

# GIANT MAMMOTH CHAIN



<b>01</b>	<b>Preview</b>	-----	<b>P. 03 – P. 07</b>
1-1	Preview		<b>P. 04</b>
1-2	Scalability improvements and constraints		<b>P. 06</b>
1-3	Meaning of blockchain scalability		<b>P. 07</b>
<b>02</b>	<b>Introduction</b>	-----	<b>P. 08 – P. 09</b>
2-1	Introduction		<b>P. 09</b>
2-2	Vision		
2-3	Consensus Mechanism		
2-4	Architecture		
2-5	Structure		
<b>03</b>	<b>Technology</b>	-----	<b>P. 10 – P. 16</b>
3-1	Modular Blockchain		<b>P. 11</b>
3-2	Layer2		<b>P. 13</b>
3-3	ZK-Rollup		<b>P. 14</b>
3-4	Validator		<b>P. 16</b>
3-5	Lightweight client security		
3-6	System transaction		
3-7	Governance		
3-8	Reward distribution		
<b>04</b>	<b>Roadmap</b>	-----	<b>P. 17 – P. 18</b>
4-1	Roadmap		<b>P. 18</b>
<b>05</b>	<b>GMMT information</b>	-----	<b>P. 19 – P. 21</b>
5-1	GMMT Summary		<b>P. 20</b>
5-2	GMMT Distribution		<b>P. 21</b>
<b>06</b>	<b>Disclaimer</b>	-----	<b>P. 22 – P. 24</b>
6-1	Disclaimer		<b>P. 23</b>
<b>07</b>	<b>Legal notice</b>	-----	<b>P. 25 – P. 26</b>
7-1	Legal notice		<b>P. 26</b>
<b>08</b>	<b>Investment risk</b>	-----	<b>P. 27 – P. 29</b>
8-1	Investment risk		<b>P. 28</b>

01

# Preview

- 1-1 Preview
- 1-2 Scalability improvements and constraints
- 1-3 Meaning of blockchain scalability



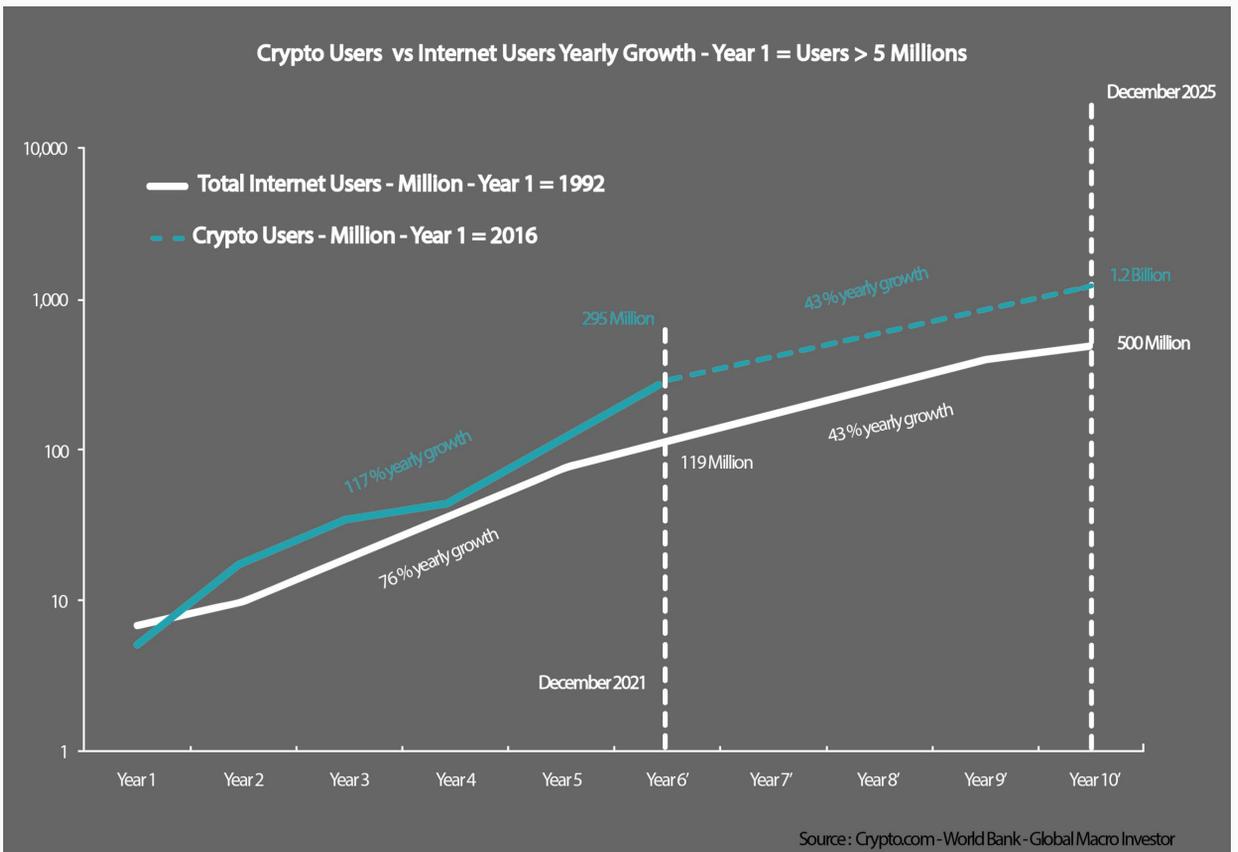
### 1-1 Preview

블록체인 기술과 Web3.0 서비스는 많은 발전에도 불구하고 아직 일반 사용자들에게 폭넓게 이용하는 Mass adoption(대중적 수용)에는 이르지 못했습니다.

Web3.0 대중화의 전제 조건은 블록체인 확장성입니다. 가상자산 네트워크의 가치 증대는 새로운 유즈케이스(Use case)의 확산과 함께 이루어져 왔습니다. 네트워크 확장성의 부족은 사용자 확대와 블록체인 대중화에 주요 장애물로 작용합니다.

Web3.0 서비스를 이용한 경험이 있는 사람들은 전송속도, 수수료, 다른 체인과의 자산전송과 교환의 불편 등 여러가지 다른 개선점에 대한 니즈가 존재합니다. 이 중 전송속도와 비용의 문제는 블록체인 네트워크의 확장성과 관련이 깊습니다. 확장성은 네트워크가 트랜잭션 증가를 감당할 수 있는 능력을 뜻하며 확장성의 미비는 대중적 수용의 병목을 만드는 요소 중 하나입니다.

인터넷 역시 확장성의 증진과 새로운 애플리케이션의 도입이 서로를 촉진하며 현재의 형태로 발전해왔습니다. 인터넷이 확장성의 증대와 함께 신규 사용처를 만들어냈던 것처럼 블록체인의 확장성 개선은 Defi, NFT 등 각 분야에서 더욱 유저 친화적인 서비스를 가능하도록 합니다.



[인터넷과 가상자산의 이용자 수 비교]

## 1-1 Preview

---

새로운 유즈케이스 출현 및 활성화는 네트워크의 활성도를 높이고 가상자산의 가치를 뒷받침하는 요인이며 다음 차례의 상승장도 단순히 가격만의 상승이 아닌 유즈케이스의 활성화와 함께 도래할 가능성이 높습니다. 인터넷의 '대중적 수용'이 저절로 찾아오지 않았던 것처럼 Web3.0의 확산 역시 자연스럽게 오는 것이 아닌 분명한 동기와 계기가 필요합니다.

주요 Layer2 프로젝트들은 최근 시장을 상회하는 가격 상승을 보이고 있습니다. 확장성 개선에 대한 수요의 구조적인 증가와 함께 자체 토큰을 발행하는 프로토콜들이 늘어나고 이더리움의 머지(Merge) 업그레이드가 진행됨에 따라 Layer2 솔루션에 대한 주목이 계속될 것으로 전망됩니다.

Mammoth는 일부 확장성 문제를 해결하기 위해 Layer2 솔루션을 도입하여 업그레이드 했습니다. 블록체인의 트릴레마를 극복할 수 있는 합리적인 방법으로 블록체인의 각 기능을 서로 다른 체인에서 병렬적으로 처리하는 모듈러 블록체인 방식을 고안했습니다.

Mammoth의 장기적인 목표는 인터넷이 그러하듯 세계 인구 대다수가 참여하는 네트워크로 일상에 자리잡는 것이라고 할 수 있습니다. 브릿지 및 상호운용 (interoperability) 솔루션들로 여러 체인들 간에 자산과 유동성을 공유하고 통합된 네트워크 효과를 누리는 방향으로 보완하여 초기 사용자 증대에 결정적으로 기여하고 전 세계를 연결하는 네트워크로서 지위를 공고히 하고자 합니다.

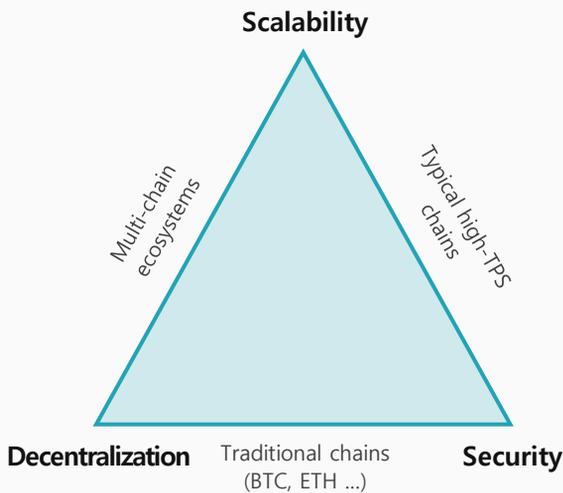
더불어 Mammoth의 궁극적인 목적은 수익을 중계자가 독차지하는 것이 아닌, 참여자 모두에게 기여한 만큼 배분하는 것으로 공익적인 차원에서 생태계를 구축하는 것입니다.

## 1-2 Scalability improvements and constraints

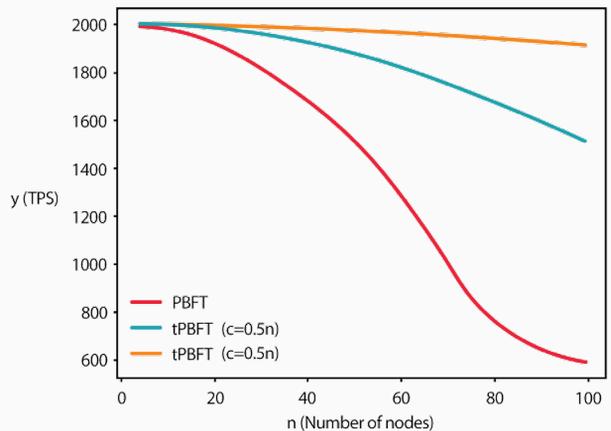
Mammoth는 '이 네트워크가 어떻게 트릴레마를 해결 하느냐' 라는 질문보다 '이 네트워크가 얼마나 실용적으로(practically) 확장을 이루느냐' 에 초점을 맞췄습니다. 더 빠르고 저렴한 블록체인 네트워크를 만드는 것은 쉽지 않은 과제입니다.

일반 데이터베이스라면 하드웨어의 추가 확충 등으로 처리 속도를 직접적으로 늘릴 수 있지만 블록체인의 특성인 특정 주체에 대한 신뢰 혹은 의존 없이 구동되는 네트워크를 유지하는 데에는 이른바 블록체인 트릴레마라는 제약이 따릅니다. 블록체인 트릴레마는 탈중앙성-보안성-확장성이라는 3개 요소 서로가 상충(trade-off) 관계를 가지고 있음을 뜻합니다.

블록의 생성은 분산되어 있는 여러 노드들의 합의에 따라 확정되는데 다른 조건이 동일하다면 노드의 수가 많을수록 탈중앙성은 높다고 할 수 있지만 중복된 연산이 발생하고 노드들 간 합의에 소요되는 시간은 늘어납니다. 블록 생성 시간을 짧게 하고 블록 용량을 키우는 방식으로 확장성 개선을 시도한다면 풀 노드(full node) 운영의 제약 조건이 높아지는 문제가 있습니다. 각 블록체인 네트워크들은 용도와 목적에 따라 상충관계 하에서 목표하는 확장성의 정도를 선택하게 됩니다. 이는 마치 경제학에서의 '제약 조건 하 최적화' 문제와도 유사합니다.



Source : Tang et al. (2022)



예를 들어 솔라나의 경우 밸리데이터로 최소 RAM 128GB 이상, CPU 2.8GHz 이상 등 고사양 운영자들만 참여할 수 있도록 제한 조건을 부여하여 탈중앙성을 다소 희생하는 대신 단위 시간당 더 많은 트랜잭션 처리를 가능하게 합니다. 다만 트릴레마의 제약 조건 자체가 고정불변인 것은 아닙니다.

앞서 상충 관계에 대한 설명 시 '다른 조건이 동일하다'는 가정이 포함되듯 통신 기술의 발전, 합의 도달 방식의 최적화, 샤딩 등 네트워크 설계 변경 등 기술적 발전으로 같은 정도의 보안성, 탈중앙성 수준에서 달성할 수 있는 확장성의 정도는 점차 개선될 수 있습니다.

### 1-3 Meaning of blockchain scalability

블록체인은 단일 주체에 의존하지 않으며 정보를 처리하고 가치를 전달하는 새로운 네트워크를 가능하게 합니다. 하지만 분산화된 검증과 기록과정은 중앙화된 네트워크에 비해 확장성을 제약하는 요인입니다. 확장성을 속도와 비용 측면으로 각각 살펴보면 비트코인의 블록생성은 약 10분마다 이루어지며 TPS(Transaction per Second)는 3~7을 기록하고 있습니다. 이더리움 네트워크는 평균 80kb 사이즈의 블록이 12~14초마다 생성되어 초당 15가량의 트랜잭션을 처리하고 있습니다.

비용 측면을 보면 8월초 이더리움 네트워크 트랜잭션당 평균 수수료는 2~3달러 가량으로 연초 40달러 수준에 비해 낮아졌지만 많은 거래를 수행하기에는 여전히 걸림돌이 됩니다. 비용의 변동성 역시 문제인데 수수료는 블록에 대한 수요와 공급에 따라 결정되기 때문에 크립토키티 사태, NFT 호황 등 네트워크 사용에 대한 수요가 몰릴 때 네트워크 전체의 가스비가 급등하는 현상이 발생합니다. 즉 인터넷 트래픽과 마찬가지로 정보가 담기는 블록스페이스(Block space)역시 희소성을 가진자원이며, 블록체인의 확장성 개선이란 블록스페이스에 더 많은 정보를 담으려는 수요를 감당할 수 있는 능력을 확대하는 과정으로 볼 수 있습니다. 블록체인 네트워크의 애플리케이션이 마주하는 확장성 제약의 예시는 다음과 같습니다.

#### ● Defi

일상에서 자연스럽게 일어나는 금융 행위 중 현재 디파이가 담당하는 부분은 극히 일부에 불과합니다. 금융 거래의 수행은 빠른 처리 속도와 극도로 높은 보안성이 함께 요구됩니다. 네트워크 확장성의 개선은 디파이 서비스의 제공 범위가 대출, 보험, 결제, 자산거래 등 더 많은 금융 행위로 침투해 나가기 위한 선결 과제라고 할 수 있습니다.

#### ● NFT

확장성의 제약은 NFT 시장 성장의 병목 중 하나입니다. 2022년 5월, BAYC의 발행사인 유가랩스가 '아더사이드'라는 신규 프로젝트를 출시해 수요가 몰리자 이더리움에서의 민팅 가스비는 순간적으로 4만 달러 이상으로 솟구쳤습니다. 이후 유가랩스는 "수요 증가에 따른 이더리움 병목 현상에서 벗어나고 적절한 확장을 이루기 위해서" 이더리움을 떠나 자체 체인으로 이전할 것이라고 발표했습니다. 향후 메타버스 세계의 주도적 프로젝트가 되려면 최대한의 확장성을 확보하는 것이 필연적입니다.

02

# Introduction

- 2-1 Introduction
- 2-2 Vision
- 2-3 Consensus Mechanism
- 2-4 Architecture
- 2-5 Structure

## 2-1 Introduction

---

Giant Mammoth Chain의 업그레이드 목적은 기존 모듈을 확장 및 재사용하고 스마트 계약의 아키텍처를 사용하여 기존 계약을 쉽게 수정할 수 있도록 하는 것으로 더 나은 아키텍처와 보안을 염두에 두고 설계되었습니다. 개발자와 노드 운영자가 내부 가치 시스템으로 대규모 사용자를 위해 맞춤형 블록체인을 구축하고 실행할 수 있도록 지원하는 인프라이며 더 많은 유연성과 탈중앙화를 제공합니다.

## 2-2 Vision

---

Mammoth의 주요 임무는 모든 프로젝트 개발자가 고유한 사양과 유효성 검사기 세트로 블록체인을 배포할 수 있으면서 여전히 Mammoth 인프라에 연결할 수 있도록 하는 것입니다. 간단하지만 기능적인 블록체인 프로젝트를 구축할 수 있는 기준이라고 할 수 있습니다. 개발자와 팀은 자체 비즈니스 규칙과 경제로 간단한 블록체인을 만들 수 있습니다. 가장 중요한 것은 기존 기능을 확장할 수 있다는 것입니다.

## 2-3 Consensus Mechanism

---

Giant Mammoth Chain은 Parlia 합의 방식을 사용하며 PoSA(Proof-of-Stakes Authority)로 설명할 수 있습니다. PoSA(지분권위증명)는 DPoS(지분증명)와 PoA(권한 증명)의 장점을 결합한 합의 알고리즘입니다.

## 2-4 Architecture

---

Giant Mammoth Chain은 Ethereum/Mammoth생태계와의 통합을 위한 프로토콜 및 기준을 제공하여 기존보다 더욱 높은 속도와 낮은 네트워크 가스비, EVM 호환, 리스크 완화 등 자체 체인을 구축하는 응용 프로그램에 적합하도록 설계되었습니다.

## 2-5 Structure

---

개발자는 스테이킹 시스템, 블록 탐색기, SDK, RPC, API 게이트웨이, 거버넌스용 인터페이스, 크로스 체인 브리지 등과 같은 유용한 제품에 자동으로 액세스할 수 있습니다.

# 03

# Technology

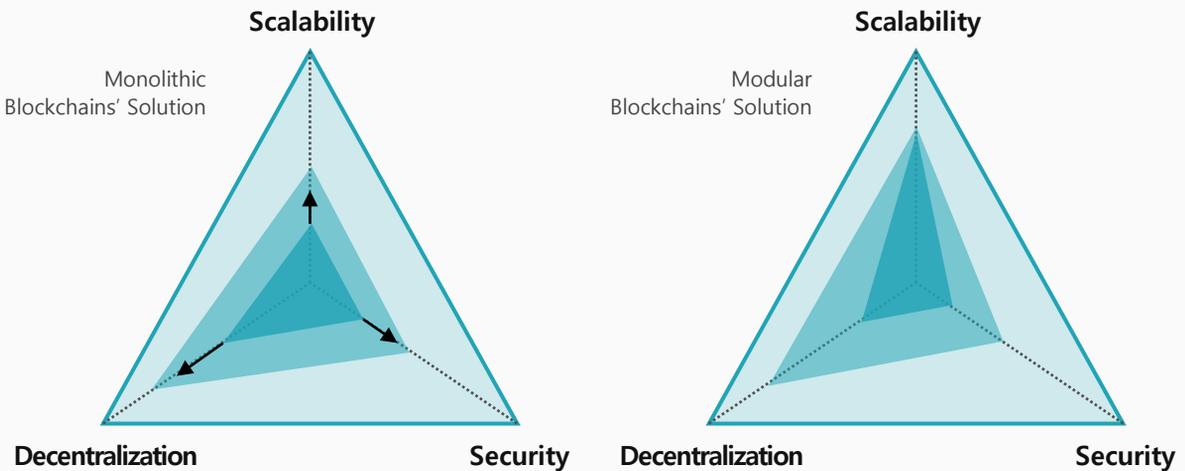
- 3-1 Modular Blockchain
- 3-2 Layer2
- 3-3 ZK-Rollup
- 3-4 Validator
- 3-5 Lightweight client security
- 3-6 System transaction
- 3-7 Governance
- 3-8 Reward distribution

### 3-1 Modular Blockchain

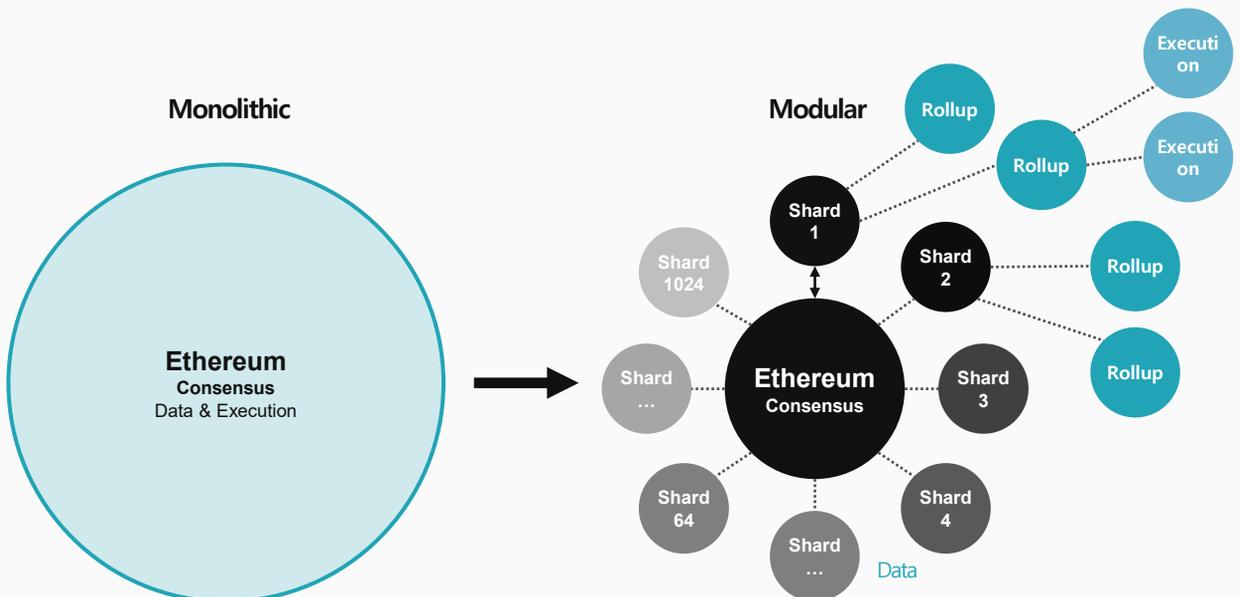
타 메인넷들이 앞선 확장성 개선 시도들에 대하여 단일 블록체인 내에서의 처리 능력을 높이는 것을 전제로 하였다면 Mammoth는 블록체인의 각 기능들을 여러 체인이 분담함으로써 트릴레마를 극복하려 접근했습니다. 블록체인의 데이터 처리 과정을 단순화해 설명하면 다음과 같습니다. 블록체인은 PoS, PoW 등 노드들 간의 합의(consensus)를 통해 현 체인 상태가 올바름을 확인 및 트랜잭션의 순서를 정하며, 트랜잭션을 실행(execution)함으로써 체인의 상태 정보를 업데이트합니다.

[트릴레마 해결의 두 가지 접근]

Source : a41



데이터의 투명성과 불변성을 보장하며 실행된 트랜잭션을 검증하는(settlement) 과정, 트랜잭션에 관한 정보는 다른 노드들이 언제나 확인 가능하도록 네트워크에 배포되어야 하는데 이를 데이터 가용성(data availability)이라고 합니다. 위의 실행, 합의, settlement, 데이터 가용성이 블록체인의 네 가지 주요 기능으로 볼 수 있습니다. 일반적인 블록체인은 위 네 가지 기능을 한 체인에서 모두 처리하는데 이러한 방식을 모놀리틱 블록체인(monolithic blockchain)이라고 합니다. 한편 모듈러 블록체인(modular blockchain)은 실행, 합의, settlement, 데이터 가용이라는 각 기능의 일부 또는 전부를 서로 다른 체인에서 분담해서 처리하기 때문에 기존보다 처리의 속도 및 효율성을 높일 수 있습니다.



### 3-1 Modular Blockchain

---

요약하자면 체인 자체의 제약 조건 하에서 도달할 수 있는 확장성의 균형점을 도출하는 방식이 모놀리식 블록체인의 접근 방식이었다면 블록체인의 각 기능을 서로 다른 체인에 분담함으로써 단일 체인의 트릴레마를 극복하려는 것이 모듈러 블록체인 방식입니다.

Giant Mammoth Chain은 모듈러 블록체인으로 BSC와 Ethereum에 보안을 귀속하고, 방대한 트랜잭션과 데이터를 소화해야 하는 이유로 모든 노드들이 지속적으로 모든 데이터를 저장할 수 없기에 IPFS를 활용한 파일코인 네트워크를 Giant Mammoth Chain의 데이터 가용성 레이어의 역할을 분담할 것입니다.

또한 지속적으로 이더리움의 업데이트를 모니터링 하며, 연산을 오프체인에서 진행하는 Rollup솔루션, 데이터 가용성을 개선하기 위한 EVM 호환, EIP-4844 - Danksharding을 통해 높은 탈중앙성과 보안성을 지님과 동시에 확장성을 개선할 수 있습니다. Giant Mammoth Chain은 EIP-4844의 Danksharding 중 미리 도입할 수 있는 부분을 Giant Mammoth Chain에 도입하며 업데이트 진행중에 있습니다.

제공되는 모듈은 아래와 같습니다.

- **Staking & Staking Pool**

온체인 스테이킹 시스템을 지원하고 PoSA(권한 지분 증명) 스테이킹 모델을 사용합니다. 이를 통해 사용자는 토큰을 특정 검증인에게 위임하고 총 스테이킹 금액을 기반으로 검증인의 보상을 공유할 수 있습니다.

- **PoSA Consensus & Staking**

사용자는 Giant Mammoth Chain 네트워크에서 승인된 검증인에게 스테이킹할 수 있고 체인에 적용된 작업의 안전성을 보장할 수 있습니다.

- **Blockchain & EVM**

블록 생성 및 EVM 트랜잭션 실행을 위해 Giant Mammoth Chain은 예를 들어 향후 WebAssembly를 기반으로 자체 런타임 실행 환경을 정의할 수 있습니다.

- **Web3 API**

MetaMask 및 기타 애플리케이션을 포함한 Web3 생태계와의 NMC 체인의 호환성을 위한 것입니다.

- **Runtime Upgrade**

시스템 스마트 계약을 통해 시스템 스마트 계약에 대한 기존 바이트 코드를 수정할 수 있습니다. 이 체계는 모든 검증자가 노드를 업그레이드할 필요가 없기 때문에 하드 포크에 비해 훨씬 간단합니다.

- **Governance**

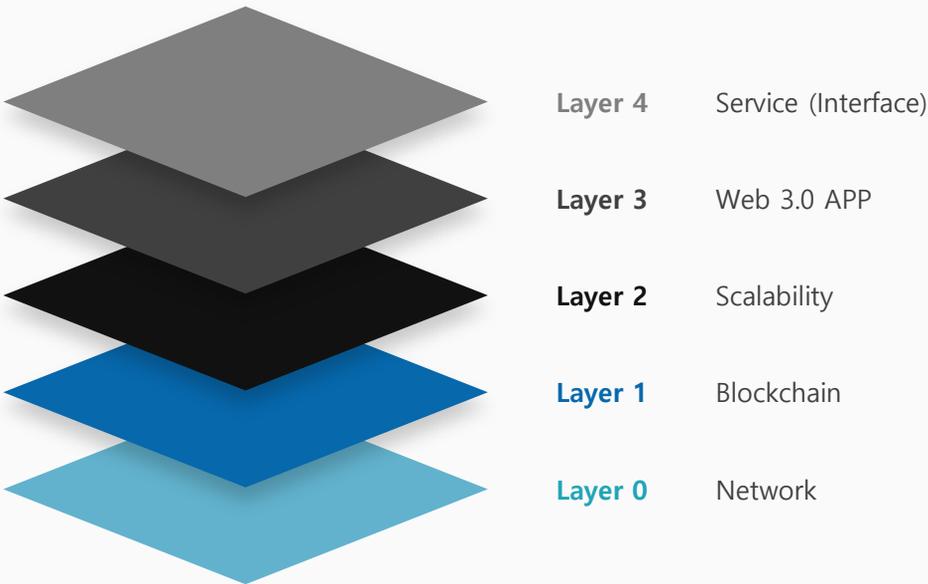
암호화폐 블록체인의 변경 사항을 관리하고 구현하기 위한 분산형 투표 시스템입니다.

### 3-2 Layer2

Giant Mammoth Chain은 모듈화 방식으로 트랜잭션 처리 능력을 개선했습니다. 가장 기본적인 아이디어는 트랜잭션 실행 기능을 분리하는 것입니다. 이처럼 블록체인의 세 가지 기능 중 트랜잭션 실행을 메인 체인 외부에서, 나머지 합의 및 데이터 가용화를 메인 체인에서 수행하는 방식을 Layer2 (L2)방식이라고 합니다. 두 개의 층(layer)이 서로 다른 기능을 분담해 수행하기에 붙여진 이름으로 기반이 되는 메인 체인을 Layer1(L1)으로, 트랜잭션을 실행하는 별도 체인을 이에 대비하여 Layer2(L2)라고 부릅니다.

Layer2는 Layer1과 연결되어 있어 필요한 작업 일부를 Layer2에게 분담하는 방식입니다. 한마디로 Layer2는 '분업'을 위한 계층입니다. 블록체인이 하는 일은 크게 합의, 실행, 저장 이렇게 세가지로 나뉩니다. '합의'는 블록에 대한 검증을 하는 것, '실행'은 상태 변경을 위한 것, '저장'은 결과를 기록하는 것입니다. '합의 - 실행 - 저장'은 원래 하나처럼 여겨진 블록체인 작업(monolithic)이나 '실행' 작업은 다른 블록체인에 분담할 수 있습니다. 마치 컴퓨터의 연산 속도를 위해 그래픽 카드를 연결해 사용하는 것과 같다고 볼 수 있습니다. 따라서 Layer2의 역할은 Layer1에서 필요한 복잡한 연산을 빠른 속도로 대신 해주는 것입니다.

#### [Layers of Crypto Universe]

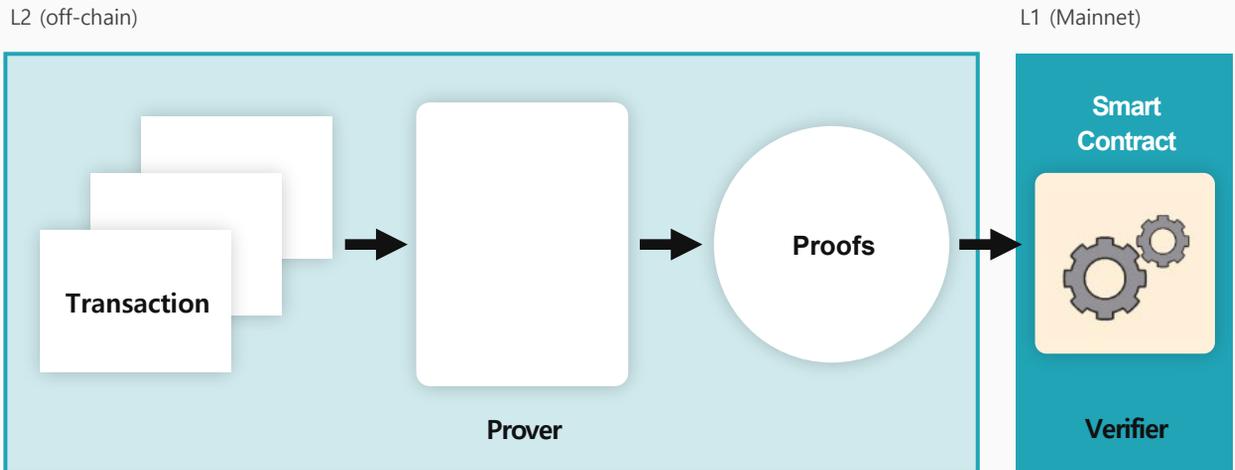


여기서 Layer1 코인은 독자적인 블록체인을 가진 코인이며 비트코인, 이더리움, 솔라나, 클레이튼 등이 있으며 Layer2 코인은 폴리곤, 오미세고, 이뮤터블X 등이 이에 해당합니다.

### 3-3 ZK-Rollup

#### [ZK-Rollup의 작동방식]

Source : ZK-SEL



롤업은 대표적인 레이어2 확장성 솔루션의 하나입니다. zk롤업은 롤업 체인에서 배치를 생성할 때마다 트랜잭션 규칙을 수학적 함수로 나타낸 뒤 암호화하는 영지식 증명 과정을 거치는데, 정형화되지 않은 범용 스마트 컨트랙트를 영지식 증명으로 처리 가능한 함수 형태로 전환하는 것은 난이도가 높은 기술입니다.

Giant Mammoth Chain은 기존 Mammoth Network에서 직면하고 있는 네트워크의 확장성 문제와, EVM 활성화 후 TPS가 제한되는 병목 현상을 개선하기 위해 ZK-Rollup을 도입했습니다. 이것은 Layer1과 동일한 보안성을 가집니다. zkSNARK 증명을 사용하기에 사용자는 사기를 방지하기 위해 제3자를 신뢰하거나 Rollup 블록을 모니터링할 필요가 사라집니다. 연산 및 state저장을 오프체인에서 진행하여, ZK-rollup을 통해 모든 데이터 대신 유효성 증명만 진행하기때문에 블록 검증이 빠르고 비용이 저렴합니다.

Zk롤업은 Key를 노출하지 않고 거래 내역을 검증하는 영지식 증명(Zero-knowledge Proof)방식을 이용합니다. Key 등 정보를 직접 주지 않고도 참인 데이터를 갖고 있는 거래 내역만 통과할 수 있는 절차를 제시하는 방식으로 원본 전체를 보지 않고 일부 증거만으로 검증하는 방식입니다. 기본적으로 계산을 수행하고, 트랜잭션을 묶고, 트랜잭션 데이터를 메인 블록체인 밖으로 이동하여 기본 블록체인 네트워크, 즉 Layer1을 확장합니다.

### 3-3 ZK-Rollup

Giant Mammoth Chain은 ZK 롤업 아키텍처를 기반으로 구축되어 수백 건의 오프체인 트랜잭션을 번들(또는 "롤업")한 다음 각 배치에 포함된 트랜잭션의 유효성을 증명하기 위한 암호화 증명을 생성할 수 있습니다. 암호학적 증명은 SNARK(succinct non-interactive argument of knowledge) 형식이며, 이는 롤업된 블록의 모든 단일 트랜잭션의 유효성을 증명할 수 있고 보안이 보장됩니다. 사용자는 사기를 방지하기 위해 제 3자를 신뢰하거나 롤업블록을 계속 모니터링할 필요가 없습니다.

원활한 L1-L2 통신 : GMMT, BSC 또는 Zk-GMMT에서 생성된 BNB 및 BEP20/BEP721/BEP1155 토큰은 BSC와 ZkGMMT 간에 자유롭게 호환됩니다.

빠른 트랜잭션 속도 및 더 빠른 완결성: Zk-GMMT는 1억 개의 지갑 주소를 지원하고 초당 최대 10,000개의 트랜잭션(TPS)을 처리할 수 있는 환경을 조성합니다.

또한 모든 계정 데이터는 트리 형식으로 구성됩니다. 트리의 루트 해시 값은 고유한 세계 상태를 식별할 수 있습니다. 동시에 Merkle 분기 검증 기술을 통해 계정 데이터가 world state에 속하는지 검증할 수 있습니다. 이것은 또한 ZK-rollup에서 트랜잭션 유효성을 증명하는 중요한 부분입니다. 이 설계 문서는 주로 기본 구조 설계, 캐시 설계 및 지속성 설계를 포함하여 ZkBNB의 세계 상태 트리 설계에 중점을 둡니다.

롤업이 확장성을 높여주는 이유는 우선 다량의 트랜잭션을 배치화해 메인 네트워크에서 처리해야 하는 트랜잭션의 수와 데이터 크기를 줄여주기 때문입니다. ETH를 전송하는 트랜잭션의 경우 롤업 체인에서 실행 시 L1에 올라가는 데이터는 12바이트 미만으로 이더리움에서 실행 시보다 10배 가까이 절약됩니다. 또 다른 이유로 이더리움 등 메인 체인은 탈중앙성 및 보안성을 유지하기 위해 속도 및 블록 용량에 제한이 있는 반면, 코드 실행만을 담당하는 롤업 체인은 그러한 제약으로부터 비교적 자유롭습니다. 확장성의 수준은 일반적으로 트랜잭션 속도 혹은 비용으로 표현될 수 있습니다. 속도의 경우 다시 트랜잭션 지연 시간(latency)이 얼마나 되는지와 단위 시간당 처리량이 얼마나 되는지(주로 TPS로 표현)를 기준으로 삼을 수 있습니다. 단 TPS는 참고의 지표일 뿐 절대적인 기준이 아님을 염두에 둘 필요가 있습니다.

비용 측면에서 Layer2Fees가 취합한 트랜잭션당 평균 가스비를 비교하면, 2022년 8월 기준으로 ETH 토큰 전송 시 이더리움과 비교해서 옵티미즘과 아비트럼은 약 10배, ZK롤업 기반인 zkSync는 약 50배 가스비 절감 효과를 거두고 있습니다. 이는 네트워크 활성 정도 등에 따라 매일 변동하는 수치입니다. 각 롤업 솔루션들은 활성 정도가 높고 트랜잭션 압축이 효율적으로 될 때 이론상 이더리움의 트랜잭션 비용을 100배 가까이 줄일 수 있다고 추산하고 있습니다.

### 3-4 Validator

Giant Mammoth Chain의 Node는 21명의 검증자(Validator)와 검증자에게 투표하는 위임자(Delegator)로 구성됩니다. 매일 가장 많은 GMMT가 예치(Staking)된 검증자들이 새로 선정되며, 권한이 있는 검증인은 차례로 PoA 방식으로 블록을 생성합니다. 여기서 이들은 Giant Mammoth Chain의 블록을 검증하고 생성하는 것에 대한 수수료를 보상으로 얻을 수 있습니다. 하나의 검증자만 블록을 생성하고 이 작업의 정확성을 확인하기 위해 확인 시간, 일반적으로  $2/3 * N + 1$ 을 기다려야 하는 BFT와 유사한 합의입니다.

[\* 여기서 N은 활성 검증자]

### 3-5 Lightweight client security

Validatorset검증인 세트 변경은 (Epoch + N/2) 블록에서 발생합니다. 라이트 클라이언트의 보안을 고려하여 N/2 블록을 지연하고 Validatorset 변경이 발생하도록 합니다. 모든 Epoch 블록에서 유효성 검사기는 계약에서 유효성 검사기 집합을 쿼리하고 블록 헤더의 Extra\_Data 필드에 채웁니다. 한편 전체 노드는 계약의 유효성 검사기 집합에 대해 확인합니다. 라이트 클라이언트는 이를 다음 Epoch 블록의 Validatorset으로 사용하지만 계약에 대해 확인할 수 없으며 Epoch 블록의 서명자를 믿어야 합니다. Epoch 블록의 서명자가 잘못된 Extra\_Data를 작성하면 라이트 클라이언트가 잘못된 체인으로 이동할 수 있습니다. Validatorset 변경이 발생하도록 N/2 블록을 지연시키면 잘못된 Epoch 블록이 다른 검증자가 서명한 다른 N/2 후속 블록을 얻지 못하므로 라이트 클라이언트가 이러한 공격을 받지 않게 됩니다.

[\* 여기서 N은 Epoch 블록 이전의 Validatorset 크기]

### 3-6 System transaction

합의 엔진은 시스템 계약을 호출할 수 있으며 이러한 트랜잭션을 시스템 트랜잭션이라고 칭하며 시스템 트랜잭션은 블록을 생성하는 검증자가 서명합니다. 증인 노드의 경우 고유 논리에 따라 시스템 트랜잭션(서명 없음)을 생성하고 적용하기 전에 블록의 시스템 트랜잭션과 비교합니다.

### 3-7 Governance

Giant Mammoth Chain은 사용자가 참여할 수 있는 온체인 거버넌스가 존재하고 이 거버넌스는 참여와 스테이킹을 통해 프로토콜의 안정성과 발전에 기여할 수 있으며 체인 내 동작을 제어하는 많은 시스템 매개변수(중개자 보상금액, 스테이킹 보상, 검증자 수, 체인 내 변동사항 등)는 안건을 제출하고 채택하는 일은 거버넌스에 의해 결정되며 이를 통해 기타 매커니즘과 스케일링 솔루션 개선도 진행될 수 있습니다.

투표권은 검증인에게 위임된 총량에 따라 분배됩니다. 정족수의 2/3에 도달하고 51% 이상의 투표가 제안에 대한 것이라면 체인의 모든 사람이 실행할 수 있도록 설계되었습니다.

### 3-8 Reward distribution

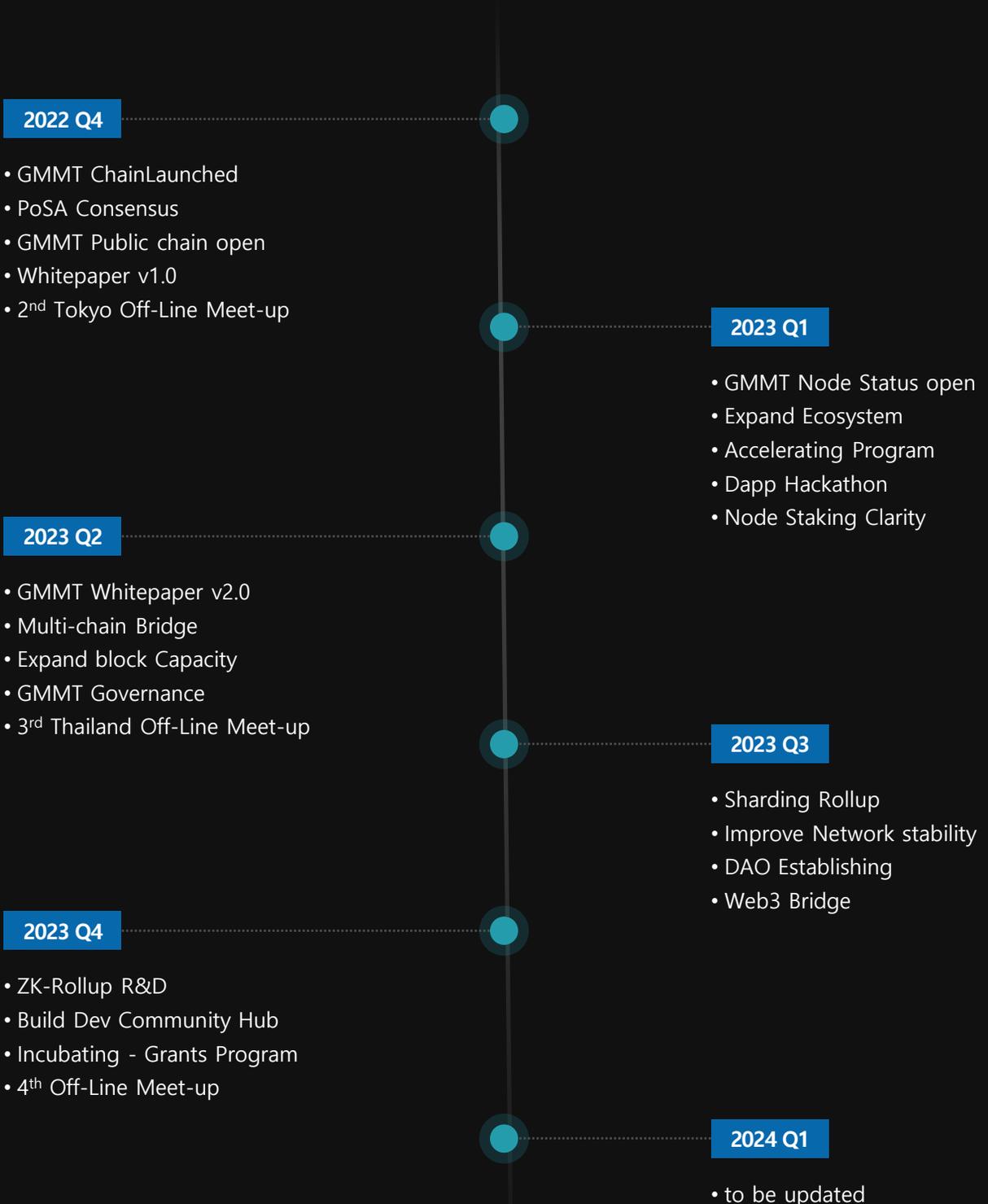
Validator는 트랜잭션을 실행하여 보상을 받을 수 있습니다. 각 트랜잭션에는 실행 비용이 있고 이 비용의 15/16은 유효성 검사기로 이동하지만 보상의 1/16은 브리징 비용 적용과 같은 시스템 요구에 이러한 자금을 사용할 수 있는 시스템 자금으로 이동합니다. 모든 블록 보상이 검증인의 소유자에게 돌아가는 것은 아닙니다. 그 중 일부는 위임자 간에도 분배됩니다.

04

# Roadmap

4-1 Roadmap

## 4-1 Roadmap



❖ 상기 로드맵은 개발 진척 상황 및 시장 상황에 따라 일정이 변동될 수 있습니다.

05

# GMMT information

- 5-1 GMMT Summary
- 5-2 GMMT Distribution



## 5-1 GMMT Summary

- Mammoth 재단은 Giant Mammoth Chain으로 업그레이드 개발 작업이 진행됐으며
- Service의 지속적인 가치 보장 및 창출을 위해 GMMT를 발행합니다.
- Platform의 모든 서비스는 GMMT로 이용되며, GMMT 사용에 대한 다양한 혜택이 주어집니다.
- GMMT는 Giant Mammoth Chain 네트워크상에서 운용됩니다.

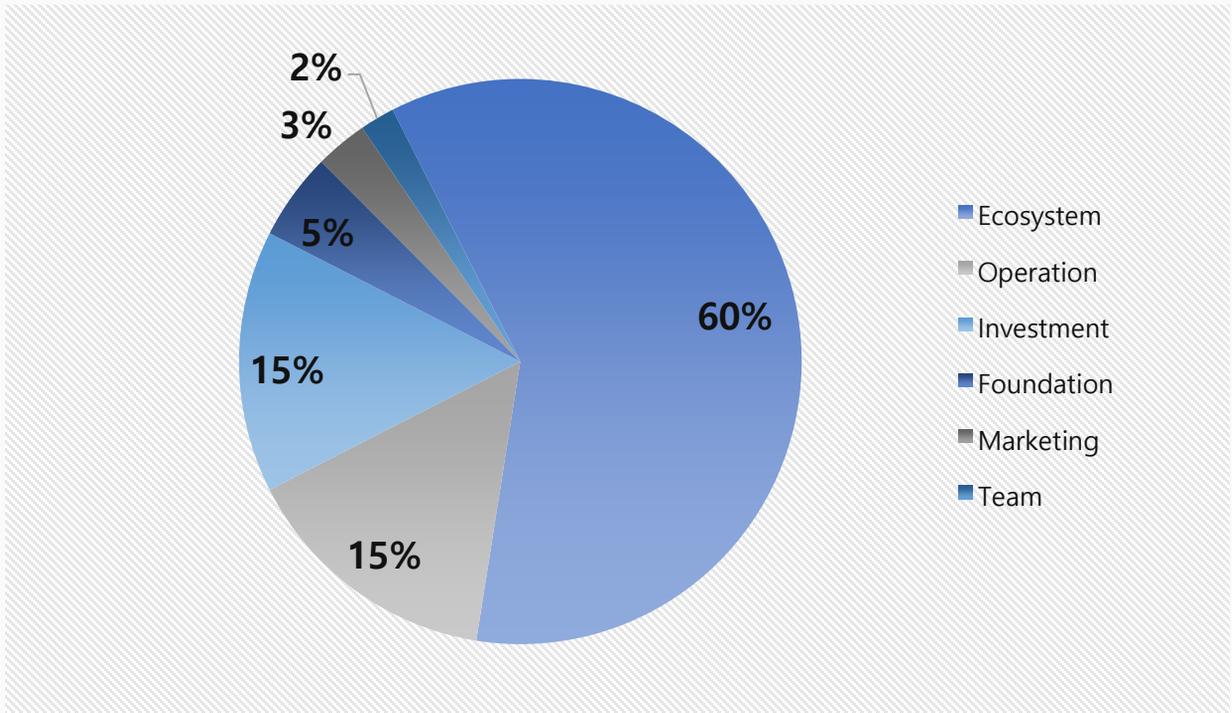
GMMT의 기본 정보는 아래와 같습니다.

구 분	내 용
NAME	Giant Mammoth
SYMBOL	
TYPE	Giant Mammoth Chain
ISSUE PRICE	-
TOTAL COIN SUPPLY	5,000,000,000

❖ Coin 발행은 여건에 따라 일정 및 비율이 변동될 수 있습니다.

## 5-2 GMMT Distribution

GMMT의 분배 계획은 아래와 같습니다.



구분	내용
Ecosystem	3,000,000,000(60%)
Operation	750,000,000(15%)
Investment	750,000,000(15%)
Foundation	250,000,000(5%)
Marketing	150,000,000(3%)
Team	100,000,000(2%)
<b>Total</b>	<b>5,000,000,000(100%)</b>

❖ Coin 발행은 여건에 따라 일정 및 비율이 변동될 수 있습니다.

06

# Disclaimer

6-1 Disclaimer

## 6-1 Disclaimer

아래 내용들을 주의 깊게 읽으시기 바랍니다. 아래 내용은 본 백서를 읽는 모든 사람에게 적용됩니다. Mammoth 백서(이하 “백서”)는 작성 당시를 기준(as is)으로 하여 작성 및 제공되므로 백서에 포함된 어떠한 내용이라도 Mammoth 재단의 재량에 따라 언제든지 변경되거나 업데이트될 수 있으며, 본 백서의 어떠한 내용이라도 장래 시점까지 변경되지 않는다는 점을 담보하지 않습니다. 만일 본 백서의 내용에 대해 어떠한 의심의 여지가 있는 경우 구매 전 회계사, 변호사 또는 기타 전문가와 상의해야 합니다.

1. 본 백서의 목적은 Mammoth 프로젝트에 대한 요약된 정보와 소개를 다루는 것에 있습니다. 본 백서는 Mammoth 프로젝트 또는 재단에 대해서 법적으로 구속력이 없으며, 백서 상 어떠한 문구들도 구독, 구매, 투자 제안 그리고 투자 강요의 성격을 띠고 있지 않습니다.
2. 본 백서 상 모든 정보나 분석 내용은 투자 결정의 근거가 될 수 없으며, 어떠한 투자 제안이나 조언도 아님을 알려 드립니다. 본 백서 상의 어떠한 내용이나 데이터는 어떠한 이유에서든 바뀔 수 있으며 정확하지 않을 수 있고 그 내용에 관한 어떠한 보장이나 약속도 없음을 알려드립니다.
3. 이사, 에이전트, 직원, 계약자, 판매 파트너를 포함한 Mammoth 재단은 다음과 같은 직접적 또는 간접적으로 발생하는 모든 종류의 손해를 책임지지 않습니다: (1) 해당 백서의 계약 내용 및 정확성 및 완전성; (2) 백서의 오류 또는 누락; (3) 확인되지 않은 원인으로 인한 백서 열람 불가능; (4) 백서 사용 또는 미사용으로 인해 발생하는 기타 모든 손해. 또한, Mammoth 재단은 다음 사항들에 대하여 전적으로 책임을 지지 않습니다: (1) 이익, 수익, 저축 및 기타 경제적 손실; (2) 사업 거래, 사업 활동, 영업 이익 관련 활동 중에 발생한 손실; (3) 데이터 손실 또는 손상; (4) 부수적 또는 특수 손해; (5) 낭비되거나 손실된 관리 시간; (6) 간접적이거나 필연적인 손해는 사전 경고가 주어졌거나 해당 손해가 예측 가능할 경우에도 보상받을 수 없습니다.
4. 본 백서 상 미래 계획적인 성격을 띠는 특정 서술들의 정확도나 현실성에 대해서는 아무런 보장이 없음을 알려 드립니다. 이러한 미래 계획적인 성격의 서술과 정보에 근거한 의사 결정은 유무형 자산의 피해를 초래할 수 있습니다. 또한 이 백서가 내포한 어떠한 금융 정보들도 회계감사를 받지 못한 정보라는 것을 알려 드립니다.
5. 진행 중인 Mammoth 프로젝트의 내용이나 시장의 변화, 기술 발전 그리고 Coin 규제 변화에 따라서 백서의 내용은 달라질 수 있습니다. 또한 차후에 본 백서에 명시된 사건, 프로젝트, 향후 계획, 추정치의 변화나 오차 범위 안의 변경 사항 등에 대해 독자들에게 통보하거나 보고할 의무가 없음을 알려 드립니다.
6. 본 백서 상 법, 세무, 규제, 금융, 회계와 같은 분야에 대한 정보들은 조언이 아님을 알려드립니다. GMMT 구입은 구매자들에게 GMMT 구매를 위해 지불한 물질적 자산을 포함해 물질적인 손실을 가져올 수 있습니다. GMMT 구입에 앞서, 구매자들은 세무, 규제, 금융, 법률 등의 전문가들에게 잠재적 위험부담, 수익 및 GMMT 거래가 초래할 수 있는 결과들에 대해서 상담할 것을 권합니다.
7. Mammoth 재단은 본 백서를 참고 또는 이용하여 한 의사 결정 행위의 결과에 대하여 모든 형태의 금전적 손해, 부채, 직·간접적인 사고, 무형 자산의 가치 하락, 수입, 매출, 자본 감소, 채무 기타 피해에 따른 어떠한 책임도 지지 않습니다. 모든 GMMT 구매자들은 GMMT의 어떠한 형태의 보증도 없는 현재 상태 그대로의 위험 부담을 인지하고 구매한다는 것에 동의한 것으로 간주됩니다.

## 6-1 Disclaimer

---

8. GMMT 구매자는 자신의 법적 관할권 내에서 GMMT의 인수와 처분 등에 관하여 발생할 수 있는 소득세 등 기타 과제 처분이 발생할 수 있으며, 이에 대하여 전적으로 GMMT 구매자가 세금과 관련한 법적 책임을 져야 합니다.

9. 백서의 출판·배포가 금지된 나라에서 본 백서의 출판·배포를 금합니다. 본 백서에 있는 정보들은 어떠한 규제 기관의 검증이나 인가도 받지 않았으며, 법에 저촉되는 어떠한 행위도 Mammoth 재단에 효력이 없습니다. 본 백서의 출판·배포가 그 발행된 나라의 규제 사항을 모두 준수하였다는 것을 보장하지 않습니다.

10. Mammoth 프로젝트에 대한 공식 자료는 본 백서이고, 이 자료는 다른 언어로 번역될 수 있으며, 예비 구매자 및 기존 구매자 등과 구두 혹은 서면 의사소통을 하는데 사용될 수 있습니다. 이 과정에서 일부 정보가 곡해되거나 잘못 해석되거나 손실될 수 있습니다. 따라서 이러한 대체적인 의사소통의 정확도를 보장할 수 없음을 숙지하시기 바랍니다. 그러한 부정확한 의사소통 발생 시 영문으로 작성된 본 공식 백서의 정보가 우선합니다.

07

# Legal notice

7-1 Legal notice

## 7-1 Legal notice

---

1. GMMT는 Mammoth 재단에 의해 통제되는 암호 유틸리티 Coin입니다. Platform 안에서의 활동성을 늘리고 Platform 생태계 구성원들의 상호작용을 촉진시키기 위해 고안된 GMMT는 Platform의 기능들과 옵션들을 이용하기 위해 Platform에서만 이용되는 Coin입니다. GMMT 보유자만이 Platform 을 제약 없이 이용할 수 있습니다.
2. 어떠한 법적 관할권 내에서도 GMMT는 담보나 금융 매개체가 아니며 마찬가지로 기업 공개형 펀드레이징이 아닙니다. 만약 GMMT가 어느 나라의 법률 제도 안에서 담보나 금융의 수단이 될 수 있다고 생각하신다면, GMMT를 구입하지 마시고 Mammoth 재단, 또는 전문가에게 먼저 잠재적 위험 부담에 대해 상담을 받아 보시기를 권장합니다.
3. GMMT는 재단의 지분이나 주식이 아닙니다. GMMT를 보유한다고 해서 차후 Mammoth 재단의 배당금, 수익, 이사회 등 회사 내부 경영 활동에 대해 권리를 행사할 수 없습니다. 또한 GMMT는 보유자에게 재단에 대한 어떠한 소유권도 부여하지 않습니다.
4. GMMT는 Mammoth 재단의 대출, 채권 그리고 부채에 해당하지 않습니다.
5. GMMT는 환불이 되지 않습니다. 재단은 GMMT 보유자들에게 어떠한 이유에서든 돈을 포함한 어떠한 환불 수단으로도 환불해야 할 의무를 지지 않습니다. GMMT의 향후 가치나 활용성에 대한 어떠한 약속도 없으며, Platform 외부에서 갖는 GMMT에 대한 보증 의무를 지지 않습니다.
6. Coin 판매가 제한된 국가의 시민, 영주권 보유자 혹은 거주자(세금 또는 기타 납부 의무자) 등은 GMMT를 구매할 수 없습니다. 만약 위 금지 국가의 국민이 GMMT를 구매했을 경우에 발생하는 모든 법적 책임은 구매자 본인에게 있습니다. GMMT 구매자는 Coin을 구매하기 전에 해당 사법관할권의 준거법에 대한 준수와 관련하여 독립적인 법률 자문을 구하시기를 권합니다. 본 백서의 원본 및 사본 또는 본 백서의 일부분은 그러한 정보의 배포 또는 보급이 금지되거나 제한되는 국가에서 수신 또는 전송할 수 없습니다.
7. 모든 백서 내용은 저작권의 보호를 받습니다. 개인적 용도 또는 기타 소유권 고지 사항이 있는 경우에만 백서의 개별 섹션을 다운로드하거나 인쇄할 수 있습니다. Mammoth 재단의 사전 서면 허가 없이는 본 백서를 전체적으로 또는 부분적으로 복제하거나 전자적 수단 또는 기타 방식으로 복제하거나, 공공 또는 상업적 목적으로 수정, 링크, 사용할 수 없습니다.

08

# Investment risk

8-1 Investment risk

## 8-1 Investment risk

Mammoth 재단은 구매자들에게 GMMT 구매대금 상당의 손실을 볼 수 있다는 위험을 포함하여 여러 가지 종류의 위험을 고지하고 있습니다. 따라서 GMMT를 구매하실 경우 이러한 가상 화폐 구매에 대한 위험 부담을 충분히 이해하고 계셔야 합니다. 아래에 쓰여진 위험 부담이나 불확실성에 관한 정보의 정확성은 담보되지 않습니다. GMMT 구입에 앞서, 구매자들은 세무, 규제, 금융, 법률 등의 전문가에게 잠재적 위험부담, 수익, Coin 거래가 초래할 수 있는 결과들에 대해서 상담을 받으시기를 권합니다. GMMT의 구입을 고려하고 있으신 분들은 아래의 위험 부담에 대한 내용을 꼭 읽어 보시고 GMMT를 구매하시기 바랍니다.

구매자들은 GMMT의 매매 및 보유로서 명백하게 다음 위험 부담에 대해 인지하고 있는 것으로 간주됩니다.

1. 블록체인 리스크 : 블록체인 시스템 혼잡으로 거래가 지연되거나 무효화될 수 있습니다.
2. 개인 정보 리스크 : 사용자의 개인 정보는 GMMT 구매자의 전자 지갑에 있는 GMMT의 분배와 통제를 위하여 필요합니다. 따라서, 개인 정보가 유출될 경우 구매자의 전자 지갑에 있는 GMMT가 유출될 수 있습니다. 더욱이, 구매자의 개인 정보 유출로 인해 제3자가 구매자의 전자 지갑을 열람하여 GMMT를 훔쳐 갈 수 있습니다.
3. Mammoth 리스크 : GMMT의 발행과 분배를 담당하는 스마트 계약은 블록체인이라는 기술에 기초하고 있습니다. 블록체인 시스템은 아직 개발 초기 단계이며 충분히 검증되지 않았습니다. GMMT 개발 절차상 아무런 에러가 없을 것이라는 사실은 보장되지 않습니다. 프로토콜은 약점과 취약성을 가지고 있을 수 있으며 GMMT가 손실되는 버그를 포함해, 각종 버그가 발생할 수 있습니다. 또한 이러한 블록체인의 문제로 재단 및 GMMT 구매자에게 물질적 피해가 발생할 수 있습니다.
4. 보안 리스크 : 다른 모든 가상 화폐와 마찬가지로 '이중 지불 공격' 혹은 '51% 공격'과 같은 마이닝 공격에 취약합니다. 해커들 혹은 다른 악의적인 의도가 있는 집단들이 위와 같은 공격 방법으로 재단 또는 GMMT를 공격할 수 있으며, 이러한 블록체인 공격이 성공할 경우 GMMT 거래와 GMMT에 큰 타격을 줄 수 있습니다.
5. 전자지갑 호환성 리스크 : GMMT를 구입하거나 저장하기 위해서 GMMT와 기술적 호환이 되는 전자 지갑을 사용해야 합니다. 만약 다른 지갑을 사용하신다면 구입한 GMMT를 확인하지 못할 수 있습니다.
6. Coin 거래 리스크 : GMMT는 Mammoth Platform에서만 사용되도록 고안되었으며 2차 Coin 거래 플랫폼이나 외부 사용에 최적화되어있지 않습니다. 또한 GMMT는 현물로서 인정받지 못하며, GMMT는 가치가 0까지 추락할 수 있는 큰 위험성을 가지고 있습니다.
7. 무보험 손실 리스크 : GMMT와 블록체인 시스템은 은행 계좌나 제도권 금융 기관과 달리 보험에 가입되어 있지 않습니다. 현재로서는, 사용자의 GMMT 손실과 GMMT 가치 하락으로 인한 손실을 배상해 주는 보험회사는 없음을 알려드립니다.
8. 시장경쟁 리스크 : Mammoth 재단은 다른 비슷한 종류의 플랫폼과 애플리케이션 그리고 허가되지 않은 오픈소스 코드나 오픈소스 프로토콜이 Mammoth 재단이나 GMMT에 불리한 영향을 미칠 수도 있다고 보고 있습니다.

## 8-1 Investment risk

---

9. 사용자 리스크 : Mammoth Platform이 완성되어 출시가 된다고 하여도 Mammoth Platform 이 많은 사용자에게 이용 되지 않거나 오직 소수만이 이용할 가능성이 있습니다. 이러한 시장에서의 관심 부족이 재단과 프로젝트의 잠재적 가치에 영향을 미칠 수 있습니다.

10. 개발과 유지 리스크 : Mammoth Platform 은 아직 개발 중에 있으며 시간이 흐름에 따라 큰 변화가 생길 수 있습니다. 재단은 Platform을 백서에 쓰인 내용 그대로 개발 및 유지하도록 노력할 것이나, 법률적 이유, 디자인, 기술, 규제 등 여러 가지의 이유에서 GMMT와 Mammoth Platform의 세부사항에서 변화가 생길 수 있습니다. 위와 같은 변화는 GMMT 구매자 또는 예비 구매자의 예상과는 다를 수 있음을 알려드립니다.

11. 프로젝트 실패 리스크 : 본 백서에 쓰인 모든 내용은 오랫동안 검증되지 않은 내용들입니다. Mammoth Platform 프로젝트는 대중의 관심 부족, 펀드 모금 실패, 상업적 이용 가치의 부재, 핵심 인력 유출과 같은 이유들로 완성 및 실행되지 않을 수도 있습니다. 위와 같은 경우 Mammoth Platform 프로젝트는 GMMT 환불 없이 와해될 수 있습니다.

12. 규제 프레임의 불확실성 리스크 : 가상 화폐 및 블록체인 기술에 대한 규제들이 아직 여러 나라에서 확립되지 못하였으며 향후 규제에 대한 예측 역시 매우 어렵습니다. 이러한 규제는 향후 AI Bitcoin Pick Platform에 부정적으로 확립되어 작용할 수 있습니다. 이러한 경우 재단은 Platform 개발을 중지할 수 있으며 이러한 행위들을 법적이나 상업 적으로 금지하는 정부 하에서의 서비스를 중단할 수 있습니다.

13. 라이선스와 허가에 관한 리스크 : 비록 현재로서는 GMMT 판매에 관해 재단이 라이선스와 인가를 받아야 한다는 등의 법적 요구사항이 없지만 앞으로 이러한 규제가 생길 가능성도 있습니다. 하지만 이러한 규제가 생긴다 하더라도 재단은 그러한 라이선스와 인가 조건에 부합하도록 프로젝트를 운영할 것 입니다. 그러나 재단은 적합한 시간과 예산 내에서 해당 법령에 대한 변화가 불가능하다고 판단할 경우 GMMT의 판매를 중지할 수 있으며, 프로젝트를 중단할 수 있습니다.

14. 과세 리스크 : 가상 화폐에 대한 과세 제도는 아직 불분명합니다. GMMT 구매자들은 자신의 국적, 거주지, 또는 거소 국가 내에서 GMMT의 인수와 처분, 보유, 사용에 대한 과세 제도를 스스로 찾아봐야 하며, 이는 GMMT 구매자에게 불리한 결과를 초래할 수 있습니다.

15. 그 외의 전망되지 않은 리스크 : GMMT를 포함한 가상 화폐는 충분히 검증되지 않은 새로운 기술입니다. 위에 나열된 리스크들 외에도, 예상할 수 없는 많은 리스크들이 GMMT를 구매, 보유, 사용함으로써 초래될 수 있습니다. 이러한 예기치 못한 리스크들이나 상기 나열된 리스크들은 예고 없이 갑작스럽게 나타날 수 있습니다.

GIANT



MAMMOTH

Thank you for watching.