유의 특징을 최대한 유지하되, 동시에 퍼블릭 블록체인의 투명성과 보안성을 갖는 것을 목표로 합니다.

Quorum에는 다양한 합의 프로토콜을 사용할 수 있으며, QuorumChain, Istanbul BFT, Raft 등이 대표적인 프로토콜입니다. 이들은 블록 생성 속도 및 방법, 그리고 트랜잭션의 최종성 등에서 각기 다른 특징을 갖는데, 그 중, Raft 프로토콜은 기존 분산시스템에서 사용되던 비동기식 합의 프로토콜로, 시스템을 구성하는 구성원들 중 일부가 시스템의 구성 활동에 실패해도 생존 가능한 일관된 시스템을 만들 수 있게 해주는 역할을 합니다. 시스템을 구성하는 구성원(서버)들은 일정 기간 동안 리더, 후보자, 팔로워의 상태 중 하나의 상태로 존재합니다.

일반적인 경우, 하나의 리더와 나머지 팔로워들로 구성되어 있으며 팔로워들은 리더 및 후보자들의 요청에 대한 응답만 할 뿐 직접 요청을 하지는 않습니다. 반면, 리더의 경우 모든 클라이언트들의 요청을 관리하며, 후보자는 새로운 리더로 선출될 때 존재하는 상태입니다. 각 구성원들은 현재 시점의 기간 번호를 저장하며, 각 기간들은 임의의 길이를 갖습니다. 그리고 해당 기간 번호는 각 구성원들이 소통할 때 교환되고, 이 때 구성원들 간의 기간 번호가 다를 경우, 최신 번호로 업데이트 됩니다. 또한, 리더 혹은 후보자가 예전의 기간 번호를 가지고 있을 경우 팔로워 상태로 바뀌며, 예전 기간 번호를 가진 요청은 거절됩니다.

이러한 과정을 통해, 구성원들 간의 정보를 공유하고 새롭게 업데이트를 진행하며 시스템이 원활히 작동할 수 있게 합니다. Raft 프로토콜은 분산시스템 상에서 구성원들의 합의를 이루는데 있어 리더 선출, 로그 복제 및 안전성 등의 주요 구성요소로 이루어져 있습니다.

### ■ 리더선출

Raft 프로토콜에서는 일정 기간마다 구성 노드들 중 하나의 노드가 리더로 선출됩니다. 만약 해당 기간에 리더 선출이 실패했을 경우, 그 다음 기간에 다시 리더를 선출하게 됩니다. 그리고 선출된 노드는 강한 영향력을 지닙니다. 이때 리더 선출은 최대 하나의 노드만 리더로 선출될 수 있도록 보장합니다. 일정 기간 동안 선출된 리더는 다른 노드들과 소통하며 로그에 추가할 사항에 대해 결정하게 됩니다.

### ■ 로그 복제

Raft 프로토콜에서는 선출된 리더가 클라이언트의 요청들을 처리합니다. 각 클라이언트들의 요청은 커맨드가 포함되어 있으며, 리더는 이 커맨드들을 로그에 새롭게 추가하고, 구성원들에게 해당 항목을 복제할 수 있도록 로그 추가에 대한 원격 절차 호출을 진행합니다. 만약, 팔로워들이 느리게 반응하거나, 작동을 하지 못하거나, 혹은 네트워크 상의 문제가 있을 경우, 리더는 계속해서 반복하여 모든 팔로워들이 추가된 로그를 저장할 수 있도록 합니다. 이때, 리더는 로그에 기록된 항목들을 수정 및 삭제가 불가능하며, 오직 새로운 항목을 로그에 추가할 수 있습니다.



## ■ 안전성

앞에서 언급한 리더 선출과 로그 복제 외에, Raft 프로토콜은 리더로 선출될 수 있는 각 구성원들에게 제약을 더해 안전성을 확보합니다. 특정 기간에 선출된 리더는, 그 이전 기간에 추가된 모든 항목들을 가지고 있어야 합니다. 즉, 특정 기간에 어떤 로그 항목이 추가되었을 때, 해당 항목은 리더의 로그 항목 중 가장 최신 항목이어야 함을 보장해야 하며, 이를 통해 안전성을 확보합니다.

Raft 프로토콜은 앞의 특성들을 바탕으로, 분산 시스템에서 각 구성원들이 시스템의 구성 활동에 실패하더라도 전체 시스템의 작동이 원활하게 이루어짐을 보장합니다.

하지만 Raft 프로토콜은 프라이빗 블록체인에 적합한 특징들을 갖고 있기 때문에, 하이브리드 블록체인인 Onyx Chain의 합의 프로토콜로 사용하기에는 적합하지 않습니다.

기존의 분산시스템 환경에서는 전체 시스템을 구성하는 각 구성원들에 대한 신뢰가 기본 바탕으로 되어있습니다. 하지만 Onyx Chain은 퍼블릭 블록과 프라이빗 블록에 페어를 이루는 구조를 갖고 있기 때문에, 참여하는 모든 노드를 신뢰하기 힘들다고 가정해야 합니다. 따라서, 일부 노드들이 자신들의 이익을 위해 행동할 때에도 전체 시스템이 문제없이 작동해야 하므로, 기존의 Raft 프로토콜을 보완할 필요성이 있습니다.



### 3.3 Consensus Protocol for Onyx Chain

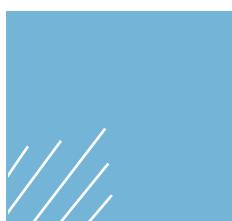


Onyx Chain에서는, 시스템을 구성하는 노드를 신뢰할 수 없는 문제를 해결하기 위해 개발된 기법인 BFT(Byzantine Fault Tolerance)를 지원하는 변형된 Raft 프로토콜을 사용합니다.

Onyx Chain에 사용되는 새로운 프로토콜은, PBFT(Practical Byzantine Fault Tolerance) 합의 알고리즘을 기반으로 합니다. 기존의 BFT 합의 알고리즘이 동기식 네트워크에서만 합의가 가능했다면, PBFT 알고리즘은 Byzantine 노드가 있는 비동기식 네트워크에서도 합의가 가능하도록 합니다.

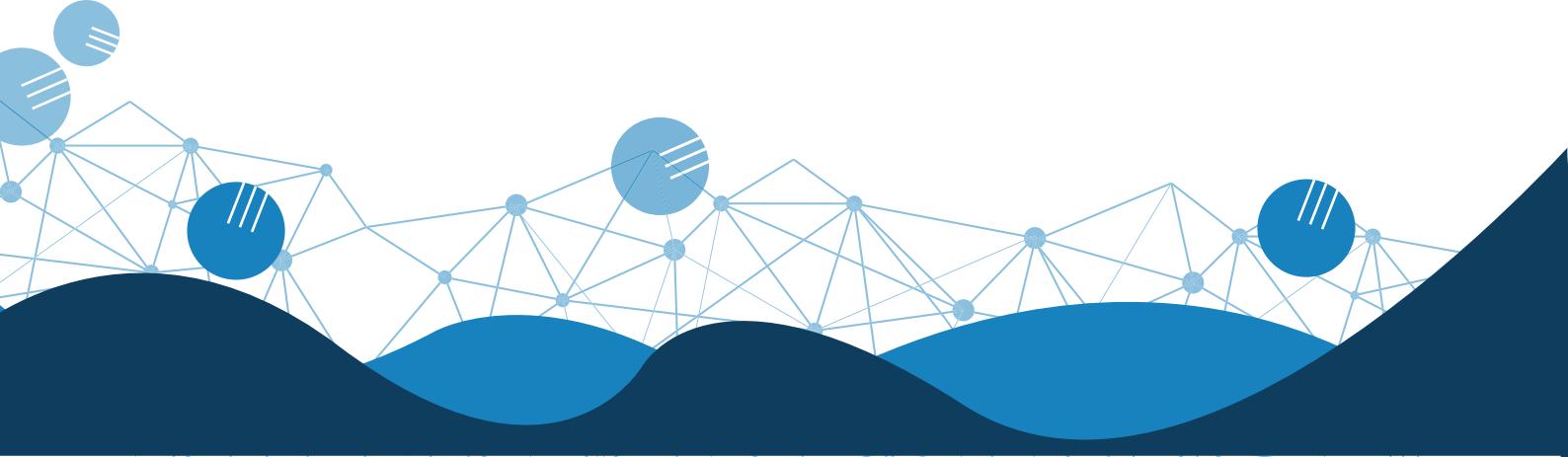
이 프로토콜에서 시스템 상의 각 노드들은 로그 항목에 대해 암호화 해시를 저장하는데, 현재 로그 항목에 대한 암호화 해시를 구하기 위해 이전 암호화 해시를 이용하는 재귀적 방법을 이용하여 과거부터 기록된 로그들의 무결성 및 완전성을 확인시켜 줍니다. 이는 이전의 기록부터 누적되는 암호화 해시의 특성을 이용하기 때문에 가능하며, 누적된 로그들의 매칭을 통해, Byzantine 노드들이 로그를 조작하는 일을 방지합니다.

Onyx Chain의 시스템 상의 노드들은 각각 고유의 공개키와 비공개키 쌍을 가지고 있습니다. 각 노드 및 클라이언트들은 서로의 공개키를 공유하며, 메시지를 전송할 때 해당 노드의 비공개키로 서명을 합니다. 메시지를 받는 측에서는 서명한 노드의 공개키를 이용해 서명을 검증하고, 만약 담긴 서명이 유효하지 않다면, 메시지는 거부됩니다. 이를 통해 Byzantine 노드들이 일반 노드들처럼 행동하는 것을 방지합니다.

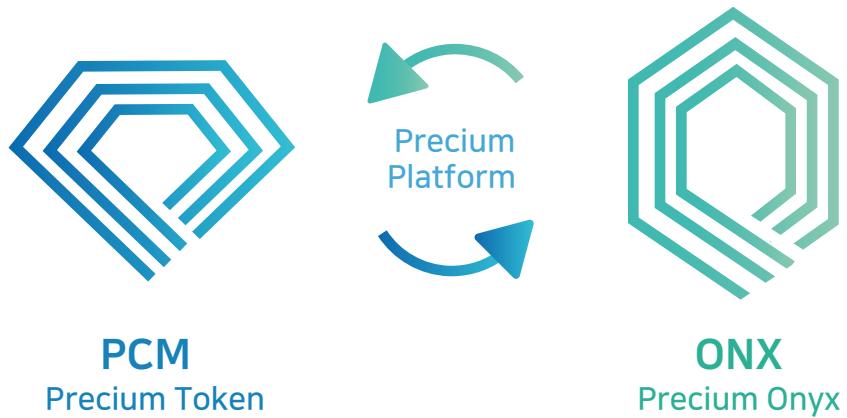


만약 현재 Onyx Chain 시스템의 리더가 Byzantine 노드일 경우, 리더가 악의적으로 시스템 상의 모든 요청을 무시하는 상황이 발생할 수 있습니다. 이를 방지하기 위해, 클라이언트들은 리더가 악의적으로 프로세스를 진행하지 않을 경우 이 리더의 권한을 중재할 수 있습니다. 그리고 새로운 리더 선출을 개시할 수 있도록 하여 Byzantine 리더가 시스템을 방해하는 것을 방지합니다. 또한, 리더 선출 시, 각 기간마다 하나의 후보자가 있어야 하며, 노드들은 여러 기간들에 대해 일정한 스케줄에 의해 후보자가 됩니다. 그리고 리더 선출 과정을 시작하기 위해, 노드는 다른 클라이언트들로부터 일정 수 이상의 선출 요청을 받아야 합니다. 이를 통해 일정 기간 이상 동안 리더가 잘못되지 않음을 보장할 수 있으며, 리더 선출이 Byzantine 노드에 의해 마음대로 시작되는 것을 방지합니다.

최근 Raft 프로토콜에 BFT를 지원하기 위한 다양한 기법들이 연구되고 있습니다. Precium은 Onyx Chain의 구조에 최적화 될 수 있는 합의 프로토콜을 지속적으로 개발할 예정이며, 이를 통해 하이브리드 블록체인의 발전을 선도 할 것입니다.



## 4. TOKEN ECONOMY

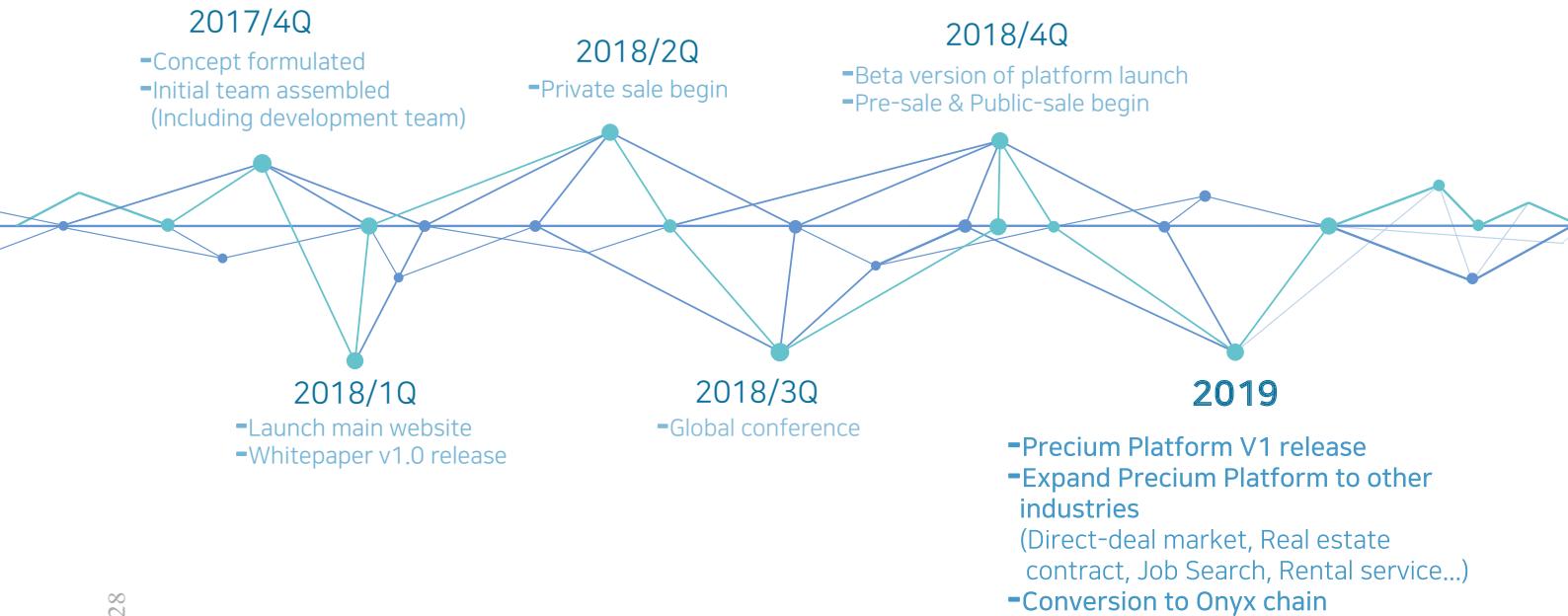


Precium의 Token economy는 Precium Token인 PCM과, Onyx Coin인 ONX로 이루어져 있습니다. PCM은 이더리움 네트워크상에서 유통할 수 있는 토큰의 호환성을 보장하는 토큰 표준인 ERC20을 사용합니다. 따라서, PCM은 수많은 사용 사례에 맞게 상호 운용이 가능하며, Precium 플랫폼 활성화를 위한 다양한 프로젝트에 활용 될 예정입니다.

ONX는 Precium 플랫폼의 기축통화로, 1달러의 고정된 가치를 갖는 Stable Coin입니다. Precium 플랫폼 상에서, ONX는 Onyx Chain의 스마트 계약에 사용되며, 계약생성자와 오라클 API 제공자들의 보상 수단으로도 활용됩니다. 또한, PCM은 Precium 플랫폼에서 ONX와 교환할 수 있으며, 둘 간의 비율은 외부에서 거래되는 PCM의 가치에 따라 결정됩니다.

## 5. ACTIVATION PLAN

### 5.1 Roadmap



Premium 22 / 28

### 5.2 Marketing strategy

Premium Foundation은 중국의 일대일로 정책에서 한-중 기업들의 교류 촉진을 담당하는 '한중실클로드국제교류협회'와 블록체인 컨설팅 업체로써 파트너십을 맺었습니다. 이를 통해, 우리 재단은 한-중 양국의 실질적인 블록체인 기술 교류의 교두보 역할을 담당할 것입니다. 또한, 인플루언서 마케팅을 선도하는 국내 엔터테인먼트 기업 KCENT, 그리고 중국의 황홍 마케팅 회사인 TWOAB와의 파트너십을 맺고, Premium 플랫폼을 활성화할 수 있는 첫번째 프로젝트로 **인플루언서 마케팅 프로젝트**를 진행 중에 있습니다.

Premium 플랫폼의 Onyx Chain은 스마트 계약에 사용될 수 있는 조건들을 사용자가 직접 조합하여 사용할 수 있도록 플랫폼 내에 제공함으로써, 중고거래 \* 렌탈 \* 구인/구직 등 모든 유/무형 거래의 계약을 지원할 예정입니다. Premium은 추후 다양한 기업들 과의 전략적 제휴를 통해 플랫폼의 실사용 영역을 넓혀 감으로써 한-중 시장뿐만 아니라 전 세계적으로 현존하는 중개 중심의 계약 체재를 대체할 수 있는 플랫폼이 될 것입니다.

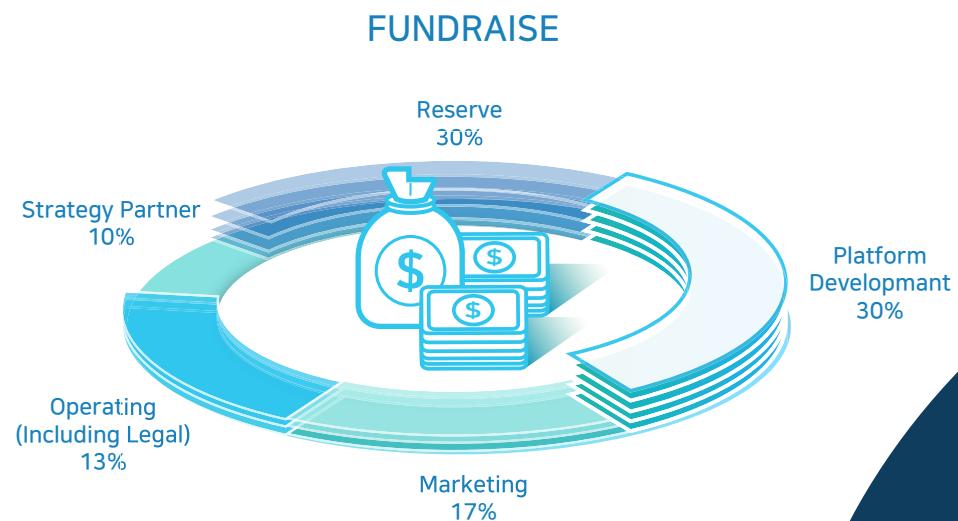
Premium Foundation은 프레시움 토큰과 플랫폼, 그리고 플랫폼 내에서 스마트 계약으로 제공하는 다양한 계약들 뿐만 아니라, 블록체인 기술과 크립토 커런시의 이점을 교육, 세미나, 컨텐츠 제작을 통해 널리 알릴 생각입니다. 우리 재단은 현재는 한국에 본사, 싱가포르에 법인을 운영 중에 있으며, 향후 중국에 자사를 설립할 계획입니다. 또한, 한국을 대표하는 우수 대학들과 연계하여 블록체인에 대한 연구 및 교육을 진행하고 블록체인 개발자 양성에 많은 힘을 쏟을 것입니다.

## 6. TOKEN DISTRIBUTION

### 6.1 Introduction

TOKEN SYMBOL	PCM	SALE TYPE	Rate	Bonus
TOKEN ISSUED	1,500,000,000 PCM	Public Pre-sale	\$0.035	15%
TOKEN SALE (40%)	600,000,000 PCM	Mainsale	\$0.040	0%

### 6.2 Token sales and ICO fundraise managements



# Team Premium



Han Kim

## CEO / Founder

- Korea Univ. Electrical Engineering
- Former Software Engineer at LG CNS
- Designed and Developed Chatbot Service for Home Shopping (70% of market share)
- CEO of HANKY&PARTNERS



Alex Lee Ph.D.

## CTO / Co-founder

- Korea Univ. Electrical Engineering
- Korea Univ. Electrical and Computer Engineering, Ph.D.
- Developed Algorithm More Than 10 Government/Enterprise Projects



Jay Ye

## Core Developer / Co-founder

- Korea Univ. Electrical Engineering
- Korea Univ. Electrical and Computer Engineering, M.S.
- Involved in International Standardization (IoT Sector)



Jiho Kim

## COO

- Korea Univ. College of Business
- CFO at TeamEXE Inc.
- Co-founder of KCENT Inc.



Ray Kim

## CFO

- Toronto Humber College, Canada
- Former Head of Overseas Business Team, Ever Techno Co., Ltd.
- Former Director of TXR Partners



Woongrae Son

## CSO

- Korea Univ. College of Business
- McKinsey & Company Consultant
- CSO at KCENT Inc.



JinYong Kim

## Developer

- Korean Minjok Leadership Academy
- Yonsei Univ. Energy Engineering
- Developed Apps for Analyzing Vehicle OBD2 Data in KewTea



JD Ahn

## Developer

- Korea Univ. Electrical Engineering
- Former System Engineer at LG Electronics Inc.
- Involved in Algorithm Development of BMS in Electric Car



Yerin Kim

## Global Partnership

- Korea Univ. College of Liberal Arts
- Vice Chairman at ITS in Korea Univ.
- Involved in Chinese Translation at IME Labs of Korea Univ.



Heily

## Design Lead

- Ewha Womens' Univ. Visual Design



### Hoontak Jung

- CEO of SidusHQ

current

- Advisor of Korea Entertainment Management Association

former

- President of Korea Entertainment Management Association
- Founder/CEO of I Love Cinema
- Founder/CEO of iFilm
- Founder of EBM production



### Jonathan Lee

- BS in Management Science, University of California San Diego
- COO of Yello Digital Marketing Group
- Business Development Director of WPP Korea
- Experienced blockchain start-up advisor, other projects include SIX Network, XCHNG, Blue Block Capital and HARA



### Joseph Jang

- Director / COO of Fantom Foundation
- VP of SL Blockchain Partners
- CFO of Global IP CAATS (Cryptocurrency Arbitrage Automated Trade-bot System)

Former

- President of Dramabeans Korea
- Director of International Investments at Sansoo Ventures



### Nicko Deng

- Master of Information Technology and Management, University of Nottingham, UK

Current

- Emerging Investor
- Professional blockchain consultant

Former

- Investment reviewer of Tencnet
- Investment reviewer of Decent Capital (Founded by Jason Zeng, Co-founder of Tencent)
- Participated in more than 15 blockchain projects



### Michael Song

Current

- Co-founder of YSK MEDIA&PARTNERS
- Advisor of YAP Chain & YAP Company
- Co-founder of E-Sports Team Worldgamestar(WGS)

Former

- Business Development Manager of Samsung Corporation



### Daniel Kang

- Sogang University BA/BS.

Current

- Deputy Managing Director at Geometry Global Korea. Part of world's largest global communication group: WPP.
- Brand communication expert providing marketing consultancy to multiple Fortune 500 companies.
- Winner of international creative awards: PMAA Dragons, Shop!, IDSA, K-Design, Luerzer's Archive.
- Youngest Senior Management official within Korea's WPP Agency Network



### Wyeth Lee

Current

- CRO, Omni Commerce (China)

Former

- CEO of Samsung Opentide China
- President of Samsung SDS China Corporation
- Owner of residence permit in China (Green Card)



### Jung Hyun Kim

- Serial Entrepreneur, Angel investor

Current

- Founder and CEO of WOOZOO shared house

Former

- Founder/CEO of Delight (Acquired By DaewonPharm)
- TNATION Founder and CEO (Acquired By IOK Entertainmet)
- The First Korean Member of the World Economic Forum's Year of The Social Entrepreneur (2015)
- Entrepreneur of the Year by Forbes Korea (2013)
- Presidential Award of the Korea Human Resources Award (2011)



### Daniel Doohyun Han

- Bachelor of Business Administration, Iowa States University

Current

- Founder of Tiny Big
- Founder of LLH Partners

Former

- Chicago Kintetsu
- KPMG Strategic Consulting Team Consultant in Korea

## Premium Specialist



Alex Kim

- Vice Chairman of Precium Foundation
- Graduate School of Media Studies, Korea University

Current

- Standing Director of National Players Association
- Delegate of The Korean Association of National Team Members
- Chairperson of Physical Education Committee of the Yeouido Institute

Former

- National player of Wrestling
- Director of Wrestling Association under the Korea Sports Council
- Publisher of MBC Economy Magazine
- Publisher of MBC Life Magazine
- Olive Nine, Managing Director, KT Group

## Premium Partners

**HANKY&PARTNERS**

**KCENT**

**O NDS**  
농심데이터시스템

 韩中丝绸之路国际交流协会  
한중실크로드국제교류협회

 新湃资本  
NewStyle Capital

**BITASSET**

**TWOAB**

  
WITH PLAYER

## 8. REFERENCE

---

- Copeland, Christopher, and Hongxia Zhong. "Tangaroa: a byzantine fault tolerant raft."
- Wang, Dennis, Nina Tai, and Yicheng An. "Byzantine Fault Tolerant Raft."
- Ongaro, Diego, and John K. Ousterhout. "In search of an understandable consensus algorithm." USENIX Annual Technical Conference. 2014.
- Abraham, Ittai, and Dahlia Malkhi. "The blockchain consensus layer and BFT." Bulletin of EATCS 3.123
- Buterin, Vitalik. "Ethereum: A next-generation smart contract and decentralized application platform, 2013."
- Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151
- Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system."

<https://www.jpmorgan.com/global/Quorum>  
<https://github.com/jpmorganchase/quorum>  
<https://raft.github.io/>  
<https://blog.theloop.co.kr/2017/07/04/lft-loopchain-consensus-algorithm/>  
<https://github.com/kadena-io/juno>  
[https://spri.kr/posts/view/21876?code=issue\\_reports](https://spri.kr/posts/view/21876?code=issue_reports)  
<http://www.itworld.co.kr/news/107168>  
<https://tokenpost.kr/terms/5822>  
<http://it.donga.com/27260>  
<https://tokenpost.kr/terms/5447>  
<http://snowdeer.github.io/blockchain>  
[https://spri.kr/posts/view/21983?code=inderstry\\_trend](https://spri.kr/posts/view/21983?code=inderstry_trend)  
[https://www2.deloitte.com/content/dam/Deloitte/kr/Documents/insights/deloitte-anjin-review/07/kr\\_insights\\_deloitte-anjin-review-07\\_10.pdf](https://www2.deloitte.com/content/dam/Deloitte/kr/Documents/insights/deloitte-anjin-review/07/kr_insights_deloitte-anjin-review-07_10.pdf)

## Disclaimer of Liability

이 백서의 내용은 아래 언급될 "법적 책임의 면제" 내용 없이 배포될 수 없습니다. 본 글을 검토하실 때 "법적 책임의 면제" 내용을 주의 깊게 검토하십시오. 투자 내용에 확신이 없으신 경우 귀하의 법률, 재무, 세금 등의 전문 상담사들과 자세히 상담하시길 권고합니다.

이 백서는 프레시움 토큰 ICO에 참가할 투자자들에게 프레시움 토큰과 프레시움 토큰의 플랫폼에 대한 정보를 제공하고 발전 가능성에 대한 비전을 공유하기 위함입니다. 투자 내용에 대한 이해도를 높기 위한 안내서 및 사업설명서일 뿐, 개발 이행을 보장하는 보증서는 아닙니다. 따라서 이 백서의 내용이 투자 계약상의 구속성을 갖는 것은 아니며, 법률적 공신력을 지닌 증서 또한 아닙니다.

본 자료에 포함된 특정 예측 내용, 추정치 및 재무 정보는 불확실한 변수로 인해 실제와 달라질 수 있습니다. 따라서 수익 등을 유추할 수 있는 관련된 모든 내용은 미래의 성과를 보장하는 것으로 간주하거나 신뢰해서는 안 됩니다. 개발 상황에 따라 백서의 수정 및 업데이트가 있을 수 있으며, 백서에 언급된 수익에 대한 정확성, 신뢰성 또는 완성도에 대해 어떠한 책임도 지지 않습니다.

결과적으로 간접적, 부수적으로 어떤 종류의 법적 책임도 지지 않습니다. 단, 이에 대한 정확성과 신뢰를 위해 백서에 소개한 법인 또는 관련인들을 통해 언제든지 내용을 확인할 수 있도록 성실히 조치를 취할 것이며, 이 백서에 포함된 정보에 관한 확인 요청은 언제든지 응대할 것입니다.

프레시움 토큰은 투자 또는 기타 재정적 목적으로 사용될 수 있지만, 이 백서에서 설명하지 않은 용도로 사용되어 수익 또는 손실이 날 경우 또한 어떠한 귀책 여부와도 무관함을 알려드립니다.

마지막으로 디지털 토큰, 디지털 통화 등의 거래가 금지된 국가나 지역 혹은 관련 법률에 따라 제한되는 국가에 거주하는 사람이나 단체는 토큰을 구매하거나 투자하지 않을 것을 권장합니다. 하지만 법률적 제한 및 규제가 있더라도 향후 프레시움 토큰을 법적으로 인정할 가능성을 배제하여 투자 자체를 거부하는 것은 아닙니다.