최종연구보고서	KISA-WP-2023-0035

블록체인 확장성 문제해결을 위한 대안기술 분석

A Study on alternative technologies for solving blockchain scalability issues

수 행 기 관 : ㈜ 지 크 립 토 (Z k r y p t o)

2023. 12.

KISA 한국인터넷진흥원

제 출 문

한국인터넷진흥원 원장 귀하

본 보고서를 “블록체인 확장성 문제해결을 위한 대안기술 분석”의 최종연구개발 결과보고서로 제출합니다.

2023년 12월 15일

수행 기관 : ㈜지크립토(Zkrypto)
연구책임자 : 대표이사 오 현 옥
참여연구원 : 전 무 김 봉 규
이 사 김 지 혜
이 사 김 두 연
선임연구원 조 승 표
연 구 원 김 경 빈
연 구 원 이 올 미
보 조 원 권 혁 태

요 약 문

1. 제목: 블록체인 확장성 문제해결을 위한 대안기술 분석

2. 연구개발의 목적 및 중요성

○ **(목적)** 블록체인의 확장성 및 프라이버시 문제의 해결을 위해 영지식 증명에 대한 기술에 대한 기본 개념과 심화 개념을 소개하고 실제 영지식 증명을 응용에 적용했을 때 여러 가지 기법 중 선택 방법을 제시함. 또한 영지식 증명을 활용한 블록체인 사례들을 조사하고 이에 따른 기술적, 산업적, 사회적 기대효과를 도출

○ **(중요성)** 블록체인은 혁신적인 기술로써 다양한 산업 분야에서 그 중요성을 지속적으로 확대하고 있음. 그러나 블록체인의 확장성과 프라이버시 문제는 여전히 큰 도전 과제로 남아 있음. 현재 대부분의 블록체인은 처리량이 제한적이며, 대규모 트랜잭션을 처리하는 데 있어서 한계를 보이고 있음. 이는 블록체인이 실제 비즈니스 환경에서 널리 채택되는 데 큰 장애물로 작용하고 있음. 영지식 증명 기술은 데이터의 유효성을 증명하면서 해당 데이터를 직접 공개하지 않는 암호학적 방법을 제공함. 영지식 증명 기술은 트랜잭션의 유효성을 간결하게 증명하면서 데이터를 공개하지 않게 되므로, 블록체인 네트워크의 부하를 줄이고 처리량을 향상시킬 수 있음. 이로 인해 블록체인의 확장성 문제를 해결할 수 있음. 또한, 현재의 블록체인 시스템에서는 투명성을 보장하기 위해 트랜잭션의 내용이 공개되는 경우가 많아, 이로 인해 개인정보 노출(예: 거래내역)과 같은 프라이버시 문제가 발생할 수 있음. 블록체인의 프라이버시 문제도 영지식 증명 기술을 통해 개선될 수 있음. 더불어, 영지식 증명 기술의 적용은 단순히 기술적인 문제를 해결하는 것을 넘어서, 블록체인의 사회적, 경제적 가치를 높일 수 있음. 프라이버시 보호와 확장성 향상은 블록체인 기반의 서비스나 애플리케이션의 사용자 경험을 향상시키며, 더 넓은 범위의 산업 분야에서 블록체인의 적용 가능성을 확대시킬 수 있음. 그러나, 영지식 증명 기술의 복잡성과 블록체인에의 적용에 있어서의 다양한 장벽들로 인해, 이 기술의 실질적인 적용과 활용은 쉽지 않음. 따라서, 영지식 증명 기술의 깊은 이해와 블록체인에 적용하는 방안, 그리고 이를 통한 실제 서비스의 사례 조사 등에 대한 체계적이고 깊이 있는 연구가 필요함. 이러한 연구를 통해 블록체인의 잠재력을 최대한 발휘하고, 다양한 산업 분야에서의 적용과 활용을 촉진시킬 수 있을 것임

3. 연구개발의 내용 및 범위

○ **(기본 개념)** 영지식 증명에 대한 이해도가 낮은 사람들을 위한 기본 개념 조사

○ **(심화 개념 및 기법 선택)** 영지식 증명의 기술적인 내용에 대해서 더 깊이 이해할 수 있도록 심화 개념 조사

○ **(확장성 및 프라이버시를 위한 영지식 증명)** 영지식 증명을 활용한 블록체인 기술 현황 및 블록체인의 프라이버시 강화를 위한 기술현황

○ **(영지식 증명 서비스)** 국내·외 영지식 증명이 적용된 서비스(전자투표, 전자신분증 등)에 대한 적용 사례 조사

○ **(기대효과)** 각 서비스별 기술적, 산업적, 사회적 기대효과를 도출하여 블록체인에 있어 영지식 증명의 중요성 확인

4. 연구결과

1) 블록체인 기술의 발전 배경과 현재 상황

○ 블록체인 기술은 4차 산업 혁명의 중심에서 주목받으며, 중앙 관리자 없이 데이터를 저장하고 활용하는 데 큰 잠재력을 보여왔음

○ 특히 금융 기술, 부동산, 투표 등 다양한 산업 분야에서 중앙 집권 구조의 서비스를 대체하는 역할을 하고 있으나, 확장성과 보안성의 트릴레마 문제에 직면함

○ 블록체인 플랫폼들은 대규모 트랜잭션 처리에 있어서 비자(VISA)와 같은 시스템에 비해 낮은 처리량을 보여주고 있음

○ 또한 투명성으로 인하여 데이터 위변조를 방지하는 장점을 가지지만 반대로 저장된 데이터의 프라이버시 문제를 야기하는 단점을 가지고 있음

2) 블록체인의 기술적 문제점과 영지식 증명의 도입

○ 블록체인의 확장성 문제와 프라이버시 문제는 다양한 산업에서 블록체인의 적용을 주저하게 만드는 큰 도전 과제로 남아 있음

○ 이러한 문제점을 해결하기 위한 방안으로 영지식 증명 기술이 주목받고 있음

○ 영지식 증명은 데이터의 유효성을 증명하면서 해당 데이터를 공개하지 않는 암호학적 방법을 제공하며, 블록체인 네트워크의 부하를 줄이고 처리량을 향상시킬 수 있음. 또한 데이터의 프라이버시를 강화하여 개인정보 보호 측면에서 강력한 기능을 제공함

3) 기술적 트렌드 및 적용 방안

○ 영지식 증명 기술은 다양한 방법 및 기술적 트렌드에 대한 연구가 진행되고 있음

○ 본 연구는 영지식 증명의 기본 개념부터 심화 내용, 응용에 적합한 기법의 선택 등을 포괄적으로 다룸

○ 또한, 블록체인에서 영지식 증명의 활용 현황과 프라이버시 강화를 위한 기술 동향,

국제 표준 및 라이브러리의 현황 등을 조사하여 제시함

○ 이러한 연구를 통해 블록체인 기술의 확장성 및 프라이버시 문제 해결 측면에서 블록체인 트릴레마를 해결할 대안기술로서 영지식 증명 기술의 중요성을 강조함

4) 영지식 증명 기술의 기대 효과와 적용 사례

○ 영지식 증명 기술의 적용은 블록체인의 확장성 문제를 해결하고 프라이버시를 보호함으로써 여러 산업에서 블록체인의 적용 범위를 넓힐 수 있음

○ 영지식 증명 기술의 적용은 블록체인의 사회적, 경제적 가치를 높이며, 사용자 경험을 향상하는데 중요한 역할을 함

○ 본 연구는 국내·외에서 영지식 증명이 적용된 서비스(전자투표, 전자신분증, 중앙은행 디지털화폐, 디지털지갑 등)의 사례를 조사하고, 이들의 기술적, 산업적, 사회적 기대효과를 분석함

서비스	내용
전자투표 서비스	• 영지식 증명은 전자투표 시스템에서 투표의 익명성과 정확성을 동시에 보장하는 데 활용됨 • 투표자의 신원 정보는 보호되면서도, 그들의 투표가 유효하고 정확하게 집계되는 것을 보증함 • 이를 통해 전자투표 시스템의 신뢰성과 투명성이 향상되며, 선거 과정에서의 사기나 부정을 방지하는 데 기여함
전자신분증 서비스	• 영지식 증명을 적용한 전자신분증은 사용자의 개인정보 보호와 동시에 신원 확인의 정확성을 제공함 • 사용자는 필요한 최소한의 정보만을 공개하면서 신원을 증명할 수 있으며, 개인정보 노출의 위험을 줄일 수 있음 • 공공 서비스 및 다양한 온라인 플랫폼에서의 안전한 신분 인증과 편리성을 제공함
중앙은행 디지털화폐 (CBDC)	• 영지식 증명은 중앙은행 디지털화폐의 거래에서 사용자의 프라이버시를 보장하는 데 중요한 역할을 함 • 사용자는 자신의 거래 내역을 보호하면서도, 거래의 유효성과 준법성을 증명할 수 있음 • 이로 인해 CBDC의 보안성과 신뢰성이 향상되며, 광범위한 디지털 경제에서의 안전하고 효율적인 금융 거래가 가능해짐

디지털 지갑 서비스	• 디지털 지갑에서 영지식 증명은 사용자의 거래 기록과 잔액 정보를 보호하는 데 사용됨 • 사용자는 자신의 재산과 거래 내역을 공개하지 않고도, 거래의 유효성을 증명할 수 있음 • 이 기술은 디지털 지갑의 보안을 강화하고, 사용자의 프라이버시를 존중하는 동시에, 금융 거래의 투명성을 유지하는 데 기여함

5) 영지식 증명 기술의 연구 필요성과 전망

○ 영지식 증명 기술은 기술의 복잡성과 적용의 다양한 장벽 때문에 실질적인 활용이 쉽지 않음

○ 따라서 이 기술에 대한 깊은 이해와 적용 방안, 실제 서비스 사례의 조사 등에 대한 체계적이고 깊이 있는 연구가 필요함

○ 이를 통해 블록체인 기술의 잠재력을 최대한 발휘하고, 다양한 산업 분야에서의 적용과 활용을 촉진시킬 수 있음

○ 블록체인 기술은 금융, 부동산, 투표 등 다양한 분야에서 중요한 역할을 하고 있으며, 영지식 증명 기술의 발전은 이러한 분야에서의 블록체인 기술 활용을 더욱 확대시킬 수 있음

5. 활용에 대한 건의

1) 블록체인의 확장성 개선

○ **(확장성 문제 해결)** 현재 블록체인 플랫폼들이 직면한 가장 큰 도전 중 하나는 제한된 처리량과 확장성 문제임. 영지식 증명 기술을 적용함으로써, 더 많은 트랜잭션을 더 빠르고 효율적으로 처리할 수 있게 되어, 블록체인의 상업적 및 산업적 활용 가능성이 크게 증가함

2) 프라이버시 보호 강화

○ **(개인정보 보호 강화)** 영지식 증명은 데이터의 유효성을 증명하면서 데이터 자체를 공개하지 않는 암호학적 방법을 제공함. 이를 통해, 블록체인 상의 개인정보 노출 위험을 감소시키고 사용자의 프라이버시를 강화할 수 있음

○ **(트랜잭션의 투명성 유지)** 블록체인의 핵심 장점인 투명성을 유지하면서도 개인의 프라이버시를 보호할 수 있음. 이는 블록체인 기술이 금융, 의료, 정부 등의 민감한 데이터를 다루는 분야에 더 널리 채택되어 사용될 수 있음

3) 산업 분야의 확장

○ **(다양한 산업으로의 적용 확대)** 영지식 증명과 블록체인 기술의 결합은 다양한 산업 분야에서 적용될 수 있음 특히, 고도의 보안과 프라이버시가 요구되는 분야에서 블록체인 기술의 적용이 가능함

○ **(혁신적인 서비스 개발)** 영지식 증명의 기술적 진보는 새로운 형태의 서비스와 애플리케이션의 개발을 촉진시킬 수 있으며, 블록체인 기반 서비스의 사용자 경험을 향상시킴. 예를 들어, 보안이 중요한 전자 투표 시스템, 개인 건강 정보의 안전한 관리, 금융 트랜잭션의 효율성 향상 등에 영지식 증명 기술이 적용될 수 있음

6. 기대효과

1) 기술적 기대효과

○ **(블록체인 기술의 발전)** 영지식 증명 기술의 발전은 블록체인 기술의 보안성과 확장성을 크게 향상시킬 수 있음. 영지식 증명은 블록체인에서의 데이터 유효성을 증명하면서도 실제 데이터 내용을 공개하지 않는 방식으로, 이는 보안성을 강화하는 동시에 네트워크 부하를 줄이는 데 기여함

○ **(효율성 증가)** 트랜잭션 처리 속도와 효율성이 향상됨으로써, 블록체인은 대규모 트랜잭션을 더 빠르고 효율적으로 처리할 수 있게 되며 이는 블록체인의 상용화와 널리 채택되는 데 중요한 요소임

2) 경제적 기대효과

○ **(비용 절감)** 영지식 증명 기술을 통해 블록체인 네트워크의 처리량이 증가함에 따라, 트랜잭션 비용이 감소함. 또한, 이 기술은 블록체인 기반 서비스의 운영 비용을 절감하는 데도 기여할 수 있음

○ **(효율성 증대)** 블록체인 서비스의 처리 속도와 효율성이 증가함으로써, 사용자 경험이 향상되고, 서비스 제공업체는 더 많은 사용자를 수용할 수 있음

3) 사회적 기대효과

○ **(프라이버시 보호 강화)** 영지식 증명은 블록체인 트랜잭션에서 개인정보의 노출 없이 데이터의 유효성을 증명할 수 있게 해, 프라이버시 보호를 크게 강화함. 이는 특히 개인 데이터 보호가 중요한 분야에서 블록체인 기술의 채택을 촉진할 수 있음

○ **(블록체인에 대한 신뢰도 및 수용도 증진)** 더 높은 보안성과 프라이버시 보호 기능은 블록체인 기술에 대한 신뢰를 증진시킴. 이러한 신뢰도 향상은 블록체인 기술의 사회적 수용도를 높이는 데 중요한 역할을 함

SUMMARY

1. Title : A Study on alternative technologies for solving blockchain scalability issues

2. Purpose of the study

○ (Purpose) This study introduces the basic and advanced concepts of zero-knowledge proof technology to solve the scalability and privacy problems of blockchain, and suggests how to choose among various techniques when applying zero-knowledge proof in practice. It also explores blockchain cases that utilize zero-knowledge proofs and derives technical, industrial, and social expectations

○ (Importance) Blockchain is a revolutionary technology that continues to grow in importance across a wide range of industries. However, scalability and privacy remain major challenges. Currently, most blockchains have limited throughput and are unable to handle large transactions. This is a major obstacle to widespread adoption in real-world business environments. Zero-knowledge proof technology provides a cryptographic way to prove the validity of a data without directly disclosing a data. Zero-knowledge proofs can reduce the load on the blockchain network and improve throughput because they can concisely prove the validity of a transaction while not revealing any data. In this way, it can solve the scalability problem of blockchains. In addition, in current blockchain systems, the contents of transactions are often made public to ensure transparency, which can lead to privacy issues such as the exposure of personal information (e.g., transaction history). The privacy issues of blockchain can be improved by using zero-knowledge proof technology. Furthermore, the application of zero-knowledge proofs goes beyond solving technical problems and can increase the social and economic value of blockchains. Improved privacy and scalability can enhance the user experience of blockchain-based services and applications and expand the applicability of blockchain to a wider range of industries. However, due to the complexity of zero-knowledge proof technology and various barriers to its application on blockchains, the practical application and utilization of this technology is not easy. Therefore, it is necessary to conduct systematic and in-depth research on the deep understanding of zero-knowledge proof technology, how to apply it to blockchain, and case studies of real-world services. Through such research, it will be possible to realize the full potential of blockchain and promote its application and utilization in various industries

3. Content and Scope of the study

○ **(Basic Concepts)** Explore basic concepts for those with a limited understanding of zero-knowledge proofs

○ **(Advanced Concepts and Choose a Technique)** Investigate advanced concepts for a deeper understanding of the technical content of zero-knowledge proofs

○ **(Zero-Knowledge Proof for Scalability and Privacy)** The current state of blockchain technology utilizing zero-knowledge proof and the current state of technology for enhancing blockchain privacy

○ **(Zero-Knowledge Proof Services)** Examine the application cases of domestic and international zero-knowledge proof services (e-voting, electronic identification, etc.)

○ **(Expected Effects)** Identify the importance of zero-knowledge proof for blockchain by deriving technical, industrial, and social expected effects for each service

4. Results of the study

1) Background and current status of blockchain technology

○ Blockchain technology has gained attention at the center of the Fourth Industrial Revolution and has shown great potential for storing and utilizing data without a centralized administrator

○ In particular, it is playing a role in replacing centralized services in various industries such as financial technology, real estate, and voting, but it faces the trilemma of scalability and security

○ Blockchain platforms have low throughput compared to systems like VISA when it comes to processing large-scale transactions

○ It also has the advantage of preventing data forgery due to its transparency, but on the other hand, it has the disadvantage of causing privacy issues of stored data

2) Technical problems of blockchain and the introduction of zero-knowledge proofs

○ Scalability issues and privacy issues of blockchain remain major challenges that make people hesitate to apply blockchain in various industries

○ Zero-knowledge proof technology is gaining attention as a way to solve these problems

○ Zero-knowledge proofs provide a cryptographic way to prove the validity of data without revealing that data, and can reduce the load on blockchain networks and improve throughput. It also provides a powerful function in terms of privacy protection by enhancing the privacy of data

3) Technical Trends and Applications

○ Various methods and technical trends are being researched for zero-knowledge proof technology

○ This study comprehensively covers the basic concepts of zero-knowledge proof, in-depth contents, and selection of suitable techniques for application

○ It also investigates and presents the current status of utilization of zero-knowledge proof in blockchain, technology trends for enhancing privacy, and the status of international standards and libraries
○ This studies emphasize the importance of zero-knowledge proof technology as an alternative technology to solve the blockchain trilemma in terms of scalability and privacy issues in blockchain technology

4) Expected effects and applications of zero-knowledge proof technology

○ The application of zero-knowledge proof technology can solve the scalability problem of blockchain and protect privacy, thereby expanding the application of blockchain in various industries
○ The application of zero-knowledge proof technology plays an important role in increasing the social and economic value of blockchain and improving user experience
○ This study investigates the cases of services (e-voting, e-Identity, central bank digital currency, digital wallet, etc.) where zero-knowledge proof has been applied at home and abroad, and analyzes their technical, industrial, and social expectations

Services	Contents
E-Voting Services	• Zero-knowledge proofs are utilized in e-voting systems to ensure both anonymity and accuracy of votes • It ensures that voters' identities are protected while their votes are counted validly and accurately. • This increases the trustworthiness and transparency of e-voting systems and helps prevent fraud and irregularities in the election process
E-ID Services	• EIDs with zero-knowledge proofs provide identity verification accuracy while protecting users' privacy. • Users can prove their identity while disclosing only the minimum necessary information, reducing the risk of personal information exposure • Provide secure identification and convenience for public services and various online platforms
Central Bank Digital Currency (CBDC)	• Zero-knowledge proofs play an important role in ensuring user privacy in central bank digital currency transactions • Users can prove the validity and compliance of their transactions while protecting their transaction history • This improves the security and trustworthiness of CBDCs and enables secure and efficient financial transactions across the broader digital economy
Digital wallet services	• In digital wallets, zero-knowledge proofs are used to protect a user's transaction history and balance information • Users can prove the validity of transactions without disclosing their property and transaction history • This technology contributes to enhancing the security of digital wallets, respecting user privacy, and maintaining transparency in financial transactions

5) Research Needs and Prospects for Zero-Knowledge Proof Technology

○ Zero-knowledge proof technology is not easy to utilize in practice due to the complexity of the technology and various barriers to application

○ Therefore, it is necessary to conduct systematic and in-depth research on deep understanding of this technology, application methods, and investigation of actual service cases

○ This will help unlock the full potential of blockchain technology and promote its application and utilization in various industries

○ Blockchain technology plays an important role in various fields such as finance, real estate, and voting, and the development of zero-knowledge proof technology can further expand the use of blockchain technology in these fields

5. Applications

1) Improving the scalability of the blockchain

○ **(Solving the Scalability Problem)** One of the biggest challenges facing blockchain platforms today is limited throughput and scalability. By applying zero-knowledge proof technology, more transactions can be processed faster and more efficiently, greatly increasing the potential for commercial and industrial utilization of blockchain

2) Enhanced privacy protection

○ **(Enhanced Privacy)** Zero-knowledge proofs provide a cryptographic way to prove the validity of data while not disclosing the data itself. This reduces the risk of personal information exposure on the blockchain and enhances user privacy

○ **(Maintain Transparency of Transactions)** Protecting individual privacy while maintaining transparency, a key advantage of blockchain. This means that blockchain technology can be more widely adopted and used in sectors that deal with sensitive data, such as finance, healthcare, and government

3) Expansion of industries

○ **(Expanding Application to Various Industries)** The combination of zero-knowledge proof and blockchain technology can be applied in various industries, especially in areas requiring high security and privacy

○ **(Developing Innovative Services)** Technological advances in zero-knowledge proofs can facilitate the development of new types of services and applications, enhancing the user experience of blockchain-based services. For example, zero-knowledge proof technology can be applied to security-critical electronic voting systems, secure management of personal health information, and improved efficiency of financial transactions

6. Expected effects

1) Technical Expectations

○ **(Advancement of Blockchain Technology)** Advancement of zero-knowledge proof technology can significantly improve the security and scalability of blockchain technology. Zero-knowledge proof is a method of proving the validity of data on a blockchain without disclosing the actual data content, which contributes to enhancing security while reducing network load

○ **(Increased Efficiency)** By improving transaction processing speed and efficiency, blockchains will be able to process large-scale transactions faster and more efficiently, which is an important factor in the commercialization and widespread adoption of blockchains

2) Economic Expectations

○ **(Cost Reduction)** As the throughput of blockchain networks increases through zero-knowledge proof technology, the cost of transactions decreases. This technology can also contribute to reducing the operating costs of blockchain-based services

○ **(Increased Efficiency)** By increasing the processing speed and efficiency of blockchain services, the user experience is improved and service providers can accommodate more users

3) Social Expectations

○ **(Enhanced Privacy Protection)** Zero-knowledge proofs can prove the validity of data in blockchain transactions without exposing personal information, greatly enhancing privacy protection. This can promote the adoption of blockchain technology, especially in areas where personal data protection is important

○ **(Increased Trust and Acceptance of Blockchain)** Higher security and privacy protections increase trust in blockchain technology. This increased trust plays an important role in increasing the social acceptance of blockchain technology

목 차

그 림 목 차

표 목 차

제 1 장. 서 론

제1절. 연구의 추진배경 및 필요성

1. 연구 추진배경

- 블록체인 기술은 4차 산업 혁명의 중심에서 대두되었으며, 중앙의 관리자 없이 공통된 데이터를 저장하고 활용하는 데 큰 잠재력을 보여왔음. 특히, 중앙은행 디지털화폐(CBDC)와 같은 금융 기술은 전 세계 다양한 국가에서의 도입과 적용을 위한 검토가 진행되고 있음

- 또한, 부동산, 투표 등의 다양한 산업 분야에서도 블록체인 기술이 중앙 집권 구조의 서비스를 대체하는 중요한 역할을 하고 있지만, 블록체인은 확장성, 탈중앙화, 프라이버시 중 두 가지는 해결할 수 있지만, 세 가지 목표를 한 번에 해결할 수 없는 트릴레마(Triliemma) 문제를 가지고 있음

- 현재의 주요 블록체인 플랫폼들은 신용카드 회사인 비자(VISA)와 같은 대규모 트랜잭션을 처리하는 시스템에 비해 상대적으로 낮은 처리량을 보임. 이를 블록체인의 확장성 문제라고 함

- 또한, 공개형 블록체인의 투명성은 데이터의 위변조를 방지하는 장점이 있지만, 동시에 저장된 데이터의 프라이버시 문제를 일으키는 큰 단점으로 작용하고 있음. 이를 블록체인의 프라이버시 문제라고 함. 이 두 가지 문제점을 같이 해결하고자 하면 블록체인이 추구하는 탈중앙성이 떨어지게 됨

- 상기 언급된 서비스 외에도 정보통신서비스 분야에서 블록체인을 활용한 서비스가 다양하게 등장함에 따라 탈중앙성의 훼손 없이 블록체인에 산재한 확장성 문제와 프라이버시 문제를 포함한 트릴레마의 해결을 위해 여러 가지 기술들을 적용 중임

- 본 연구에서는 확장성 문제와 프라이버시 문제를 해결하기 위한 영지식 증명 기술을 분석하고 이를 적용한 실제 서비스의 사례를 조사하여 확장성 문제와 프라이버시 문제 해결에 대한 영지식 증명 기술의 기대 효과를 도출하고자 연구를 추진함

2. 연구 필요성

- 블록체인은 혁신적인 기술로써 다양한 산업 분야에서 그 중요성을 지속해서 확대하고 있음. 그러나 블록체인의 확장성과 프라이버시 문제는 여전히 큰 도전 과제로 남아 있음. 이러한 문제점을 극복하기 위한 가장 유망한 해결책 중 하나로 영지식 증명 기술이 주목받고 있음. 영지식 증명 기술은 데이터의 유효성을 증명하면서 해당 데이터를 직접 공개하지 않는 암호학적 방법을 제공함

- 현재 대부분 블록체인은 처리량이 제한적이며, 대규모 트랜잭션을 처리하는 데 있어서 한계를 보임. 이는 블록체인이 실제 비즈니스 환경에서 널리 채택되는 데 큰 장애물로 작용하고 있음. 이를 해결하기 위해 영지식 증명을 블록체인에 도입하였는데 이 기술은 트랜잭션의 유효성을 간결하게 증명하면서 데이터를 공개하지 않게 되므로, 블록체인 네트워크의 부하를 줄이고 처리량을 향상할 수 있음. 이로 인해 블록체인의 확장성 문제를 해결할 수 있음

- 또한, 현재의 블록체인 시스템에서는 투명성을 보장하기 위해 트랜잭션의 내용이 공개되는 경우가 많아, 이로 인해 개인정보 노출과 같은 프라이버시 문제가 발생할 수 있음. 이러한 블록체인의 프라이버시 문제 또한 확장성 문제와 같이 영지식 증명 기술을 통해 개선될 수 있음

- 더불어, 영지식 증명 기술의 적용은 단순히 기술적인 문제를 해결하는 것을 넘어서, 블록체인의 사회적, 경제적 가치를 높일 수 있음. 프라이버시 보호와 확장성 향상은 블록체인 기반의 서비스나 애플리케이션의 사용자 경험을 향상하며, 더 넓은 범위의 산업 분야에서 블록체인의 적용 가능성을 확대할 수 있음

- 그러나, 영지식 증명 기술의 복잡성과 블록체인에의 적용에서 다양한 장벽들로 인해, 이 기술의 실질적인 적용과 활용은 쉽지 않음. 따라서, 영지식 증명 기술의 깊은 이해와 블록체인에 적용하는 방안, 그리고 이를 통한 실제 서비스의 사례 조사 등에 대한 체계적이고 깊이 있는 연구가 필요함. 이러한 연구를 통해 블록체인의 잠재력을 최대한 발휘하고, 다양한 산업 분야에서의 적용과 활용을 촉진할 수 있을 것임

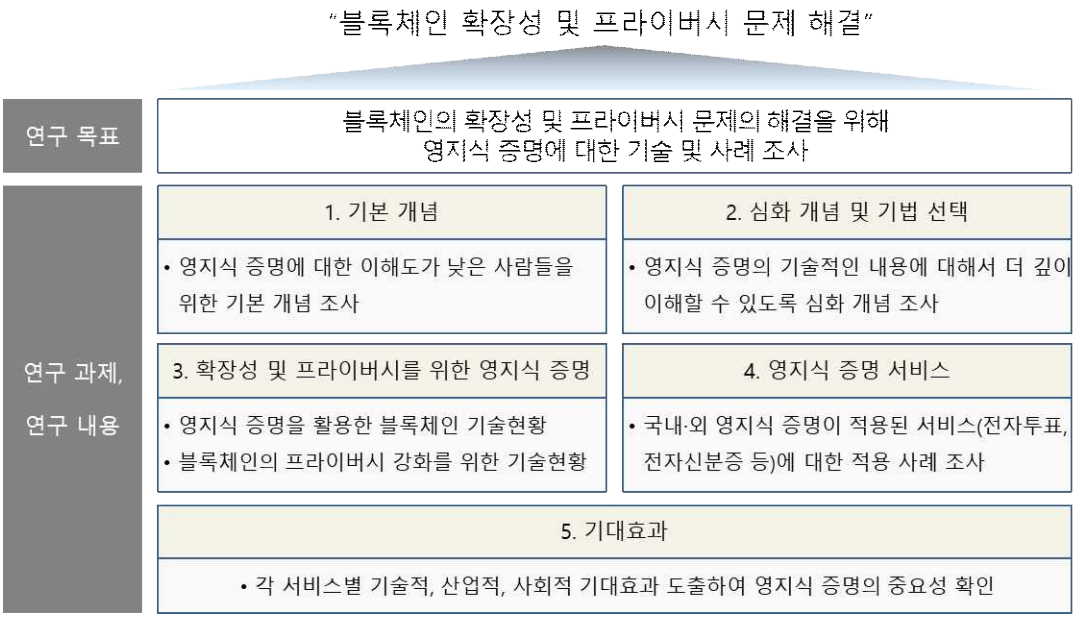
제2절. 연구의 목적, 구성 및 범위

1. 연구 목적 및 범위

○ 블록체인의 확장성 및 프라이버시 문제의 해결을 위해 영지식 증명에 관한 기술 및 사례 조사를 연구 목표로 하며, 다음과 같이 세부 연구과제를 수행함

- **(기본 개념)** 영지식 증명에 대한 이해도가 낮은 사람들이 영지식 증명 기술을 쉽게 이해할 수 있도록 기본 개념을 조사함
- **(심화 개념 및 기법 선택)** 영지식 증명을 어느 정도 이해하고 있는 사람들이 영지식 증명의 기술적인 내용에 대해서 더 깊이 이해할 수 있도록 여러 가지 방법 및 기술적 추세를 조사하고 여러 가지 기법들을 응용에 맞게 분류하여 실제 영지식 증명을 응용에 적용하고자 했을 때 선택하는 방법에 대하여 작성함
- **(확장성 및 프라이버시를 위한 영지식 증명)** 영지식 증명을 활용한 블록체인 확장성 기술현황과 영지식 증명을 활용한 블록체인 프라이버시 기술현황, 국제 표준 및 라이브러리의 현황을 조사함
- **(영지식 증명 블록체인 서비스)** 국내·외 영지식 증명이 적용된 서비스(전자투표, 전자신분증, 중앙은행 디지털화폐, 디지털 지갑, 공급망 관리 시스템)에 대한 적용사례를 조사하고 서비스별 기술적, 산업적, 사회적 기대효과를 도출하여 블록체인의 확장성 및 프라이버시 측면에서 영지식 증명의 중요성을 확인함

2. 연구 구성



[그림 1] 본 연구 목표 및 내용

3. 연구 범위

[표 1] 연구의 범위

구분	연구의 범위
제1장. 서론	• 본 연구의 추진배경과 필요성에 대해 상세히 기술함. 또한, 본 연구의 목표, 구성, 그리고 연구 범위에 대해서도 체계적으로 설명함
제2장. 영지식 증명 주요 기술 조사	• 영지식 증명의 기본적인 개념부터 심화 내용까지를 정리하였으며, 다양한 기법에 따른 분류와 그 기법들을 실제 응용할 때의 선택 방법을 제안함. 또한, 블록체인에서의 영지식 증명 활용 현황과 프라이버시 강화를 위한 기술 동향을 조사함. 마지막으로 국제 표준에서 인정받은 영지식 증명 기술과 실제 응용에서 활용되는 라이브러리들에 대한 조사 결과를 제시함
제3장. 영지식 증명 서비스 국내·외 적용사례 조사 및 기대효과	• 국내·외에서 영지식 증명이 도입된 서비스들, 예를 들면 전자투표, 전자신분증, 중앙은행 디지털화폐, 디지털 지갑 등의 적용사례를 분석하였고 각 사례에서는 기술적, 산업적, 그리고 사회적 측면에서의 기대효과를 파악함

제4장. 결론	• 앞장의 개념 및 서비스와 기대효과들을 근거로 하여 확장성 및 프라이버시 문제 해결 측면에서 블록체인 트릴레마를 해결할 대안기술로써 영지식 증명 기술의 필요성과 중요성을 강조함

제 2 장. 영지식 증명 주요 기술 조사

제1절. 영지식 증명 기술 개요

본 절에서는 영지식 증명 기술의 기본 개념의 이해를 돕는 기본 개념과 영지식 증명의 세부 동작 원리를 이해하기 위한 심화 개념에 대한 설명을 제공함

1. 영지식 증명 기술의 기본 개념

영지식 증명 기술의 기본 개념은 영지식 증명의 정의 및 특성, 영지식 증명의 종류를 설명하고, 이를 활용할 수 있는 방안을 설명함

○ 영지식 증명의 정의

- 1985년 Shafi Goldwasser, Silvio Micali, Charles Rackoff의 논문 “The Knowledge Complexity of Interactive Proof-Systems” [GMR85]에서 처음 소개된 개념임. 영지식 증명(Zero-Knowledge Proof, ZKP)이란 어떠한 사실을 증명할 때, 어떤 문장의 참, 거짓 여부를 제외하고는 어떠한 정보도 노출하지 않는 것임

○ 영지식 증명의 특성

- 완전성 (Completeness) : 어떤 문장이 참이면, 정직한 증명자는 정직한 검증자에게 이 사실을 이해시킬 수 있어야 함
- 건전성 (Soundness) : 어떤 문장이 거짓이면, 어느 부정직한 증명자라도 정직한 검증자에게 이 문장이 사실이라고 이해시킬 수 없어야 함
- 영지식성 (Zero-Knowledgeness) : 어떤 문장이 참이면, 검증자는 문장의 참 거짓 이외에는 아무것도 알 수 없어야 함

[표 2] 영지식 증명 참여 주체 및 구성요소 개념설명

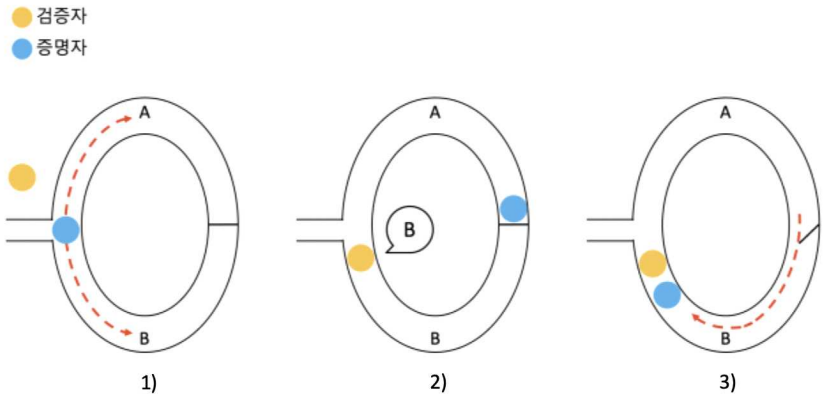
구분	내용
증명자(Prover)	어떤 명제가 참임을 증명하는 역할
검증자(Verifier)	증명자의 주장이 올바른지 검증하는 역할
진술(Instance)	증명자와 검증자에게 모두 제공되는 정보로, 어떤 함수의 입력/출력에 해당함. 증명자는 검증자에게 주어진 입력에 대해 함수를 실행했을 때 해당하는 출력이 나옴을 주장함
비밀 정보(Witness)	주어진 입력을 통해 함수를 계산하는 과정을 담은 정보
문장(Statement)	증명하고자 하는 정보
관계식(Relation)	증명할 사실과 비밀 정보로 이루어진 쌍

○ 영지식 증명의 종류

- 영지식 증명은 (1) 대화형 영지식 증명(Interactive Zero-Knowledge Proof)과 (2) 비대화형 영지식 증명(Non-Interactive Zero-Knowledge Proof)으로 나눌 수 있음

(1) (대화형 영지식 증명) 1989년 Jean-Jacques Quisquater의 논문 “How to Explain Zero-Knowledge Protocols to Your Children” [QG90]에 나온 예제인 알리바바의 동굴(Alibaba’s cave) 비유를 통해 쉽게 이해할 수 있음

- 둥근 고리 형태의 동굴에는 A와 B라는 길이 있으며, 그 사이에는 비밀 주문을 말해야 열리는 문이 있다고 가정함. 그리고 비밀 주문을 알고 있다고 주장하는 증명자와 증명자가 정말로 비밀 주문을 알고 있는지 검증하는 검증자가 있음. 증명자는 검증자에게 비밀 주문이 무엇인지 알려주지 않고 자신이 비밀번호를 알고 있음을 증명하고자 함. 증명 방식은 다음과 같음



[그림 2] 영지식 증명을 알리바바 동굴에 비유한 그림

1) 증명자가 먼저 A 또는 B 갈림길을 선택해 동굴로 들어감
2) 검증자가 A와 B 중 하나를 골라 증명자에게 그 길로 나오기를 요청함
3) 증명자는 검증자가 말한 길로 나옴

※ 이 과정을 한 번 시행했을 때, 검증자는 증명자가 정말로 비밀 주문을 알고 있다고 확신하기 어려움. 증명자가 우연히 검증자가 말한 길로 들어갔다면 비밀 주문을 모르더라도 그 길로 나올 수 있기 때문이며 확률로 따지면 $\frac{1}{2}$임 그러나 이 과정을 여러 번 시행한다면 증명자가 계속해서 검증자의 지시를 모두 따를 확률은 매우 낮아짐. 예를 들어 위의 과정을 20번 시행하고 증명자가 비밀 주문을 모른 채 검증자의 지시를 모두 따를 수 있는 확률은 $\left(\frac{1}{2}\right)^{20}$, 즉 100만분의 1 정도로 낮아짐. 따라서 이 과정을 40번 정도만 반복해도 비밀 주문을 모르고 검증자의 지시를 따를 수 있는 확률은 1조분의 1이 되고 이는 0에 수렴하는 수치임

(2) (비대화형 영지식 증명) 증명 검증 시 상호작용(Interaction)이 필요하지 않은 시스템임. 위에서 살펴본 대화형 영지식 증명에서는 증명자와 검증자가 여러 번 메시지를 교환해야 하므로 효율성이 떨어짐. 하지만 비대화형 영지식 증명에서는 증명자가 검증자에게 증거를 한 번만 보내면 됨. 증명자가 검증자에게 증거를 보낸 후 추가적인 메시지 교환이 일어나지 않으므로 블록체인에서는 대화형 영지식 증명보다 비대화형 영지식 증명을 적용하는 것이 더 효율적임

내가 이 문제에서 아는 정보를 보이지 않고 안다는 사실만 증명할게!
=
내가 Check_age에서 age를 보이지 않고 age > 19만 증명할게!

관계식 : Relation
비밀 정보 : Witness
진술 : Statement
증명 : Proof/Argument

[그림 3] 나이 체크를 위한 영지식 증명

- 비대화형 영지식 증명을 더 쉽게 이해하기 위해 증명자의 나이가 19세 이상인지 검증하는 상황을 가정함. 검증자는 증명자가 성인인지 검증하고자 하고, 증명자는 자신의 나이가 몇 살인지는 공개하지 않고 19세 이상임을 증명하고 싶음. 이때 비대화형 영지식 증명을 이용하면 검증자가 증명자의 실제 나이를 모르고도 19세 이상임을 검증할 수 있음

※ 증명자가 본인의 나이를 비대화형 영지식 증명 시스템에 입력하고 시스템은 입력받은 내용을 암호화함. 그런 다음 암호화된 내용을 바탕으로 만들어진 증거를 검증자에게 전송하고, 검증자는 전송된 증거를 가지고 시스템 내에서 나이를 검증할 수 있는 프로그램을 실행하여 증명자의 나이가 19세 이상인지 판단함

○ 전통적 방식의 영지식 증명 기술

- 영지식 증명 기술은 2013년에 임의의 관계식에 대해서 효율적으로 증명할 수 있는 기술이 개발된 이후, 2013년 이전 기술과 이후 기술로 크게 나눌 수 있음.
- 2013년 이전 영지식 증명 기술은 개개의 특정 문제에 대해서 효율적으로 영지식 증명을 하는 알고리즘에 대한 연구가 개발됨
- [GMR85]에서 처음 영지식 증명이 소개된 이후 CL(Camenisch-Lysyanskaya) 서명과 BBS+(Boneh-Boyen-Shacham Plus) 서명이 개발됨. 이러한 기법들은 프라이버시를 보장하면서도 신뢰성 있는 인증을 가능케 하여 영지식 증명의 응용 확장에 도움을 줌. 이에 대한 자세한 설명은 2장 1절 2. 영지식 증명 기술의 심화 개념의 CL 서명과 BBS+ 서명에 언급됨

○ 영지식 증명 전환기

- 2013년도 이후에는 일반적인 문제를 해결하는 효율적인 영지식 증명 기술과 이를 활용하는 응용 기술 연구들이 크게 연구됨

※ 특히 2013년 이후의 영지식 증명 기술은 비대화형 영지식 증명인 zk-SNARK(Zero-Knowledge Succinct Non-Interactive Argument of Knowledge)로 통칭하는 기술을 중심으로 발전함[PHGH13]. 증명의 크기가 관계식의 크기와 관계없이 상수로 고정되거나 선형 이하의 크기를 가지고, 검증에 필요한 시간이 비밀 정보의 크기에 대비해 선형 이하의 시간 복잡도를 가져야 함

○ 비대화형 영지식 증명 사례

- 비대화 영지식 증명의 대표적인 예시로는 (1) zk-SNARKs, (2) zk-STARKs, (3) Bulletproofs가 있음

(1) zk-SNARKs[Gro16] : 영지식 증명(zk)의 크기가 작으면서도 빠르게 확인할 수 있는 간결함(Succinct)과 논쟁 없이 증명과 검증(Argument of Knowledge)이 이루어지는 비대화형(Non-interactive) 기법임. 간결성은 증명의 검증이 간단하게, 증명 알고리즘을 통해 생성된 증명의 크기가 물리적으로 작음(로그 크기의 증명 크기 및 검증 시간)을 의미함

- zk-SNARKs는 신뢰 기관을 이용해 증명자와 검증자에게 공개 매개변수를 전달하는 신뢰 기반 설정을 활용함. 이 덕분에 증명자는 검증자에게 증거가 담긴 메시지를 딱 한 번 전송하여 증명할 수 있음

※ 그러나 신뢰 기관(Trusted Party)이라는 제삼자에 대해 증명자와 검증자의 신뢰를 기반으로 동작하고, 특정 기관이 없이 동작하는 탈중앙화라는 블록체인의 가치를 떨어뜨린다는 단점이 있음

(2) zk-STARKs[BBHR18] : 충돌 저항성 해시 함수를 이용한 암호화 방식을 이용하기 때문에 zk-SNARKs의 신뢰 기반 설정이 필요하지 않음. 또한, zk-SNARKs보다 확장성이 더 높은 확장성을 제공하고, 통신 및 검증의 복잡성이 증가하더라도 연산 처리능력에 큰 변화가 없다는 장점이 있음

※ 하지만 증명 크기가 zk-SNARKs에 비하여 크기 때문에 블록체인에 사용하기 어렵다는 한계점이 있음

※ 해시 함수란 임의의 길이의 데이터(입력값)를 고정된 길이의 값(해시값)으로 매핑하는 함수임. 하나의 동일한 해시 결괏값에 매핑되는 둘 이상의 서로 다른 입력값을 찾았을 때 충돌이 발생했다고 표현함. 충돌 저항성 해시 함수(암호학적 해시 함수)는 해시 함수의 일종으로 충돌이 발생할 확률이 무시할 수 있는 정도의 확률 이하여야 함. 일반적으로 사용되는 충돌 저항성 해시 함수는 SHA-256, MiMC, Poseidon 등이 있음

(3) Bulletproofs[BBB+16] : 2017년 스탠포드에서 처음 제안된 Bulletproofs는 zk-SNARKs와 zk-STARKs의 장점들을 이용한 효율적인 알고리즘임. zk-STARKs와 마찬가지로 실행 및 작동을 위한 신뢰 기반 설정(Trusted Setup)이 필요하지 않고, zk-SNARKs처럼 작은 증거 크기를 가짐

※ 네트워크 크기가 커지면 증명 및 검증 시간이 zk-SNARKs와 zk-STARKs에 비해 길어진다는 단점이 있으나 추가 거래비용 없이 대규모 확장이 가능함

○ 영지식 증명 블록체인 활용방안

- 블록체인에서 개인정보를 노출하지 않고 트랜잭션의 유효성을 판단할 수 있게 함. 그러므로 영지식 증명은 퍼블릭 블록체인의 프라이버시 보호를 위한 솔루션으로 적합하다고 볼 수 있음

※ 영지식을 활용한 블록체인의 예시로, ZCash[BCG+14]와 Monero는 블록체인에 영지식 증명을 도입하여 가상자산에 익명성을 제공함

[표 3] ZCash 및 Monero 설명

• (ZCash) zk-SNARK를 활용하여 블록체인 네트워크 내 송수신 자의 정보와 거래 대금을 공개하지 않고 익명 거래가 가능한 서비스임. zk-SNARKs를 이용해 사용자의 주소와 사용자의 코인 양을 숨김. ZCash는 사용자에게 공개주소로 t-address와 z-address를 제공하고, 사용자는 z-address를 선택해 거래 정보를 비밀로 할 수 있음. 모든 사용자에게 거래 정보가 보이지 않으나 zk-SNARKs의 검증 과정을 통해 유효한 거래 내역임을 검증받아 해당 거래 정보가 블록체인에 기록될 수 있음 • (Monero) Bulletproof를 사용해 전송된 코인의 양을 숨김. 2014년 출시 당시에는 Bulletproofs를 도입하지 않았으나 2018년 10월 Bulletproofs를 도입하여 거래내역의 크기를 약 80% 축소함. 이에 따라 거래 수수료도 기존 $0.6에서 $0.02로 감소하였음이 확인됨

※ 블록체인 내에는 크게 ‘코인(Coin)’과 ‘유효식별자(Nullifier)’가 저장됨. 코인은 익명화된 화폐 개념으로, 돈의 금액(예: 1 ETH 등의 화폐 단위), 수신자의 익명 주소 등의 정보를 약정 값의 형태로 유형화한 개념임. 블록체인에 저장된 코인은 오직 해당 코인의 소유자만 사용할 수 있으며, 익명 주소가 코인에 활용되기 때문에 코인을 통해 익명 거래를 지원할 수 있음. 유효식별자는 코인과 쌍을 이루어 블록체인에 저장되며, 코인의 이중 사용(Double Spending) 방지라는 중요한 역할을 수행함

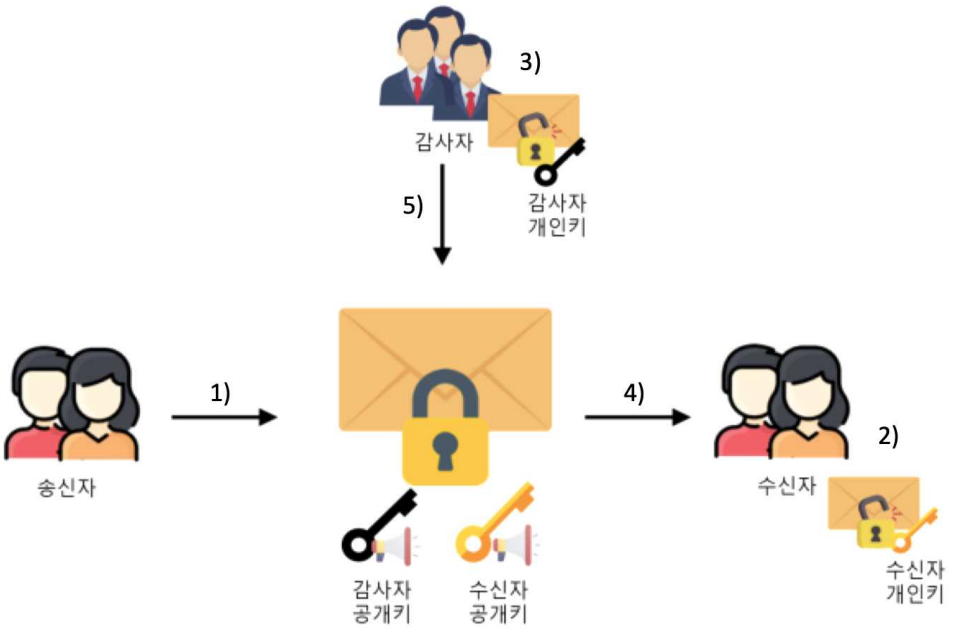
[표 4] 이중 사용 설명

이중 사용이란 이미 사용된 코인을 재사용하는 것을 뜻함. 중앙화된 시스템의 경우 들어온 거래에 대해 순차적으로 유효성 검증과 거래 처리를 진행하여 이중 사용을 방지하지만, ZCash와 같은 익명 거래 프로토콜은 블록체인 검증자가 들어온 거래에 대해 유효성을 검증할 방법과 사용된 코인임을 확인할 방법이 없음. 따라서, 유효성은 영지식 증명을 통해 검증하고 사용된 코인임을 기록하기 위해 유효식별자를 사용함

※ 트랜잭션에는 모든 익명 거래 과정이 올바르게 진행되었다는 사실에 대한 영지식 증명이 포함되어 누구나 익명 트랜잭션에 대한 유효성 검증이 가능함

- 열거한 프라이버시 보호 방안들은 익명성을 위주로 기술이 발전해옴. 프라이버시 솔루션들은 코인 및 토큰의 익명 전송에 초점을 맞춰 프라이버시는 강력하게 보호되지만, 거래에 있어서 중요한 규제인 자금 세탁 금지(Anti-Money Laundering, AML)를 만족하고 있지 않기 때문에 한국, 미국 등 주요 나라에서는 해당 서비스를 불법으로 규정하고 접근을 차단하고 있음

※ 이러한 단점을 보완하고자 트랜잭션의 프라이버시를 보호하되 특정 감사자가 감사할 수 있는 감사 기능을 추가할 수 있음. 이를 이용하여 자금 세탁을 감사하거나 특정 트랜잭션의 악의적인 목적을 확인할 수 있음



[그림 4] 트랜잭션 프라이버시를 위한 감사 가능 영지식 증명 도입

1) 송신자가 트랜잭션을 생성할 때, 송신자는 수신자와 감사자의 공개키를 모두 입력받아 암호문을 생성함
2) 수신자가 이 트랜잭션을 복호화할 때 자신의 개인 키를 이용하여 해당 트랜잭션에 대한 평문을 획득할 수 있음. 복호화된 평문에서는 암호화된 내역을 확인할 수 있음
3) 감사자가 이 트랜잭션을 복호화할 때 자신의 개인 키를 이용하여 해당 트랜잭션에 대한 평문을 획득할 수 있음
4) 복호화된 평문에서는 암호화된 내역을 확인할 수 있음
5) 감사자는 수신자와는 다르게 모든 트랜잭션을 감사자의 개인 키로 복호화가 가능하여 자금 세탁이나 악의적인 전송 등을 감사할 수 있음

2. 영지식 증명 기술의 심화 개념

영지식 증명 기술의 심화 개념은 영지식 증명에서 실질적으로 증명하고자 하는 것은 무엇인지, 그리고 증명하고자 하는 것을 어떤 식으로 일반화할 수 있는지에 대해 설명함. 또한, 현재 널리 사용되는 증명 방식인 다항식 기반 상호 오라클 증명 및 선형 확률적 검증 가능 증명과 이를 뒷받침하는 암호학적 기법들을 깊이 있게 이해할 수 있도록 설명함

○ 익명 크리덴셜 기법을 위한 영지식 증명 기법

1) CL 서명[CL04]

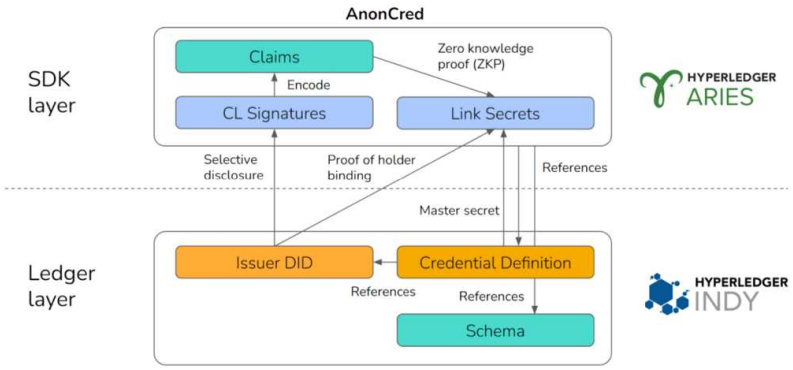
- CL 서명은 Jan Camenisch와 Anna Lysyanskaya가 2001년에 발표한 전자서명 기법으로, 익명 크리덴셜(Anonymous Credential) 기법의 구성요소로 사용되면서 대중화됨
- CL 서명은 사용자의 정보 $m_1,\cdots,m_L$를 하나의 값으로 서명을 생성해둔 뒤, 그 중 공개하고자 하는 일부 정보와 그 외의 정보에 대한 추가적인 계산값을 제공하여 서명이 유효한지 검증하는 방식임
- CL 서명은 하나의 큰 값을 두 개의 소수로 인수분해하는 것이 현실적으로 불가능함을 뜻하는 RSA 가정을 기반으로 하고 있음
- 동작 원리는 다음과 같음

[표 5] CL 서명 알고리즘

• **(키 생성)** 두 소수(prime number) p,q 를 생성한 뒤 $n=pq$ 을 계산해주고, 랜덤값 $a_1, a_2, \cdots, a_L, b, c$를 생성해줌
• **(서명 생성)** 랜덤값 e를 생성해주고, 서명하고자 하는 메시지 $m_1,\cdots,m_L$를 이용해 v를 다음과 같이 계산해줌 $$v^e = a_1^{m_1}\cdots a_L^{m_L} b^s c \bmod n$$ 메시지 $m_1,\cdots,m_L$에 대한 서명은 (e,s,v)로 구성됨
• **(서명 검증)** 주어진 서명 (e,s,v)과 메시지 $m_1,\cdots,m_L$를 이용해 아래 식의 양변이 같은 값을 갖는지 확인함 $$v^e \equiv a_1^{m_1}\cdots a_L^{m_L} b^s c \bmod n$$

- 서명 검증 단계에서 메시지 $m_1,\cdots,m_L$를 모두 공개할 필요 없이, 공개

하지 않고자 하는 메시지는 $a_i^{m_i}$의 형태로 검증자에게 전달하여 선택적 공개 기능을 지원함. 예를 들어, 메시지 m_1, m_2, m_3가 있을 때, m_1과 m_3는 공개하고 싶지만 m_2는 공개하고 싶지 않을 때, $a_2^{m_2}$를 계산해서 전달하여 검증자는 m_2를 알지 못해도 서명을 검증할 수 있음



[그림 5] CL 서명 적용사례

2) BBS+ 서명[BBS04]

- BBS+ 서명은 Dan Boneh, Xavier Boyen, Hovav Shacham이 개발한 전자서명 기법으로, CL 서명과 같이 선택적 공개를 지원하여 익명 크리덴셜 기법에 사용됨. BBS+ 서명을 활용한 익명 크리덴셜 기법으로는 AnonCred 2.0이 있음
- CL 서명의 RSA 가정은 충분한 안전성을 갖기 위해서 키와 서명의 길이가 길어야 하고, 이는 암호학적 연산을 위한 계산 시간이 필요하므로 성능적인 측면에서 단점이 있음
- 이에 반해 BBS+ 서명은 SDH(Strong Diffie-Hellman) 가정과 페어링 기반 암호학을 활용하기 때문에, 더 짧은 길이의 키와 서명으로도 CL 서명과 비슷한 정도의 안전성을 얻을 수 있음. 동작 원리는 다음과 같음

[표 6] BBS+ 서명 알고리즘

• **(키 생성)** 군 G_1으로부터 랜덤값 $h_0,\cdots,h_L$를 생성하고, 비밀키로 사용할 랜덤값 x를 생성함. 그리고 $w \leftarrow g_2^x$ 를 계산해줌. 공개키는 $(w, h_0, \cdots, h_L)$로 구성됨.
• **(서명 생성)** 랜덤값 e,s를 생성해주고, 다음과 같이 A를 계산해줌. $$A \leftarrow (g_1 h_0^s h_1^{m_1} h_2^{m_2} \cdots h_L^{m_L})^{\frac{1}{e+x}} = (g_1 h_0^s \prod_{i=1}^{L} h_i^{m_i})^{\frac{1}{e+x}}$$ 메시지 $m_1,\cdots,m_L$에 대한 서명은 (A,e,s)로 구성됨.
• **(서명 검증)** 주어진 서명 (A,e,s)과 메시지 $m_1,\cdots,m_L$, 공개키 $(w, h_0, \cdots, h_L)$를 이용해 아래 식의 양변이 같은 값을 갖는지 확인함. $$e(A, wg_2^e) = e(g_1 h_0^s \prod_{i=1}^{L} h_i^{m_i}, g_2)$$

- BBS+ 서명 또한 CL 서명과 유사하게 선택적 공개를 지원함. 특정 메시지를 공개하지 않고 서명에 대한 검증을 받고 싶은 경우, 공개하지 않을 메시지에 대해 $h_i^{m_i}$를 계산하여 검증자에게 전달하면 이를 이용하여 검증할 수 있음

○ 영지식 증명 산술 회로식

- 영지식 증명 과정은 크게 증명하고자 하는 관계식을 산술 회로식으로 변환하는 프론트엔드와 산술 회로식에 대해 증명을 생성하는 백엔드로 나눌 수 있음. 이때, 산술 회로식은 덧셈과 곱셈으로만 이루어진 식을 의미함
  ※ 프론트엔드 과정은 하드웨어 설계에서 HDL(Hardware Description Language)로 기술된 코드를 하드웨어 합성기를 통해서 논리 게이트로 변환하는 것과 비슷하게, 고급 프로그래밍 언어로 주어진 임의의 관계식을 덧셈, 곱셈 게이트로 만들어지는 산술 회로식으로 만드는 것을 의미함
  ※ 백엔드는 크게 증명자와 검증자가 공유하는 키를 생성하는 키 생성 과정과 진술과 비밀 정보를 이용해 실제로 증명을 생성하는 증명 생성 과정으로 구분할 수 있음

○ 영지식 증명 공유키

- 증명자와 검증자가 공유하는 키를 CRS(Common Reference String)이라고 부르며, CRS는 크게 SRS(Structured Reference String)과 RRS(Random Reference String)으로 구분할 수 있음

※ SRS는 구조적인 성질을 가지고 있는 키이며, 대수적인 성질을 갖는 키임. RRS는 랜덤한 값을 기준으로 만드는 키이며, 보통 해시 함수의 출력을 사용함.

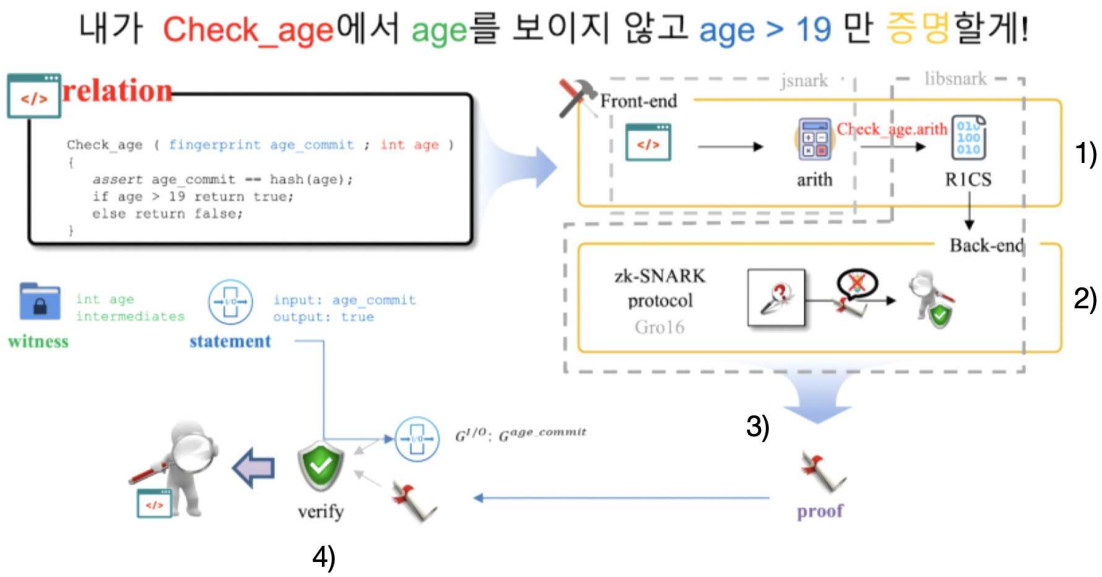
※ RRS는 반대로 신뢰 기관이 필요하지 않다는 장점이 있지만, 증명 크기와 검증 시간이 SRS에 비해 크다는 단점이 존재함

※ SRS를 사용하는 영지식 증명 기법은 증명의 크기와 검증 시간이 매우 효율적이라는 장점을 갖고 있지만, SRS를 생성하는 과정에서 신뢰 기관이 필요로 한다는 단점이 존재함

○ 영지식 증명 증명법

- 백엔드 과정은 크게 회로 특화 영지식 증명법(Circuit specific ZKP)과 유니버설 영지식 증명법(Universal ZKP)으로 구분 가능할 수 있음
  - 회로 특화 영지식 증명법은 산술 회로를 주면 주어진 회로에 맞는 키(SRS)를 생성함
  - 유니버설 영지식 증명법은 회로와 관계없이 키(SRS 또는 RRS)를 미리 생성함

※ 회로 특화 영지식 증명법이 증명 크기와 검증 시간에서 이점이 있지만, 회로에 따라 키 생성을 새로 해야 한다는 단점이 있음



[그림 6] 영지식 증명 과정

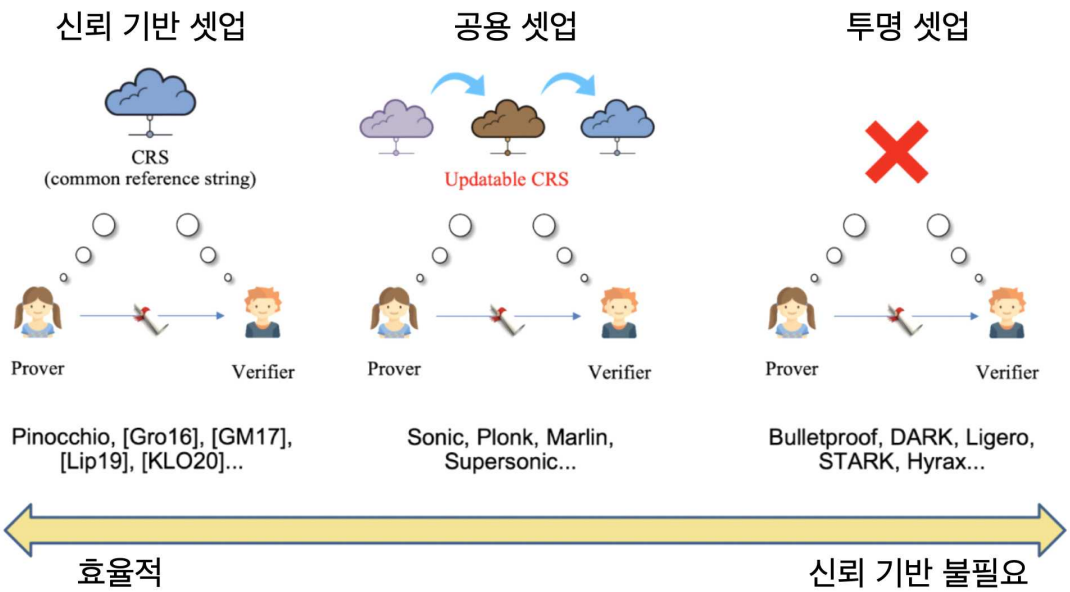
- [그림 6]에서 보듯이, 먼저 증명자와 검증자는 모두 관계식에 해당하는 함수 코드를 알고 있음

1) 함수 코드에 대해서 먼저 증명자와 검증자를 위한 공개 파라미터값 (CRS : common reference string)을 생성함 (setup)

2) 이후 증명자는 비밀 입력에 해당하는 나이 (age)와 입력에 해당하는 나이의 해시값 (age_commit)을 모두 아는 상태로 함수 코드를 실행하여, 코드 내에서 만들어지는 모든 변숫값을 계산함

3) 주어진 관계식에 대해서 프론트엔드는 산술 회로라는 중간 코드를 만들고, 이 산술 회로와 변숫값들을 모아서 백엔드에서 증명 값(proof)을 생성하게 되며 이 과정을 증명 (prove)이라고 함

4) 생성된 증명 값은 입력값과 함께 검증자에게 전달되게 되고, 검증자는 증명 값과 입력값이 맞는지 공개 파라미터를 활용하여 검증하게 되며 이를 검증 (verify)이라고 함



[그림 7] 영지식 증명 셋업

○ 파라미터 설정

- 공개 파라미터를 생성하는 설정하는 과정을 크게 세 가지로 분류할 수 있는데, 신뢰 기반 설정 (Trusted setup), 보편적 설정 (Universal setup), 투명 셋업 (Transparent setup)이 있음

  ※ 신뢰 기반 설정과 보편적 설정의 경우, 공개 파라미터를 생성하는데 사용되는 비밀 값들이 셋업 이후에는 폐기되어야 함. 왜냐하면, 폐기되지 않은 비밀 값들을 이용하여 가짜 증명을 생성하는 것이 가능하기 때문임. 따라서, 다중 기관 계산 (Multi-Party Computation, MPC)을 통해서 설정이 이루어지며 다중 기관 계산에 참여한 기관 중 하나라도 비밀 값을 안전

하게 폐기하게 되면 공개 파라미터는 안전하게 생성된 것임

※ 신뢰 기반 설정의 경우에는 관계식을 나타내는 함수 코드마다 설정 시에 비밀 값이 필요하지만, 공용 셋업의 경우에는 처음 한 번만 비밀 값으로 파라미터를 만들고, 이 파라미터를 활용해서 함수 코드마다 비밀 값없이 공개 파라미터를 만들 수 있으므로 훨씬 더 편리함

○ 상호적 증명

- 증명자가 검증자에게 어떤 주장(관계식을 만족함)이 사실임을 증명하기 위한 대화 과정을 의미함
  - 상호적 증명은 완전성(Completeness)과 건전성(Soundenss)을 만족해야 함

  ※ 완전성 : 증명자의 주장이 참이라면 검증자는 항상 주장을 받아들임

  ※ 건전성 : 만약 증명자가 거짓 주장을 하려고 한다면 검증자는 이를 거의 항상 거부함
- 상호적 증명은 검증자가 랜덤한 값을 보내고 해당 값에 대해 알맞은 답을 증명자가 보내는 과정으로 이루어짐. 이 과정을 여러 번 성공하게 되면 증명자는 검증자가 확실히 답을 안다고 믿을 수 있음

  ※ 실제 응용에서는 증명자와 검증자가 여러 번 상호작용 하기 힘들어서 검증자가 랜덤한 값을 매번 보내는 대신 증명자가 해시 함수의 결괏값을 랜덤값으로 치환하여 함께 전송하여 상호작용을 없앨 수 있음. 이런 방식을 피앗-샤미르(FS) 휴리스틱이라고 하며, 많은 상호적 증명 방식이 이를 이용하여 비상호적 증명 방식을 구현함

○ 산술 회로식 변환[1)]

- 산술 회로식은 셋업 과정을 통해 다항식으로 변환하고, 증명자는 다항식에 대한 증명을 생성함. 산술 회로식을 다항식으로 변환하는 방식으로 대표적인 방식은 QAP(Quadratic Arithmetic Program)가 있음

- QAP는 다음과 같은 과정을 거침

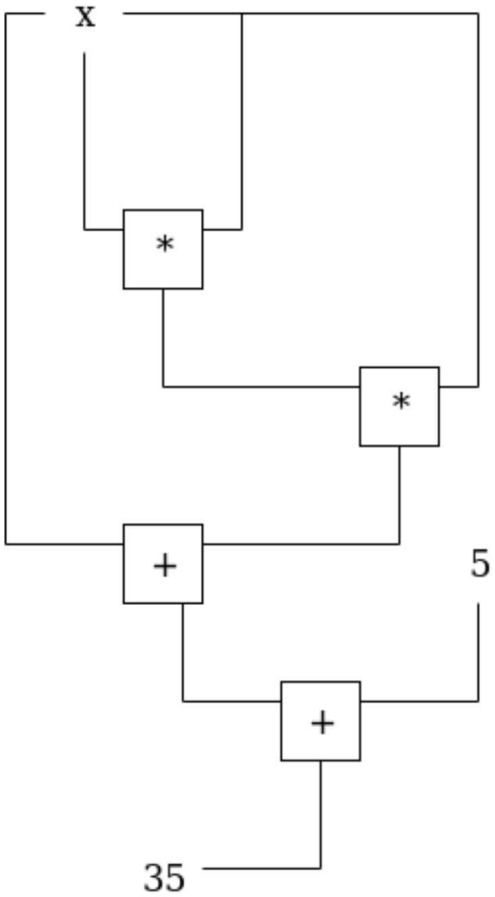
  1) 산술 회로식을 평탄화함. 평탄화란 함수를 하나의 곱셈으로 표현할 수 있는 여러 식으로 나누어주는 과정임. 예를 들어, $x^3+x+5 \equiv 35$라는 식을 증명하려 할 때, 아래와 같이 각 식을 하나의 곱셈을 갖도록 변환함

---

1) https://medium.com/@VitalikButerin/quadratic-arithmetic-programs-from-zero-to-hero-f6d558cea649

$$sym_1 = x \times x$$
$$y = sym_1 \times x$$
$$sym_2 = y + x$$
$$out = sym_2 + 5$$

해당 식에서 입/출력 x, out은 각각 3, 35이고, 중간 계산 값(비밀 정보) sym_1, y, sym_2는 각각 9, 27, 30으로, 해답 벡터 $s = (1, x, out, sym_1, y, sym_2)$ = (1, 3, 35, 9, 27, 30)이 됨



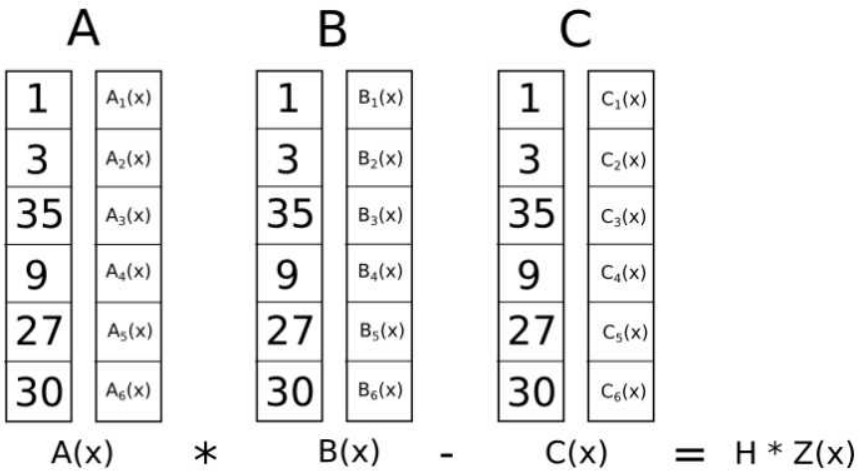
[그림 8] $x^3 + x + 5 \equiv 35$의 산술 회로식 변환 예시

2) 평탄화한 식을 R1CS(Rank-1 Constraint System)으로 변환함. R1CS는 평탄화한 각 식을 3개의 벡터 (a,b,c)로 바꾸어 주는 과정을 뜻함. 위의 예시 중 $out = sym_2 + 5$는 $out = (sym_2 + 5) \times 1$로 생각할 수 있고, 벡터 (a,b,c)를 다음과 같이 설정했을 때, $s \cdot a + s \cdot b - s \cdot c = 0$을 계산 시

기존의 $out = (sym_2 + 5) \times 1$ 식을 얻을 수 있음. 이처럼, 평탄화한 모든 식에 대해 벡터 (a,b,c)를 변환함

$$a = \begin{pmatrix} 0 & 0 & 0 & 5 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad c = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

3) 벡터 (a,b,c)의 각 열에 대해 라그랑주 보간법(Lagrange interpolation)을 통해 다항식으로 변환함. 최종적으로 아래의 [그림 9]와 같이 변환됨



[그림 9] QAP 변환식 예시

- 증명자가 증명하고자 하는 문장은 QAP로 변환하여 다항식 A,B,C가 됨

○ 다항식 약정

- 변환된 다항식은 증명자와 검증자가 공유하고 있지만, 다항식에 검증자가 직접 값을 대입하여 계산하기에 다항식의 크기가 너무 큼. 다항식 약정 기법은 다항식을 약정하고 추후 특정 입력에 대해 전체 다항식을 공개하지 않고 계산 결괏값을 공개할 수 있는 프로토콜로, 다항식을 간결하게 표현하는 방법임
- 영지식 증명의 종류 중 일부는 증명하고자 하는 관계식을 다항식으로 표현함. 이때 다항식의 크기가 큰 경우, 증명자가 다항식 전체를 검증자에게 전송하는 것과 검증자가 다항식 전체를 저장하고 있는 것이 비효율적이기 때문에 다항

식 약정을 통해 다항식을 간결하게 검증자에게 보내준 뒤, 검증자의 요청에 따라 다항식의 계산 값을 제공함

- 다항식 약정은 다음과 같은 속성을 만족함
  ※ Hiding: 주어진 약정은 특정 시점에서 공개되기 전에 약정 값 자체만으로 다항식에 대한 정보를 노출하지 않음
  ※ Evaluation Binding: 다항식 약정 후에, 누구도 거짓으로 어떤 입력에 대한 다른 계산 값을 공개할 수 없음. 즉, 같은 입력에 대해 다른 계산 결괏값을 도출할 수 없음
- 다항식 약정은 페어링(Pairing) 연산 기반의 KZG[KZG10], 이산 로그(Discrete log) 기반의 Bulletproofs[BBB+16], 그룹의 크기를 모르는 그룹 (unknown order group) 기반의 DARK[BFS19], 상호 오라클 증명(IOP) 기반의 FRI[BBHR18], 부호화 가능 오류정정 코드(Encodable Error Correcting Code) 기반의 Orion[XZS22] 등 여러 가지 기반 기술로 구현할 수 있음

○ Orion[XZS22] 다항식 약정

- Orion은 IOP 기반의 다항식 약정법으로 증명 생성 시간이 $O(N)$(선형 시간)인 Brakedown[GLS+]의 다항식 약정을 기반으로 설계됨
- Brakedown은 증명 생성 시간이 $O(N)$으로 빠르지만, 증명 크기가 크다는 한계를 지님($N=2^{21}$일 때 약 10MB를 상회함)
- Orion은 증명 생성 시간을 $O(N)$을 유지하면서 증명 크기를 $O(\log^2 N)$을 달성 ($N=2^{27}$ 기준 Brakedown 대비 증명 크기 약 16배가량 감소)
- Orion 다항식 약정은 다음과 같이 동작함[2)]
  1) 다항식의 계수를 k x k 크기의 행렬 크기로 표현함
  2) 이 행렬을 행과 열별로 한 번씩 Spielman 오류 수정 코드(ECC, Error Correction Code)를 통해 인코딩(행을 인코딩한 행렬을 C_1, 열을 인코딩한 행렬을 C_2라 함)
  3) 최종적으로 생긴 행렬을 열별로 머클 트리 약정 수행 ($rt_i = Merkle.Commit(C_2[:,i])$)하고, 각 커밋 별로 생성된 커밋 값인 루트 값을 다시 한번 머클 트리 약정($R = Merkle.Commit(rt_0,\cdots,rt_{n-1})$)을 수행
  4) 최종 머클 트리 루트 값 R을 약정 값으로 사용
  5) 검증자는 다항식 계수 행렬과 같은 길이(k)의 랜덤 벡터 γ를 뽑아 증명자

2) 실제 Orion 다항식 약정 방법은 유사성 테스트(Proximity test)와 일관성 테스트(Consistency test)를 증명/검증해야 하므로 실제로는 더 복잡하지만, 이해의 편의를 위해 다항식 약정 방법을 설명하는 것에 초점을 맞추어 간소화하게 명세함. Code switching 역시 수학적으로 복잡한 배경이 있어 개념적으로만 설명함. 정확한 프로토콜은 논문(Orion: Zero Knowledge Proof with Linear Prover Time) 참조.

에게 전달

6) 증명자는 랜덤 벡터 γ 인코딩 행렬, 다항식 계수 행렬과 각각 일차 결합(linear combination)을 계산하여 검증자에게 전달
7) 검증자는 랜덤 인덱스를 고르고, 증명자는 검증자가 보내준 랜덤 인덱스에 대한 머클 트리 증명을 검증자에게 전달. 이때 머클 트리 증명은 3)의 최종 머클 트리가 아닌 행렬의 열별 머클 트리(rt)에 대한 증명임
8) 검증자는 검증에 내적(Inner product) 연산과 인코딩을 통해 6)에서 전달받은 일차 결합 값이 맞는지를 확인하고, 머클 트리 검증을 하여 다항식 약정에 대한 검증을 수행함
9) Orion은 code switching이라는 효율적인 증명 압축 기법을 통해 증명 크기를 최소화함
10) Code switching은 간단히 말해 검증 식을 영지식 증명 회로 내에서 수행하여 증명 크기를 압축하는 방법임
11) Orion 다항식 약정은 code switching을 통해 검증을 위한 내적 계산과 인코딩을 영지식 증명 회로 내에서 수행하게 설계
    - 하지만 여전히 Orion 역시 증명 크기가 MB 단위로 실용적으로 사용하기에 다소 크다는 한계를 가짐

[표 7] 다항식 약정 알고리즘 비교 분석표

Scheme	신뢰 주체 필요성	증명 시간	검증 시간	증명 크기
KGZ10	Yes	$O(n)-\mathrm{EXP}$	$O(1)-Pairing$	$O(1)$
Bulletproofs	No	$O(n)-\mathrm{EXP}$	$O(n)-\mathrm{EXP}$	$2\log n\, G_p$
DARK	No	$O(nlog(n))-\mathrm{EXP}$	$O(\log(n))-\mathrm{EXP}$	$O(\log(n)\, G_U)$

○ 다항식 기반 상호 오라클 증명(Polynomial Interactive Oracle Proof, PIOP)

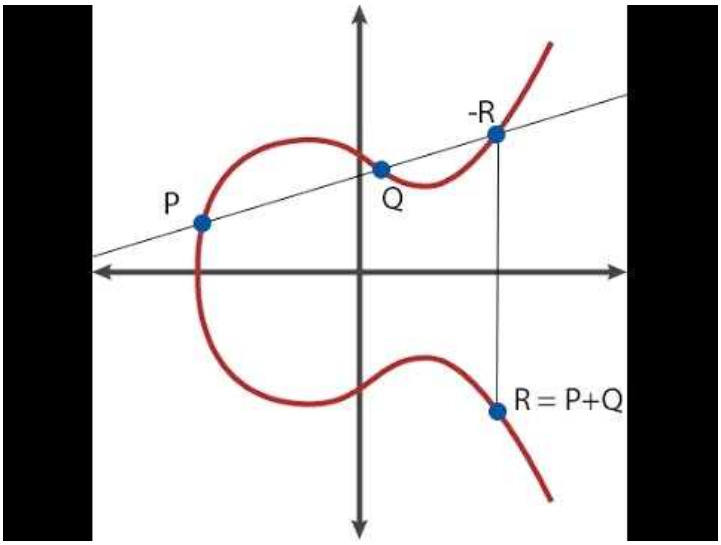
- 상호 오라클 증명(Interactive Oracle Proof, IOP)은 상호적 증명의 종류로, 증명자가 검증자에게 증명을 전송하고 검증자는 증명 일부에 접근하여 검증하는 방식임. 이때, 증명자가 검증자에게 전송하는 증명을 오라클(Oracle)이라고 하고, 검증자가 증명 일부에 접근하는 것을 오라클 쿼리(Oracle query)라고 함

- 다항식 기반 상호 오라클 증명은 오라클을 다항식의 형태로 전송하고, 검증자가 다항식의 계산 값을 쿼리하는 프로토콜임. 영지식 증명의 관계식을 다항식으로 변환했을 때, 다항식이 검증자가 계산하기에 너무 크기 때문에 증명자에게 계산을 위임하는 방식임
- 실제로는 증명자가 검증자에게 다항식을 전송하는 것도 오버헤드로 작용하기 때문에, 다항식 약정을 통해 다항식을 간결하게 검증자에게 전송하는 것으로 다항식 전체를 전송하는 것을 대체함
- PIOP는 Sonic[MBKM19], Plonk[GWC19], Marlin[CHMMVW20] 등이 있으며, 그중 Plonk는 다양한 블록체인 애플리케이션에서 증명 시스템으로 채택이 됨

○ 선형 확률적 검증 가능 증명(Linear Probabilistic Checkable Proof, Linear PCP)
- Linear PCP는 복잡한 문제의 해를 검증하기 위한 수학적 도구로, 검증을 위한 복잡도를 낮추고 정확성을 높여 효율적인 검증 방식임
  - Linear PCP는 PIOP과 유사하게 증명자가 검증자에게 증명 문자열을 전송하고, 검증자는 해당 문자열을 모두 읽는 것이 아닌 특정 위치에 대하여 쿼리를 시도함
  - 해당 쿼리를 통해 증명 문자열을 모두 확인하지 않고 충분히 높은 확률로 정답이 맞다는 것을 확인할 수 있는 방식임
  - PIOP와 달리 Linear PCP는 하나의 라운드로만 이루어져 있다는 차이점이 있음
- Linear PCP의 대표 스킴으로는 Gro16으로 널리 알려진 Jens Groth가 저술한 “On the Size of Pairing-based Non-interactive Arguments” 논문이 존재함
  - 해당 논문은 현대 SNARK 시스템의 근간으로, 다양한 연구가 해당 논문의 프로토콜을 기반으로 발전됨

○ 페어링 기반 암호학(Pairing-based Cryptography)

- 페어링 함수란 쌍 선형사상(Bilinear map)으로 2개의 군(G_1, G_2)의 원소를 입력으로 연산하여 또 다른 군(G_T)의 원소를 출력하는 함수임. 주로, 페어링 함수 $e : G_1 \times G_2 \rightarrow G_T$로 정의함. 페어링 함수는 [그림 10]과 같이 작동함[3)]



[그림 10] 페어링 함수의 계산 방식

- 페어링 함수는 쌍선형성이라는 특징을 갖고 있어, $e(g^a, g^b) = e(g,g)^{ab}$를 만족함. 이러한 특징은 a,b를 알지 못하는 사용자에게 g^a, g^b 만을 사용해 a,b의 관계성을 파악하는 데 도움을 줄 수 있음

○ FRI(Fast Reed-solomon Interactive Oracle Proofs of Proximity)[BBHR17]

- FRI는 리드-솔로몬 코드(Reed-Solomon code, RS code)라고 하는 오류정정 코드를 활용한 프로토콜임
- 오류정정 코드란 어떤 문자열에 대해 해당 문자열이 변형/조작되었음을 감지하고 복구할 수 있는 기법임. 리드-솔로몬 코드는 오류정정 코드의 종류 중 하나로, d 길이의 문자열이 주어졌을 때 $3d$ 길이만큼의 추가적인 코드가 붙음. FRI에서는 d 길이의 문자열 중 하나의 비트라도 변형/조작되었을 경우 추가적인 $3d$ 길이의 코드가 크게 변한다는 리드-솔로몬 코드의 특징을 활용함
- FRI는 상호적 증명의 한 종류로, 상호작용을 통해 다항식의 길이(최고 차수)를 절반으로 줄여나가는 방식을 사용함

3) https://medium.com/@VitalikButerin/exploring-elliptic-curve-pairings-c73c1864e627

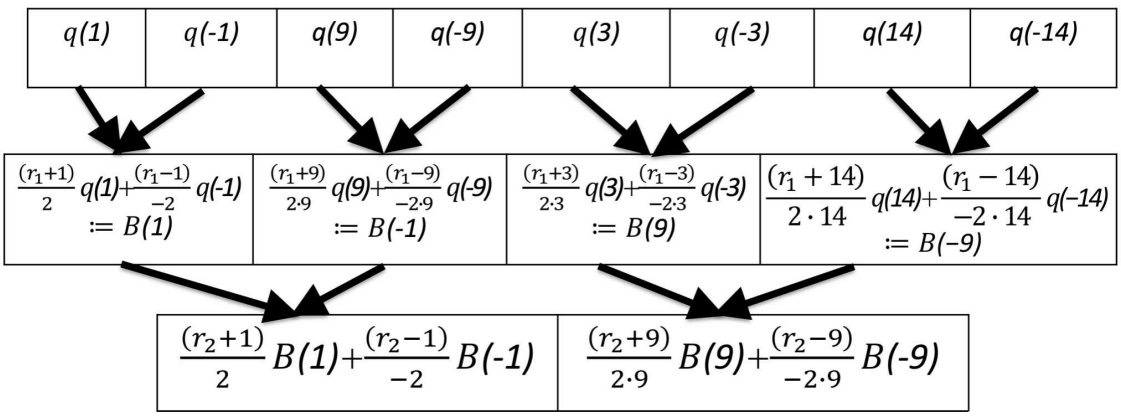
- 예를 들어, 어떤 다항식 $f^1(x) = 5+3x+2x^2+7x^3$ 에 대해 아래와 같이 차수가 짝수인 항과 홀수인 항을 각각 모은 다항식 2개를 만들 수 있고, 기존의 $f^1(x)$ 또한, 두 다항식을 이용해 정리할 수 있음

$$f_e^1(x) = 5+2x^2$$
$$f_o^1(x) = 3+7x^2$$
$$f^1(x) = f_e^1(x^2) + xf_o^1(x^2)$$

새로 정리한 다항식의 x^2를 y로 치환해준 뒤, 두 다항식을 랜덤한 값 α_1을 이용해 아래와 같이 새로운 다항식을 만들어주면, 새로운 다항식은 기존의 $f^1(x)$ 보다 절반의 최고 차수를 갖게 됨

$$f^2(y) = f_e^1(y) + \alpha f_o^1(y)$$

새로운 다항식 $f^2(y)$ 에 대해 검증자는 랜덤한 값 r을 생성한 뒤 $f^2(r)$ 에 대한 계산을 증명자에게 요청하고, 리드-솔로몬 코드의 특성상 제대로 생성된 다항식이 아니라면 정상적인 결괏값이 아닌 값을 검증자에게 반환하기 때문에 제대로 생성된 다항식에 대해서만 검증을 통과할 수 있게 됨. 이러한 과정을 최고 차수가 1이 될 때까지 반복하는 프로토콜을 FRI라고 함



[그림 11] FRI 프로토콜 예시

○ PLONK[GWC19]

- PLONK는 “Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge” 논문에서 제시한 프로토콜로, 다항식 기반 상호 오라클 증명 중 가장 널리 사용되고 있음
- PLONK는 증명하고자 하는 문장을 산술 회로식으로 변환한 뒤, 이를 라그랑주 보간법(Lagrange interpolation)을 통해 하나의 다항식으로 변환해줌. 해당 다항식을 $T(x)$라고 표기함. l 번째 게이트에 대하여 $T(w^{3l})$은 게이트의 왼쪽 입력, $T(w^{3l+1})$은 게이트의 오른쪽 입력, $T(w^{3l+2})$는 게이트의 출력으로 계산됨
- 게이트가 덧셈, 곱셈 중 어떤 연산인지 구분해 주기 위해 추가적인 다항식 $S(x)$를 만듦. $S(w^{3l})$는 덧셈일 경우 1, 곱셈일 경우 0을 출력하는 다항식이며, PLONK에서는 덧셈과 곱셈 이외의 연산을 추가로 정의할 수 있기에 추가로 정의된 연산에 대하여 $S(w^{3l})$가 미리 정의된 연산과 겹치지 않는 값을 출력하게 설정함
- 위와 같이 생성된 다항식은 다음과 같은 관계식을 만족하는지 증명하는 과정을 거침

$$S(w^{3l})*(T(w^{3l})+T(w^{3l+1}))+(1-S(w^{3l}))*T(w^{3l})*T(w^{3l+1})=T(w^{3l+2})$$

  해당 식은 $S(w^{3l})$가 1인 경우 덧셈에 해당하는 부분만 남고, 0인 경우 곱셈에 해당하는 부분만 남게 되어 모든 게이트에 대해 검증을 해볼 수 있음
- 하나의 게이트에서 출력된 값은 다른 게이트의 입력으로 사용되며 최종적인 출력이 나오는데, 이러한 연결성을 확인하는 과정이 포함됨
- 필요한 성능 지표에 따라 다항식 약정 기법을 선택하여 PLONK와 결합하여 사용할 수 있음. 예를 들어, 속도가 중요하다면 KZG10 다항식 약정을 선택하고, 신뢰 셋업을 피하고 싶다면 FRI를 선택하는 방식을 사용함

[그림 12] zk-SNARK 변환 과정

○ zk-SNARK(zero-knowledge Succinct Non-interactive ARguments of Knowledge)

- 간결성(Succinctness)과 비대화형(Non-interactive) 속성을 갖는 영지식 증명의 일종임. 증명의 크기가 산술 회로의 크기와 관계없이 상수로 고정되거나 선형 이하의 크기를 가진다면 검증자는 증명 시간과 비교하여 매우 빠르게 검증을 할 수 있다는 이점을 가짐. 즉, 증명 검증에 필요한 시간이 실제 수행보다 더 빠르기 때문에 검증자의 계산량이 적어짐
- zk-SNARK는 구성 방식에 따라 몇 가지 종류로 분류될 수 있음. 크게, 다항식 기반 상호 오라클 증명과 다항식 약정을 결합한 방식(Plonk)과 선형 확률적 검증 가능 증명과 페어링 기반 암호학을 결합한 방식(Gro16)이 있음
- zk-SNARK는 검증하고자 하는 함수에 대해서 산술 회로식으로 표현한 뒤, 이를 R1CS의 형태로 변환해주고 라그랑주 보간법을 통해 QAP로 바꾸어 줌. 증명자는 이를 통해 나오는 다항식에 대해 증명함
- 일반적으로 영지식 증명은 완전성(Completeness), 건전성(Soundenss), 영지식성(Zero-Knowledge)의 특성을 갖는데, zk-SNARK는 여기서 간결성(Succinctness)을 추가로 만족해야 함
  ※ 간결성: 증명의 크기가 간결하고, 검증 시간은 비밀 정보의 크기보다 현저하게 작음[4)]

○ zk-STARK(zero-knowledge Scalable Transparent ARgument of Knowledge)

- 확장성(Scalable)과 투명성(Transparent)을 제외하고 zk-SNARK와 흡사함

※ zk-STARK는 관계식의 크기에 따라 상승하는 연산 처리능력 필요치가 zk-SNARK에 비해 적어 확장성에 도움이 됨. 처음 zk-STARK를 제시한 “Scalable, transparent, and post-quantum secure computational integrity” 논문에서 zk-SNARK보다 증명 생성 시간이 약 10배 빠르다고 제시함. 하지만, zk-SNARK보다 증명의 크기가 크다는 단점이 있음

※ zk-SNARK의 초기 설정에서는 이산로그, RSA와 같은 가정에서 신뢰할 수 있는 기관이 필요하지만, zk-STARK는 충돌 저항성 해시 함수를 기반으로 하므로 초기 신뢰 설정이 필요치 않은 투명 셋업으로 zk-SNARK에 비해 큰 투명성을 가짐

※ 이산 로그 기반을 갖는 zk-SNARK는 양자컴퓨팅에 취약하지만, zk-STARK는 해시 함수를 기반으로 하기 때문에 양자컴퓨팅으로부터도 안전함

※ zk-STARK의 예시로 FRI(Fast Reed-solomon Interactive Oracle Proofs of Proximity)를 활용한 기법이 있음

※ 관련 기법으로는 Ligero[AHIV17], Aurora[BCR+19], Fractal[COS20] 등이 존재함

[표 8] 여러 가지 영지식 증명 알고리즘 세부 내용

	zk-SNARKs	zk-STARKs	Bulletproofs
증명자 알고리즘 복잡도	O(N*log(N))	O(N*poly-log(N))	O(N*log(N))
검증자 알고리즘 복잡도	~O(1)	O(poly-log(N))	O(N)
증거 크기	~O(1)	O(poly-log(N))	O(log(N))
신뢰 기반 설정 여부	O	X	X
Post-quantum secure	X	O	X

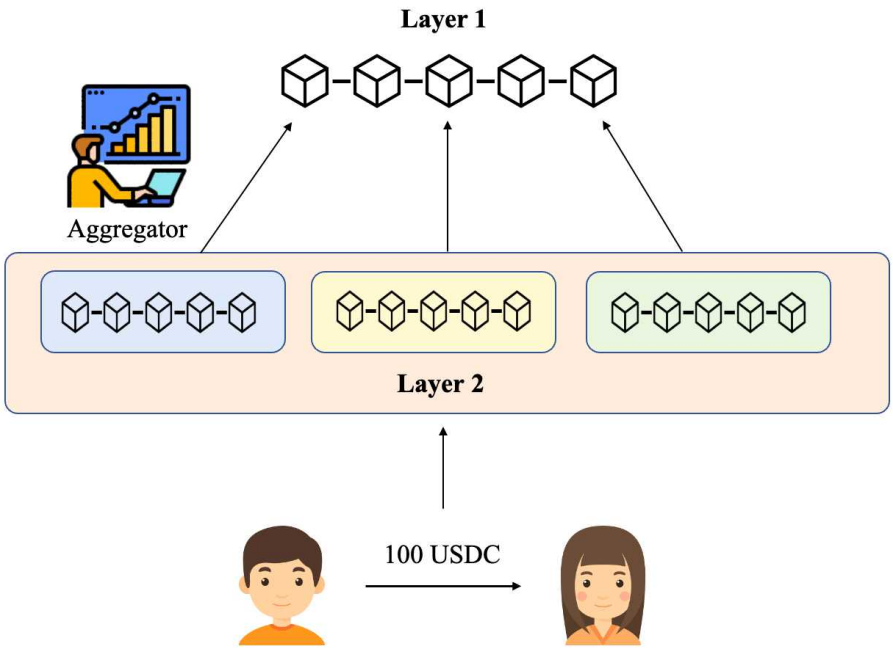
4) 증명의 크기가 λ에 다항식 크기인 poly(λ)를 가지며, 검증은 poly(λ)poly(λ,log|w|) 시간 안에 수행됨.

제2절. 영지식 증명을 활용한 블록체인 기술현황 조사

1. 영지식 증명 기반 롤업(Rollup) 기술

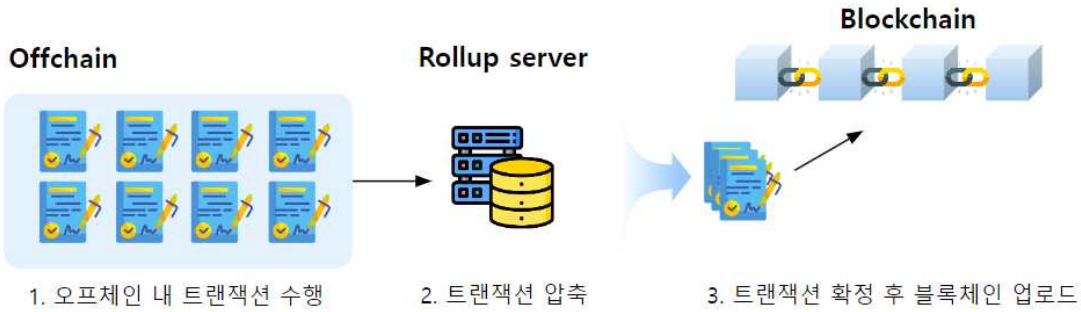
○ 이상적인 블록체인은 (1) 확장성, (2) 탈중앙화, (3) 보안성 세 가지를 모두 만족하여야하지만 세 가지 성질을 동시에 만족할 수 없음. 이를 블록체인 트릴레마(Blockchain Trilemma)라고 함. 현재의 블록체인 환경에서는 처리 용량의 한계와 트랜잭션 비용 문제로 인해 확장성과 효율성이 현저히 떨어짐

○ L2(Layer-2, 레이어2) 솔루션이란, 확장성 개선 대상 체인(L1)의 트랜잭션을 해당 블록체인 외부의 별개 체인인 L2에서 실행하되, 처리된 트랜잭션들의 결과를 대상 체인에 기록하여 보안성을 보장하는 방식으로, 최대한 빠르고 저렴하게 트랜잭션을 실행하는 것을 목표로 함. L2 솔루션의 종류는 크게 롤업, 사이드체인, 스테이트 채널, 발리디움 등이 있지만, 이 중 영지식 증명 기술이 도입된 분야는 롤업이 유일하므로 롤업에 관한 기술현황을 중점적으로 조사함



[그림 13] L1-L2 구조도

- 이러한 문제를 해결하기 위해 여러 트랜잭션을 하나의 블록으로 집약하여 처리함으로써 효율적으로 공간을 활용하고, 트랜잭션 비용을 절감함. 또한, 블록체인에서 더 복잡한 스마트 컨트랙트를 실행할 수 있도록 하여 다양한 분야에서 활용성을 높이고, 추가적인 보안 기능을 제공하여 안전한 트랜잭션 처리를 가능하게 하는 롤업 기술을 도입함



[그림 14] 롤업 기술 개요도

Type	Bitcoin	Ethereum	BSC	Cardano	Ripple	Tron	Harmony ONE	Avalanche	VISA	Solana
TPS	7	15	132	257	1,500	2,000	2,000	4,500	24,000	45,000

[그림 15] L1 블록체인별 최대 TPS(Transaction Per Second)

○ 롤업 기술은 계산 및 상태의 저장을 오프체인으로 이동하여 메인넷의 처리량을 높이는 L2 확장 솔루션임. L2에서 많은 양의 트랜잭션을 실행 및 처리한 뒤 그 결괏값들을 배치(batch)로 합친 뒤 L1에 저장하는 기술이고, 이러한 작업을 실행하는 스마트 컨트랙트를 롤업 컨트랙트라고 함

※ 접근 방식에 따라 낙천적 롤업(Optimistic Rollup), 영지식 롤업인 zk-Rollup, 그리고 두 방법을 혼용하는 하이브리드 롤업으로 분류됨

○ 영지식 증명은 프라이버시 강화와 확장성 개선을 위해 롤업 기술의 트랜잭션 압축 시 계산의 정당성 주장, 오프체인 내의 트랜잭션 수행의 유효성 증명 등의 과정에서 사용되고 있음. 영지식 증명은 현재 상용으로 나온 Polygon, StarkNet, ZKSync 등에서 적용되고 있음

[표 9] Optimistic Rollup / ZK-Rollup 비교표

구분[5]	Optimistic Rollup	ZK-Rollup
보안성	사기증명에 의존하여 보안성이 낮음	영지식 증명을 활용해 보안성이 매우 높음
가스 비용	Layer 1보다 낮은 수준으로 비용이 낮음	영지식 증명 계산으로 인해 비용이 많이 듦
개발자 경험	EVM 호환성이 좋음	영지식 증명에 대한 이해가 필요해 복잡함
프라이버시	트랜잭션 내용이 체인에 노출되어 프라이버시 수준이 높음	영지식 증명으로 인해 트랜잭션 내용을 숨길 수 있어 프라이버시 수준이 높음
도입 용이성	높음(호환성과 개발자 경험이 좋음)	낮음 (영지식 증명의 진입 장벽으로 인해 적용 방안이 다소 복잡)
ZKP 활용 여부	X	O
증명 방식	사기증명 방식	영지식 증명

○ Optimistic Rollup

- Optimistic Rollup은 말 그대로 낙천적 롤업, 즉 시스템이 문제없이 수행된다는 가정을 하고, 누군가 문제를 제기하지 않는 한 롤업 컨트랙트는 트랜잭션의 실행을 검증하지 않고 일단 사실로 간주하여 새로운 스테이트 루트를 업데이트함
- 롤업 컨트랙트란 롤업에서 이용되는 스마트 컨트랙트로 여러 거래를 하나의 데이터 셋으로 압축, 오프체인에서의 데이터 처리, 위반 거래에 대한 보안 처리를 담당함
- Optimistic Rollup은 데이터 가용성 문제, 즉 트랜잭션을 제대로 처리했는지에 대한 문제를 해결하기 위해 진위확인에 필요한 모든 트랜잭션을 블록체인에 전송하는 방식을 택한 방식임
- 블록 생산자(aggregator, block producer)는 사용자들의 트랜잭션을 모두 모아 연산을 해서 상태 루트(state root)를 구함. 그리고서 트랜잭션 전체와 상

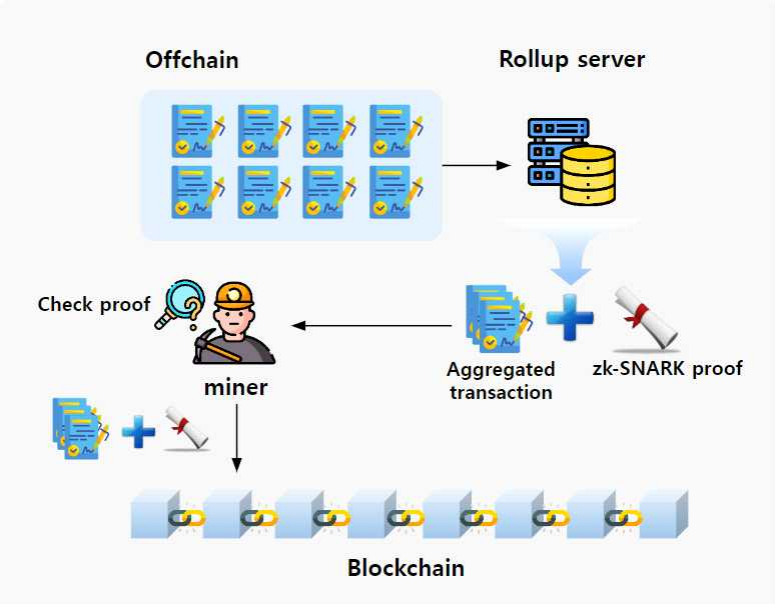
5) https://tokeninsight.medium.com/zksync-vs-starkware-whats-the-difference-between-the-top-two-zk-rollups-66d1a7d08ef3

태 루트 값을 블록체인에 기록함. 모든 트랜잭션 자체가 블록에 올라가고, 누구나 블록 생산자가 될 수 있음

- Optimistic Rollup은 상태 업데이트를 잘못하였을 경우 그것을 교정하기 위해 사기 증명(Fraud proof)을 활용함. 사기증명은 잘못된 상태에 대한 증거를 제시하는 방법으로, 검증자가 사기증명을 검증하여 잘못된 상태를 발견할 경우 변경 이전의 상태와 트랜잭션, 그리고 올바르게 연산한 후의 상태를 롤업 컨트랙트에 제출함
- Optimistic Rollup은 블록체인에서 처리되는 트랜잭션을 대신 처리하고 그 결과만 블록체인에 전송하여 속도를 향상하지만 사기증명 절차는 기술적, 구조적 제약(시간제한, 데이터 가용성, 데이터 처리 자원, 네트워크 지연, 인센티브) 때문에 아무 때나 가능하지 않음

○ zk-Rollup

- 옵티미스틱 롤업과 유사하지만, 보안 기능이 향상됨. 수백 개의 트랜잭션을 하나의 트랜잭션으로 묶어 블록체인 네트워크에 올리는 것은 같지만 각 트랜잭션에는 zk-SNARK 증명이 포함됨. 또한, 블록체인 네트워크에 전송되기 전 유효성 검증을 통해 트랜잭션의 크기를 더욱 줄일 수 있음. 아래 [그림 16]과 같이 오프체인(Layer-2)에서 발생한 트랜잭션을 롤업 서버에서 롤업 스마트 컨트랙트를 통해 압축해줌. 옵티미스틱 롤업과의 차이점은 이러한 압축 과정에 대한 증명도 함께 생성하여 Layer-1의 블록체인 검증자가 압축된 트랜잭션의 유효성을 검증한 뒤에 블록체인에 해당 트랜잭션을 저장함



[그림 16] zk-Rollup 개요도

- 영지식 롤업의 참여자는 트랜잭터(Transactors), 릴레이어(Relayers)라는 두 종류로 구성됨. 트랜잭터는 전송을 생성하고 이를 네트워크에 브로드캐스트하며, 릴레이어는 트랜잭터에게 받은 데이터들을 모아 하나의 트랜잭션을 생성함. 즉, 어떠한 거래가 맞다는 증명을 트랜잭션마다 함께 보내기 때문에 더욱 빠르게 결괏값을 확정할 수 있음. 이러한 증명은 스마트 컨트랙트에서 zk-SNARK 검증 알고리즘을 통해 구성하고 있는 트랜잭션의 유효성을 검증한 뒤 L1 체인에 저장됨

[표 10] 국내외 블록체인 롤업 솔루션 주요 사례

• **(국내)** 블록체인 롤업 솔루션은 ㈜라이트스케일의 Kroma가 있음. Kroma는 영지식 기반 사기 증명(zk Fault proof)과 영지식 이더리움 가상 머신(zkEVM)인 Scroll을 활용하여 Optimistic Rollup 서비스를 수행함. 2023년 1분기 테스트 넷을 시작으로 3분기 메인넷을 런칭했음. Kroma는 궁극적으로 zk Rollup으로 전환하는 것을 목표로 삼고 있음
• **(해외)** 블록체인 롤업 솔루션은 국내보다 활성화되어 있음. Optimistic Rollup의 경우 대표적으로 Plasma group의 Optimism, Offchain Labs의 Arbitrum이 있음

○ 하이브리드 롤업

- 하이브리드 롤업 솔루션은 기존 롤업 기술인 Optimistic rollup과 zk-Rollup의 장점을 혼용한 기술로 기존 롤업 서비스들과는 달리 연구 단계에 위치함

[표 11] 해외 하이브리드 롤업 솔루션 주요 사례

• **(해외)** Metis의 롤업 서비스로 최초의 하이브리드 롤업 서비스를 제공할 예정임.[6] Metis는 이 2가지 아키텍처를 결합함으로써 이더리움 개발자가 모든 유형의 분산 애플리케이션을 배포할 수 있도록 안전하고 개발자 친화적인 레이어 2를 제공할 예정임. 이 두 가지를 결합함으로써 Metis는 zk-Rollup의 보안 및 최종성과 함께 Optimistic Rollup의 확장성을 제공함

2. 영지식 증명 기반 이더리움 가상 머신(zkEVM)

○ 이더리움 가상 머신(Ethereum Virtual Machine, EVM)이란, 이더리움 가상 머신은 이더리움 블록체인에서 스마트 계약을 실행하는 가상 환경임. 이더리움 가상 머신은 이더리움이 정의한 규칙대로 스마트 계약 코드를 실행하고, 실행 결과에 따른 상태 변화를 모든 노드 간에 동기화해주어 전체 블록체인의 일관성을 유지함

○ 영지식 증명 기반 이더리움 가상 머신(zero-knowledge EVM, zkEVM)이란, 현재 이더리움 블록체인은 모든 트랜잭션 정보가 공개되어 있어, 사용자의 개인정보가 노출될 우려가 있음. 또한, 높은 트랜잭션 비용과 느린 처리 속도가 사용자 경험을 저해하고 있음. zkEVM은 영지식 증명을 활용하여 보안성과 개인정보 보호를 강화한 이더리움 가상머신의 일종으로, 기존 이더리움의 트랜잭션 처리 속도를 증가시킴과 동시에 보안을 강화하는 것을 목표로 함. 기존의 이더리움 가상 머신은 영지식 증명 계산을 지원하지 않지만, zkEVM은 기존의 이더리움 가상 머신과 호환되면서도 영지식 증명 계산을 지원하는 가상 머신임

  - 국내의 경우 영지식 증명 자체에 관한 연구/개발 난도가 높아 zkEVM 서비스를 개발한 곳이 없음
  - 국외의 경우 영지식 증명에 관한 관심이 국내보다 더 일찍 발생했고, 연구도 활발히 이루어져 zkEVM 관련 서비스가 존재함
  - zkEVM은 기존 이더리움 가상 머신(EVM)과의 호환성과 성능에 따라 크게 4가지 타입으로 구분 가능함

    ※ zkEVM은 다음과 같이 구분 가능함[7]

---

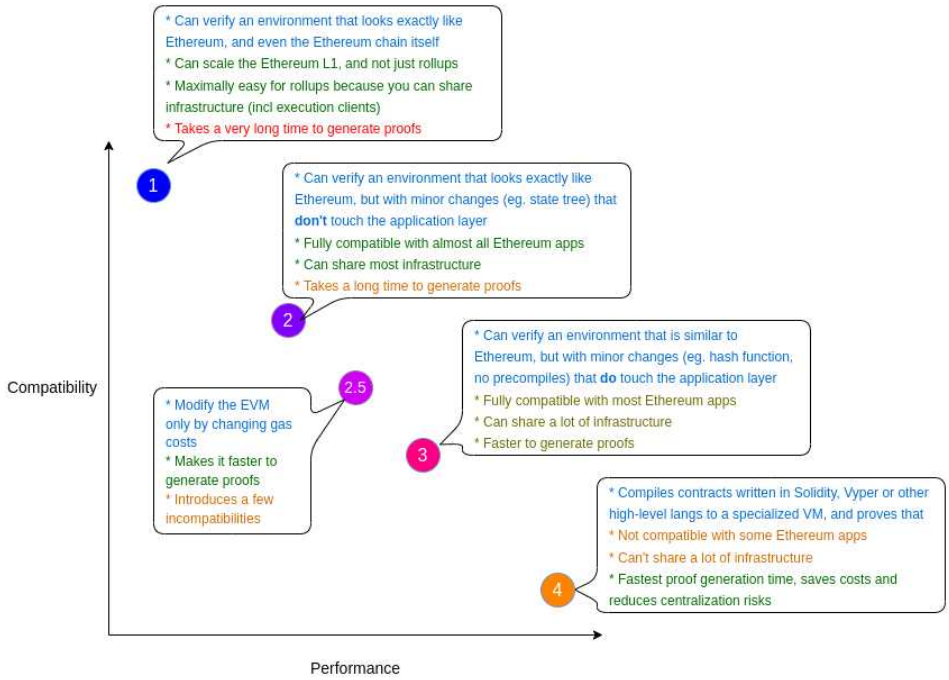
6) Introducing Hybrid Rollup, https://metisdao.medium.com/introducing-hybrid-rollups-8da384225b5e

7) Vitalik Buterin blog “The different types of ZK-EVMs”, https://vitalik.eth.limo/general/2022/08/04/zkevm.html

[표 12] 이더리움 가상 머신(EVM) 분류표

EVM 타입	특징
Type 1 : Fully Ethererum-equivalent	Type 1 zkEVM은 기존 이더리움과의 완벽한 호환성에 초점을 둔 zkEVM으로 해시 함수 종류, state tree 등을 전혀 변경하지 않은 것이 특징임. 하지만 영지식 증명에 필요한 계산에 대한 최적화를 고려하지 않아 증명 생성 시간이 오래 걸린다는 단점을 갖고 있음. 영지식 증명 회로 내에서 이더리움 가상머신의 OPCODE와 동일하게 동작하도록 구현하였기 때문에 트랜잭션 처리 방법, 스마트 컨트랙트 등의 처리 방식이 기존 이더리움과 같음
Type 2 : Fully EVM-equivalent	Type 2 zkEVM은 이더리움 가상머신(EVM)과의 호환성을 초점에 둔 zkEVM으로 Type 1과 달리 이더리움을 구성하고 있는 해시 함수 종류, state tree 등을 EVM과 완전히 호환되는 범위 내에서의 변경이 허용되는 zkEVM임. 영지식 증명 생성 수행 시간에 있어 큰 오버헤드로 작용하는 해시 함수를 Poseidon과 같은 해시 함수로 변경할 수 있어 증명 생성 시간에서 Type 1 zkEVM보다 강점이 있지만, 메모리와 관련된 OPCODE의 경우 영지식 증명 친화적이지 않은 부분이 남아 있으므로 여전히 증명 생성 시간이 느린 편에 속함
Type 3 : Almost EVM-equivalent	Type 3 zkEVM은 대부분의 이더리움을 활용한 응용과 호환되는 zkEVM으로, EVM 개발 난도를 낮추고 증명 생성 시간을 개선함. 하지만, 호환되지 않는 응용에 대해서는 사전에 컴파일된 어플리케이션을 덮어 써야 하므로 Type 1, 2보다 호환성이 떨어짐
Type 4 : High-level-language equivalent	Type 4 zkEVM은 Solidity, Viper와 같은 고급 프로그래밍 언어를 사용하여 컴파일한 zkEVM으로 영지식 증명 계산에 불리한 부분을 영지식 증명 친화적으로 설계할 수 있다는 장점이 있어 증명 생성 시간이 모든 EVM Type 중 가장 빠름. 하지만 기존 EVM에서 사용하는 것과 다르게 EVM 바이트 코드를 사용하고 있으므로, 이더리움에서 정의한 컨트랙트와 호환되지 않는 경우가 발생하고, 기존에 존재하는 디버깅 도구를 사용할 수 없으므로 모든 zkEVM 중 이더리움 및 이더리움 가상머신과 호환성이 가장 부족함

○ zkEVM은 영지식 증명을 트랜잭션 내용을 공개하지 않고도 유효성을 증명하기 때문에 사용자의 프라이버시를 보호하면서도 거래의 정확성을 확보할 수 있어 프라이버시 강화에 이점이 있음. 또한, 상세한 데이터를 메인넷에 게시할 필요가 없으므로 더 적은 비용으로 안전한 스마트 계약 실행이 가능함. 그로 인해 빠른 상태 업데이트를 제공할 수 있어 트랜잭션 최종성의 측면에서도 롤업 기술 대비 빠르다는 장점이 있게 되고, 같은 시간 높은 처리량을 유지할 수 있어 확장성 향상에 도움이 됨



[그림 17] 호환성과 성능에 따른 이더리움 가상 머신의 분류 그래프[7)]

※ 대표적인 zkEVM 서비스는 다음과 같음

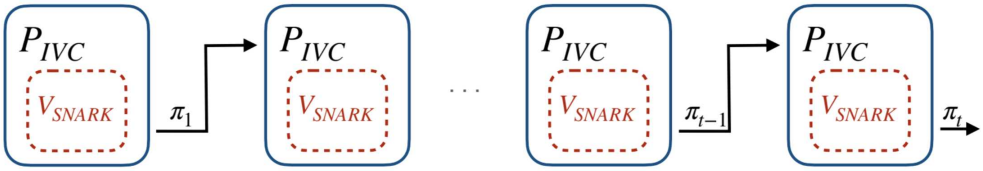
[표 13] 대표적인 zkEVM 서비스

• **(Polygon Hermez)** Polygon에서 개발한 zkEVM으로 EVM opcode를 Almost EVM-Equivalent(Type 3) 수준으로 구현함. Fully EVM-equivalent 수준(Type 2)의 zkEVM보다 증명 생성 시간이 빠르지만, 기존 EVM에 대한 호환성은 약간 낮음. 검증이 내부 언어인 zkASM으로 수행된다는 특징을 가짐
• **(Scroll zkEVM)** Scroll zkEVM 역시 Fully EVM-equivalent(Type 2)가 아닌 Almost EVM-equivalent zkEVM(Type 3)임. Scroll zkEVM은 Plonk PIOP 기반으로 Plookup, 하드웨어 가속 등을 통해 증명 생성 시간을 줄임
• **(zkSync 2.0)** zkSync는 zkSync 2.0 High-level-language equivalent zkEVM(Type 4)으로 호환성이 아주 낮은 대신 증명 생성 시간이 Polygon Hermez와 Scroll zkEVM에 비해 빠름. zkSync는 Solidity와 Zinc라는 언어를 사용하여 zkEVM 바이트 코드로 컴파일할 수 있음
• **(Cairo-VM, Kakarot)** Cairo-VM은 Starkware의 가상머신으로 Starkware에서 자체 개발한 Cairo라는 언어를 사용하지만, Solidity도 호환이 됨. Cairo-VM은 zkEVM이 아니며, Starkware에서 개발한 zkEVM은 Kakarot로 이 또한 Cairo로 프로그래밍 되어 있음. 언어 단계에서 호환이 되므로 Type 4 zkEVM으로 구분 가능함

3. 재귀적 증명(Recursive SNARK)

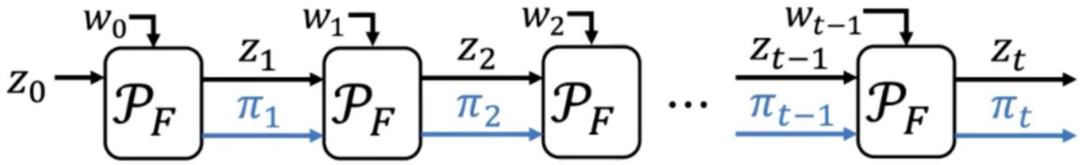
○ 재귀적 증명 개념

- 재귀적 증명이란 영지식 증명에 이전에 생성된 증명에 대한 검증 코드를 포함하는 것을 뜻함. 재귀적 증명은 영지식 증명을 이용하여 특정 조건이 충족되었음을 증명하는데, 블록체인 네트워크에 데이터를 노출하지 않으면서도 검증할 수 있게 함. 스마트 컨트랙트를 효율적으로 실행하면서 높은 수준의 프라이버시를 유지하기 위해 사용됨
- 재귀적 증명은 PCD(Proof-Carrying Data)의 한 방법으로 사용되는데, PCD란 한 함수는 여러 번 실행했을 때 각 단계에 대한 증명을 모두 생성하는 것이 아닌 하나의 증명만 검증함으로써 모든 단계의 함수 실행에 대한 정당성을 증명하는 기법임



[그림 18] 재귀적 증명 예시

- 재귀적 증명의 응용으로는 점진적 검증 가능 계산(Incrementally Verifiable Computation, IVC)이 있음. 점진적 검증 가능 계산은 함수를 여러 번 실행한 뒤 최종적으로 나오는 하나의 증명만 검증한다는 방식은 PCD와 같지만, 이전 단계의 계산 값이 다음 단계의 입력값으로 주어진다는 차이점이 존재함



[그림 19] IVC 예시

- IVC에 관한 연구는 Nova[KST22], SuperNova[KS22], HyperNova[KS23] 등이 있음
  ※ Nova[KST22] : Nova는 폴딩 기법(Folding scheme)을 통한 점진적 검증 가능 계산을 제시한 논문임. 폴딩 기법이란 두 개의 진술과 두 개의 비밀 정보를 하나의 진술과 비밀 정보로 압축한 뒤, 압축한 진술과 비밀 정보를 검증함으로써 기존 두 개의 진술과 비밀 정보가 정당함을 검증할 수 있는 기법임. 즉, R1CS 관계식을 만족시키는 진술과 비밀 정보 쌍 $(x_1,w_1),(x_2,w_2)$을 압축하여 (x^*,w^*)를 생성하고, (x^*,w^*)에 대한 정당성을 검증하는 것을 통해 $(x_1,w_1),(x_2,w_2)$의 정당성을 동시에 검증하는 방식으로 효율성을 향상하는 방식임. Nova는 점진적 검증 가능 계산의 각 단계에서 새로 생성되는 (x,w)와 압축된 (x^*,w^*)를 매 단계 재압축하여 최종적으로 출력된 진술, 비밀 정보 쌍 (x^*,w^*) 만을 검증하여 모든 단계의 계산이 정당함을 보임
  ※ SuperNova[KS22] : SuperNova는 Nova를 일반화한 버전임. Nova는 단일 명령어에 대한 점진적 검증 가능 계산을 지원하지만, SuperNova는 임의의 명령어에 대해 점진적 검증 가능 계산을 지원함. 즉, Nova는 함수 F

에 대하여 l번의 계산을 한 결과 $y = F^{(l)}(x)$가 정당함을 증명하는 기법이지만, SuperNova는 $(F_1, \cdots, F_l)$와 모든 $i \in \{0, \cdots, n-1\}$에 대하여 $y_{i+1} = F^{(i)}(x_i, y_i)$를 만족함을 보이는 기법임. 이를 활용하면 사용자가 정의한 명령어에 대한 점진적 검증 가능 계산을 지원할 수 있음

※ HyperNova[KS23] : HyperNova는 기존 Nova에서 R1CS 관계식에 대하여 폴딩 기법을 적용했던 것과 달리 CCS(Customizable Constraint System)[STW23]에 대하여 폴딩 기법을 적용한 연구임. CCS란 R1CS, Plonkish 산술화, AIR(Algebraic Intermediate Representation)를 추가적인 오버헤드 없이 일반화한 관계식임. 이를 위해 멀티-폴딩 기법(Multi-folding scheme)을 제안함. 멀티-폴딩 기법이란 같은 구조를 갖는 진술, 비밀 정보 쌍을 입력받아 압축하는 기법임

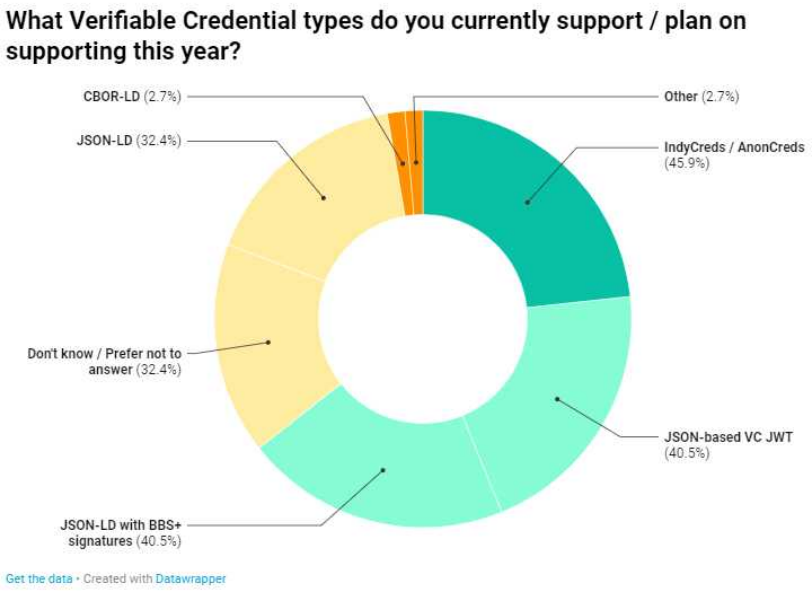
제3절. 프라이버시 강화를 위한 영지식 증명 기술현황 조사

○ 영지식 증명은 실제 정보를 드러내지 않고 해당 정보를 소유하고 있음을 증명하는 기술로, 개별 사용자가 자신의 민감한 정보를 완전히 숨기면서도 원하는 정보 일부를 특정 조건으로 증명할 수 있음. 이러한 속성은 블록체인과 같은 분산 시스템에서 신원 확인이나 거래 검증 등에서 프라이버시 강화에 도움이 됨. 예를 들어, 금융 거래에서 얼마를 소유하고 있는지에 대한 증명을 통해 소유한 자산을 드러내지 않으면서 거래를 발생시키기 충분한 자산을 갖고 있음을 보일 수 있음

○ 본 절은 프라이버시 강화를 위해 활용되는 주요 영지식 증명 기술을 살펴본 뒤, 영지식 증명 기술을 활용한 프라이버시 강화할 수 있는 기법으로 약정, 선택적 제출, 범위증명, 그리고 멤버십 증명을 기술함. 마지막으로, 프라이버시 강화를 위한 국제적 요구는 어떤 것이 있는지 다양한 정책 사례를 위주로 살펴보고, 영지식 증명이 이러한 요구를 어떻게 만족할 수 있는지를 소개함

1. 프라이버시 강화 관련 주요 영지식 증명 기술

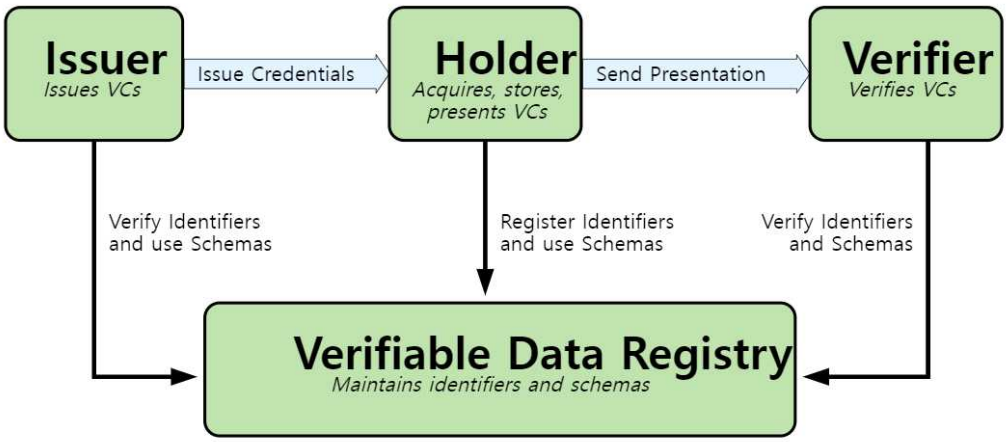
○ 분산 신원에서 프라이버시 강화 목적으로 영지식 증명 기술을 활용하고 있음. 하이퍼레저 인디(Hyperledger Indy)의 AnonCreds는 선택적 제출을 위해 CL 서명이 활용되고 있고, 하이퍼레저 우르사(Hyperledger Ursa)의 Anonymous Credential 2.0에서는 BBS+ 서명이 활용되고 있음



[그림 20] Hyperledger Anoncreds 설문조사 결과

○ 영지식 증명 전자 신원 인증은 전자서명 방법의 하나인 CL(Camensisch-Lysyanskaya) 서명을 활용한 분산 신원(DID, Decentralized Identifier) 2.0이 대표적임

- DID 2.0은 현재 웹 기술 표준 기관인 W3C(World Wide Web Consortium)에서 표준화 작업 진행 중
- DID 2.0의 핵심은 CL 서명을 이용하여 영지식 증명 특성을 만족하는 것으로, 선택적 공개(Selective Disclosure)가 가능하게 설계하는 것임
- 선택적 공개란 필요한 것에 대해서만 공개하고 불필요한 개인정보는 공개하지 않는다는 것을 의미함
- DID 2.0의 특징은 인증서(Credential) 내 속성에 대한 범위증명이 가능하다는 것임. 예를 들어, 나이 등의 특징에 대해서 나이를 공개하지 않고 성인 여부(만 19세 이상)를 증명할 수 있음
- 상기 사례에서 보여야 하는 필요한 것(성인 여부)은 공개하지만 불필요한 개인정보인 정확한 나이는 비공개함



[그림 21] W3C DID 2.0의 역할 및 데이터 흐름

- 해외에는 다양한 서비스들이 있음. Hyperledger Indy의 DID 역시 선택적 공개를 지원
- DID 2.0은 인증서 폐기[8]에서 프라이버시 문제가 발생. DID 2.0은 인증서별로 고유 일련번호를 생성. 폐기된 인증서의 일련번호 리스트에 현재 증명하고자 하는 인증서의 일련번호가 부재하면 유효한 인증서로 간주함. 이때 일련번호와 인증서 간의 연결성을 확인할 수 있어 프라이버시 문제가 발생

8) 인증서 폐기는 유효 기간 만료, 재산의 증감, 나이 증가 등 인증서의 종류에 따라 다양하게, 빈번히 발생할 수 있음.

○ DID 2.0 이외에 zk-SNARKs 기반 전자 신원 인증 서비스는 상용화 단계 진입 전 연구 단계임
- 현재 서비스 중인 zk-SNARKs 기반 전자 신원 인증 서비스는 Polygon에서 개발한 Polygon ID가 유일함
- 신원 소유자는 SNARK 증명을 통해 검증자에게 본인의 신원 인증을 프라이버시 노출 없이 진행함. 발급 기관(혹은 발급인)은 현실 세계의 신뢰 체계, 즉 정부 기관 등에 대한 신뢰를 기반으로 함
- **(발급)** 발급자는 신원에 대한 검증 가능한 자격 증명을 구축함. 여기에는 KYC, DAO 회원 증명, 정부 문서 등이 있으며 자격 증명은 사용자가 요청하고 검증자가 수락할 수 있음
- **(저장 및 검증)** 사용자는 자격 증명을 요청, 저장 및 관리할 수 있음. 자격 증명을 사용할 때 어떤 정보를 공유할지 선택할 수 있음. 예를 들어 사용자는 정확한 생년월일을 밝히지 않고도 확인 가능한 자격 증명을 사용하여 이름과 나이를 증명할 수 있음

2. 영지식 증명 기술을 활용한 프라이버시 강화 기법

○ 영지식 증명은 영지식 증명 프로토콜 그 자체부터 선택적 제출, 범위증명, 약정 기법, 멤버십 증명을 영지식 증명 프로토콜과 같이 활용하여 영지식 증명 응용 기법을 설계할 수 있음

○ 특히, 2장 2절에서 소개한 바와 같이 약정 기법은 영지식 증명 프로토콜 설계과정에서 빈번하게 사용됨. 선택적 제출과 범위증명은 검증 가능한 자격 증명(Verifiable Credential)을 구현하기 위한 구성요소로 주요한 역할을 함. 마지막으로, 멤버십 증명 기술의 경우 블록체인 환경에서 자주 사용되는 기술로써, 프라이버시 보호를 위해 영지식 증명과 같이 사용됨

1) 약정(Commitment)

○ 약정은 정보나 값을 숨기면서도 나중에 그 내용을 공개할 수 있는 기법임. 전술한 바와 같이 약정 기술은 영지식 증명 프로토콜의 기반 기술로써 활용됨

○ 약정 기법은 크게 약정 단계(Commitment phase)와 공개 단계(Open phase)의 2단계로 나뉨
- 약정 단계 : 증명자는 비밀 정보와 랜덤값을 이용해 약정 값을 계산함
- 공개 단계 : 증명자는 비밀 정보와 랜덤값을 공개하고, 검증자는 해당 비밀 정보와 랜덤값을 이용한 약정 값이 맞는지를 확인함

○ 약정은 hiding과 binding이라는 2가지 특징을 가짐.

- Hiding : 검증자가 약정 값을 통해 비밀 값과 랜덤값에 대한 정보를 얻을 수 없음
- Binding : 증명자가 약정 값에 대해 다른 비밀 정보를 통해 검증 식을 통과하는 것이 불가능함

○ 대표적인 약정 기법으론 Pedersen 약정과 KZG10 약정이 있음

- Pedersen 약정

※ Pedersen 약정은 타원 곡선 기반 약정 기법으로, 입력 x와 랜덤값 r을 이용해 $c = g^x h^r$를 계산하여 약정하는 방법임

※ Pedersen 약정은 동형 성질을 갖고 있어 서로 다른 두 약정을 곱하면 입력 $x_1 + x_2$과 랜덤값 $r_1 + r_2$에 대한 약정 값이 됨

※ 벡터 $\vec{x}$ 를 입력받아 하나의 약정으로 계산하는 벡터 약정 응용도 존재함

- KZG10 약정

※ KZG10 약정은 다항식 약정에 많이 사용되는 약정 기법임

※ KZG10 약정은 다항식 $f(x)$의 계수 $\vec{f} = (f_1, \cdots, f_d)$를 입력받아 약정하고, 검증자가 $f(r)$에 대한 계산을 요청하면 $f(r)$과 해당 계산에 대한 증명 π를 제공하는 방식임

※ KZG10 약정은 증명 생성 시간이 $O(d \log d)$이지만, 검증 시간이 다항식의 차수와 무관하게 상수 시간이 걸려 효율적인 약정 방식으로 널리 사용됨

○ 적용사례

- 대표적으로 약정 기법이 사용되는 예시에는 UTXO(Unspent Transaction Output) 블록체인 모델이 있음. 거래를 진행할 때 금액을 직접 공개하는 것이 아닌, 금액을 약정하고, 다음에 약정을 공개함. 약정의 특성으로 거래에 대한 프라이버시를 보장하면서 무결성을 보장할 수 있음

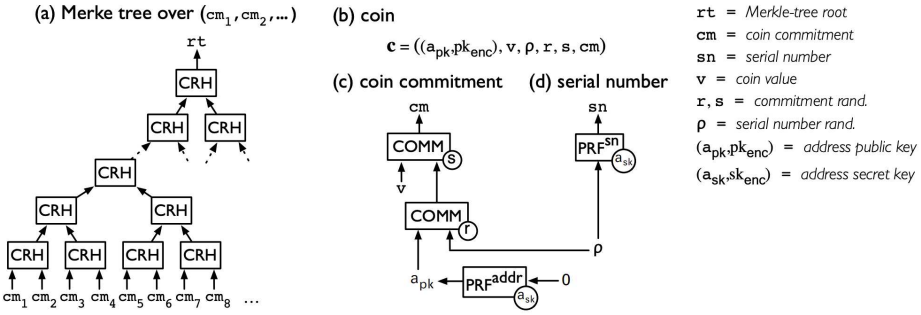


Fig. 1: **(a)** Illustration of the CRH-based Merkle tree over the list CMList of coin commitments. **(b)** A coin **c**. **(c)** Illustration of the structure of a coin commitment cm. **(d)** Illustration of the structure of a coin serial number sn.

[그림 22] 제로캐시(Zerocash)에서 프라이버시 보호를 위한 약정 값 이용

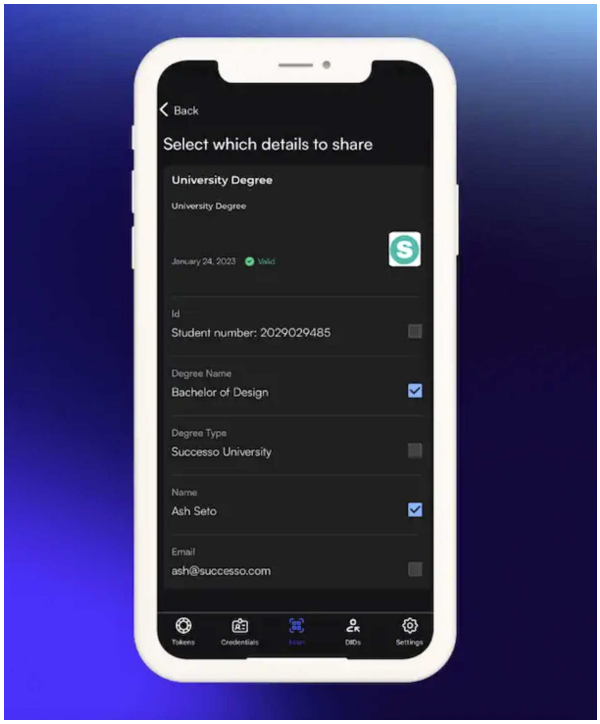
- 제로캐시에서는 발행 트랜잭션을 통해 사용자는 특정 비트코인 주소에서 지정된 수의 익명이 아닌 비트코인을 지정된 제로캐시 주소에 속한 같은 수의 제로코인으로 변환할 수 있음. 발행 거래 자체는 코인의 가치, 소유자 주소, (고유) 일련번호를 지정하는 새 코인에 대한 암호화 약정으로 구성됨. 약정 값은 SHA-256 해시 함수를 기반으로 하며 코인의 가치와 소유자 주소를 모두 숨겨 프라이버시를 보장함
- 개별 제로캐시 노드는 지금까지 표시된 모든 코인 약정 값에 대해 머클 트리를 유지하며 모든 사용자는 영지식 증명을 통해 코인 약정 값의 소유권을 증명할 수 있음
- 이러한 약정 기술을 기반으로 데이터에 대한 프라이버시를 보장하면서 데이터를 이용하는 방법을 이용할 수 있게 되며 이를 이용하여 다양한 응용을 개발할 수 있음

2) 선택적 제출(Selective Disclosure)

○ 선택적 제출이란 검증 가능한 자격 증명(Verifiable Credential) 기술의 한 특징으로, 특정 집단에 원하는 정보만 공개하는 것을 뜻함. 선택적 제출을 통해 정보의 주체가 본인의 정보에 대한 접근을 스스로 제어할 수 있음. 검증 가능한 자격 증명은 정보에 대한 프라이버시뿐 아니라 하나의 디바이스에 본인의 정보를 모두 담아 다닐 수 있다는 점에서 정보의 휴대성이 뛰어나다는 장점이 있음. 또한, 증명하고자 하는 정보만을 드러내기 때문에 주고받는 데이터의 양을 최소화할 수 있음

○ 적용사례

- 선택적 제출을 활용한 기술로는 익명 크리덴셜(Anonymous Credential)이 있음. 익명 크리덴셜은 공공기관으로부터 인증받은 한 개인의 이름, 주소, 생일 등의 정보 중 일부만을 다른 집단에 증명하는 기법으로, 익명 크리덴셜에서 주요하게 사용된 기술은 CL 서명, BBS+ 서명 등이 사용되어옴
- 선택적 제출을 통한 검증 가능한 자격 증명을 서비스하는 예로 Dock[9]의 ID Wallet이 있음. 아래 [그림 23]과 같이 대학 학위와 같은 특정한 정보를 타인에게 증명할 수 있고, QR 코드 등과 같은 방식으로 검증받을 수 있음



[그림 23] Dock의 ID Wallet

3) 범위 증명(Range Proof)

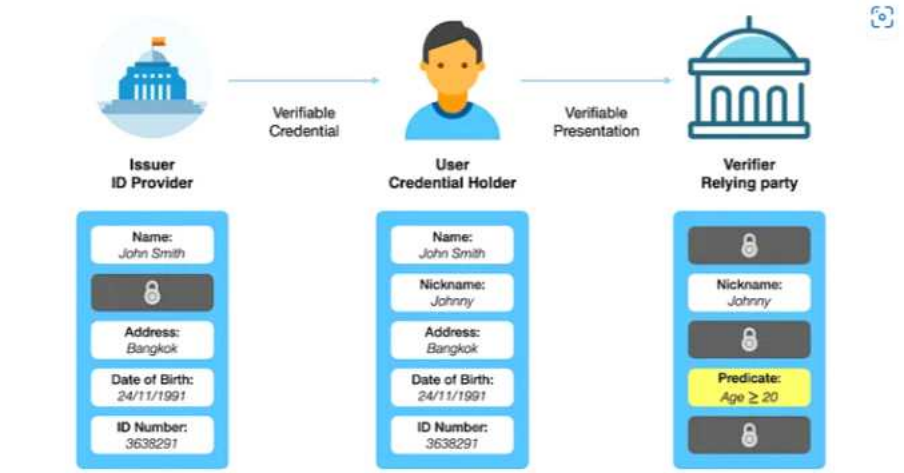
○ 선택적 제출의 또 다른 방법으로 범위 증명(Range Proof) 기법이 있음. 범위 증명이란 숫자 자체를 공개하지 않고 숫자가 특정 범위 내에 있음을 증명하는 방법임. 이는 정확한 숫자를 공개하면 민감한 정보가 유출될 수 있는 개인정보 보호 중심의 암호화 애플리케이션에서 특히 중요함

○ 활용방안

- 범위증명은 검증 가능한 자격 증명 기술에서 사용자의 정보에 대해 실제

9) https://www.dock.io/

값을 드러내지 않고 자격 요건을 충족한다는 것을 증명하기 위해 사용됨. 예를 들어 성인 인증의 경우, 사용자가 특정 나이(22세 등)를 공개하지 않고 단순하게 19세를 넘는다는 것만 증명하는 것임. 나이뿐만 아니라, 소득 수준 등을 요구하는 응용 서비스에도 적용될 수 있는데, 예를 들어 대출 심사 등을 진행할 때, 대출 신청자의 연간 소득이 특정 금액을 초과한다는 것을 증명하는 데 활용될 수 있음



A demonstration of CL-signature with a zero-knowledge proof of age. Here, a credential contains name, nickname, address, date of birth and ID number. The user binds his nickname to the credential without revealing it to the issuer. The user then presents his credential to the verifier, showing only his nickname and a zero-knowledge proof that he is above 20 years old.

[그림 24] 범위증명 예시

4) 멤버십 증명(Membership Proof)

○ 영지식 증명(ZKP)의 맥락에서 멤버십 증명이란 특정 요소가 어떤 요소인지 밝히지 않고도 집합의 구성원임을 증명하는 데 사용되는 방법임

○ 다시 말해 멤버십 증명은, 원소 u가 특정한 유효 집합 S에 속함을 증명하는 것임. 특히, 블록체인에서는 UTXO 모델 등에서 해당 트랜잭션이 이전에 사용된 트랜잭션이 아님을 증명하여 이중 지불(Double spending)을 방지하기 위해 사용됨

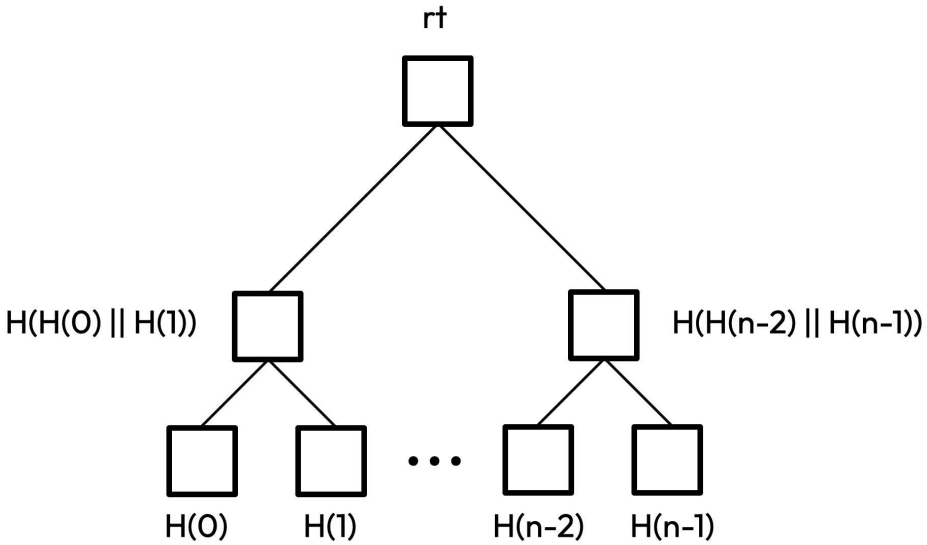
○ UTXO 모델은 사용되지 않은 코인에 대한 약정 값으로 머클 트리를 생성함. 사용자가 거래를 진행할 때 이중 지불을 확인하기 위해 사용하고자 하는 코인이 머클 트리에 존재하는지를 멤버십 증명을 생성함. 즉 사용하고자 하는 코인이 머클 트리에 존재할 경우 사용되지 않은 코인의 집합에 속하는 것이기 때문에 정당한 코인임. 하지만, 존재하지 않으면 이미 사용된 코인이기 때문

에 이중 지불이되어 올바른 멤버십 증명을 생성할 수 없음. 이 과정에서 이중 지불을 방지할 수 있음

○ 다만 멤버십 증명을 그냥 수행하게 되면 사용자에 대한 연결성 추적이 가능하므로 프라이버시를 보장하기 위해 영지식 증명을 동반한 멤버십 증명 기술들이 연구・개발되고 있음

○ 프라이버시 보장 멤버십 증명을 위해 일반적으로 멤버십 증명 생성을 영지식 증명 회로 내에서 수행하는 방법을 취함. 하지만 이 경우 머클 트리 계산을 위한 해시 함수 연산, 또는 RSA 군 지수 연산 등을 수반하여 증명 생성 시간에 부하를 일으킴

○ 일반적으로 머클 트리 기반 멤버십 증명이 사용되고 있으며, 성능과 용도에 따라 RSA 누산기(RSA Accumulator) 기반 멤버십 증명이 있음

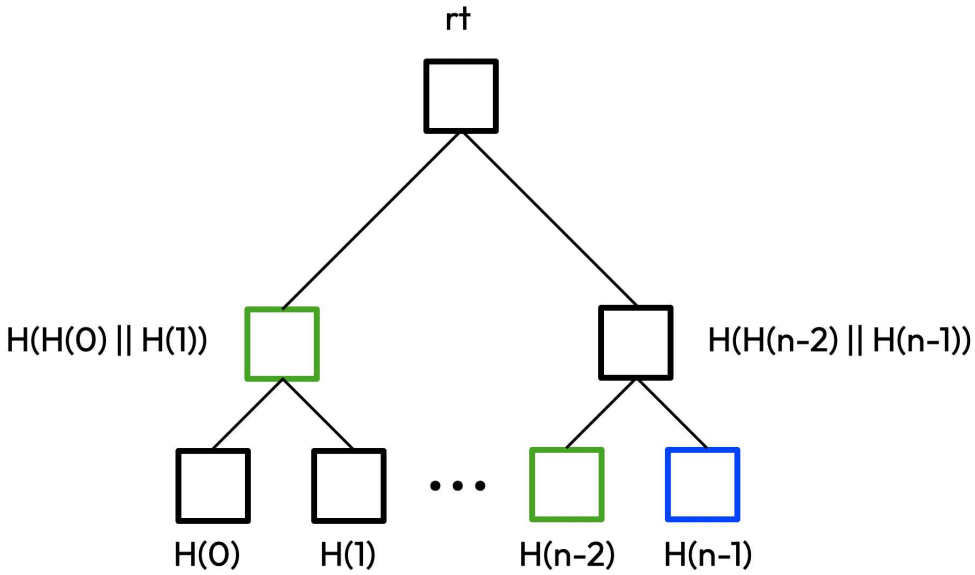


[그림 25] 머클 트리 구조

○ 머클 트리 기반 멤버십

- 증명의 경우 집합 원소를 리프 노드로 설정하고, 자식 노드의 해시값, 즉 i번째 노드와 i+1번째 노드의 해시값을 부모 노드로 설정함([그림 25] 참조) 이 작업을 반복하여 루트 값을 생성함
- 증명자는 i번째 멤버인 u_i와 그것에 해당하는 인증 경로(co-path, [그림 26] 참조), 루트 값을 제공. 따라서 증명 시간과 증명 크기는 전체 집합의 로그 스케일만큼 소요됨
- 검증자는 인증 경로와 i번째 멤버로 루트 값을 직접 계산하고, 주어진 루트

값과 같은지 확인을 통해 검증함



[그림 26] 머클 트리의 인증 경로(co-path, 초록색)

○ RSA Accumulator 기반 멤버십

- RSA Accumulator는 RSA 군(Group)의 생성원(Generator)에 모든 집합 원소를 지수 연산하여 Accumulator 생성: $ACC = g^{u_1 u_2 \cdots u_n}$
- 증명자는 i번째 원소 u_i를 제외한 나머지 집합 원소를 모두 지수 연산하여 증명으로 제공: $W = g^{\prod_{u_j \in S, u_j} u_j}$. 증명 생성 시간은 집합 크기에 비례한 군 연산 소요. 증명 크기는 RSA 군의 크기로 상수 크기(RSA-2048의 경우 2048-bit)
- 검증자는 주어진 W에 u_i를 지수 연산한 값이 ACC와 같은지 확인을 통해 검증. 검증 시간은 1번의 군 연산 소요

○ Bilinear-Map Accumulator 기반 멤버십

- 머클 트리 기반 멤버십과 RSA Accumlator 기반 멤버십 증명 이외에 Bilinear-Map 기반 Accumulator가 존재함
- Bilinear-Map Accumulator 기반 멤버십 증명에서 Accumulator는 각 집합 원소와 비밀 트랩도어 값을 더한 값들을 지수 연산하여 생성: $g^{\prod(s+u_i)}$
- RSA Accumulator 기반 멤버십 증명과 유사하게 증명은 증명하고자 하는 원소를 제외한 값들을 지수 연산하여 생성함. 검증자는 페어링 연산으로 증명에 i번째 원소를 지수 연산한 값이 Accumulator와 같은 값인지를 확인

하여 검증

- RSA 군보다 지수 연산이 빠르다는 장점이 있지만[10], 공개 파라미터 크기가 전체 집합 크기에 선형 비례하여 매우 크다는 단점을 가짐

○ 상술한 멤버십 증명 기법에 프라이버시를 보장하기 위해서 영지식 증명 회로 내에서 각 알고리즘을 수행하게 되면 증명자의 증명 생성 시간에 부하가 야기됨. [CFH+22]와 [BCF+23]의 경우 효율적인 프라이버시 보장 멤버십 증명 기법을 RSA accumulator 기반 멤버십 증명을 기반으로 설계함. 두 논문 모두 RSA 지수 연산을 영지식 증명 회로에서 분리하여 증명 생성 부하를 줄이는 접근법을 사용. [BCF+23]의 경우 하나의 멤버에 대해서만 증명을 하는 단일 멤버십 증명이 가능하지만 [CFH+22]의 경우 다수의 멤버십을 하나의 증명으로 증명할 수 있는 일괄 멤버십 증명이 가능하게끔 설계함. 이를 통해 프라이버시를 보장하면서도 효율적인 일괄 멤버십 증명 프로토콜을 구현함

3. 블록체인 프라이버시 요구수준 조사

○ 현재 블록체인에 대한 프라이버시 요구수준에 대한 기준이 없어 국내·외 개인정보 보호에 대한 사항들을 기술하였음. 기술이 발달함에 따라, 특히 초연결 사회에 진입하면서 개인 데이터에 접근하는 것이 이전에 비해 수월해짐. 이에 따라 개인정보 유출로부터 야기되는 문제가 대두됨. 또한, 데이터의 가치가 중대해지면서 개인정보 보호에 대한 요구수준이 강화되고, 데이터 주권에 대한 논의가 활발하게 진행됨. 이러한 시장의 프라이버시 요구에 발맞추어, 각국은 개인정보 보호 정책을 수립함

○ 디지털 권리장전(2023년 9월)

- **(목적)** 디지털 시대에 필요한 국가적 기준과 원칙을 제시하고, 글로벌 디지털 질서 규범의 기본 방향을 담은 문서로, 전문과 6장, 28개 조문으로 구성됨
- **(기본원칙)** 디지털 환경에서의 자유와 권리 보장, 디지털 접근의 공정성, 안전하고 신뢰할 수 있는 디지털 사회, 디지털 혁신 촉진, 인류 후생 증진 등 5가지 기본원칙을 포함함
- **(향후 계획)** 디지털 권리장전을 기반으로 디지털 시대의 쟁점 해결 및 법·제도 정비에 나설 계획. 이에는 '인공지능법', '디지털 포용법' 제정 등이 포

10) 단, 점근적 복잡도는 RSA Accumulator 기반 멤버십 증명과 같음. RSA 군 연산 대비 겹선형 군의 연산이 더 부하가 적기 때문에 실질적 시간이 더 빠름.

함됨. 정부는 UN, OECD 등 국제기구와 협력하여 디지털 규범 논의를 주도하고, 국가 간 디지털 격차 해소를 위한 노력을 강화할 예정임

- 『디지털 권리장전』의 제2장 제9조와 제4장 제19조 두 조항은 블록체인과 같은 기술에서 개인 데이터의 보호와 통제를 강조함

[표 14] 디지털 권리장전 상세 내용

목차	제목	내용
제1장	기본원칙 설정	• 디지털 공동번영사회를 위한 기본원칙을 명시. • 원칙에는 디지털 환경에서의 자유와 권리 보장, 디지털에 대한 공정한 접근과 기회의 균등, 안전하고 신뢰할 수 있는 디지털 사회 구축, 자율과 창의 기반의 디지털 혁신 촉진, 인류 후생 증진 등이 포함됨.
제2장	자유와 권리 보장	• 디지털 환경에서의 권리 보장에 중점을 둠. • 예시로, 모든 사용자가 키오스크와 같은 디지털 서비스에 차별 없이 접근할 수 있도록 하는 '디지털 접근의 보장', 개인정보의 열람, 정정, 삭제, 전송 등을 보장하는 '개인정보의 접근 및 통제' 등이 포함됨. • **(제2장 제9조)** 모든 사람은 디지털 환경에서 자신에 관한 정보를 열람·정정·삭제·전송할 것을 요구하는 등 이에 대해 접근하고 통제할 수 있어야 한다
제3장	공정한 접근과 기회의 균등	• 데이터 및 디지털 저작물 등 디지털 자산에 대한 법적, 정책적 보호 강화. • 디지털 리터러시 향상을 통한 디지털 격차 해소에 초점을 맞춤.
제4장	안전하고 신뢰할 수 있는 디지털 사회	• 디지털 위험에 대응하는 체계적인 시스템 구축. • 디지털 기술의 윤리적 개발과 사용에 대한 원칙을 제시 • **(제4장 제19조)** 디지털 환경에서 개인의 프라이버시는 디지털 감시, 위치추적 등을 비롯한 불법적인 식별과 추적으로부터 보호되어야 한다
제5장	디지털 혁신의 촉진	• 디지털 환경에 맞지 않는 규제의 개선 및 전문 인력 양성, 연구개발 투자 등을 통한 디지털 혁신 지원. • 디지털 기술 발전을 촉진하는 정책과 프로그램의 추진에 중점을 둠.
제6장	인류 후생의 증진	• 디지털 기술의 국제적 성격을 인식하고, 국제사회와 협력하여 인류 후생을 증진하는 디지털 국제규범 형성에 기여. • 국가 간 디지털 격차 해소를 위한 글로벌 노력 강조.

○ EU-GDPR(일반개인정보보호법)[11]

- GDPR은 개인에 관한 기본권과 자유 및 특히 개인정보 보호에 대한 권리를 보호하고, EU 역내에서 개인정보의 자유로운 이동을 보장하는 것을 목적으로 하는 개인정보 보호법임

[표 15] GDPR이 적용되는 범위

• 사용자가 사용하는 장치, 애플리케이션, 도구와 프로토콜을 통해 제공되는 개인식별이 가능한 경우의 쿠키(cookie) ID, IP 주소, RFID(무선 인식) 태그 등 • 위치정보 • 특수한 범주의 개인정보, 유전정보와 생체인식정보 • 가명 처리(pseudonymisation)된 개인정보

[표 16] 개인정보 처리의 7가지 원칙

• 합법성・공정성・투명성 원칙 • 목적 제한의 원칙 • 개인정보 최소처리 원칙 • 정확성의 원칙 • 보유 기간 제한의 원칙 • 무결성과 기밀성의 원칙 • 책임성의 원칙

- 개인정보 처리의 합법성・공정성・투명성 원칙에 따라 개인정보 처리는 GDPR에서 허용한 요건에 해당해야 합법 처리로 인정됨

[표 17] 개인정보 처리에 관한 GDPR 허용 요건

• 정보 주체가 하나 이상의 특정한 목적을 위하여 본인의 개인정보 처리에 동의한 경우 • 정보 주체가 계약 당사자로 있는 계약의 이행을 위하여 또는 계약 체결 전 정보 주체의 요청에 따라 조처하기 위하여 처리가 필요한 경우 • 컨트롤러에 적용되는 법적 의무를 준수하는데 처리가 필요한 경우 • 정보 주체 또는 사용자인 제3자의 생명상의 이익을 보호하기 위하여 처리가 필요한 경우 • 공익상의 이유 또는 컨트롤러에 부여된 직무권한을 행사할 때 처리가 필요한 경우 • 컨트롤러 또는 제3자의 적법한 이익을 달성하기 위하여 처리가 필요한 경우

11) https://gdpr.kisa.or.kr/gdpr/bbs/selectArticleDetail.do?bbsId=BBSMSTR_000000000101&nttId=758

○ CCPA(California Consumer Privacy Act)[12)]

- CCPA는 미국 캘리포니아 소비자 프라이버시 보호법으로 2020년 7월 1일부터 시행됨. 글로벌 IT 기업이 다수 위치한 실리콘 밸리가 있는 캘리포니아에서 시행하는 주법(state law)으로 캘리포니아 주민들에게 본인의 개인정보에 대한 강화된 통제권을 부여함
- CCPA는 투명성, 프라이버시 통제, 책임성을 강조하고 있으며, 열람권, 삭제권, 판매거부권 등 정보 주체 권리를 보장함

※ CCPA의 적용 범위 및 대상은 다음과 같음

[표 18] CCPA 적용 범위 및 대상

• **(캘리포니아에서 사업을 영위)** CCPA는 사업자가 지리적으로 캘리포니아에 존재하지 않더라도 캘리포니아 주민의 개인정보를 수집, 판매 등 처리하는 경우에 적용됨. 공동 브랜드를 공유하는 모회사 또는 자회사가 캘리포니아 주민의 개인정보를 처리하는 때도 CCPA가 적용되지만, 캘리포니아 기업이라도 모든 상업적 활동이 캘리포니아 밖에서만 이루어진 경우 CCPA가 적용되지 않음
• **(소비자)** CCPA에서 정의하는 소비자는 고유식별자에 의해서 식별되는 캘리포니아 주민임. 물건을 구매하는 사람뿐만 아니라 모든 근로자, 협력업체 또는 공급업체 임직원, 개인사업자 등도 소비자에 포함됨
• **(개인정보)** CCPA에서 정의하는 개인정보는 “직・간접적으로 특정 소비자 또는 가계(household)를 식별 또는 설명하거나, 특정 소비자 또는 가계와 관련되어 있거나, 연관될 수 있거나, 합리적으로 연결될 수 있는 정보”로 정의함
• **(일정 규모 이상의 영리 사업자)** 일정 규모 이상의 영리 사업자: 사업자란 (1) 캘리포니아에서 영리를 목적으로 사업을 경영하는 자로서 (2) 주민의 개인정보를 직접 또는 타인을 통해 수집하고 (3) 단독 또는 다른 사업자와 공동으로 개인정보 처리의 목적과 방법을 결정하는 (4) 개인회사, 조합, 유한회사, 법인, 협회 그 밖의 법률 주체를 의미함. 즉, 비영리 단체나 법인, 주 또는 지방정부는 사업자에 해당하지 않음. 단, 실리콘밸리 스타트업 등 소규모 사업자 보호를 위해 일정 요건을 충족한 사업자에게만 적용됨

○ 영지식 증명은 사용자의 프라이버시를 보호하면서도 필요한 검증을 가능하게 하는 효과적인 수단으로, 디지털 신원, 금융 거래, 개인정보 관리 등 다양한 분야에서 그 중요성이 점점 더 커지고 있음

12) https://privacy.naver.com/download/NAVER_CCPA_Guideline.pdf

○ 영지식 증명을 통해 개인 데이터의 프라이버시를 보호할 수 있다는 점에서 디지털 권리장전 제4장 제19조를 만족할 수 있음. 그뿐만 아니라, 데이터 주권이 데이터 소유자 개인에게 부여되고, 이는 디지털 권리장전 제2장 제9조를 만족할 수 있음

○ 또한, 영지식 증명은 국제적인 정책을 만족할 수 있음. 영지식 증명을 통해 개인 데이터에 대해 최소한으로 공개할 수 있으므로 GDPR의 개인정보 최소처리 원칙을 만족할 수 있으며, 영지식 증명 검증으로 무결성과 기밀성의 원칙을 기술적으로 만족할 수 있음. 미국의 CCPA에서 요구하는 프라이버시 통제를 만족함. 영지식 증명 기술을 통해 데이터 주권을 개인에게 부여할 수 있으므로 삭제권, 판매거부권 등의 정보 주체 권리를 보장할 수 있음

○ 이처럼 영지식 증명은 블록체인 기술의 발전과 함께 디지털 권리 보호에 대한 새로운 접근 방식을 제공하며, 높아지는 각국의 프라이버시 요구수준을 만족할 수 있는 주요한 기술로 자리매김할 수 있을 것으로 보임. 영지식 증명은 궁극적으로 데이터 사회에서 사용자의 권리와 안전을 강화하는 데 이바지할 것임

제4절. 영지식 증명 국제 표준 및 라이브러리 조사

1. 영지식 증명 국제 표준 현황 조사

○ 영지식 증명 국제 표준 현황

- 영지식 증명 분야는 1985년 Shafi Goldwasser 등에 의해 처음 소개된 개념으로, 그 역사가 비교적 길지 않아 표준화 작업 등에 대한 논의가 부재했음
- 근래 개인정보 보호에 대한 요구 증가와 블록체인의 트릴레마 해결 기술로 주목받음에 따라 표준화 논의 진행됨
- 2018년 ZKProof Standards의 운영위원회가 발촉되어 최초로 영지식 증명과 관련된 표준화 작업을 시작함

○ ZKProof Standards

- ZKProof standard는 국제 유일 영지식 증명 기술을 표준화하는 단체로 Shafi Goldwasser 등을 비롯해 미국 스탠포드 대학의 Dan Boneh 교수, UC 버클리의 Alessandro Chiesa 교수 등이 위원회를 구성
- 또한, 딜로이트, 이더리움 재단, ING, 마이크로소프트, 구글 등 다양한 국제 유수 기업이 파트너로 참여하고 있음
- ZKProof Standards는 매년 워크숍을 개최해 영지식 증명 표준화 기고문을 전 세계 학자, 기업에서 받고 있으며, 그중 일부를 채택하여 표준 문서에 추가, 혹은 추가를 위한 논의를 진행함
- 특히, 다양한 Working Group(WG)을 구성하여 매년 활발하게 표준화 활동을 지속적으로 진행함
- 2023년 기준으로, Plonkish Constraint System, Fiat-Shamir Compiler, Sigma Protocol에 대한 WG를 구성함

[표 19] ZKProof Standards 주요 연혁

일자	내용
2023.11.30.	ZKProof Policy 개최
2023.08.02.	5.5th ZKProof Standards Workshop 개최
2022.11.15.	5th ZKProof Standards Workshop 개최
2022.07.17.	ZKProof Community Reference Version 0.3 발간
2021.04.19.	4th ZKProof Standards Workshop 개최
2020.04.20.	3rd ZKProof Standards Workshop 개최
2019.12.31.	ZKProof Community Reference Version 0.2 발간
2019.10.28.	ZKProof Community Event Amsterdam 개최

일자	내용
2019.04.11.	ZKProof Community Reference Version 0.1 발간
2019.04.10.	2nd ZKProof Standards Workshop 개최
2018.05.10.	1st ZKProof Standards Workshop 개최
2018.01.31	ZKProof Standards 운영위원회 발족

[그림 27] 제5회 ZKProof Standard 워크샵

○ ZKProof standard 내 영지식 증명 구현 기술

- ZKProof standard는 표준화 작업을 진행 중으로 1.0 버전이 아직 발간되지 않음. 따라서, 보고서 작성 시점에서 최신 문서인 0.3 버전을 참조하여 작성됨
- ZKProof standard는 영지식 증명의 프론트엔드와 백엔드 구현 기술, API와 파일 포맷, 벤치마크 등을 다루고 있음. 각각에 대해 고려사항 등을 기술하고 있음
- (백엔드) 영지식 증명의 백엔드 시스템은 R1CS/QAP 등으로 표현될 수 있는 산술 회로, 논리 회로에 대한 증명 시스템임. 논문 등에서 제안하는 시스템의 산술 연산, 직렬화 포맷, 테스트, 벤치마크 등으로 구성

[표 20] 벡엔드 구현 시 고려사항

① 알고리즘의 안전성과 가정
② 점근적 성능
③ 정밀 성능
④ 프로그래밍 언어와 API 종류
⑤ 지원 플랫폼
⑥ 오픈 소스 가용성
⑦ 사용자와 유지보수 자의 커뮤니티
⑧ 감사와 검증 등을 통한 구현체의 정확성과 건전성
⑨ 응용 어플리케이션

- (프론트엔드) 영지식 증명의 프론트엔드 시스템은 Statement를 편리한 언어로 표현할 수 있는 수단과 저수준 표현 식으로 컴파일하고 적절한 백엔드를 호출함으로써 영지식 상태로 진술을 증명하는 수단을 제공. 프론트엔드 선택 시 고려사항은 다음과 같음

[표 21] 프론트엔드 선택 시 고려사항

• Statement 표현을 위한 고수준 언어 명세
• 고수준 언어로 표현된 관계식을 적절한 백엔드를 위한 저수준 언어로 컴파일 해주는 컴파일러
• 고수준 인스턴스를 저수준으로 변환(R1CS 인스턴스 변수 할당 등)
• 고수준 witness를 저수준으로 변환(witness 변수 할당 등)
• 가젯 라이브러리

- (API) API 디자인은 아직 표준화 작업 진행 중임. 파일 포맷은 R1CS에 관해서만 기술함
- (벤치마크) 싱글 스레드에서의 증명자/검증자 수행시간과 증명 크기 등을 포함한 통신 복잡도(Communication complexity)를 측정 항목으로 제시. 권장 항목은 다음과 같음

[표 22] 벤치마크 권장 항목

- 병렬 가능(Parallelizability)
- 일괄 처리(Batching)
- 메모리 사용량
- 연산 수행 수(Filed 연산, multi-exponentiation, FFT 등)
- 디스크 사용량/저장 장치 요구 사항
- 크로스오버 포인트: 계산 수행보다 검증이 더 빨라지는 시점
- 가장 큰 인스턴스
- Witness 생성
- 측정 항목 간 상충 점(Trade-off)

2. 영지식 증명 라이브러리 현황 조사

○ **(회로구현)** 영지식 증명 회로구현은 작성 언어에 따라 다양하게 존재함.

- 대표적인 회로 작성 라이브러리는 다음과 같음

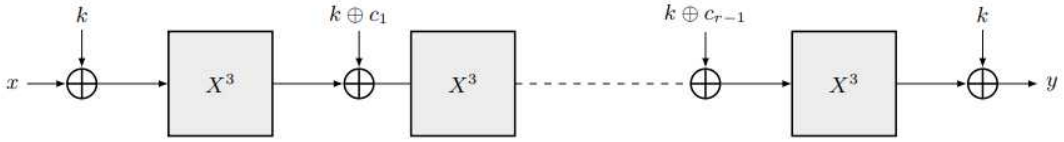
[표 23] 대표적인 회로 작성 라이브러리

라이브러리명	설명	라이브러리 주소
bellman	sampling-crypto 내 다양한 가젯이 있는 Rust 기반 회로 작성 라이브러리	https://github.com/zkcrypto/bellman
libsnark	전처리 zk-SNARKs를 위한 회로 작성 라이브러리로 C++로 작성	https://github.com/scipr-lab/libsnark
jsnark	전처리 기반 회로 작성 라이브러리로 Java로 작성	https://github.com/akosba/jsnark
ZoKrates	이더리움 상 zk-SNARKs를 위한 툴박스로 Rust로 작성	https://github.com/Zokrates/ZoKrates
Snarky	Ocaml으로 작성된 R1CS SNARKs 작성을 위한 프론트엔드	https://github.com/o1-labs/snarky
Circom	JavaScript 기반의 R1CS SNARKs 작성을 위한 언어	https://github.com/iden3/circom
Circomlib	Circom을 위한 기초 회로 라이브러리	https://github.com/iden3/circomlib
ZEXE SNARK Gadget	회로 생성을 위한 모듈로 Rust 기반으로 작성.	https://github.com/arkworks-rs/snark
ZkVM	Bulletproof R1CS 증명 생성을 위한 스마트 컨트랙트 작성 언어로 Rust 기반	https://github.com/stellar/slingshot/tree/main/zkvm

○ **(해시 함수)** 영지식 증명 회로 내에서 해시 함수를 많이 사용하며 기존 SHA-2 등의 해시 함수를 영지식 증명 회로 내에서 연산 수행 시 비트 연산 등으로 인해 증명 생성 시간에 부하를 줌. SHA-2의 경우 회로 내 1회 수행 시 약 25,000개의 constraint number를 발생시킴

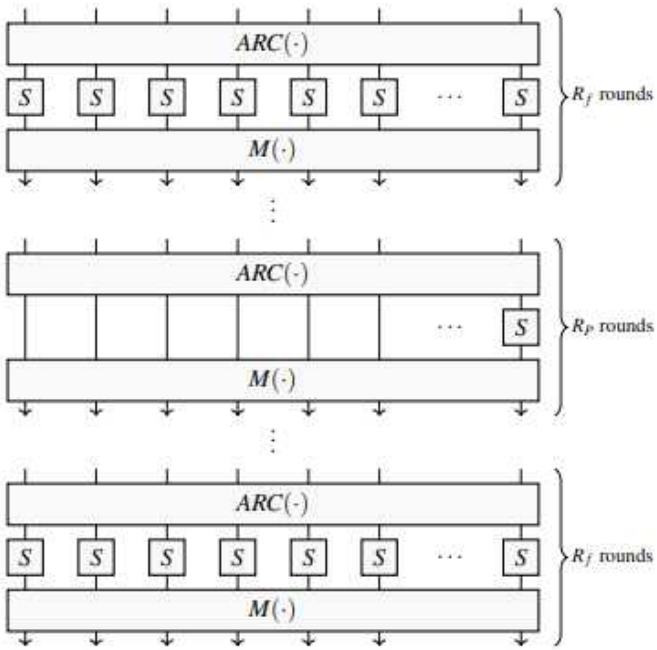
이에 회로 내에서 연산량을 적게 소모하는(constraint number를 적게 발생시키는) SNARK 친화 해시 함수가 개발됨. 논문으로 발표된 SNARK 친화 해시 함수의 경우 구현체에서 자주 활용되는 MiMC, Poseidon 등이 있음. 대표적인 SNARK 친화 해시 함수는 다음과 같음. MiMC와 Poseidon 모두 공통으로 SNARK 회로 내에서 해시 함수 연산 수행 부하를 줄여 constraint 개수를 줄임, 즉 증명자의 증명 생성 시간 단축에 이바지함

- MiMC: 최초의 SNARK 친화 해시 함수로 ASIACRYPT 2016에서 소개. 간단한 $F(x) := x^3$ 함수가 키 덧셈과 함께 반복 수행됨. 곱셈 연산이 2번($x \cdot x, x^2 \cdot x$)으로 라운드 당 constraint 개수가 2개로 효율적임([그림 28] 참조)



[그림 28] MiMC 해시 함수 연산 구조

- Poseidon: Poseidon은 USENIX 2021에 소개된 SNARK 친화 해시 함수로 SPN (Substitution-Permutation Network) 기반 HADES 디자인을 토대로 설계됨. 라운드마다 라운드 상수를 더하고 S-box라는 함수를 수행하고 레이어를 섞음([그림 29] 참조). S-box 함수 연산이 x^α로 정의됨[13]. α가 5일 경우, 3개의 constraint가 발생함($x \cdot x, x^2 \cdot x^2, x^4 \cdot x$)



[그림 29] Poseidon 해시 함수 연산 구조

13) α는 전체 라운드 횟수 p에 대해 p-1과 최대공약수가 1임을 만족하는 3보다 크거나 같은 가장 작은 양수.

제 3 장. 영지식 증명 서비스 국내·외 사례조사 및 기대효과

○ 영지식 증명을 활용한 블록체인 서비스는 특히 신뢰도 측면에서 크게 요구됨. 영지식 증명과 블록체인을 융합함으로써 이용자 보호와 데이터 무결성으로부터 비롯되는 서비스의 신뢰도 향상 측면을 기대할 수 있음. 이에 3장은 강한 신뢰도가 요구되는 서비스들을 중심으로 소개함

- 전자투표: 전자투표의 경우 영지식 증명을 활용한 가장 효과적인 서비스 중의 하나임. 비밀 선거 보장을 하여 이용자(유권자) 보호와 투표 결과의 무결성 등을 통해 투표 조작 논란에서 벗어날 수 있음
- 전자 신원 인증: 전자 신원 인증은 대표적인 블록체인 응용 서비스 중 하나임. 하지만, 현존 전자 신원 인증의 대부분은 프라이버시 보장 수준이 완전하지 않음. 특히, 상황에 따라 인증해야 하는 내용이 다르고, 모든 개인정보를 공개할 필요가 없으므로 영지식 증명을 통해 일부, 즉 선택적 공개를 하여 최대한의 프라이버시를 보장할 수 있음
- 중앙은행 디지털화폐(CBDC): CBDC는 자산, 정보에 대한 프라이버시 보장을 통한 경제 주체 보호와 악의적 금융 행위 규제(AML, CFT 등)의 2가지 큰 필요조건이 상충함[14]. 전술한 조건을 동시에 만족하기 위해 영지식 증명을 기반으로 합법적 수준에서 CBDC 추적, 감사를 할 수 있음
- 디지털 지갑: 디지털 지갑은 디지털 자산 거래뿐만 아니라, 지갑 소유자의 자격 인증, 문서 보관 서비스 등 종합 플랫폼으로써 자리 잡음. 사용자로서는 금융/개인정보 등이 일원화되어 편의성이 증진되나, 개인정보 유출로 인한 광범위한 피해로 이어질 수 있어 고수준의 개인정보 보호가 요구됨
- 공급망 관리 시스템: 공급망 관리 시스템에 영지식 증명을 적용하면, 기업은 내부 기밀 정보를 공개하지 않으면서도 제공 상품의 무결성을 보장할 수 있음. 소비자는 이를 통해 구매한 상품에 대한 정품 인증 등이 가능하여, 궁극적으로 공급망 전체에 신뢰도를 확보할 수 있음

14) 미국 백악관 보고서는 (The White House, 2022, Technical Evaluation for a U.S. Central Bank Digital Currency System, pp. 11) 설계 시 고려 가능한 기술적 요소 18개에 따른 각각의 장단점을 소개하고 있음. 특히, 설계론에 따라 악의적 금융 행위 규제 준수와 경제 주체 보호 측면이 절충됨.

제1절. 전자투표

1. 사례 조사

○ Privacy and verifiability in voting systems: methods, developments and trends[JMP13]에서는 안전한 온라인 투표 시스템을 위한 고려사항이 기술되어 있음. 크게 프라이버시와 검증 가능성으로 분류되며 자세한 고려사항은 다음과 같음

[표 24] 안전한 온라인 투표 시스템을 위한 고려사항

구분	고려사항	설명
프라이버시	투표 프라이버시	투표에서 유권자의 선택이 드러나서는 안 됨
	영수증 무정보성	유권자는 자신이 어떻게 투표했는지 다른 사람에게 증명할 수 없어야 함
	강압 저항성	유권자는 어떤 강압에도 본인이 하고 싶은 투표를 할 수 있어야 함. 강압 저항성을 만족한다면 투표 프라이버시와 영수증 무정보성을 만족함
	유권자 익명성	투표에서 유권자의 정보가 드러나서는 안 됨
검증 가능성	개별 검증성	유권자는 자신의 투표가 투표함에 잘 반영되었는지 검증할 수 있어야 함
	전체 검증성	누구든지 개표 결과가 모든 투표를 집계한 결과임을 검증할 수 있어야 함
	종단 간 검증성	유권자는 본인의 투표가 본인이 원한대로 만들어지는지, 투표함에 기록되고 개표 결과에 포함되었음을 검증할 수 있어야 함. 개별 검증성과 전체 검증성을 만족하면 종단간 검증성을 만족함
	자격 검증성	투표가 적법한 유권자로부터 만들어졌음을 누구나 검증할 수 있어야 함

○ 국내 사례 조사 및 분석

- 지케이보팅은 국내 영지식 증명 기반 블록체인 프라이버시/확장성 솔루션 제공 기업인 ㈜지크립토가 개발한 공개 블록체인 기반 온라인 비밀 투표 서비스임
- 지케이보팅은 미국 소비자 기술협회(CTA, Consumer Technology Association)에서 주관하는 국제전자제품박람회 CES 2023(Consumer Electronics Show)에서 최고 혁신상(분야: 사이버 보안 & 개인정보 보호)과 혁신상(분야: 소프트웨어 & 모바일 어플리케이션) 또한 CES 2024에서 최고 혁신상(분

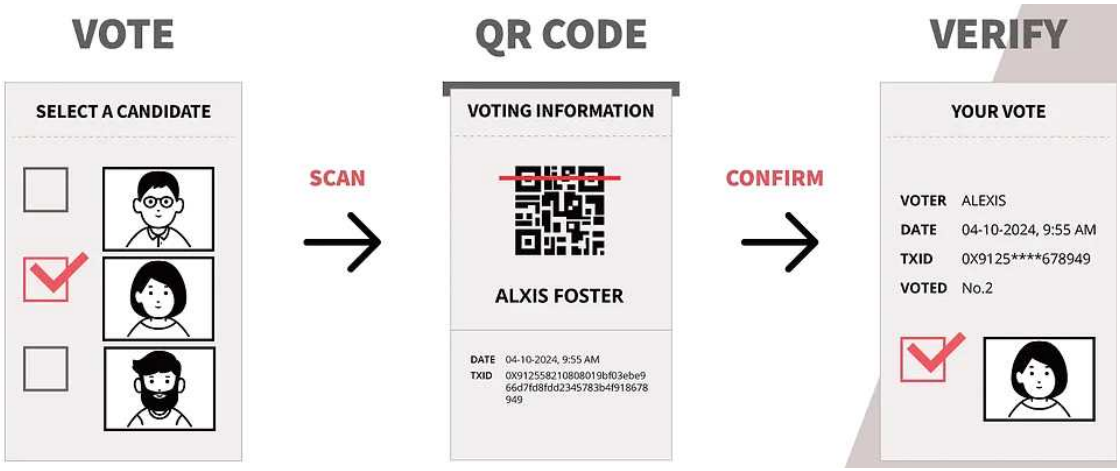
야: 사이버 보안 & 개인정보 보호)을 2년 연속 수상함

- 또한, 2023년 중앙 선거 관리 위원회의 블록체인 온라인 투표 서비스로 채택되어 2024년부터 공공 분야 투표로 활용 예정인 서비스임
- 지케이보팅은 zk-SNARK 기술을 활용해 투표자에 대한 익명성과 암호화된 투표의 정당성을 동시에 보장함

[표 25] 지케이보팅 투표 단계

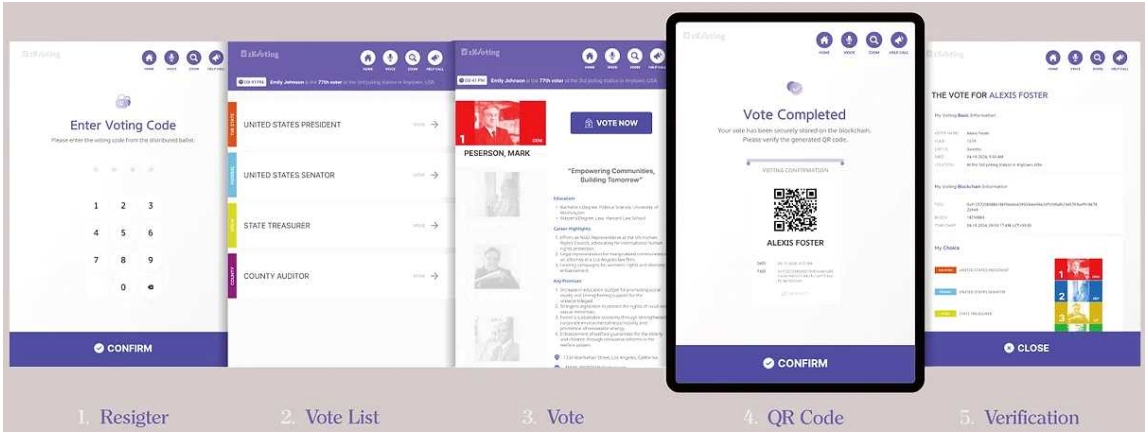
단계	내용
선거 준비 단계	• 선거 관리인이 유권자 정보를 포함하여 투표 개설 • 유권자가 특별한 공개키 알고리즘을 통해 생성된 공개키를 선거 관리인에게 제공함으로써 유권자 등록
투표 단계	• 유권자는 투표를 수행하는 기기(개인 휴대 전화 등)에서 암호화된 투표와 해당 투표의 정당성에 대한 영지식 증명 생성 • 암호화된 투표와 영지식 증명을 공개 블록체인에 업로드 • 유권자는 자신의 투표가 잘 등록되었는지 공개 블록체인을 통해 확인 가능
투표 종료 단계	• 선거 관리인은 분산화된 복호화키를 취합하여 암호화된 투표들을 복호화하여 개표 진행 • 선거 관리인은 최종 개표 결과가 암호화된 투표들의 합의 복호화 결과와 같다는 영지식 증명 생성 • 이를 통해 누구나 개표 결과의 정당성을 공개적으로 검증 가능

- 투표소용 지케이보팅(zkVoting at the poll station)은 영지식 증명을 활용한 블록체인 기반 대면 투표 시스템임. 유권자는 투표소에서 실시간으로 투표용지가 정확하게 기표가 되었는지 확인할 수 있음



[그림 30] QR 코드를 이용한 검증 방식

- 유권자는 투표소에서 QR 코드를 이용한 이중 인증 절차를 통해 투표용지 제출을 확인할 수 있음. 이 과정을 통해 사용자는 자신의 투표가 블록체인에 정확하게 저장되고 자신이 선택한 후보자에게 올바르게 배분되었음을 확인할 수 있음
- 투표 단말기와 분리된 전용 인증 장치를 도입해 보안을 강화함. 디바이스 테스터는 '가짜 키'를 사용해 모의 투표를 진행하며 디바이스의 적법성을 검증할 수 있음. 누구나 단말기 테스터가 될 수 있으므로 단말기 진위를 보편적으로 검증할 수 있음
- 독립적인 모바일 기기로 이러한 모의 투표를 검증할 수 있어 투표 및 검증 기기의 조작을 방지하는 교차 검증이 가능함. 암호 해독 단계에서는 가짜 투표를 식별하고 걸러내어 투표 집계 결과의 무결성과 보안을 보장함
- 투표 장치와 검증 장치를 분리하면 변조 방지 보안이 한 층 더 강화되며 이 설정을 통해 검증 장치는 부정확하거나 손상된 기계와 같은 불일치를 식별하고 의심스러운 투표용지를 무효로 할 수 있음



[그림 31] 투표소용 지케이보팅의 과정

○ 해외 사례 조사 및 분석

- VoteAgain[LQT20]

※ 유권자는 어떠한 강압에도 본인이 하고 싶은 투표를 할 수 있는 특징인 강압 저항성을 만족함

※ 영지식 증명을 사용하여 종단간 검증성을 보장하여 유권자는 본인의 투표가 본인이 원한대로 만들어지는지, 투표함에 기록되고 개표 결과에 포함되었음을 검증할 수 있음

※ 하지만 유권자 익명성을 만족하지 못하여 관리자는 투표자가 누구인지 알 수 있으며 자격 검증성을 만족하지 못하여 투표가 적법한 유권자로부터 만들어졌음을 증명할 수 없음

- Provotum[KRS+20]

※ 블록체인과 영지식 증명을 사용한 투표 시스템으로, 유권자는 본인의 투표가 본인이 원한대로 만들어지는지, 투표함에 기록되고 개표 결과에 포함되었음을 검증할 수 있어 종단간 검증성을 만족

※ 투표가 적법한 유권자로부터 만들어졌음을 증명할 수 있어 자격 검증성을 만족함

※ 투표는 유권자의 선택을 드러내지 않아 투표 비밀성은 만족하지만, 관리자는 투표자가 누구인지 알 수 있어 유권자 익명성은 만족하지 않으며 강압 저항성을 만족하지 못함

2. 기대 효과

○ 기술적 기대효과

- 영지식 증명 기반 공개 블록체인 전자투표는 전자투표에 프라이버시를 보장하여 최초로 블록체인 기반 전자투표에서 기존 투표의 특성을 모두 만족시키는 기술 선점 가능
- 블록체인에서 발생하는 투명성과 프라이버시 보장이라는 상충하는 특성을 영지식 증명을 통해 유권자 투표 데이터의 무결성을 보장하면서도 유권자의 프라이버시를 보장 가능

○ 경제적 기대효과

- 투표 진행 과정, 개표에 대한 공개 검증을 누구나 할 수 있어, 부정 투표에 대한 의혹을 해소하고, 이로 인해 발생할 수 있는 사회적 비용을 감소
- 오프라인 투표 진행 대비 운영 비용 등에서 투표 진행 비용 절감

○ 사회적 기대효과

- 투표 불신 문제를 해소하여 오프라인 투표에서 안전한 전자투표로의 전환을 유도할 수 있음
- 투표에 대한 신뢰도를 높여 투표율을 높일 수 있고, 이는 유의미한 결과 도출을 끌어낼 수 있음. 특히, 여론 조사, 주민 선호도 조사 등의 의견 수집형 투표에서 양질의 결과를 산출할 수 있음
- 오프라인 투표 여건이 어려운 유권자에게도 투표할 수 있는 환경을 제공하여 대의민주주의 실현에 이바지할 수 있음

제2절. 전자 신원 인증

1. 사례 조사

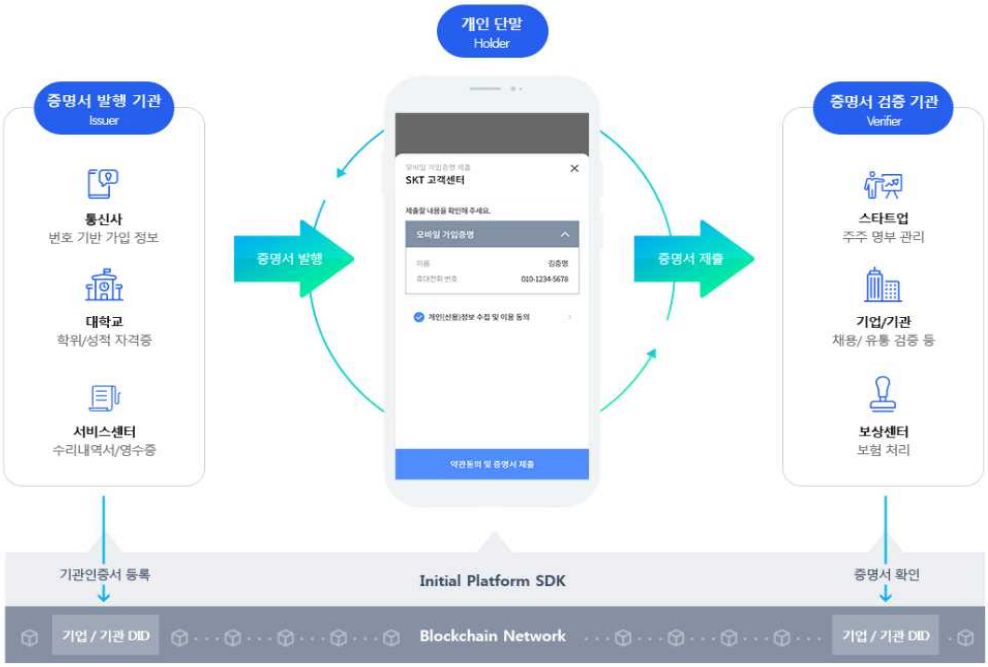
○ 국내 사례 조사 및 분석

- 모바일 운전면허증 : 모바일 운전면허증은 행정안전부에서 발행하는 전자 신원으로, 기존의 운전면허증과 같은 효력을 가짐
- 모바일 운전면허증은 스마트폰 애플리케이션을 통해 제공되며, 이를 통해 사용자는 실제 플라스틱 카드를 소지하지 않고도 자신의 운전면허증을 제시할 수 있음
- 블록체인 기술(DID)을 사용하여 개인정보를 보호하고, 위조나 도용을 방지함. QR 코드를 통해 개인정보를 검증받거나 검증할 수 있음

[그림 32] 모바일 운전면허증

- 대한민국 정부는 모바일 운전면허증을 법적으로 유효한 신분증으로 인정하며, 이는 경찰이나 다른 공공기관에서 신분 확인 수단으로 사용될 수 있음
- 일상생활에서의 신분 확인뿐만 아니라, 은행 업무나 공항 보안 검사 등에서도 사용될 수 있으며 점차 사용처가 늘어가는 중임

- 코로나 19 전자 예방접종 증명(COOV) : COOV는 질병관리청에서 운영하는 서비스로, 코로나 19의 예방접종 여부를 증명할 때 사용될 뿐 아니라 성인 인증과 같은 다양한 인증 시스템으로 활용할 수 있는 서비스임
- COOV는 블록체인 기반의 코로나 19 예방접종 인증 시스템으로, 대한민국 질병관리청과 블록체인랩스가 함께 개발함. 질병관리청, 보건복지부, 행정안전부 국가정보자원관리원, 한국보건의료원이 5개 노드를 구성하여 운영됨. 질병관리청은 코로나 19 예방접종을 받은 시민의 개인 키로 서명·암호화한 전자 예방접종 증명서를 발급한 다음 그 시민의 공개키를 블록체인에 기록함. 공개키 이외의 정보는 블록체인에 기록되지 않으므로 개인정보 유출의 위험이 적음. 예방접종 증명서를 발급받은 시민은 증명서를 제시하기 위해 모바일 QR 코드 애플리케이션을 사용하며, DID 기술을 기반으로 증명서의 진위를 확인하는 검증자가 QR 코드를 제시한 스마트폰과 통신해 접종 관련 최소 정보만을 확인하게 됨
- 이니셜은 SKT Enterprise에서 개발한 전자 신원으로, 통신사/대학교/서비스센터 등에서 발급한 증명서를 개인 단말에 저장한 뒤 증명서 검증 기관에 이를 온라인으로 제출할 수 있도록 만든 서비스임
- SKT는 2019년에 KT, LG 유플러스, 삼성전자 등과 함께 '이니셜 얼라이언스'라는 컨소시엄을 구축하고, 다음 해인 2020년에 DID 서비스 애플리케이션 '이니셜(initial)'을 출시함. '이니셜'은 SKT의 하이퍼레저를 기반으로 한 컨소시엄 블록체인 플랫폼인 '스톤'의 네트워크를 통해 노드를 운영함
- 이니셜 서비스의 주요 특징을 살펴보면 다음과 같음. 먼저 PKI 인프라 기반 인증서를 활용하여, 사용자가 아이디와 패스워드 없이 간편하게 로그인할 수 있게 됨. 그리고 단일 DID로 여러 사이트를 접속했을 때 발생 가능한 프라이버시 이슈를 방지하기 위해 서로 다른 서비스에 접속할 시, 서로 다른 DID가 생성됨. 또한, 개인 발급받은 DID와 증명서에 대한 정보는 블록체인에 저장되지 않고 개인 단말기에만 저장되고, 발급받은 증명서 데이터 중 사용자가 선택한 정보만 제출할 수 있도록 하여 개인의 데이터 주권(Self-sovereign)을 보장함



[그림 33] 이니셜 서비스 개요도

○ 해외 사례 조사 및 분석

- EU EBSI(European Blockchain Service Infrastructure)

※ EBSI는 유럽 위원회(European Commission)와 유럽 블록체인 파트너십(European Blockchain Partnership)의 주도로, 유럽 전역에 분산된 노드로 연결된 블록체인 네트워크를 공공 서비스로 제공하여 EU 정책과 규제를 준수하면서 보안과 지속 가능성 측면에서 시민과 기업에 국경 너머의 공공 서비스와 정부 또는 공공기관의 협력을 증진하고자 함. 이를 통해 범유럽 디지털 인프라 핵심 표준 확보 및 블록체인 기반 공공 서비스 제공을 목표로 함

※ 유럽 진행위원회의 유럽 블록체인 파트너십(European Blockchain Partnership, 이하 EBP)에서 추진하여 노르웨이, 리히텐슈타인 등 총 29개국이 참여함. EBP 회원국을 중심으로 블록체인 노드 등 인프라 구축과 4개 분야 블록체인 공공 서비스(감사목적 문서 공증, 졸업증명서 인증, EU 자기 주도 신원 인증 프레임워크, 신뢰할 수 있는 데이터 공유)를 제공함. EU 각 회원국이 국가 단위에서 자체적인 EBSI 노드를 운영하고, 노드가 분산원장 업데이트와 거래 생성 및 전송하는 기능을 수행하도록 구성됨

※ 자기 주권 신원: EBSI는 검증 가능 인증(Verifiable Credential)을 지원함.

EBSI는 특히 신원 증명 및 인증에 대한 용례를 확인하였는데, 신원 인증 사례에는 실시간 폐기 기능을 지원해야 함

※ EBSI의 프레임워크는 모듈식 폐기 방식을 지원함. 모듈식 폐기 방식의 경우 여러 가지 폐기 방식을 VC의 용도와 목적에 따라 적합한 폐기 방식을 선택하는 것임. EBSI는 VC 폐기 시 고려해야 할 사항으로 크게 3가지 기준을 제시함

[표 26] EBSI 보고서 내 VC 폐기 시 고려사항

출처	내용
프라이버시	제3자와 공유되는 폐기 상태 기록은 개인의 고유한 식별자로 구성되면 안 됨.
삭제 & 관리	GDPR을 준수하기 위해, 발급자는 인증서의 수정, 삭제 등의 관리가 가능해야 하며, 인증서 소유자가 그들의 상태 정보 공유를 스스로 관리할 수 있어야 함
확장성	프라이버시와 삭제&관리를 만족하기 위해 기술적으로 복잡해지지만, 확장성도 고려해야 함

※ 문서 공증: 문서의 진위 및 무결성을 보장하는 검증 기능 제공하여 데이터 또는 문서의 변화를 추적함. 신뢰 되는 디지털 감사 개체를 만들어 규정 준수 확인(Compliance check)을 자동화하고 데이터 무결성을 보장하는 서비스임

※ 학위증명: 학위증서 또는 자격 증명을 개시하는 것과 같이 증명서를 관리할 때 모바일 이용자들이 디지털 신원을 인증하는 비용을 줄이고 신뢰성을 향상하는 서비스를 제공함. 이를 통해 대학교 졸업증명서를 VC (Verifiable Credentials) 형태로 사용자에게 발행하고, 검증할 수 있는 기능을 지원함

※ 지적 재산권(Intellectual Property) 관리: 지적 재산의 관리 및 권리 보유자를 확인하는 서비스임

- Pan-Canadian Trust Framework(PCTF)

※ PCTF는 캐나다에서 디지털 신원 생태계를 조성하기 위해 개발된 일련의 원칙과 가이드라인임. 이 프레임워크는 캐나다인이 안전하고 편리하게 온라인 서비스를 이용할 수 있도록 지원하며, 서비스 제공업체와 개인의 신원에 대한 검증을 목표로 함

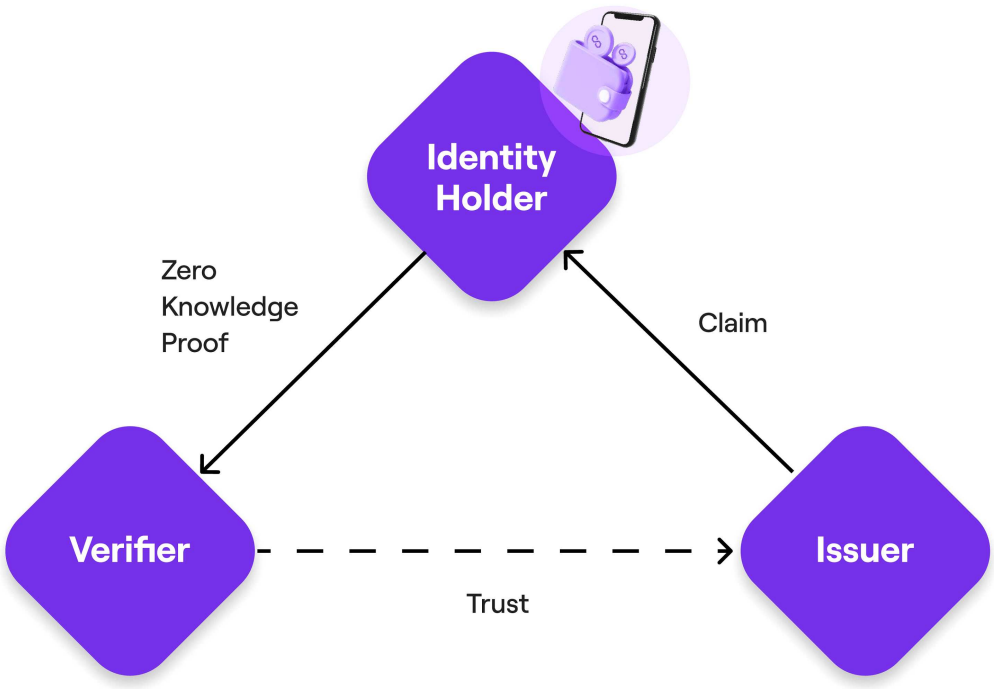
※ PCTF는 캐나다의 정부, 의료, 금융 등이 포함된 다양한 관할권 및 부문에서 디지털 신원 확인에 대한 접근 방식을 표준화하기 위해 개발됨

※ 프레임워크는 일반적으로 거버넌스, 기술 표준, 개인정보 보호, 보안, 상호운용성과 같은 구성요소로 이루어져 있으며 이러한 구성요소는 디지털 ID 시스템이 강력하고 안전하며 사용자 친화적임

※ PCTF의 주요 목표 중 하나는 서로 다른 시스템과 관할권 간의 상호운용성을 보장하는 것임. 이는 한 주에서 확인된 디지털 신원이 다른 주에서도 인정될 수 있음

○ 전자 신원 인증 영지식 증명 적용 내용

- (신원 확인) CL 서명 기반의 DID 2.0을 통해 개인 신원에 대한 선택적 공개가 가능하여 그 외 불필요한 정보에 대한 프라이버시를 보호함
- (전자신분증 관리) 영지식 증명 적용을 통한 프라이버시 보장 신원 확인 기술을 토대로, 전자신분증 발급자는 영지식 증명 체계를 구축함. 이에 따라, 전자신분증 자격 검증을 할 때는 선택적 공개를 가능하게 하며, 사용자가 개인 전자신분증 저장 및 관리를 자율적으로 선택하여 사용할 수 있음



[그림 34] 영지식 증명을 이용한 Polygon ID

2. 기대 효과

○ 기술적 기대효과

- 분산 신원 인증 기술의 경우 데이터 주권이 개인에게로 부여되면서 개인정보 관리 부담이 개인에게 지워짐. 영지식 증명 기반 분산 신원 인증의 경우 선택적 공개가 가능하여 사용자 편의에 따라 공개하고 싶은 정보만 공개할 수 있음
- 영지식 증명 분산 신원 인증의 표준화 선점 가능
- 신원 인증에 대한 증명 크기를 최소화하여 통신 비용을 줄이고, 검증에 드는 비용을 절감할 수 있음

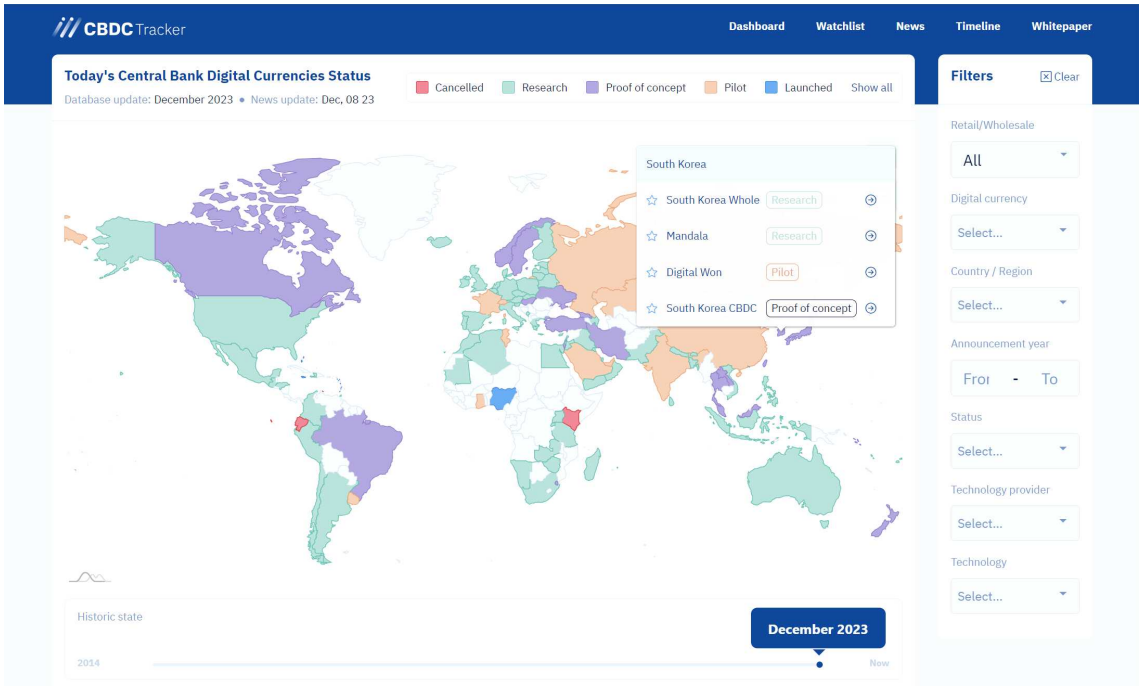
○ 경제적 기대효과

- 영지식 증명 분산 신원 인증 서비스를 통해 각 기관별로 다른 인증서 포맷의 표준화를 추구할 수 있음. 또한, 관리 주체가 발급 기관에서 인증서 소유주인 개인에게로 이동하면서, 각 기관에서 인증서 관리에 드는 비용을 절감할 수 있음
- 각 기관별로 필요하면 매번 발급하던 기존의 신원 인증 서비스와 달리 분산 신원 인증 서비스는 본인의 인증서를 공개 분장에 저장하여 관리하기 때문에, 유효 기간 내에서 발급을 1회만 한다는 편의성을 제공함. 이런 편의성은 발급에 드는 유형적 비용뿐만 아니라, 시간 등의 무형적 비용을 절감하는 효과를 제공함
- 기존 신원 인증 서비스를 대체할 뿐만 아니라 기존 대비 이점을 제공함으로써 블록체인 산업의 연착륙에 이바지할 수 있음

○ 사회적 기대효과

- 데이터 주권이 신원 인증서 소유주 본인에게 부여되어 인증서 관리에 대한 신뢰 문제를 해결할 수 있음
- 인증서가 블록체인에 등록되어 누구든 공개 검증할 수 있으므로 신원에 대한 위변조로부터 야기될 수 있는 사칭, 학력 위조 등의 잠재적 문제를 예방하는 효과를 가짐
- 궁극적으로 자격 증명 등의 신원 인증 응용 서비스에 대한 전반적인 신뢰 구축 달성이 기대됨

제3절. 중앙은행 디지털화폐(CBDC)



[그림 35] 나라별 CBDC 개발 현황을 조회하는 사이트(cbdctracker.org)

○ CBDC(Central Bank Digital Currency)는 중앙은행이 발행하는 디지털 형태의 화폐로 기존 가상자산과 전자적 형태로 저장된다는 공통점을 갖지만, 관리 주체가 각국의 중앙은행으로 화폐 발행에 대한 보증이 가능하다는 점에서 차이를 지님

○ CBDC는 사용 주체에 따라 범용(Retail/General purpose)과 기관용(Wholesale) CBDC로 구분됨. 범용 CBDC는 모든 경제 주체들에게 현금과 같은 형태로 직접 발행되어 일상적으로 사용될 수 있음. 기관용 CBDC는 지급준비금과 유사한 형태로 금융기관에 발행되어 금융기관 간 자금 거래와 최종 결제 등에 활용될 수 있음

○ 국제통화기금(IMF, International Monetary Fund)의 경우 각국 중앙은행의 CBDC 연구 강화 추세와는 반대로 CBDC에 소극적인 태도를 보였음. 긍정적인 측면을 인정하면서도 동시에 금융 시스템에 끼치는 부정적 영향 및 규제 등을 크게 우려함

- 거래비용 절감, 금융 포용 확대, 국경 간 결제 시스템 개선 등의 장점을 확인함
- 2021년 IMF는 회원국의 80%가 법적으로 CBDC를 발행할 수 없거나, 법적 프레임워크가 불명확하다는 조사 결과를 발표함
- CBDC의 연착륙을 위해 기존 금융 시스템과 원활한 통합, 국가 내에서의

광범위한 수용을 보장하는 강력한 법적 기반이 선행되어야 한다는 의견을 제시함
- 2022년에 IMF는 CBDC의 잠재력에 대해 좀 더 포용적인 자세를 취했지만, 여전히 우려를 표명하며 소극적 태도를 견지함

○ 2023년 들어 IMF는 CBDC 표준화 작업에 대한 각국 중앙은행들의 합의를 요청하고, 글로벌 CBDC 인프라 개발에 관련된 연구를 진행 중임을 천명하는 등 CBDC에 대한 적극적 태도로 전환함
- 2023년 4월, IMF는 CBDC 역량개발에 관한 IMF 접근 방식이라는 보고서를 발간하며 IMF가 개발, 지원한 40개국 이상의 CBDC 역량개발 프로젝트를 공개하였고, 향후 역량개발에 관한 핸드북 제작 계획을 발표함
- 2023년 6월, IMF 총재는 각국의 CBDC 간 상호 운용을 허용하는 글로벌 CBDC 인프라 개발에 관한 연구를 진행 중임을 밝히며, 더 많은 사람에게 금융 포용성을 높이는 것을 도모함
- 국가 간 결제, 송금 등의 거액 결제용 CBDC에 대해서는 적극적이나 소액결제용 CBDC에 대해서는 잠재적 위험을 여전히 우려함

○ IMF의 소극적 태도와는 별개로 각국의 중앙은행은 CBDC 도입 논의 및 실험 등을 빠르게 진행해왔음. 특히, 코로나 19로부터 비롯된 범유행 등을 계기로 2021년부터 소액결제용 CBDC에 관한 연구가 강화되는 추세임

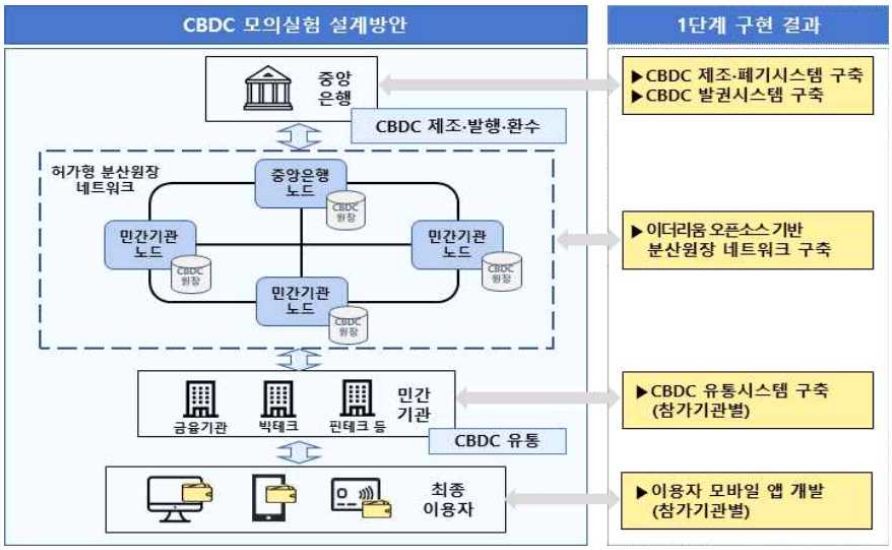
○ BIS(국제결제은행, Bank for International Settlements)의 2023년 7월 조사에 따르면 86개의 조사 대상국 중앙은행 중 93%가 CBDC 관련 작업을 진행 중이며, 전체 조사 대상의 75% 이상이 소액 결제와 거액결제용 CBDC를 모두 연구 중임

1. 사례 조사

○ 국내 CBDC의 경우 한국은행 주도하에 모의실험을 진행 중임
- 한국은행은 2021년 8월부터 10개월간 CBDC 모의실험 연구[15]를 두 단계에 걸쳐 진행하였음
- 1단계는 제조, 발행, 유통 등의 모의 시스템의 기본 기능을, 2단계에선 오프라인 거래, 디지털 자산 거래, 정책 지원 업무 등에 대한 구현 가능성을 점검함
- 1단계는 CBDC 제조·폐기시스템, CBDC 발권 시스템, CBDC 유통시스템 등 한국은행, 참가 기관과 이용자가 CBDC 업무를 전자지갑을 통해 수행하는 것에 대한 IT시스템 구현을 초점에 두었음. 1단계에서 구축한 시스템은 중앙은행이 CBDC를 제조 및 발행하고 참가 기관이 이용자에게 유통하는 혼

15) “CBDC 모의실험 연구사업 2단계 결과 및 향후 계획”, 보도자료, 한국은행, 2022.11.07.

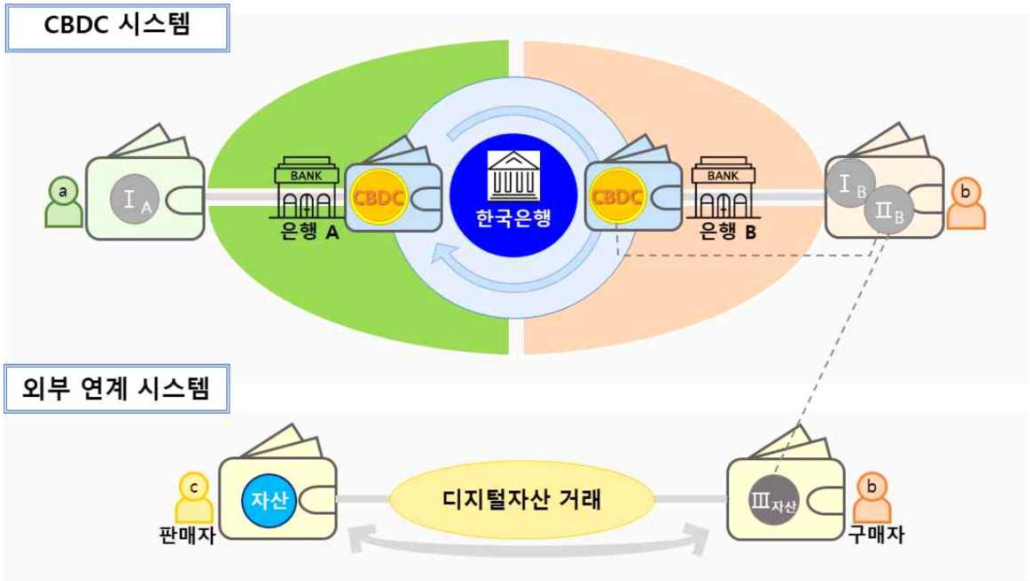
합형 CBDC 운영방식임



[그림 36] CBDC 모의실험 1단계 구현 결과, 출처: 한국은행

- 2단계는 CBDC 시스템이 실질적으로 활용되기 위한 기능 및 주요 시사점에 대한 분석이 진행됨. 2단계 모의시험을 통해 송금인과 수취인의 모바일 기기, IC 카드 등 전산기기가 모두 인터넷 통신망에 연결되지 않은 상황에서도 자체 통신 기능을 활용해 CBDC 거래가 가능함을 확인하였으나, 대량 거래 처리에 필요한 응답 대기시간의 개선이 필요함을 보였음. 국내의 소액 결제 시스템의 하루평균 초당 이용 건수는 1,000건 미만으로, CBDC 모의 시스템은 최대 초당 2,000건의 거래를 처리할 수 있을 것으로 측정하였으나, 초당 거래 처리 건수가 늘어날수록 응답 대기시간이 증가하는 것을 확인하였음. 이로 인해 점심시간, 납부 마감일 등 평상시보다 거래가 집중되는 피크타임시 거래의 실시간 처리에 한계가 있을 수 있다고 분석함
- 이러한 한계점을 해결하기 위한 확장성 솔루션으로 롤업 등 Layer 2 기술의 성능을 확인함. 개인정보 보호 강화를 위한 영지식 증명 기술과 분산원장 확장 기술에 대한 가능성도 점검함
- 모의실험 결과 정상 작동하였으며, 오프라인 CBDC 기능과 온라인 CBDC가 독립적으로 운영 가능하다는 것을 확인함
- 후속 단계로 금융위원회, 금융감독원과 공동으로 ‘CBDC 활용성 테스트’를 추진할 예정임
- CBDC 활용성 테스트는 기관용 CBDC를 중심으로 진행될 예정으로, 은행들

이 희망하는 고객에게 예금 기반 토큰인 예금 토큰을 발행해 실제 활용을 테스트할 계획임



[그림 37] CBDC 네트워크 구성도, 출처: 한국은행

○ 해외 역시 다양한 국가에서 CBDC 도입을 적극 논의 중이고, 도입을 위한 연구를 적극 진행 중[16)]

[표 27] 국가별 CBDC 현황

국가명	설명
중국	중국은 중국인민은행을 필두로 2014년부터 유관 연구를 수행하여 2019년 일반 대중을 대상으로 전국 26개 지역에서 디지털 위안화의 시범 사용을 진행 중임 시범 사용 시작 이후 디지털 위안화의 총 거래 건수는 9.5억 건, 거래 금액은 1.8조 위안, 발행된 디지털 지갑은 1.2억 개, 평균 거래액은 약 1,895위안 수준으로 집계됨

16) “IMF의 CBDC에 대한 입장 변화와 주요국의 개발 현황”, 자본시장포커스 2023-16호, 자본시장연구원, 김보영, 2023.08.07. 사례 일부 참조

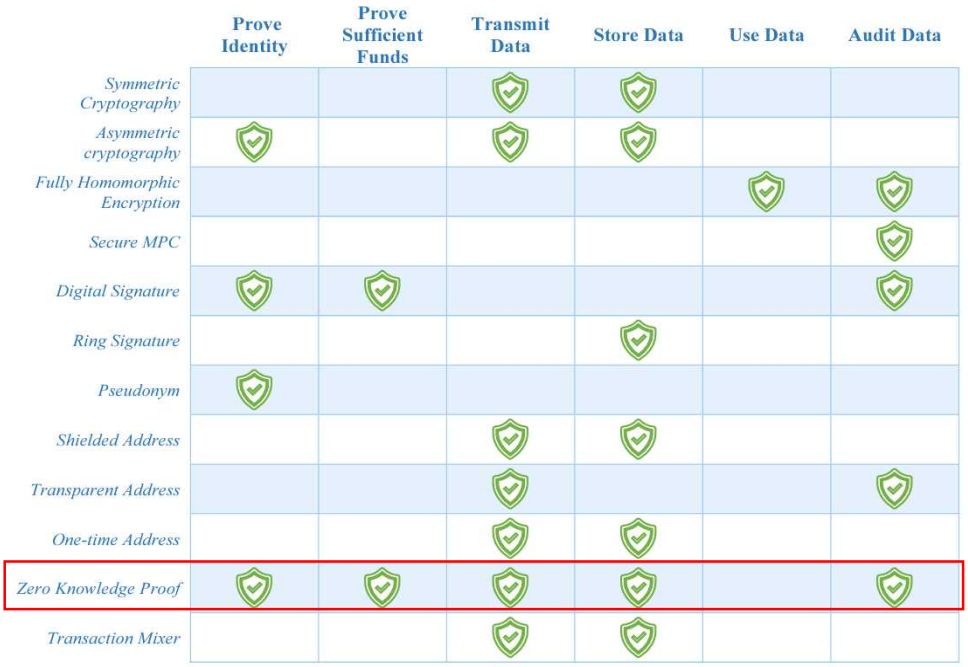
스웨덴	스웨덴은 중앙은행인 릭스방크(Riksbank) 주도로 자체 CBDC인 ‘e-크로나’ 프로젝트를 진행함 스웨덴 중앙은행은 e-크로나 2단계 시범 프로젝트를 통해 기존 디지털 뱅킹 인프라 내에서 기능할 수 있는 기술적 능력에 대한 조사를 받았고, 기술적으로 은행 네트워크에 통합되어 거래할 수 있음을 확인함 e-크로나 3단계에선 통화의 미래에 대한 의문들을 조사할 계획임
싱가포르	싱가포르는 2016년부터 CBDC 관련 연구를 순차적으로 진행 중이며, 제도적 장치 구비에도 신경을 쓰고 있음 싱가포르 통화청(MAS, Monetary Authority of Singapore)은 2016년부터 2021년까지 단계별 CBDC 프로젝트인 Project Ubin을 완료하여 분산원장기술 바탕으로 거액 결제용 CBDC 중심의 저비용, 고효율 결제 시스템 구축에 관한 연구를 수행함 2020년 1월, CBDC를 포함한 가상화폐 지불 및 결제 관련 지불서비스법(PSA, Payment Services Act)를 시행
영국	영국은 2020년부터 CBDC 연구를 본격적으로 진행 2023년 2월, 영국 중앙은행인 잉글랜드 은행과 재무부는 디지털 파운드화의 필요성 증가를 대비한 관련 자문 보고서와 기술 보고서를 공동 발표
미국	미국 연방준비위원회(이하 연준)는 바이든 정부가 들어서며 관계기관과의 협업을 통해 CBDC 프로젝트를 진행하며 CBDC 연구 가속화 2022년 2월, 보스턴 연준과 MIT가 공동 수행한 CBDC 프로젝트인 Project Hamilton에서 처리 성능 향상, 개인정보 보호 강화 등을 중심으로 하는 새로운 방식의 CBDC 기반 기술 구현 2022년 11월, 뉴욕 연준은 상업은행 토큰화 예금과 CBDC 간 상호운용성 확보 관련 기술 검증을 위한 모의실험 착수

○ CBDC 프라이버시 필요성

[표 28] 여러 기관의 CBDC 프라이버시에 관한 의견

출처	내용
금융위원회	“셋째, 기타 이용자에 대한 보호조치 마련입니다. … 세부 모델 설계과정에서 거래기록 암호화, 접근 권한 등에 대한 기술적 조치”
국제결제은행(BIS)	“CBDC 이용자와 데이터의 프라이버시 보호, 금융 시스템의 무결성, CBDC와 다른 형태의 화폐 중에서 선택할 수 있는 사람들의 권리 등 세 가지 핵심 요소가 필수적”
유럽연합 위원회	디지털 지갑 이용자의 개인정보 보호를 위해 ‘영지식 증명’(ZK-proof) 기술을 지갑에 포함하도록 규정
미연방준비제도 (Federal Reserve)	디지털 자산에 대한 데이터 프라이버시 보호 영지식 증명이 프라이버시를 위한 다양한 Use case를 만족
한국은행 경제연구	CBDC 도입 시 프라이버시 및 익명성 보장 방안을 매우 세심하게 고려할 필요가 있음을 시사

- CBDC 개발과 구현에서 프라이버시 보호는 필수적인 요소로 강조됨. 여러 글로벌 기관과 정부 기관에서 프라이버시의 중요성을 인식하고 있음
- CBDC의 성공적인 구현과 테스트에 있어 개인정보 보호와 프라이버시 보장이 필수 불가결한 요소임을 확인함



[그림 38] 미연방준비제도의 여러 프라이버시 강화 기술 평가

- 미연방준비제도에서는 영지식 증명을 CBDC에 적용할 때 가장 여러 가지 측면에서 활용도가 높은 기술로 평가하고 있음

○ CBDC 영지식 증명 적용 내용

- CBDC는 현재 각국에서 도입을 위해 논의를 하는 단계로, 특별한 표준이나 구현체가 확립되지 않음
- 프라이버시 보장에 대한 논의가 대두되고 있으며, 그중 프라이버시를 보장할 방법으로 영지식 증명에 대한 필요성을 강조하고 있음. ([그림 38] 참조)
- 영지식 증명 적용을 통해 거래자의 개인정보를 보호하고, 민감 정보인 금융정보에 대한 프라이버시를 보장하면서 동시에 금융 주체의 무결성 등을 보장할 수 있음
- 나아가 불법 테러 자금 조달, 혹은 자금 세탁 등을 방지하기 위한 적법한 감사를 진행하면서도 금융 주체의 프라이버시 보호를 보장할 수 있을 것으로 기대돼, 악의적 금융 행위를 방지하는 데에도 이바지할 수 있을 것으로 예상함

2. 기대 효과

○ 기술적 기대효과

- 영지식 증명 기반 CBDC를 통해 기존 CBDC가 개인 거래 내역 추적이 가능하다는 프라이버시 문제를 해소할 수 있음, 즉 현존 화폐에 준하는, 혹은 그 이상의 프라이버시를 제공할 수 있음
- 영지식 증명은 프라이버시 문제뿐만 아니라, 확장성 측면에서도 긍정적인 기대를 자아내는데, 현존하는 대표적 지불 수단인 비자, 마스터 카드 등의 트랜잭션 처리량(TPS, Transactions Per Second) 수준[17]의 성능, 혹은 상회하는 수준에 도달할 수 있을 것으로 예상함

○ 경제적 기대효과

- CBDC는 기존 화폐와 양립할 수 있을 뿐만 아니라 지역 화폐, 바우처 등에 사용하기에도 쉬움. 지급 및 사용이 기존 지역 화폐, 바우처에 비하여 간단하여 주민들의 활용을 독려할 수 있고, 이는 지역 경제 활성화를 촉진할 수 있을 것으로 기대됨
- CBDC는 그 자체로 실물 화폐 대비 전자 화폐의 발급 비용이 절감되는 효과가 기대됨. 영지식 증명이 CBDC와 결합하여 프라이버시 이슈로부터 비롯될 수 있는 불필요한 잠재적 사회 비용을 완화하는 효과를 가짐

○ 사회적 기대효과

- CBDC는 현금 의존도가 높고 은행 산업 발달이 미진한 저개발 국가, 계좌 개설에 어려움을 겪는 사회적 약자 계층의 계좌 보급률을 향상할 수 있음. 이를 통해 포용적 금융 수준을 제고하여 취약 계층에 금융 서비스 확산의 촉매제 역할을 할 수 있음
- 영지식 증명 기반 CBDC는 개인의 거래기록을 쉽게 추적하지 못하게 하여 기존 CBDC에 내재하는 문제인 프라이버시 문제를 해소함. 궁극적으로 각국의 중앙은행 및 국제 금융기구의 우려를 완화하여 CBDC의 연착륙에 이바지할 수 있음

17) 비자 및 마스터카드의 처리량은 평균 2,000TPS 수준임. “블록체인인 환경에서 합의의 확장성 개선을 위한 무효표를 활용한 비잔틴 합의 방법”, 2021년도 한국통신학회 동계종합학술발표회, 정성욱, 유민수, 2021.02

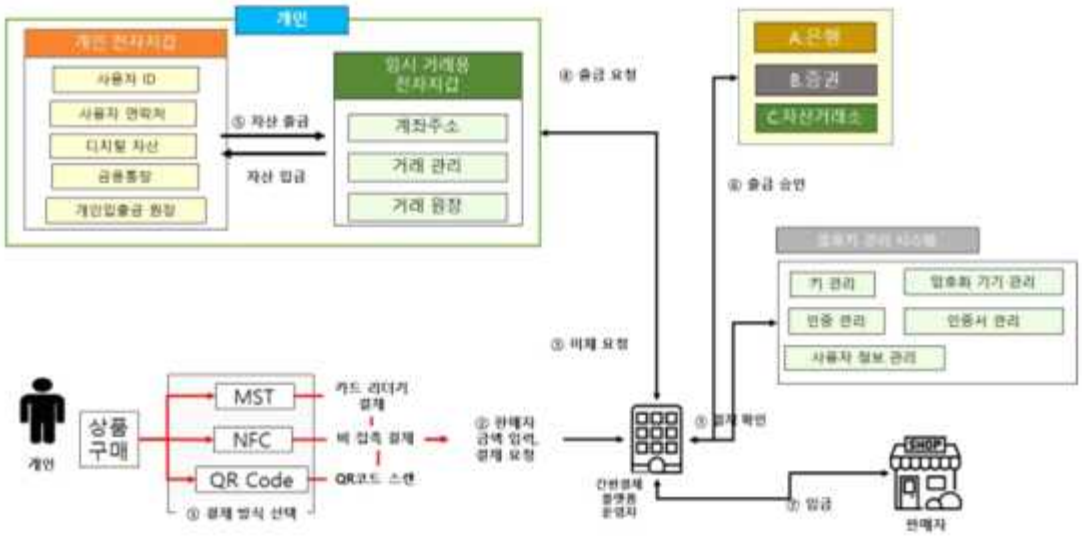
제4절. 디지털 지갑

○ 디지털 지갑 정의 및 동향

- 디지털 지갑(digital wallet, 전자지갑)은 컴퓨터 또는 단말기를 통해 온라인으로 물품을 구매하거나, 지갑에 예치된 돈을 타인·기업의 은행 계좌로 송금하는 초기 전자적 거래방식의 하나라는 의미의 e-wallet이라고도 하였음
  - ※ (기존) 기능적 측면에서 컴퓨터 또는 단말기를 통해 온라인으로 물품을 구매하거나, 지갑에 예치된 돈을 타인·기업의 은행 계좌로 송금하는 경제적 기능에 한정
  - ※ (현재) 디지털 지갑의 활용에 따라 기본적 금융 거래뿐 아니라 보유자의 자격 인증, 필수적인 문서를 보관·유통, 서비스를 신청하는 서명 등의 수단으로 확대
- 디지털 전환 가속화에 따라 기존 지갑의 주요 역할인 지불을 위한 현금 소지를 디지털 지갑을 통한 결제로 전환함을 넘어 본인 확인을 위한 신분증을 디지털 지갑을 활용하는 경우가 늘어남
- 현재 디지털 지갑은 기본적인 금융 거래뿐 아니라 보유자의 자격 인증, 필수적인 문서의 보관·유통, 서비스를 신청하는 전자서명 등의 다양한 기능이 지속해서 추가되며 그 범위가 확대되고 있음
- 국내·외 디지털 지갑은 간편결제/간편송금을 지원하는 금융 거래 서비스, 디지털 신원 인증을 위한 디지털인증 서비스, 가상자산 등을 취급하는 블록체인 기반 서비스 등으로 구분할 수 있음

○ 간편결제/간편송금을 지원하는 금융 거래 서비스

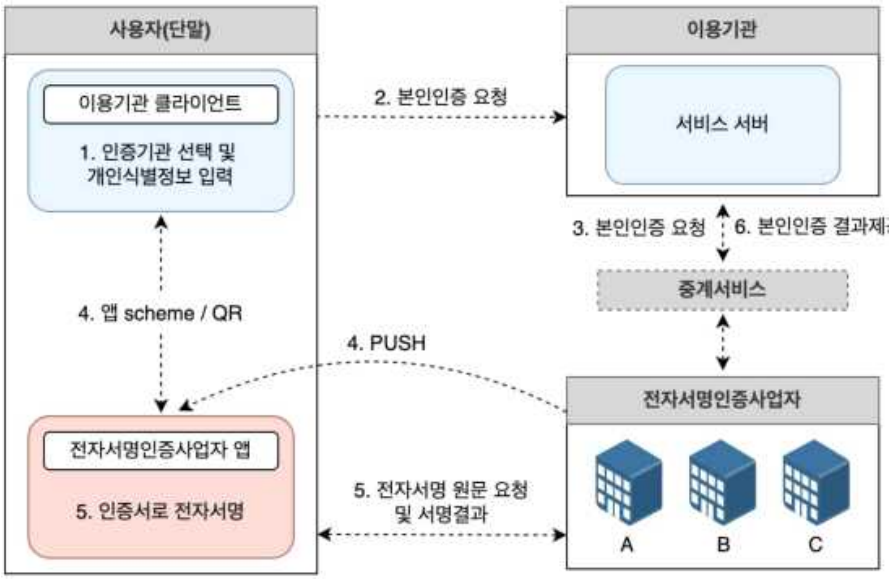
- 간편결제란 모바일에 신용카드, 은행 계좌 정보 등을 사용자가 미리 저장해둔 뒤, 결제 시 비밀번호 입력 혹은 단말기 접촉 등과 같은 방법으로 결제하는 방식을 뜻함. 간편송금은 계좌이체 등의 방식으로 충전한 선불금을 전화번호, SNS 등을 활용해 송금하는 서비스를 뜻함
- 모바일 간편결제 서비스는 구매한 상품을 온라인 환경에서 모바일 기기를 이용해 결제하는 온라인 결제 서비스와 실제 오프라인 매장에서 현금 및 신용카드 대신 모바일 기기를 NFC·MST 등의 방식을 통해 카드 결제 단말기에 사용하는 방식의 오프라인 결제 서비스로 구분할 수 있음
- 온라인 결제 서비스의 예시는 네이버페이, 페이팔(PayPal), 구글페이 등이 있으며, 오프라인 결제 서비스의 예시는 삼성페이, 애플페이 등이 대표적임
- 간편송금의 예시는 비바리퍼블리카의 토스, 카카오페이의 카카오페이 등이 대표적임



[그림 39] 간편결제용 디지털 지갑 아키텍쳐

○ 디지털 신원 인증 서비스

- 디지털인증이란 디지털화된 정보를 통해 본인 확인, 금융 거래, 온라인쇼핑 등의 경제·사회 활동 시 사용자의 신원에 관한 주장 및 검증 과정을 뜻함
- 최근 디지털 지갑을 활용하여 각종 신분증, 결제용 카드, 필수 정보 및 문서를 안전하게 보관하고 이동하는 서비스의 확대가 관찰되고 있음. 이러한 추세는 오프라인 및 온라인 환경에서 즉각적이며 대면이 아닌 활동이 요구되는 경우가 늘어나면서, 업무와 관련된 자신의 신원을 신속하고 정확하게 인증받는 방법의 필요성을 높임. 이와 함께, 이러한 요구를 충족시키기 위해 인증 과정과 디지털 지갑을 효과적으로 결합한 '디지털 신원(ID) 지갑'이 새롭게 등장함
- 디지털 신원 인증 서비스의 국내 사례로는 국민은행의 KB 국민인증서 서비스, 금융결제원의 YesKey 인증서 서비스 등이 있고, 국외 사례는 유럽연합의 유럽 디지털 ID 월렛 등이 있음
- 디지털 신원 인증 서비스를 블록체인을 활용하여 제공하는 사례는 3장 2절 전자 신원 인증의 DID를 참고



[그림 40] 간편인증 인터페이스

○ 블록체인 기반 전자지갑 서비스

- 블록체인 기반 전자지갑은 디지털 자산을 안전하게 보관하고 관리하는 도구로, 사용자의 개인정보와 자산을 안전하게 저장하는 서비스임. 이러한 전자지갑은 사용자에게 고유한 개인 키를 제공하여 해당 자산에 액세스하는 기능을 제공함. 이 개인 키는 무결성이 보장된 형태로 암호화되어 저장되며, 블록체인 기술을 활용하여 안전하게 관리됨
- 소프트웨어, 하드웨어, 웹 기반 등의 다양한 종류의 전자지갑이 있음. 소프트웨어 전자지갑(핫 월렛)은 앱 혹은 소프트웨어 프로그램으로, 일반적으로 컴퓨터나 모바일 기기에 설치됨. 하드웨어 전자지갑(콜드 월렛)은 전용 장치로, 오프라인에서 자산을 보호하고 온라인에서 필요할 때에만 액세스할 수 있음. 웹 기반 전자지갑은 온라인에서 액세스할 수 있으며, 브라우저를 통해 자산을 관리할 수 있음

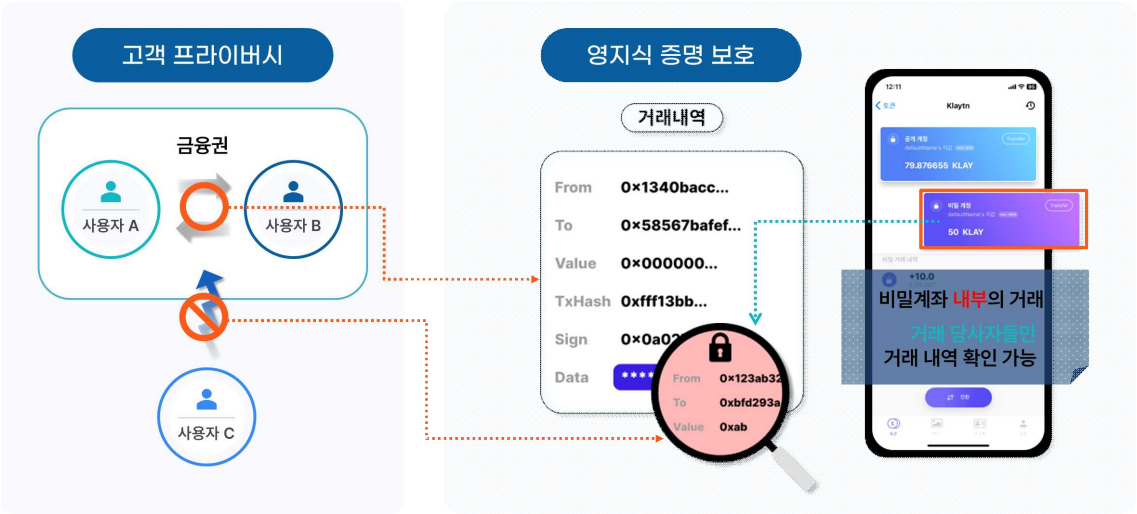
[그림 41] 핫 월렛과 콜드 월렛의 차이

- 블록체인 기술을 활용하기 때문에, 전자지갑은 높은 수준의 보안을 제공함. 블록체인은 탈중앙화된 시스템으로, 정보를 여러 노드에 분산 저장하여 외부 공격이나 변조를 방지함. 또한, 모든 거래 내역은 블록체인상에 공개적으로 기록되어 검증됨
- 주로 암호화폐가 블록체인 전자지갑을 통해 보관 및 전송되지만, 디지털 자산의 종류에 따라 대체 불가능 토큰(Non-Fungible Token, NFT)와 같은 다양한 토큰 및 기타 자산도 관리할 수 있음
- 블록체인을 활용한 전자지갑은 메타마스크, 코인베이스 월렛 등이 있음

1. 사례 조사

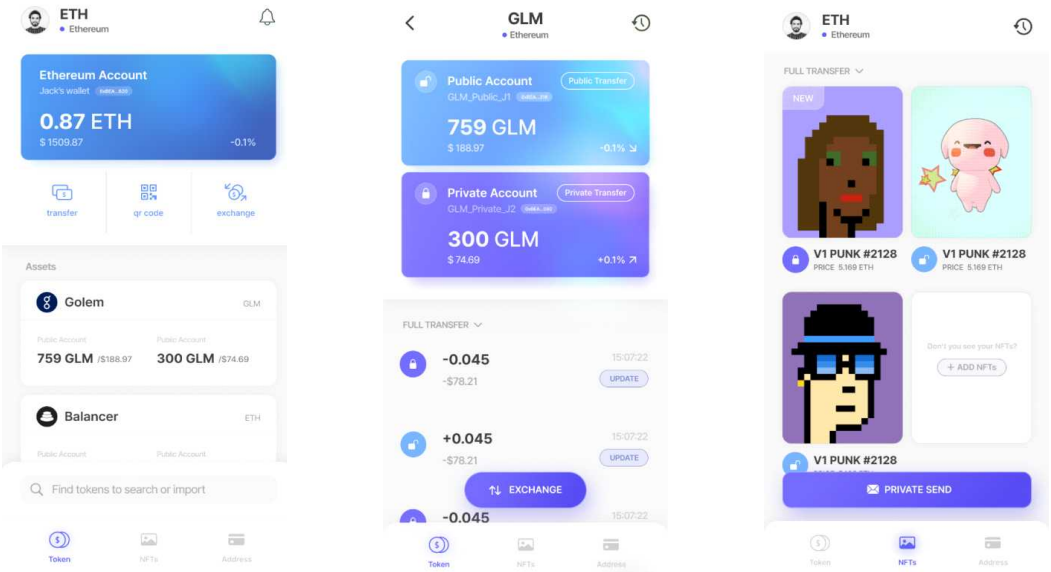
○ 영지식 증명을 활용한 블록체인 기반 전자지갑 국내 서비스

- 영지식 증명을 활용한 디지털 지갑으로는 지크립토의 zkWallet이 있음. zkWallet은 NFT를 포함한 다양한 디지털 자산을 안전하게 거래하고, 프라이버시를 보장하면서 감사 기능을 지원하는 앱임



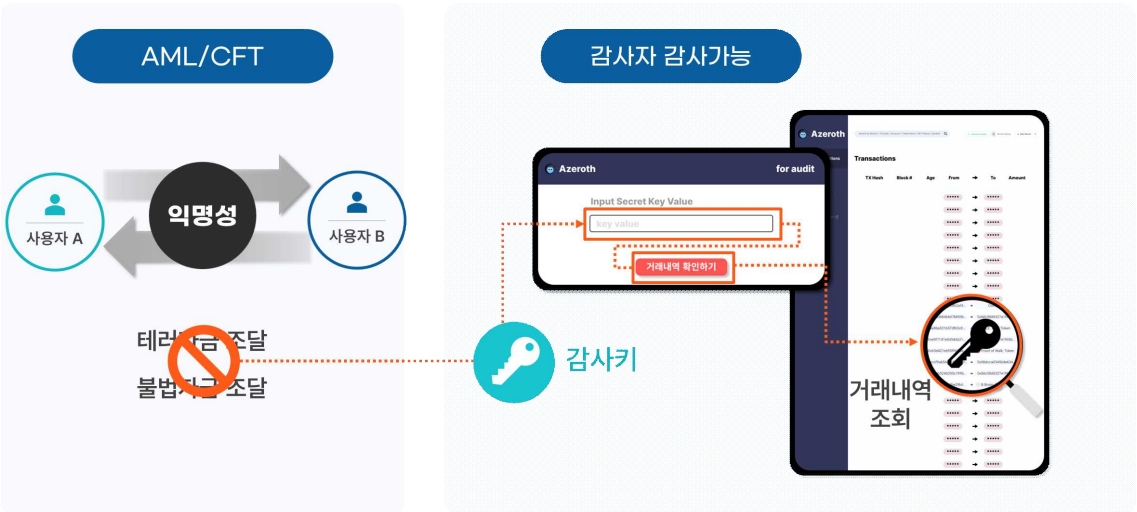
[그림 42] 디지털 지갑에서의 영지식 증명 적용사례

- zkWallet는 공개 블록체인상에서 영지식 증명 기술을 이용하여 트랜잭션의 프라이버시를 보장하는 소프트웨어임
- 비트코인, 이더리움과 같이 널리 사용되는 퍼블릭 블록체인 내 트랜잭션이 저장되면서 수신자, 송금액 등 많은 정보가 대중들에게 노출되는 문제가 있음
- 트랜잭션의 프라이버시에 대한 해결책으로 zkWallet에서는 영지식 증명을 이용함. 영지식 증명은 개인의 비밀 정보를 드러내지 않으며 암호화된 데이터의 유효성을 증명할 수 있음. 다시 말해 이용자는 트랜잭션의 프라이버시를 보호함과 동시에 분산원장에 공개적으로 등록된 암호화된 데이터를 복호화하지 않고 유효성을 확인할 수 있음



[그림 43] 디지털 지갑 어플리케이션 사례(zkWallet)

- 후술할 국외 사례들의 경우 송수신 자 및 금액 등을 제안하는 본 기술과 같이 영지식 증명 등을 이용하여 프라이버시를 보장하지만 완전한 익명성을 보장하기 때문에 자금 세탁 및 악의적 금융 행위에 대한 예방책이 없음
- 개인정보의 프라이버시 보호와 악의적인 거래 방지 사이의 합의점이 도출 되어야 하므로 이를 해결하고자 zkWallet에서는 프라이버시 보호를 위하여 블록체인 내 트랜잭션의 프라이버시를 보장하면서 악의적인 거래 방지를 위해 트랜잭션의 감사가 가능한 기술을 제공함



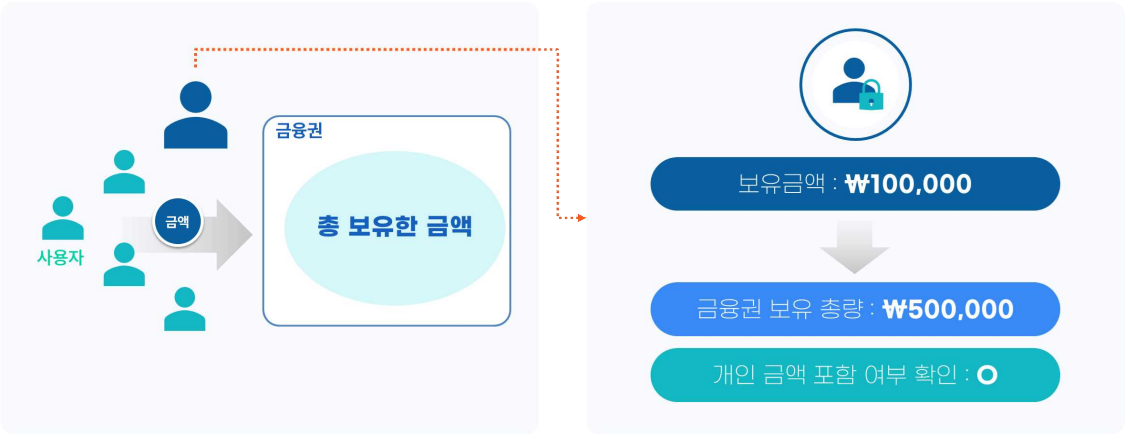
[그림 44] 감사키를 이용한 트랜잭션 감사

○ 영지식 증명 기반 준비금 증명 서비스(zkPoR)

- zkPoR은 기관의 명시된 보유액이 안전하게 보유하고 있는 유형 자산과 일치하는지 검증하는 지크립토가 영지식 증명을 이용하여 개발한 고성능 준비금 증명(PoR) 프로토콜임

[그림 45] 기존 준비금 증명 방식

- **(기존 준비금 증명 방식 문제점 - 회계법인 감사 방식)** 개인 계좌 보유량이 공개되어 개인의 프라이버시를 침해하며 회계법인과 거래소의 장부 조작 가능성이 존재함
- **(기존 준비금 증명 방식 문제점 - 머클 트리 방식)** 가상화폐 거래소 바이낸스가 사용하는 방식으로 머클 트리의 다수 연산으로 인한 성능 저하(최대 36시간 소요) 및 현재 시점의 스냅샷으로 준비금 증명을 연산하기 때문에 스냅샷 이후의 준비금 증명은 불가능함
- **(영지식 증명이 적용된 준비금 증명)** 지크립토의 준비금 증명은 고객이 거래소 내 예치한 자금의 규모, 자금에 대한 권한을 수탁자가 갖는지에 대한 여부, 거래소가 보유한 자산 내에 고객의 예치금이 포함되어 있는지에 대한 여부 등을 영지식 증명을 이용하여 프라이버시를 침해하지 않고 증명할 수 있음
- 페더슨 약정 값을 이용하여 최대 1초 미만의 성능으로 준비금 증명의 실시간성을 보장함

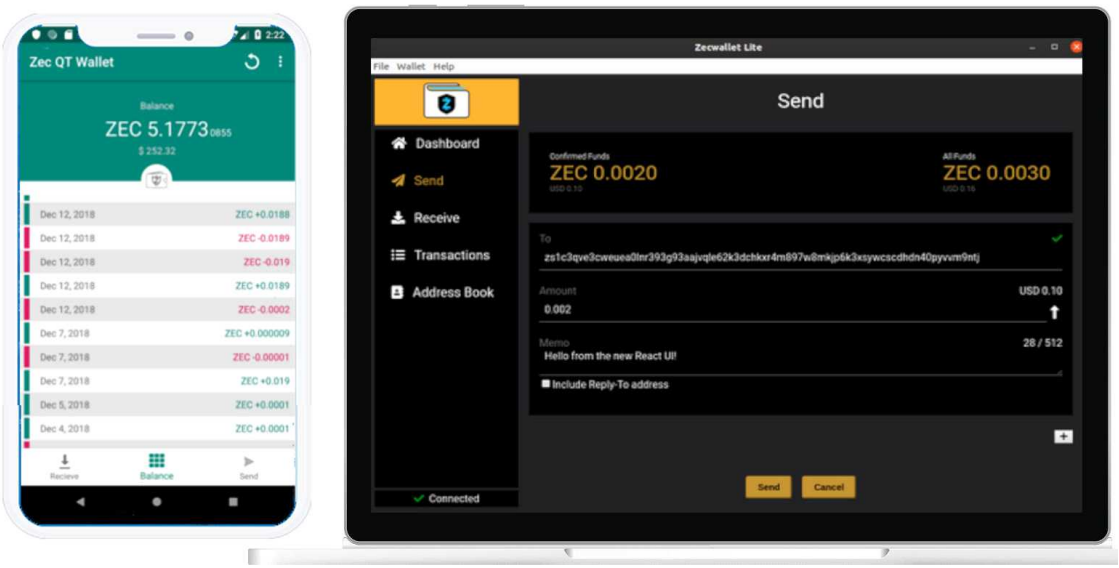


[그림 46] 영지식 증명을 이용한 준비금 증명

○ 영지식 증명을 활용한 블록체인 기반 해외 서비스

- Zerocash는 전통적인 비트코인 및 기타 암호화폐와 비교하여 더 높은 익명성을 제공하기 위해 설계된 암호화폐 시스템임. 비트코인은 블록체인에 기록되어 누구나 추적하고 연결할 수 있는 문제가 있음. 영지식 증명 기반 UTXO 모델 블록체인으로 송수신 자의 거래에 대한 프라이버시를 제공함
- Hawk는 영지식 증명을 통해 임의의 스마트 컨트랙트를 설계할 때 프라이버시를 보장할 수 있는 기술을 제안함
- Blockmaze는 프라이버시 보장 트랜잭션을 생성하기 위해 zk-SNARK를 사용, 즉 일반 잔액과 개인 잔액 간 연결성을 소멸하면서도 트랜잭션의 정당성을 증명할 수 있음

○ Zerocash 지갑



[그림 47] Zerocash 지갑 UX/UI

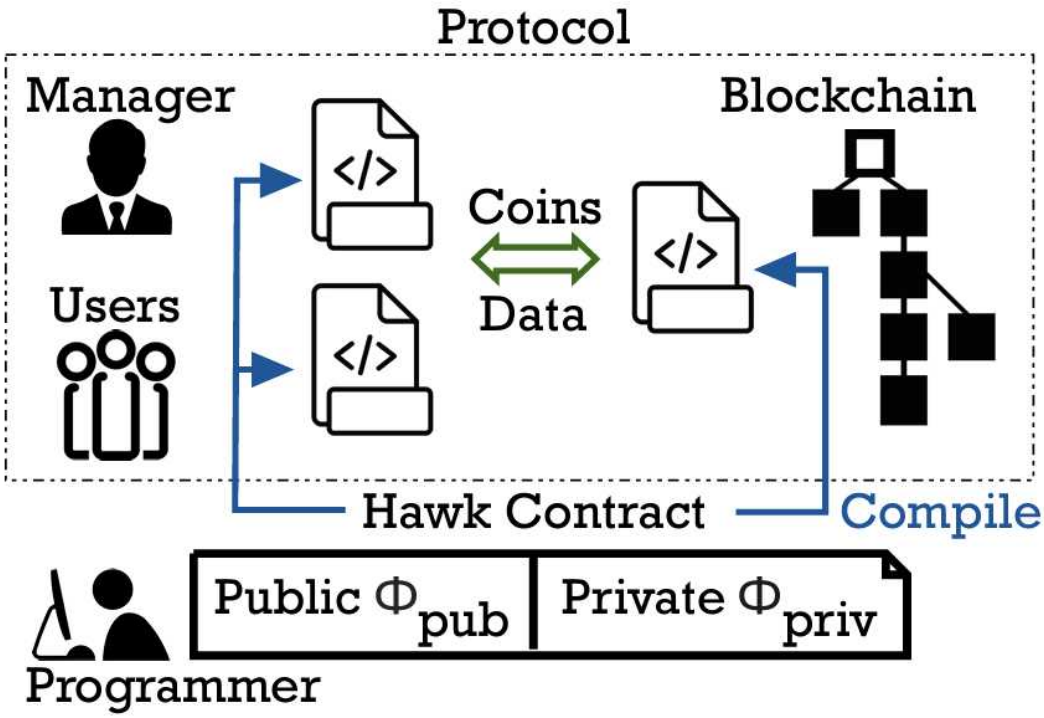
- Zerocash 지갑은 다른 암호화폐 지갑과 유사하게 작동하지만, 특히 제로캐시 프로토콜의 프라이버시 보존 거래 기능을 지원하기 위해 특별히 설계됨
- 사용자는 개인정보 보호 및 보안이 보장된 방식으로 결제를 보내고 받을 수 있음. 지갑은 이러한 거래를 관리하기 위해 영지식 증명이 적용된 제로캐시 프로토콜을 이용함
- 지갑은 일반적으로 사용자의 개인 키와 거래 데이터를 보호하기 위해 암호화 및 다중 인증 요소와 같은 보안 계층을 포함함
- 제로캐시의 프라이버시는 개별 거래가 구별되지 않는 큰 익명성 집합에 의해

부분적으로 제공됨

- 다른 지갑과 마찬가지로, 제로캐시 지갑에는 잔액 관리, 거래 내역 보기 자금 송수신을 위한 사용자 친화적인 인터페이스를 제공함

○ Hawk

- Hawk는 영지식 증명을 통해 임의의 스마트 컨트랙트를 설계할 때 프라이버시를 보장할 수 있는 기술을 제안함
- 이더리움과 같은 블록체인에서의 스마트 계약은 완전히 투명하여 모든 거래 세부 사항이 모두에게 보이지만 Hawk는 특정 거래 세부 사항(예: 금액 및 관련 당사자)을 비공개로 유지하면서 스마트 계약의 실행을 허용함
- Hawk 컴파일러는 개발자들이 작성한 고급언어 코드를 두 부분으로 변환함. 하나는 블록체인용이고 다른 하나는 ZKP를 계산하는 매니저용임
- Hawk는 거래 입력 및 출력에 대한 프라이버시 보장을 제공하지만, 계약의 제어 흐름에 대해서는 보장하지 않음. 이는 전송된 값이 숨겨져 있지만, 계약의 특정 기능이 실행되었다는 사실이 공개될 수 있다는 것을 의미함
- 스마트 컨트랙트가 잘 수행됐다는 것을 zk-SNARK 증명을 통해 입증하지만, 신뢰 기반의 매니저가 그 증명을 생성한다는 한계를 지님



[그림 48] Hawk 프로토콜

○ BlockMaze

- Blockmaze는 Account 모델 블록체인을 위한 이중 잔액을 제안함. 이중 잔액이란, 일반 잔액(public balance)과 개인 잔액(private balance)으로 구성됨
- 일반 잔액은 블록체인 네트워크에 공개되며, 개인 잔액은 암호화되어 개인 거래의 내용을 보호함
- 프라이버시 보장 트랜잭션을 생성하기 위해 zk-SNARK를 사용, 즉 일반 잔액과 개인 잔액 간 연결성을 소멸하면서도 트랜잭션의 정당성을 증명할 수 있음

2. 기대 효과

○ 기술적 기대효과

- 영지식 증명 기반 전자지갑은 지갑 소유자의 프라이버시를 보장하여 디지털 자산을 안전하게 관리하고 거래할 수 있음
- 특히, 영지식 증명 기반 디지털 지갑인 zkWallet의 경우 프라이버시 보장과 감사 기능을 모두 지원함으로써, 프라이버시 보장으로 야기될 수 있는 자금 세탁 등의 악의적 부정 금융 행위를 방지할 수 있음

○ 경제적 기대효과

- 암호화폐와 더불어 은행 계좌, 포인트 카드 정보까지 안전하게 통합 관리할 수 있어 개인의 자산 관리 측면에서 효율성을 증대하는 효과를 자아낼 것으로 기대됨
- 안전한 개인 계좌 관리를 위한 각 금융기관의 비용을 절감할 수 있을 것으로 기대됨
- 디지털 지갑의 안전성 확보로 디지털 지갑 시장의 저변을 확대할 수 있고, 나아가 핀테크 시장 확대를 가속할 수 있음

○ 사회적 기대효과

- 영지식 증명 기반 디지털 지갑을 통해 개인 지갑의 안전성을 강화하고 금융기관에 대한 신뢰도 향상 효과를 도모할 수 있음
- 프라이버시 보호 기능뿐만 아니라 합법적 감사 기능을 통해 악의적 부정행위를 탐지하고 예방하여 건전한 금융 행위의 확산에 긍정적 영향을 끼칠 수 있음

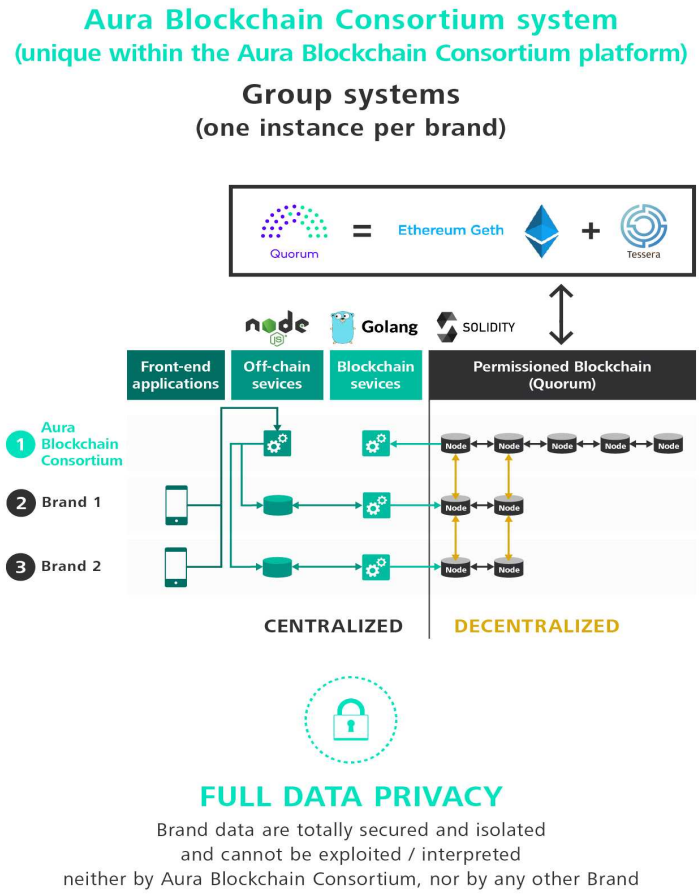
제5절. 공급망 관리 시스템

1. 사례 조사

○ 전통적인 공급망은 참가자 수가 적고 규모가 작았던 반면, 현대의 공급망은 수많은 제조업체, 물류 업체, 소매점이 상호 연계되며 참가자 수가 많아져 공급망은 복잡해짐. 복잡한 공급망은 관리의 어려움을 초래하고, 이러한 부적절한 원자재 사용, 불법 위조·모조품 등의 문제점을 발생시킴. 이를 해결하고자 인공지능, 블록체인 등 다양한 신기술이 접목된 공급망 관리 시스템이 상용화되고 있음

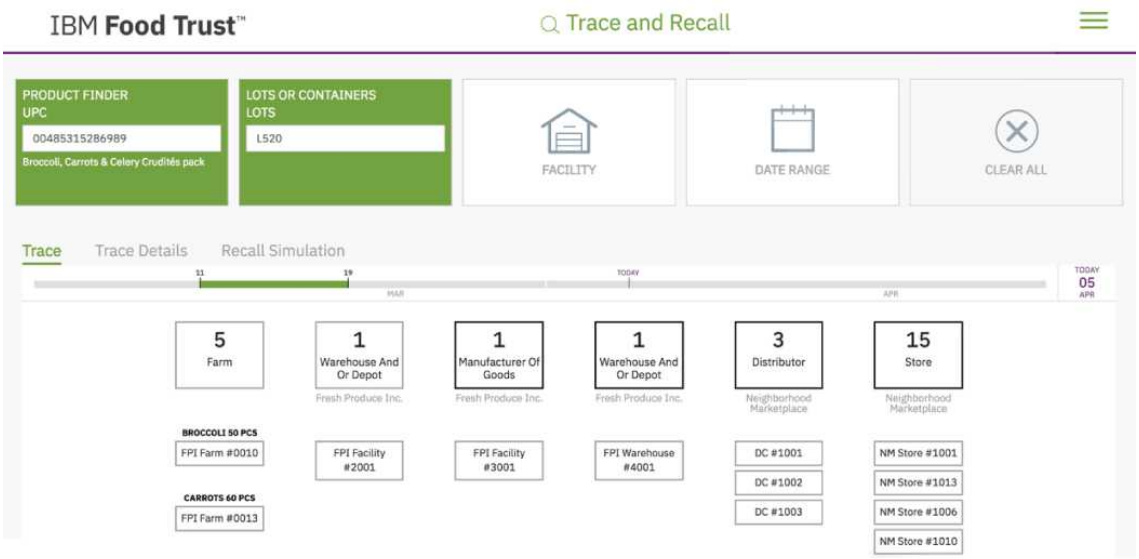
○ 해외 블록체인 기반 공급망 관리 시스템

- Aura 블록체인 컨소시엄: Aura 블록체인 컨소시엄은 LVMH, 메르세데스 벤츠, 프라다 그룹 등 다양한 고가 패션 소비재 및 화장품, 주류 등을 판매하는 기업이 모인 컨소시엄으로, 블록체인 기술을 활용하여 정품 여부를 보증하는 시스템과 NFT 등을 개발하였음



[그림 49] Aura 블록체인 컨소시엄 시스템

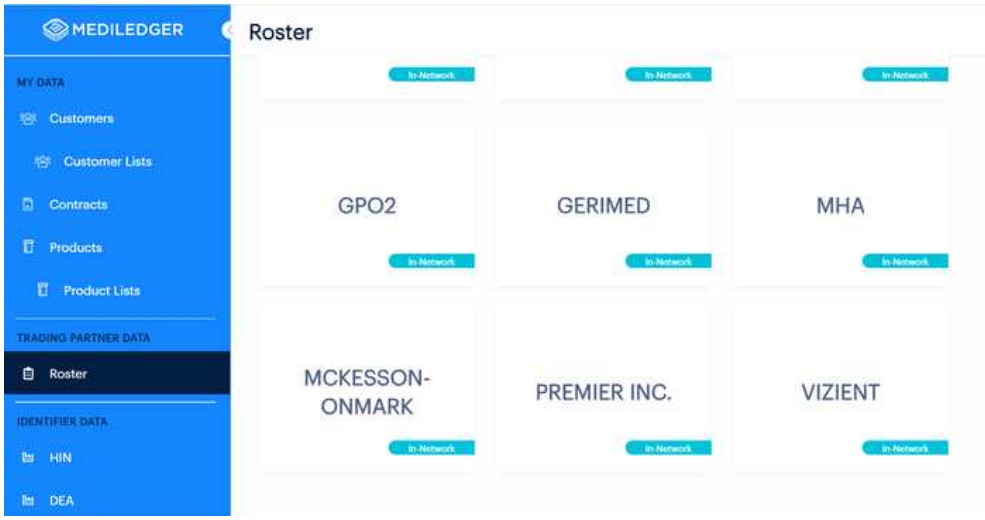
- ProductChain: ProductChain은 블록체인 기술을 활용해 제품의 진위를 확인하고 공급망의 투명성을 높이는 B2B 플랫폼임. ProductChain은 각 제품에 고유한 디지털 식별자를 부여하고, 식별자에 대한 생산지, 유통 과정, 재고 관리 등에 대한 상세한 정보를 블록체인에 저장함
- IBM 푸드 트러스트(IBM Food Trust): IBM 푸드 트러스트는 식품의 생산, 가공, 유통 과정을 블록체인에 기록하고, 이를 통해 추적을 지원하는 플랫폼임. 이 시스템은 식품 공급망의 각 단계에서 발생하는 IoT 데이터를 취합하여 저장하여, 식품 안전사고가 발생했을 경우 원인을 신속하게 파악하고 대처할 수 있음. 미국의 월마트(Walmart)와 프랑스의 까르푸(Carrefour) 등 세계적인 프랜차이즈 대형 할인매장에서 사용하고 있음



[그림 50] IBM Food Trust 서비스

○ 영지식 증명 활용 블록체인 기반 공급망 관리 시스템

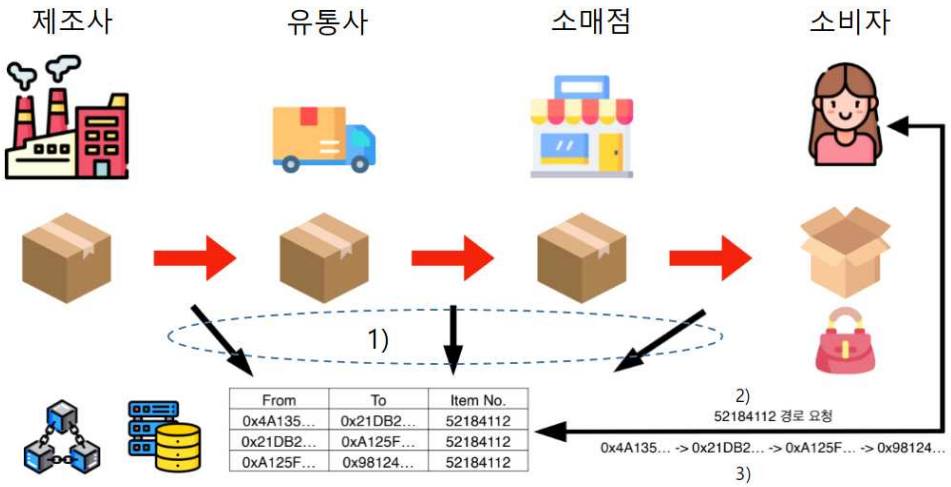
- 메디레저(MediLedger): 메디레저는 크로니클드(Chronicled)가 운영하는 제약 산업을 위한 블록체인 네트워크임. 해당 네트워크는 제약회사 화이자(Pfizer), 의약품 도매업체 아메리소스버겐(AmerisourceBergen) 등이 협력해 개발한 의약품 유통시스템으로, 의약품 공급망에서 투명성과 안전성을 향상하기 위해 개발됨. MediLedger 보고서는 영지식 증명(zero-knowledge proof, ZKP) 기술을 사용함으로써 제약 업계의 데이터 프라이버시 요건을 준수할 수 있다고 설명함. 블록체인의 불변성을 유지하면서 기밀 정보의 사업적 정보는 노출되지 않도록 할 수 있다고 함



[그림 51] Mediledger 처방약 추적 시스템

○ 공급망 관리 블록체인 시스템에 영지식 증명 적용 방안

- 현재 상용화된 블록체인 기반 공급망 관리 시스템은 공급망에서 발생하는 데이터의 프라이버시와 성능 향상을 위해 대다수 폐쇄형 블록체인을 사용하고 있지만, 허가된 대상만 블록체인을 열람하고 정보를 기록할 수 있는 특성으로 인해 공급망 관리 시스템의 확장성이 떨어짐
- 또한, 공급망에 관련된 데이터를 취합하면 제품에 대한 안전성, 정품 여부 등에 대한 정보를 얻을 수 있지만, 소비자는 블록체인에서 자신이 구매한 제품에 대한 정보를 직접 열람할 수 없고 관련 업체에서 제공해주는 정보를 신뢰할 수밖에 없음. [그림 52]는 블록체인 기반 공급망 관리 시스템의 개요도임



[그림 52] 블록체인 기반 공급망 관리 시스템 개요

1) 공급망의 각 단계에서 발생하는 거래 정보를 블록체인과 같은 분산원장에 기록함
2) 블록체인에 속한 사용자가 자신이 소유한 제품에 대한 유통 경로에 대한 정보를 요청함
3) 요청받은 제품에 대한 정보를 블록체인으로부터 읽어와 사용자에게 제공함

- 이러한 한계점은 폐쇄형 블록체인을 대신해 공개형 블록체인을 사용하면 해결할 수 있음
- 하지만, 모든 사용자가 블록체인의 데이터에 접근할 수 있다는 공개형 블록체인의 특성상, 유통 이력과 같은 공급망 데이터를 블록체인에 공개하는 것은 불가능하므로 암호화와 같은 적절한 프라이버시 보호 방안이 필요함
- 프라이버시 보호를 위한 암호화는 블록체인 검증자에게 거래의 유효성을 입증하기에 어려움이 있지만, 영지식 증명을 활용하면 검증 가능성과 프라이버시 보호를 동시에 만족하는 공급망 관리 시스템을 구축할 수 있음

2. 기대 효과

○ 기술적 기대효과

- 영지식 증명을 통해 공개형 블록체인상에서도 높은 수준의 프라이버시 수준을 제공하며, 소비자에게도 자신이 구매한 제품에 대한 정보를 기업이 제공해주는 정보에 의존하는 것이 아닌 블록체인으로부터 직접 열람할 수

있는 권한을 주어 신뢰성을 높임

- 공개형 블록체인을 채택함으로써 더 많은 기업의 참여를 유도할 수 있고, 이를 통해 다양한 제품군에 대한 정품 인증 플랫폼을 구축할 수 있음

○ 경제적 기대효과

- 제품의 원산지로부터 최종 소비자에게 도달할 때까지의 과정이 블록체인에 저장되고 이를 통해 제품의 사실 여부를 추적할 수 있는 시스템을 구축하면 위조·모조품 시장의 규모를 크게 줄일 수 있을 것으로 기대됨
- 스마트 계약을 통한 가상화폐 결제 시스템 등을 활용하면 결제 시스템을 간소화하고 거래 수수료를 절감할 수 있음

○ 사회적 기대효과

- 소비자에게 제품이 어떤 유통 과정을 통해 도달하였는지에 대한 정보를 제공해줌으로 식품, 의약품의 안전성 및 품질을 보장해줄 수 있고, 불법 위조·모조품에 대한 우려를 줄일 수 있음
- 공급망의 단계마다 발생하는 온실가스, 유해 물질 등의 안전한 추적을 통해, 비단 공급망 관리뿐 아니라 지속할 수 있는 친환경 산업 구조로의 변화를 이끌 수 있음

제 4 장. 결론

○ 블록체인 기술은 4차 산업 혁명의 핵심 기술로 대두되었으나, 확장성과 프라이버시 문제, 탈중앙화 등의 도전 과제(블록체인 트릴레마)가 있음. 이러한 문제들은 블록체인이 실제 비즈니스 환경에서 널리 채택되는 데 주요한 장애물로 작용하고 있음. 특히, 현재의 주요 블록체인 플랫폼들은 대규모 트랜잭션 처리에 있어 제한된 처리량을 보여주는 확장성 문제와 블록체인의 투명성은 장점이기도 하지만 데이터의 프라이버시 문제를 일으키는 단점으로 작용함

○ 이러한 문제를 해결하기 위해 영지식 증명 기술이 현재 주목받고 있음. 영지식 증명은 데이터의 유효성을 증명하면서 해당 데이터를 공개하지 않는 암호학적 방법을 제공함. 영지식 증명 기술은 블록체인 네트워크의 부하를 줄이고 처리량을 향상할 수 있어 확장성 문제의 해결에 이바지하며, 동시에 트랜잭션의 내용이 공개되어 발생할 수 있는 프라이버시 문제도 같이 해결할 수 있음

○ 본 연구는 영지식 증명 기술의 기본 개념부터 심화 내용까지를 조사하고, 영지식 증명을 활용한 블록체인 기술현황과 프라이버시 강화 기술 동향을 조사함. 또한, 국내·외에서 영지식 증명이 적용된 서비스들의 사례를 분석하고 기술적, 산업적, 사회적 측면에서의 기대효과를 파악함

○ 연구결과, 영지식 증명 기술은 블록체인의 확장성 및 프라이버시 문제해결에 있어 매우 유망한 해결책으로 확인됨. 이 기술은 단순히 기술적 문제를 해결하는 것을 넘어서 블록체인의 사회적, 경제적 가치를 높일 수 있음. 프라이버시 보호와 확장성 향상은 블록체인 기반의 서비스나 애플리케이션의 사용자 경험을 더욱 증진하며, 더 넓은 범위의 산업 분야에서 블록체인의 적용 가능성을 확대할 수 있음

○ 이에 따라, 블록체인 기술의 진화와 발전을 위해서는 영지식 증명 기술에 대한 깊은 이해와 적용 방안 연구가 필요함. 영지식 증명 기술의 복잡성과 블록체인에의 적용에 있어 다양한 문제점들을 극복하기 위한 연구와 더불어, 점차적인 실제 서비스 사례에서의 영지식 증명 기술 적용을 통해 블록체인의 확장성 및 프라이버시 문제를 해결하고 다양한 산업 분야에서의 적용과 활용을 촉진할 수 있을 것으로 기대됨

참 고 문 헌

[1] [BBB+16] Bünz, Benedikt, et al. “Bulletproofs: Short proofs for confidential transactions and more.“ 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018.

[2] [BBHR18] Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M. “Scalable, transparent, and post-quantum secure computational integrity.” IACR Cryptology ePrint Archive 46, 2018.

[3] [BFS19] Bünz, Benedikt, Ben Fisch, and Alan Szepieniec. “Transparent snarks from dark compilers.” Cryptology ePrint Archive, Report 2019/1229, 2019, https://eprint. iacr. org/2019/1229, 2019.

[4] [GM17] Jens Groth and Mary Maller. Snarky signatures: Minimal signatures ofknowledge from Simulation-Extractable SNARKs. InAdvances in Cryptol-ogy - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II, pages581-612, 2017.

[5] [Gro16] Groth, Jens. “On the size of pairing-based non-interactive arguments.“ Annual international conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 2016.

[6] [GWC19] Gabizon, Ariel, Zachary J. Williamson, and Oana Ciobotaru. PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge. Cryptology ePrint Archive, Report 2019/953, 2019.

[7] [KLO19] Kim, Jihye, Jiwon Lee, and Hyunok Oh. Qap-based simulation-extractable snark with a single verification. Cryptology ePrint Archive, Report 2019/586, 2019. https://eprint. iacr. org/2019/586, 2019.

[8] [MBKM19] Maller, Mary, et al. “Sonic: Zero-knowledge SNARKs from linear-size universal and updatable structured reference strings.“ Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. 2019.

[9] [KZG10] Kate, Aniket, Gregory M. Zaverucha, and Ian Goldberg. “Constant-size commitments to polynomials and their applications.“Advances in Cryptology-ASIACRYPT 2010: 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore,

December 5-9, 2010. Proceedings 16. Springer Berlin Heidelberg, 2010.

[10] [GMR85] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactiveproof-systems (extended abstract). In 17th ACM STOC, pages 291-304. ACM Press, May 1985.

[11] [QG90] Quisquater, JJ.et al.(1990). How to Explain Zero-Knowledge Protocols to Your Children. In: Brassard, G. (eds) Advances in Cryptology — CRYPTO' 89 Proceedings. CRYPTO 1989. Lecture Notes in Computer Science, vol 435. Springer, New York, NY.

[12] [PHGR13] B. Parno, J. Howell, C. Gentry and M. Raykova, "Pinocchio: Nearly Practical Verifiable Computation," 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2013, pp. 238-252, doi: 10.1109/SP.2013.47.

[13] [BCG+14] E. Ben Sasson et al., "Zerocash: Decentralized Anonymous Payments from Bitcoin," 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2014, pp. 459-474, doi: 10.1109/SP.2014.36.

[14] [JMP13] Jonker, H., Mauw, S., Pang, J.: Privacy and verifiability in voting systems: methods, developments and trends. Comput. Sci. Rev.10, 1-30 (2013)

[15] [XZS22] Tiancheng Xie, Yupeng Zhang, and Dawn Song. 2022. Orion: Zero Knowledge Proof withLinear Prover Time. In Advances in Cryptology - CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part IV. Springer-Verlag, Berlin, Heidelberg, 299-328.

[16] [CHMMVW20] Chiesa, Alessandro & Hu, Yuncong & Maller, Mary & Mishra, Pratyush & Vesely, Noah & Ward, Nicholas. (2020). Marlin: Preprocessing zkSNARKs with Universal and Updatable SRS. 10.1007/978-3-030-45721-1_26.

[17] [BBHR17] Ben-Sasson, Eli, Iddo Bentov, Yinon Horesh and Michael Riabzev. "Fast Reed-Solomon Interactive Oracle Proofs of Proximity." Electron. Colloquium Comput. Complex.(2017).

[18] [KST22] Kothapalli, A., Setty, S., Tzialla, I. (2022). Nova: Recursive Zero-Knowledge Arguments from Folding Schemes. In: Dodis, Y., Shrimpton, T. (eds) Advances in Cryptology - CRYPTO 2022. CRYPTO 2022. Lecture Notes in Computer Science, vol 13510. Springer, Cham.

[19] [KS22] Abhiram Kothapalli,Srinath T. V. Setty: SuperNova: Proving universal

machine executions without universal circuits.IACR Cryptol. ePrint Arch.2022:1758(2022)

[20] [KS23] Abhiram Kothapalli,Srinath T. V. Setty: HyperNova: Recursive arguments for customizable constraint systems. IACR Cryptol. ePrint Arch.2023:573(2023)

[21] [STW23] Srinath T. V. Setty,Justin Thaler,Riad S. Wahby: Customizable constraint systems for succinct arguments.IACR Cryptol. ePrint Arch.2023:552(2023)

[22] [LQT20] Lueks, Wouter, Iñigo Querejeta-Azurmendi, and Carmela Troncoso. "{VoteAgain}: A scalable coercion-resistant voting system."29th USENIX Security Symposium (USENIX Security 20). 2020.

[23] [KRS+20] Killer, Christian, et al. "Provotum: A blockchain-based and end-to-end verifiable remote electronic voting system." 2020 IEEE 45th Conference on Local Computer Networks (LCN). IEEE, 2020.

[24] [AHIV17] Ames, S., Hazay, C., Ishai, Y., Venkitasubramaniam, M.: Ligero: lightweight sublinear arguments without a trusted setup. In: Thuraisingham, B.M., Evans, D., Malkin, T., Xu, D. (eds.) ACM CCS 2017, pp. 2087–2104. ACM Press (2017).

[25] [BCR+19] Ben-Sasson, E., Chiesa, A., Riabzev, M., Spooner, N., Virza, M., Ward, N.P. (2019). Aurora: Transparent Succinct Arguments for R1CS. In: Ishai, Y., Rijmen, V. (eds) Advances in Cryptology – EUROCRYPT 2019. EUROCRYPT 2019. Lecture Notes in Computer Science(), vol 11476. Springer, Cham.

[26] [COS20] Chiesa, A., Ojha, D., Spooner, N. (2020).FRACTAL: Post-quantum and Transparent Recursive Proofs from Holography. In: Canteaut, A., Ishai, Y. (eds) Advances in Cryptology – EUROCRYPT 2020. EUROCRYPT 2020. Lecture Notes in Computer Science(), vol 12105. Springer, Cham.

[27] [CL04] Camenisch, J., Lysyanskaya, A. (2004). Signature Schemes and Anonymous Credentials from Bilinear Maps. In: Franklin, M. (eds) Advances in Cryptology – CRYPTO 2004. CRYPTO 2004. Lecture Notes in Computer Science, vol 3152. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-28628-8_4

[28] [BBS04]Boneh, D., Boyen, X., Shacham, H. (2004). Short Group Signatures.

In: Franklin, M. (eds) Advances in Cryptology - CRYPTO 2004. CRYPTO 2004. Lecture Notes in Computer Science, vol 3152. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-28628-8

블록체인 확장성 문제해결을 위한 대안기술 분석

인 쇄 : 2023년 12월
발 행 : 2023년 12월

발행인 : 이 원 태
발행처 : 한국인터넷진흥원(KISA, Korea Internet & Security Agency)
전라남도 나주시 진흥길 9 한국인터넷진흥원
Tel: 061-820-1457 | Fax: 061-820-2608
인쇄처 : 하이넷시스템
Tel: (02) 2297-2049

<비매품>