IITP 정보통신기획평가원

2019년 블록체인 융합기술 개발사업

확장가능한 탈중앙화 보안성(DeSecure)

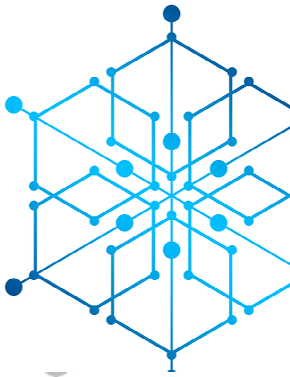
ECCPoW 블록체인

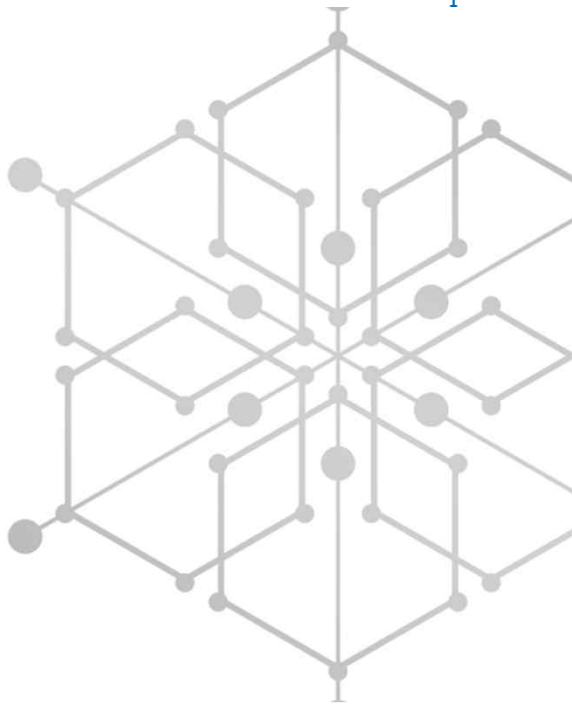
2019.12.05

블록체인 인터넷 경제연구센터 / 센서지능화센터
발표자 : 이흥노 교수

광주과학기술원
Gwangju Institute of Science and Technology

목 차





01

수행기관 현황

수행기관 현황

총괄책임자 연구 역량

연구책임자 | 광주과학기술원 **블록체인 인터넷 경제연구센터 / 센서지능화센터 센터장**

GIST 이흥노 교수

국가스마트도시위원회 민간위원, (사)대한전자공학회 통신소사이어티 회장
우정사업본부 블록체인이니셔티브 민간위원

연구실적

- **국제 논문 (SCI) : 200+편(71+편)**
- 국제 특허 : 출원 9건, 등록 7건
- 국내 특허 : 출원 7건, 등록 22건
- **기술이전 : 2건 (2억 1천만원)**
- 저술 : 8건
- 기술가치평가 : 1건(중앙기술평가원)

대표언론보도

- 프레시안, “GIST, 글로벌 블록체인 개발회사 ‘컨센시스’ 와 MOU” (2019.07.21)
- 스마트시티랩, “블록체인 스마트시티의 유기적 연결의 중추 역할 할 것” (2018.08.24)
- 전자신문, “대한전자공학회 통신소사이어티(회장 이흥노), 19일 블록체인으로 여는 미래’ 워크숍 개최” (2018/04/16)
- 블록체인허브, “블록체·인AI·빅데이터 융합산업 육성 정책토론회”, (2018/12/06)

연구분야

- 블록체인 융합기술
- 블록체인경제
- 지능형 네트워크
- 센서지능화

관련수상이력

- **2019년 대한전자공학회 해동학술상 수상**
- 2016년 GIST 연구상
- **2016년 GIST 대표기술상**
- **2014년 1월 이달의 과학기술자상, 미창부**
- 2013년 기초연구 우수성과 50선, 미창부
- **2012년 국가연구개발 우수성과 100, 미창부**

보유기술현황

보유기술

- GIST는 블록체인의 재중앙화 문제 해결을 위한 **부호-암호 기반의 작업증명** 방식 연구 및 특허 확보 및 출원한 **부호-암호 작업증명 특허** (GIST IP)를 기반으로 블록체인 시스템 개발
- ㈜온더는 이더리움관련 개발 프로젝트를 수행, **블록체인 관련 특허 확보**

특허

특허	출원인	출원번호/등록일	핵심기술
부호-암호 화폐 시스템	광주과학기술원	10-2019-0151246 / 2019.11.12	블록체인의 재중앙화 문제 해결을 위한 핵심 기술
블록체인거버넌스	광주과학기술원	10-2019-0084800 / 2019-07-12	블록체인 거버넌스와 규제
블록체인의 거래검증시스템, 및 블록체인이 거래검증방법	광주과학기술원	10-2019-0120655 / 2019-09-30	블록체인거래검증

02

기술개발의 필요성

블록체인 트랜잭션에 따른 최적 합의 알고리즘 문제 해결

제안 요청서의 문제 정의

01 블록체인 성능 및 신뢰성을 향상시키기 위하여 트랜잭션 종류와 목적에 따라 최적 합의 알고리즘 문제 해결

02 거래처리 속도, 확장성, 보안 등 현 블록체인의 트릴레마 문제를 해결하고 분산 신뢰 인프라 서비스 제공에 필요한 트랜잭션에 따른 합의 알고리즘 필요

블록체인 트릴레마?

01 블록체인에서 분산성/보안성/확장성의 3가지 특성을 확보하는 문제

02 Decentralized Secure (DeSecure) 블록체인으로 문제 해결!

분산성과 보안성 문제 해결의 중요성

분산성을 제고하여 Satoshi Nakamoto가 의도 한 바와 같이
one-cpu-one-vote에 접근 가능하도록 하는 새로운 작업증명 방식의 개발이 필요함

ASIC/FPGA개발, 그리고 채굴 Pool 형성의 억제가 가능하면, 규모의 경제의 효율을 떨어뜨릴 수 있고,
절대 다수의 소규모 채굴 노드의 참여 동기를 부여함

작업증명(Proof-of-Work, PoW)의 효과

01 보안성이 검증된 합의 알고리즘은 작업증명(Proof-of-Work, PoW)

02 가장 규모가 큰 블록체인인 비트코인과 이더리움이 PoW를 사용
지난 수년간 보안 관련 사고 사례가 보고된 적이 없음

03 PoW는 시빌 공격(Sybil Attack)과 이중 지불 공격(Double-Spending Attack)등에 매우 강인하여 화폐 및 금융응용에 적합

분산성과 보안성 문제 해결의 중요성

작업증명(Proof-of-Work, PoW)의 해결과제

01 **ASIC (Application Specific integrated Circuit)의 등장으로 인한 분산성 훼손**

02 ASIC장비와 CPU 혹은 GPU와의 연산속도는 수십만 배 수준으로 차이 발생

03 ASIC을 다수 보유한 전문 채굴업체와 그렇지 않은 소규모 채굴 노드 간의 해시 파워 격차가 크게 발생

04 **규모의 경제 효과에 의한 분산성 훼손**

05 자금력이 풍부한 ASIC장비 투자자들은 소규모 채굴자보다 압도적인 이익을 얻음(기대수익 초선형 양상)

06 반면 투자 여력이 크지 않은 절대다수의 소규모 채굴자들은 참여 동기를 상실함

07 **분산성 약화는 보안성 약화를 유발함**

확장성 문제 해결의 도전성

분산성과 보안성을 훼손하지 않고, TPS를 상향하는 확장성 솔루션이 필요함

01 초당 거래 속도(TPS) 상향의 한계

02 TPS는 블록생성주기를 짧게 설정하거나 블록의 크기를 늘려서 달성 가능

03 비트코인, 이더리움 등의 블록체인 (세계적 네트워크 보유)은 전송지연 문제 보유

04 전송지연 비 고려시 수많은 분기 발생으로 이중 지불 공격에 취약함

05 다중 복합구조 블록체인의 필요

06 다수의 블록체인을 용도/지역/서비스 등 목적에 따라 최적화 후 연결하여 확장성 개선 가능

07 분산성과 보안성이 확장된 작업증명은 파라미터 변경으로 용도별 적용가능

08 다중 블록체인들간의 정보를 교환하는 프로토콜을 개발 할 필요가 있음

작업증명 이외의 다른 합의알고리즘 사용 가능성은?

분산성/보안성/확장성 3요소를 모두 충족하는 합의알고리즘은 없음

01 Proof-of-Stake, Proof-of-Activity, Proof-of-Publication, Delegated PoS, BFT, PBFT 등 다양한 합의알고리즘들이 제안됨

02 이런 합의알고리즘들의 공통된 특징은 블록생성 및 검증에 관여하는 노드의 숫자를 제한하고, 필요한 절차를 간소화해 TPS를 상향함

03 그러나 선별된 소수의 노드가 블록 생성권한을 갖기 때문에 분산성과 보안성이 훼손될 수 있음

04 합의 알고리즘을 분류하면 크게 세 가지로 나눌 수 있음

05 **블록생성과 검증 단계가 통합된 모델 (비트코인 PoW 모델)**

06 블록생성과 블록검증 단계가 분리된 모델(하이퍼레저, PoA 모델, DPoS 모델)

07 블록생성과 블록검증 단계를 분리해서 시작하지만, 결과적으로 통합하는 모델(이더리움2.0 PoS)

작업증명 이외의 다른 합의알고리즘 사용 가능성은?

작업증명에는 블록생성과 블록검증이 통합된 모델이 주는 장점이 있음

01 **블록생성과 검증 단계가 통합된 PoW의 이점**

02 참여한 모든 노드는 블록전파 과정에서 비잔티움 장애, Sybil 공격, 이중지불 문제 등에 노출

03 Longest chain wins 룰과 같은 간단한 정책으로 위의 문제를 모두 해결함

04 나아가 전세계에 분포된 모든 노드에 '일관성'있는 상태 갱신을 보장함

05 즉, 매 블록 생성과 검증을 새로운 상태에서 다시 시작할 수 있는 글로벌 참조 값도 제공함

06 인센티브 메커니즘과 결합하여 지속적이고 자발적 참여를 이끌어 냄

07 분산성을 기반으로 네트워크 지연, DDoS공격, 단일 취약점 장애, 비잔티움 문제에 강인하게 대처

Lex Cryptographia

작업증명은 Lex Cryptographia 실현을 촉진함

01 **Lex Cryptographia란 On-chain 정책의 사회적 확대에 의해 국제사회에서 P2P를 통해 계약을 맺고, 이행과 결산을 신뢰받는 제 3자 개입 없이 합의 할 수 있게 되는 이상적 미래 사회를 의미함 (P. De Filippi 교수)**

02 전통적 사회적 규범에 의존하지 않고 블록체인 프로토콜에 의해 합의를 의미

03 재 시점에서 Lex Cryptographia의 완전한 실현은 현실적이지 않음

04 On-chain 정책의 확대에도 불구하고 사람들 사이에 새로운 권력의 출현은 불가피함 (e.g., 영향력이 큰 소수의 개발자, 압도적 해시 파워의 채굴자)

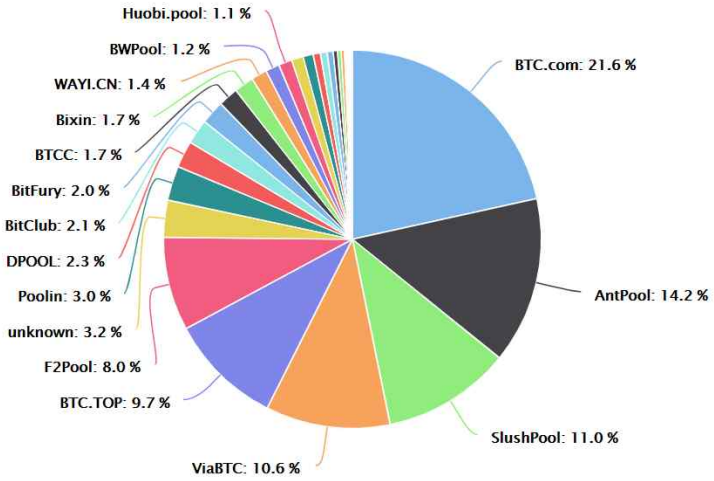
05 따라서 Off-chain 기존의 정치/경제/법제도 등에 의존하게 됨

06 만약 작업증명의 분산성이 보장되면 Off-chain 정책의 의존도를 크게 완화할 수 있음

PoW 문제점을 해결, 제안기술의 도전성, 혁신성

PoW 재 중앙화, 전력소비 문제를 해결하는 새로운 작업증명 기술 개발 필요

- ASIC 채굴기의 출현, 소수의 채굴 점유, 재 중앙화 문제 발생
- 소수 채굴업자 블록체인 보상 독점
- 채굴업자 담합, 블록 ·위변조 위험 대두



중앙화 된 블록체인 네트워크

탈 중앙화 된 블록체인 네트워크

Proof-of-XXX, Alternatives to PoW

	Pros	Cons	Coins within top 50 rank
PoW (Proof-of-Work)	▪ Strong security ▪ Difficult to produce ▪ Easy to verify	▪ Extreme computing power ▪ 51% attacks ▪ Transaction speed / Transaction throughput	Bitcoin, Ethereum
PoS (Proof-of-Stake)	▪ Energy & hardware efficiency ▪ Much more expensive 51% attacks	▪ Recentralization ▪ The rich-get-richer ▪ “Nothing at stake” problem	Qtum, Stratis
DPoS (Delegated PoS)	▪ Scalability and speed ▪ Energy & hardware efficiency ▪ Encouraging good behavior by real-time voting	▪ Recentralization ▪ DDoS attacks	EOS, NEO smart economy
PoA (Proof-of-Activity)	▪ Much more expensive 51% attacks ▪ Decentralization ▪ Validators are randomly selected.	▪ Extreme computing power ▪ Recentralization ▪ The rich-get-richer	decred

03

기술개발의 목표

기술 개발 개요

GIST 블록체인

- 블록체인의 재중앙화 문제 해결을 위한 부호-암호 기반의 작업증명 방식 연구
- 출원한 암호-부호 작업증명 특허(GIST IP)를 기반으로 블록체인 시스템 개발
- 개발한 블록체인 시스템을 기존 암호화폐(비트코인/이더리움)에 적용 및 확산

1차년도

ECCPoW 코어 1.0 연구 및 개발

확장성	기존 암호화폐(비트코인, 이더리움) 적용
보안성	매 블록 변경 암호퍼즐, 디코더 개발
분산성	블록 생성 주기 제어

2차년도

ECCPoW 코어 2.0 연구 및 개발

확장성	다중 복합구조 블록체인, 플라즈마 EVM 적용
보안성	거래검증 최적화 알고리즘, 데이터 가용성 개선
분산성	블록 생성 제어 방법 고도화

트릴레마 문제 해결 전략

1단계	ASIC 채굴에 저항성이 있는 ECCPoW를 개발 **(분산성 향상)**
1단계	비트코인과 이더리움에 ECCPoW를 탑재 및 하드포크
2단계	이중 지불 공격 등 블록체인에서 문제가 되는 공격들에 대한 방지 알고리즘을 개발 **(보안성 향상)**
2단계	다중 복합구조의 DeSecure 블록체인들을 설계하여 **거래의 종류/목적에 따라 독립적으로 최적화**하고, 이들을 계층적으로 연결함 **(확장성 향상)**
2단계	이더리움의 레이어2 확장성 솔루션인 플라즈마를 DeSecure 블록체인에 적용 **(유연성 향상)**

- 오류 정정 부호 (Error Correction Codes)를 활용한 새로운 Anti-ASIC PoW 알고리즘인 ECCPoW를 개발하고자 함
- DeSecure 블록체인은 비트코인과 이더리움에 ECCPoW를 탑재하여 하드포크한 새로운 블록체인을 의미함

04

성과내역 (1차 년도 보고)

연구 개발 성과 _ 특허

(목표) 2건의 국내 출원, 2건의 국외 출원
(성과) 4건의 국내 출원, 2건의 국외 출원 – 1건은 현재 진행 중
(달성도) 국내 : 200% 달성 확정, 국외 : 100% 달성 예정

번호	지식재산권 등 명칭	국명	출원		
			출원인	출원일	출원번호
1	부호-암호 화폐 시스템[증빙자료 p.154]	KOR	광주과학기술원	2019-11-12	10-2019-0151246
2	블록체인의 거래검증시스템 및 블록체인이 거래검증방법[증빙자료 p.76]	KOR	광주과학기술원	2019-09-30	10-2019-0120655
3	블록체인거버넌스[증빙자료 p.113]	KOR	광주과학기술원	2019-07-12	10-2019-0084800
4	블록체인의 거래검증시스템, 및 블록체인이 거래검증방법[증빙자료 p.76]	PCT	광주과학기술원	진행 중	

연구 개발 성과 _ 국내 및 국외 논문 게재

(목표) 0건의 국내, 0건의 국외
(성과) 2건의 국내 학회, 2건의 석사 학위 논문, 4건의 국외 논문 준비 중

번호	논문명	학술지명	국명	발행기관	SCI 여부	게재일
1	A Blockchain For The Collision Avoidance And The Recovery of Crashed UAVs[증빙자료 p.199]	대한전자공학회 2019년도 하계종합학술대회	국내	대한전자공학회	비 SCI	2019-06-07
2	A Permissioned ISPs Blockchain For The End to End Quality of Service Enhancement[증빙자료 p.192]				비 SCI	2019-06-07
3	Time-Variant Proof-of-work using Error-Correction codes	Under revision	국외			
4	Profitable Double-Spending Attacks	Under revision	국외			
5	A Blockchain-Based Distributed Patient-Centric Image Management System	Under revision	국외			
6	Fine difficulty control for ECCPoWs	Under revision	국외			

연구 개발 성과 _ 국내 및 국제 학술대회 발표

8건의 국내 학술대회 발표
1건의 학술 대회 조직

번호	논문명	발표자	발표일시	장소
1	블록체인 법학회 컨퍼런스	이흥노	2019.10.22	서울
2	블록체인 법학회 컨퍼런스	이흥노	2019.08.28	서울
3	대한전자공학회 2019년도 하계종합학술대회	Yaseen Jabarulla	2019.06.27	제주도
4	대한전자공학회 2019년도 하계종합학술대회	Michele Scarlato	2019.06.27	제주도
5	블록체인으로 여는 미래사회 Workshop	이흥노	2019.06.17	서울
6	ETHcon Korea 2019	이흥노	2019.05.27	서울
7	ETHcon Korea 2019	장재혁	2019.05.27	서울
8	JCCI 2019	이흥노	2019.05.01	강릉
9	한국 ICT 금융학회 세미나	이흥노	2019.04.19	국회 도서관

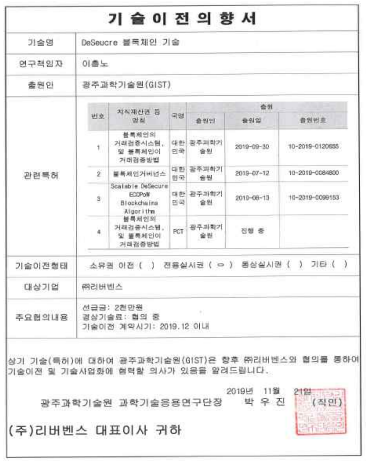
블록체인으로 여는 미래 사회
Workshop

연구 개발 성과 _ 기술 이전

(목표) 1건의 기술 이전, 1000만원의 기술료
(성과) 1건의 기술 이전, 2000만원의 기술료
(달성도) 기술료 200%달성

번호	기술 이전 유형	기술 실시 계약명	기술 실시 대상 기관	기술 실시 발생일	기술료 (해당 연도 발생액)	누적 징수 현황
1	전용실시	DeSecure 블록체인 기술	LiberVance (리버밴스)	2019.12 (체결 예정)	20,000,000 (선급기술료)	20,000,000 (선급기술료)

LiberVance는 본 과제의 연구책임자가 설립한 회사
12월 중으로 체결 예정 – (기술 이전 의향서 완료) [증빙자료 p.204]
대상은 본 과제의 실적으로 보고된 광주과학기술원의 특허
중기부 예비창업자패키지 과제선정 (2019.10.1 ~ 2020.7.31, 5500만원)



기 술 이 전 의 향 서

기술명	DeSecure 블록체인 기술
연구책임자	이홍노
출원인	광주과학기술원(GIST)
관련특허	출원 — 번호 / 지식재산권 등의 명칭 / 국명 / 출원인 / 출원일 / 출원번호
	1 / 블록체인의 거래검증시스템, 및 블록체인이 거래검증방법 / 대한민국 / 광주과학기술원 / 2019-09-30 / 10-2019-0120685
	2 / 블록체인거버넌스 / 대한민국 / 광주과학기술원 / 2019-07-12 / 10-2019-0084800
	3 / Scalable DeSecure ECDHE Blockchains Algorithm 블록체인의 / 대한민국 / 광주과학기술원 / 2019-08-13 / 10-2019-0099153
	4 / 거래검증시스템, 및 블록체인이 거래검증방법 / PCT / 광주과학기술원 / 진행 중 /
기술이전형태	소유권 이전 ( ) 전용실시권 (⇔) 통상실시권 ( ) 기타 ( )
대상기업	㈜리버밴스
주요협의내용	선금금: 2천만원 결상기술료: 협의 중 기술이전 계약시기: 2019.12 이내

상기 기술(특허)에 대하여 광주과학기술원(GIST)은 향후 ㈜리버밴스와 협의를 통하여 기술이전 및 기술사업화에 협력할 의사가 있음을 알려드립니다.

2019년 11월 21일

광주과학기술원 과학기술융용연구단장 박 우 진 (직인)

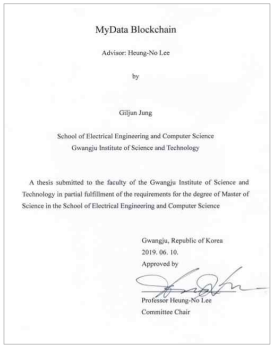
(주)리버벤스 대표이사 귀하

연구 개발 성과 _ 연구 인력 양성 및 고용 창출

(목표) 0건의 연구 인력 양성, 2건의 고용 창출
(성과) 2건의 연구 인력 양성, 5건의 고용 창출
(성과도) 연구 인력 양성은 초과 달성, 고용 창출은 250% 달성

번호	소속	이름	학위	제목
1	광주과학기술원	정길준 [증빙자료 p.523]	석사	MyData Blockchain
2	광주과학기술원	박상준 [증빙자료 p.522]	박사	Compressed Sensing for Support Set Reconstruction : Information-Theoretic Results and Design of Practical Algorithm

번호	채용기관	이름	채용 직위	채용	직무내용
1	광주과학기술원	이수민	위촉 연구원	2019.8.1. ~	블록체인 개발/경제/하드포크
2	광주과학기술원	이명은	위촉 연구원	2019.11.20. ~	블록체인 연구 및 기획
3	광주과학기술원	조성민	인턴	2019.3.1 ~ 2019.7.31	블록체인 개발
4	광주과학기술원	김석주	인턴	2019.3.1 ~ 2019.7.31	블록체인 개발
5	광주과학기술원	Michele Scarlato	인턴	2019.4.1 ~	블록체인 관련조사 및 연구


MyData Blockchain

Advisor: Heung-No Lee

by

Giljun Jung

School of Electrical Engineering and Computer Science
Gwangju Institute of Science and Technology

A thesis submitted to the faculty of the Gwangju Institute of Science and Technology in partial fulfillment of the requirements for the degree of Master of Science in the School of Electrical Engineering and Computer Science

Gwangju, Republic of Korea
2019. 06. 10.
Approved by

Professor Heung-No Lee
Committee Chair


Compressed Sensing for Support Set Reconstruction:
Information-Theoretic Results and Design of Practical Algorithm

Advisor: Heung-No Lee

by

Sangjun Park

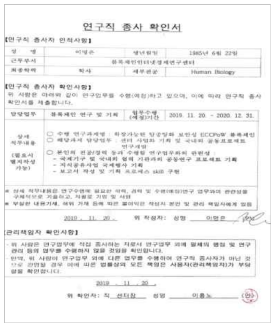
School of Electrical Engineering and Computer Science
Gwangju Institute of Science and Technology

A thesis submitted to the faculty of the Gwangju Institute of Science and Technology in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the School of Electrical Engineering and Computer Science

Gwangju, Republic of Korea
May 31, 2019
Approved by

Professor Heung-No Lee
Committee Chair


기간제근로자 고용계약서


연구직 종사 확인서

연구 개발 성과 _ 기술요약정보 & 보고서 원문

(목표) 1건의 기술요약정보, 1건의 보고서 원문
(성과) 1건의 기술요약정보, 3건의 보고서 원문
(성과도) 기술요약정보 100% 달성, 보고서 300% 달성

연도	기술명	요약 내용	기술 완성도
2019	DeSecure 기술	LDPC 코드명세서, DeSecure Blockchain 매뉴얼 (Code Level, Bitcoin-ECC Build 및 Docker 사용 법) [증빙자료 p.192] **총 58페이지**	V. 1.0

연도	보고서 구분	발간일
2019	DeSecure 블록체인의 미래 성장 전략 도출 [증빙자료 p.265] **총218페이지**	2019. 11
2019	ECCPoW 적용 영역 연구	2019. 12월 중
2019	ECCPoW Blockchain 확장가능 비즈니스 모델 개발 [증빙자료 p.483] **총38페이지**	2019. 11

연구 개발 성과 _ 프로그램 산출물

부호-암호 작업증명 (ECCPoW)
부호-암호 작업증명이 탑재된 비트코인/이더리움

이름	목적	Github 주소
ECCPoW	암호 퍼즐 생성 (디코딩) 암호 퍼즐 해결 유무 판단 암호 퍼즐 난이도 조절	github.com/cryptoecc/bitcoin_ECC 최초생성일 : 2019.5.23 commit : 66회
BTCECC	ECCPoW가 탑재된 비트코인	
ETHECC	ECCPoW가 탑재된 이더리움	github.com/cryptoecc/go-ethereum_ECC 최초생성일 : 2019.5.20 commit : 82회

05

기술개발 내용 (1단계 보고)

5.1 ECCPoW 버전 1.0 개발
5.2 ECCPoW 개발 및 기존 암호화폐(비트코인) 시스템에 적용
5.3 ECCPoW 개발 및 기존 암호화폐(이더리움) 시스템에 적용
5.4 BTCECC/ETHECC 평가 결과

당해 (연·도단계) 연구 개발 목표 및 결과

ECCPoW 코어 버전 1.0 연구 및 개발

세부 연구 목표	연구개발 수행 내용	연구 결과	담당
ECCPoW 버전1.0 개발	▪ 매 블록마다 바뀌는 암호 퍼즐 생성 연구 ▪ 매 블록마다 바뀌는 암호 퍼즐 디코더 개발	▪ 매 블록마다 바뀌는 암호 퍼즐 생성/디코더 개발 완료	주관 기관
ECCPoW 개발 및 기존의 암호화폐(비트코인) 시스템에 적용	▪ 블록 생성 주기 제어 방법 연구 ▪ 시스템 테스트 및 고도화	▪ 블록 생성 주기 제어 방법 연구 및 구현 완료 ▪ 시스템 테스트 및 고도화 완료	
ECCPoW 개발 및 기존의 암호화폐(이더리움) 시스템에 적용)	▪ go-ethereum 패키지 연구 및 분석 (합의 계층 내부구조 변경, 공통 계층 최적화, 응용 계층 개발, 데이터 계층 개발) ▪ 블록 생성 주기 제어 방법 연구 ▪ 시스템 테스트 및 고도화	▪ go-ethereum에 ECCPoW 탑재 완료 ▪ 블록 생성 주기 제어 방법 연구/구현 완료 시스템 테스트 및 고도화 완료	참여 기관

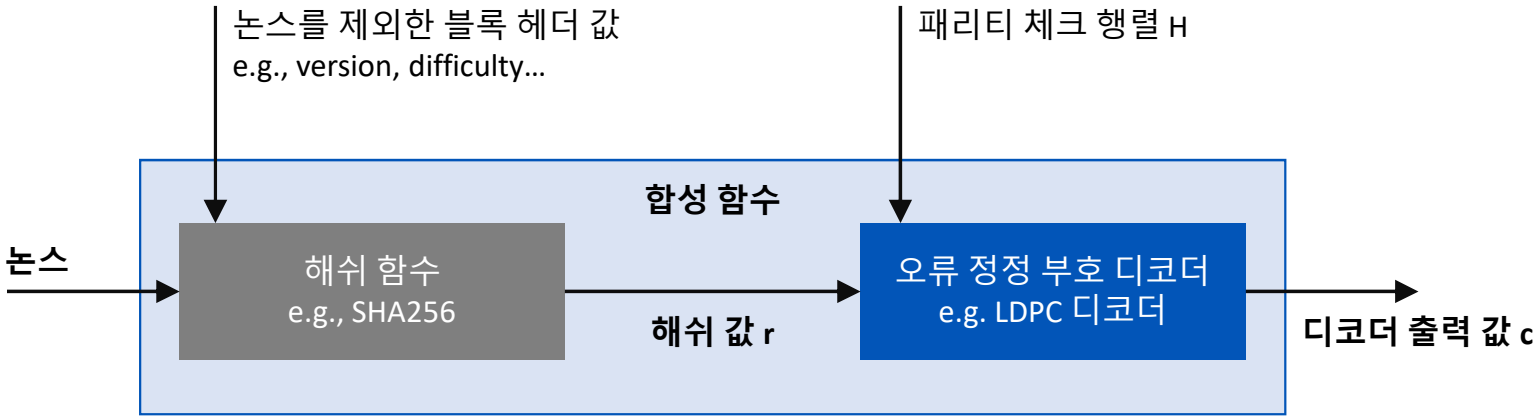
부호 – 암호 작업증명 버전 1.0 주요 함수

함수 이름	인력 값	설명
set_difficulty	int level	암호 퍼즐의 난이도 설정
generate_seeds	uint64_t hash	이전 해시 값으로부터 시드를 결정
generate_H	none	시드를 이용하여 패리티 체크 행렬을 생성. 행렬의 크기는 level에 의해 결정
generate_hv	Unsigned char hash[]	해시 값을 0/1로 구성된 문자들로 전환하여 hash_vector에 저장
decoding	none	메시지 전달 알고리즘을 사용하여 디코딩하고 그 결과를 output_word에 저장
decision	none	output_word가 암호 퍼즐의 해결 유무를 만족하는지 판단
binary_to_hex	none	2진 문자열인 디코더의 출력 값을 16진수 문자열로 치환

- 부호-암호 작업증명의 주요 함수
- https://github.com/cryptoecc/bitcoin_ECC/blob/ecc-0.1/src/ldpc/ldpc.h
- C++언어로 작성

부호 – 암호 작업증명

- 부호-암호 작업증명 (ECCPoW) 정의 :
  오류 정정 부호와 작업증명을 동시에 사용하여 분산성/보안성을 확보하기 위해 개발된 작업증명 기술임.
- ECCPoW은 매 블록마다 변하는 합성 함수를 사용함.



- (**시변성**) 패리티 체크 행렬을 매 블록 마다 변경함으로써, 함성 함수를 매 블록 마다 변경 할 수 있음.
- (**무한성**) 무한히 많은 패리티 체크 행렬을 사용하면, 무한히 많은 합성 함수를 생성 할 수 있음.

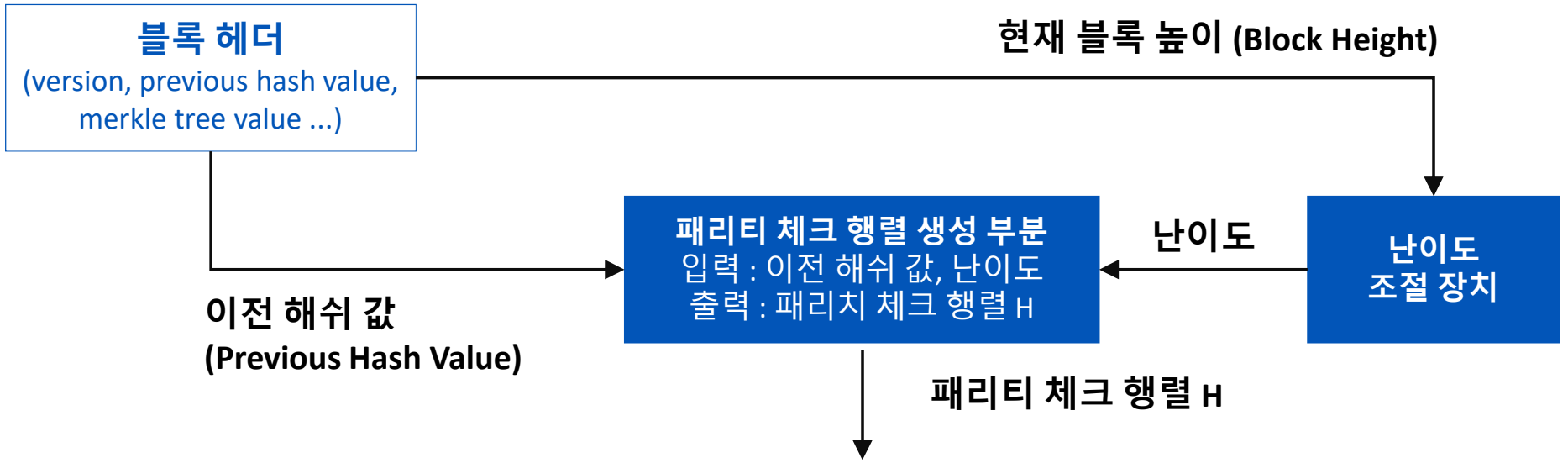
부호 – 암호 작업증명 _ 5가지 특성

요건 1	암호 퍼즐은 풀기 어려우나, 반대로 검증은 쉬워야 함.
요건 2	풀린 암호 퍼즐의 정답은 재사용되지 않아야 함.
요건 3	암호 퍼즐의 난이도는 조절 가능해야 함.
요건 4	암호 퍼즐은 외부 공격으로부터 견고한 저항성을 가져야 함.
요건 5	**(시변성/무한성) 작업증명에 쓰이는 함수는 매 블록마다 변화하여 바꿀 수 있어야 함.** 부연 설명 : 매 블록마다 패리티 체크 행렬이 변경됨. 따라서 디코더의 입력 값과 출력 값의 관계가 바뀌므로 합성 함수의 입력 값과 출력 값이 관계 또한 바뀜. 작업증명에 사용되는 함수의 변경을 의미함.

- 요건 1 – 4는 작업증명이라면 가져야 할 기본 요건.
- 요건 5는 고유 특징으로써 시변성과 무한성을 뜻함.
- 패리티 체크 행렬은 "블록 길이", "부호 비율" 등을 변경함으로써 서로 다른 행렬들을 무한히 많이 생성 가능함.

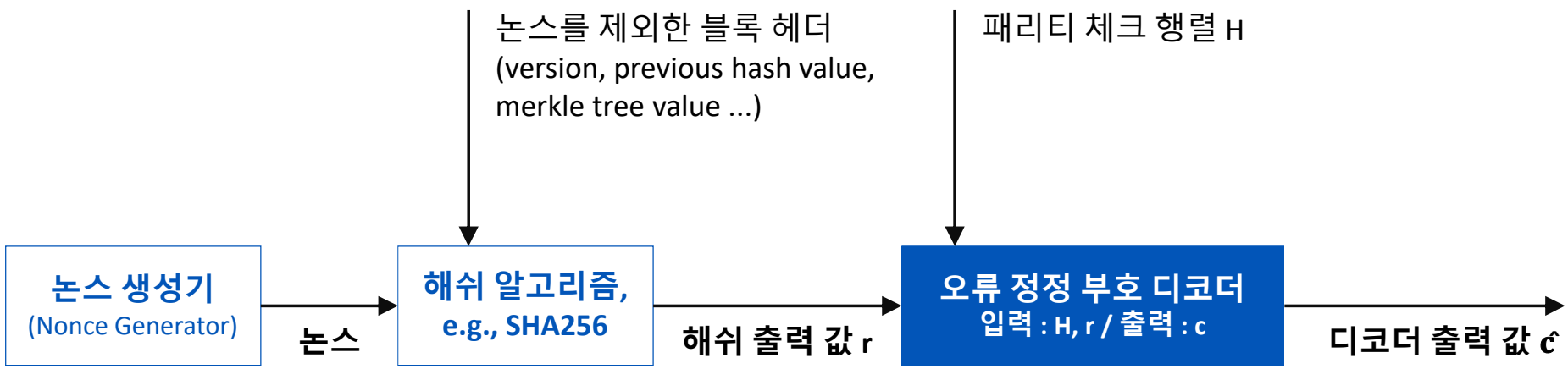
매 블록마다 바뀌는 암호 퍼즐 생성 (1)

- 난이도는 "블록 길이" 및 "부호의 비율"을 결정
- 이전 해쉬 값을 이용해 Gallager 생성 방법의 순열 순서를 결정



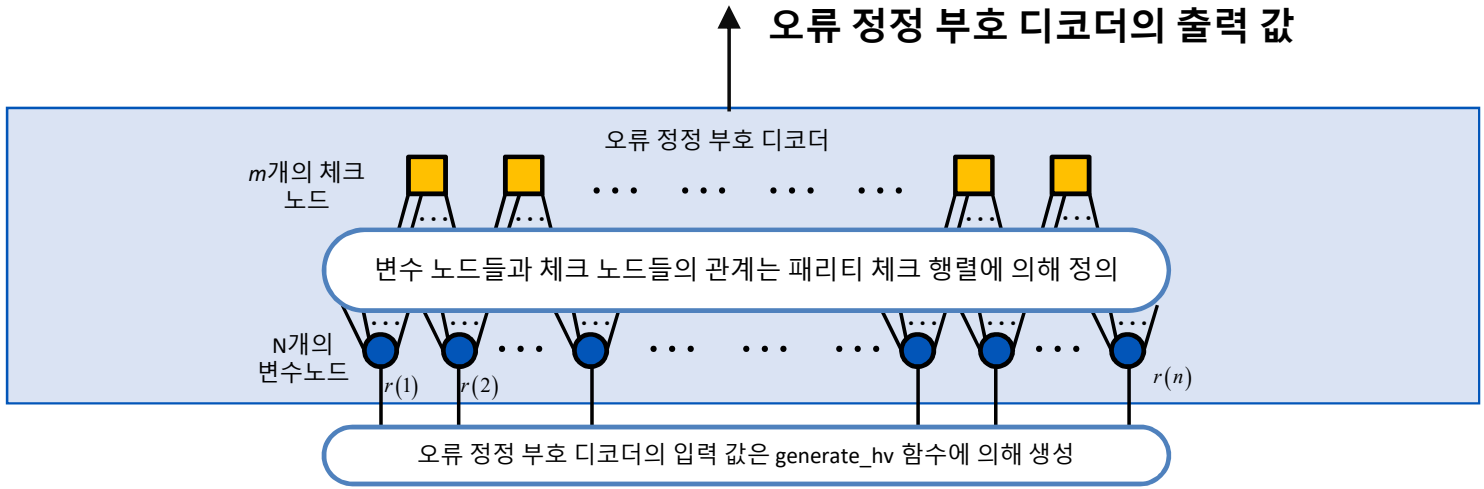
매 블록마다 바뀌는 암호 퍼즐 디코더 개발 (1)

- 오류 정정 부호 디코더 입력 값 생성



매 블록마다 바뀌는 암호 퍼즐 디코더 개발 (2)

- 오류 정정 부호 디코더 입력 값 생성



- 패리티 체크 행렬의 변경은 변수/체크 노드들의 관계의 변경을 야기함.
- 즉, 동일한 입력 값을 취득하더라도, 패리티 체크 행렬이 변경되면 상이한 값을 산출함.
- 디코딩은 메시지 전달 알고리즘에 의해 이뤄짐.

암호 퍼즐 해결 유무 판단 기준

- 2가지 서로 다른 암호 퍼즐 해결 유무 판단 기준을 제시함

기준 1	**독자적인 방식 :** 디코더의 결과 값이 a) 부호이고, b) 특정 해밍 가중치를 가지면 해결 한 것으로 판단.
기준 2	**기존 작업증명 방식 :** 디코더의 결과 값을 다시 해싱 하여 나온 값이 특정 값 보다 작으면 해결 한 것으로 판단.

- **(기준 1)** 디코더의 출력 값 c가 다음 2가지 조건들을 만족시키면, 암호 퍼즐을 해결 하는 것으로 판단
  (조건 1) 출력 값이 부호일 것.
  (조건 2) 출력 값의 해밍 가중치가 주어진 집합 S의 원소 일 것.

조건 1이 만족할 확률 $p_1 := \Pr\{\mathbf{c} | \mathbf{Hc} = \mathbf{0}\}$

조건 2가 만족할 확률 $p_2 := \Pr\{\|\mathbf{c}\|_h \in S\}$

기준 1 _ 부호의 특징을 이용한 것

- 조건 1과 조건 2를 만족시킬 확률을 구하고, 이를 통해 암호 퍼즐의 난이도를 총 380개로 세분화 함.

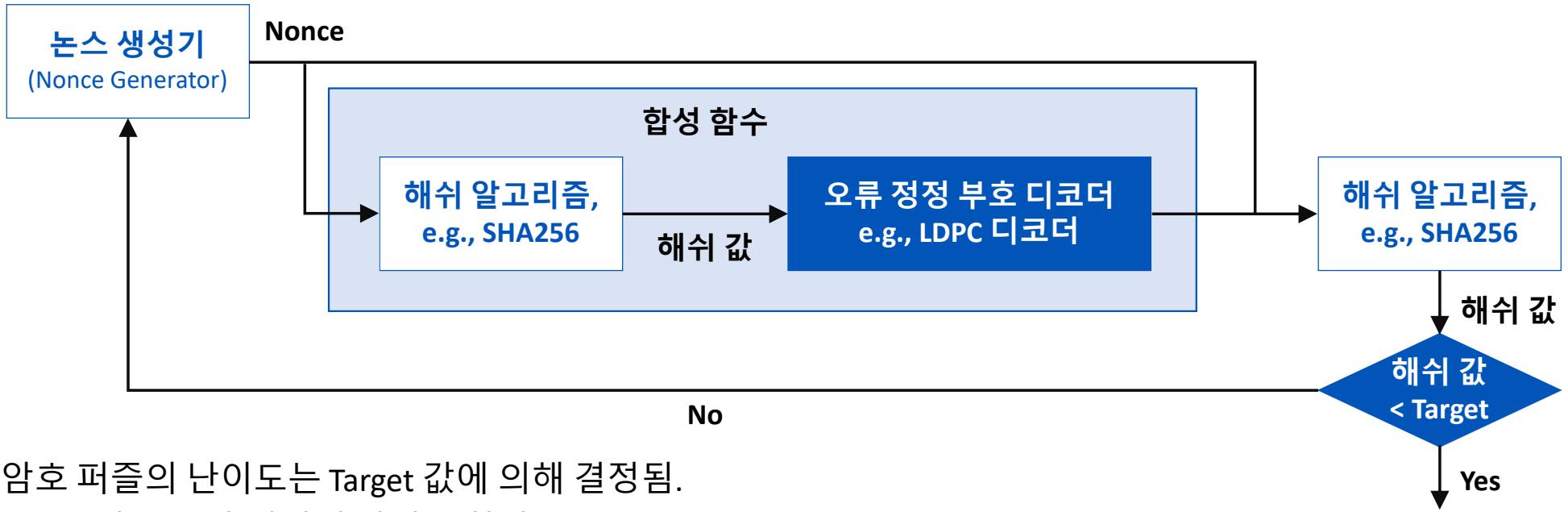
Level	n	w_c	w_r	집합 S	$p := \Pr\{\mathbf{c}\|\mathbf{Hc}=\mathbf{0}\} \times \Pr\{\|\mathbf{c}\|_h \in S\}$
1	32	3	4	{10,12,…,20,22]	$\approx 3.07 \times 10^{-5}$
2	32	3	4	{10,12,…,14,16}	$\approx 2.02 \times 10^{-5}$
				…	
379	128	3	4	{34,94}	$\approx 5.12 \times 10^{-23}$
380	128	3	4	{34}	$\approx 2.60 \times 10^{-23}$

난이도 하락

난이도 상승

기준 2 _ 기존 작업 증명 것

- 합성 함수의 출력 값을 다시 한번 해싱하여 나온 결과 값으로 판단함.



- 암호 퍼즐의 난이도는 Target 값에 의해 결정됨.
- Target 값을 증가 시키면 난이도 하락
- Target 값을 감소 시키면 난이도 상승

부호-암호 작업증명 버전 1.0 주요 함수

	함수 이름	입력 값	설명
암호 퍼즐 난이도 조절	set_difficulty	int level	암호 퍼즐의 난이도 설정
암호 퍼즐 생성	generate_seeds	uint64_t hash	이전 해시 값으로부터 시드를 결정
	generate_H	none	시드를 이용하여 패리티 체크 행렬을 생성 행렬의 크기는 level에 의해 결정
암호 퍼즐 디코더	generate_hv	unsigned char hash[]	해시 값을 0/1로 구성된 문자들로 전환하여 hash_vector에 저장
	decoding	none	메시지 전달 알고리즘을 사용하여 디코딩하고 그 결과를 output_word에 저장
암호 퍼즐 해결 유무 판단	decision	none	output_word가 암호 퍼즐의 해결 유무를 만족하는지 판단
	binary_to_hex	none	2진 문자열인 디코더의 출력 값을 16진수 문자열로 치환

- https://github.com/cryptoecc/bitcoin_ECC/blob/ecc-0.1/src/ldpc/ldpc.h
- C++언어로 작성

ECCPoW 하드포크의 의미는 합의엔진 교체

블록체인 프로그램 코어 (블록체인 구성 요소 3가지)

1. Web server interface networking of peers

- Node registration, get-address, give-address
- Full node or light node
- Communication among the wallets and the miners

2. Wallet for TX generations

- Make private and public keys, address, store UTXOs, make TX, put signature, announce it to the neighbor, check to see if the TX is supported by the blockchain.

합의엔진

3. Consensus Mechanism

- **Data :** Genesis block + regular blocks, one block every 10 min, block-size 1Mbyte
- **Protocol :** consensus, block header, difficulty level adjustment, …
- **Mining :** Get the longest chain, validate it and all transactions within it, get transactions from mempool and form a block, run SHA repeatedly until you hit a good hash, put the proof into the block header, and attach the proofed block to the longest chain, and make announcement ASAP.

- 비트코인/이더리움의 작업증명을 ECCPoW로 교체

ECCPoW가 적용된 비트코인 (BTCECC)

- 비트코인의 블록 헤더를 그대로 사용.
- BTCECC (ECCPoW가 적용된 비트코인)의 제네시스 블록 생성.
- 비트코인의 작업증명과 관련된 부분을 ECCPoW의 것으로 교체.
- 비트코인의 난이도 조절과 관련된 부분을 변경.

<주요 변경 및 추가 함수>

타입	함수 이름	위치	함수의 역할
변경	CMainParams	chainparms.cpp	제네시스 블록 생성 함수
추가	CheckProofOfWork	pow.cpp	암호 퍼즐 해결 유무 판단 함수
	GetLevelfromnBits	pow.cpp	비트코인의 난이도를 ECCPoW 암호 퍼즐 난이도로 맵핑

기본 비트코인의 난이도 조절

- 2016개의 블록 채굴 후에 난이도 조절이 발생하게 설계됨.
- 관련 함수는 CalculateNextWorkRequired

```
unsigned int CalculateNextWorkRequired(const CBlockIndex* pindexLast, int64_t nFirst
{
    int64_t nActualTimespan = pindexLast->GetBlockTime() - nFirstBlockTime;
    if (nActualTimespan < params.nPowTargetTimespan / 4)
        nActualTimespan = params.nPowTargetTimespan / 4;
    if (nActualTimespan > params.nPowTargetTimespan * 4)
        nActualTimespan = params.nPowTargetTimespan * 4;

    const arith_uint256 bnPowLimit = UintToArith256(params.powLimit);
    arith_uint256 bnNew;
    bnNew.SetCompact(pindexLast->nBits);
    bnNew *= nActualTimespan;
    bnNew /= params.nPowTargetTimespan;

    if (bnNew > bnPowLimit)
        bnNew = bnPowLimit;

    return bnNew.GetCompact();
```

01 급격한 난이도 변경을 막기 위함

02 난이도 변경을 위해 Target 값을 증감

03 만일 변경된 Target이 최소 값 보다 작으면, 최소 값으로 설정

- CalculateNextWorkRequired는 매 블록을 생성/검증 할 때 마다 호출됨.

BTCECC 난이도 조절

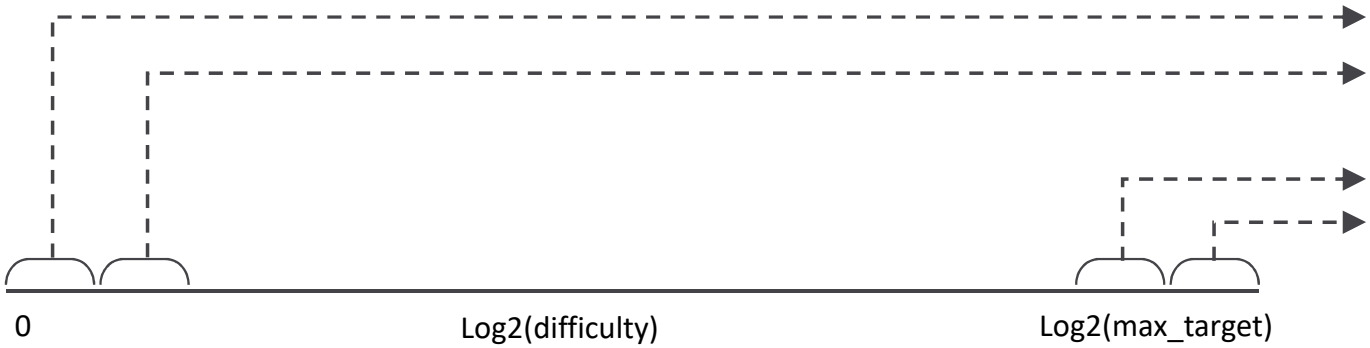
- ECCPoW 암호 퍼즐의 난이도를 380개로 세분화
- nBits를 이용해 difficulty를 계산하고, 이 difficulty 값을 이용해 기 제작된 난이도 테이블로 맵핑

```
int GetLevelfromnBits(uint32_t nBits)
{
    int level = 1;
    double dDiff = 0.0, log_dDiff = 0.0;
    dDiff = GetDifficulty(nBits);
    log_dDiff = log2(dDiff);
    level = floor(log_dDiff / 0.3) + 1;

    if (level >= 380)
        level = 380;
    if (level <= 1)
        level = 1;

    return level;
}
```

01 ECCPoW 암호 퍼즐 난이도로 맵핑

02 현재는 380레벨만 지원

Level	n	w_c	w_r	집합 S
1	32	3	4	{10,12,…,20,22]
2	32	3	4	{10,12,…,14,16}
				…
379	128	3	4	{34,94}
380	128	3	4	{34}



BTCECC 작업증명

- pow.cpp의 CheckProofOfWork 함수를 변경

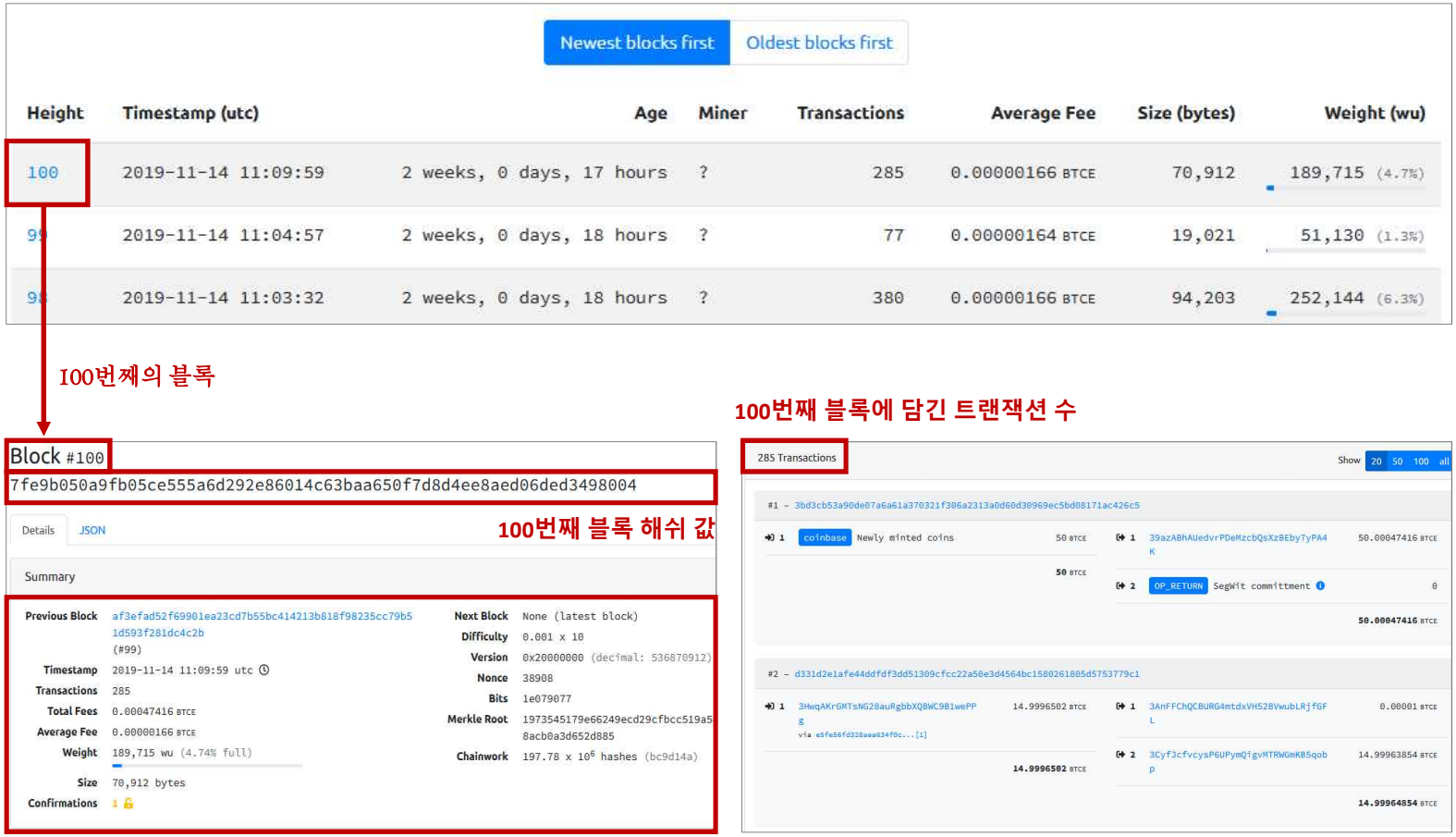
```
bool CheckProofOfWork(CBlockHeader block, const Consensus::Params& params)
{
    bool fNegative; bool fOverflow; bool result = false;

    arith_uint256 bnTarget;
    bnTarget.SetCompact(block.nBits, &fNegative, &fOverflow);

    // Check range
    if (fNegative || bnTarget == 0 || fOverflow || bnTarget > UintToArith256(params.powLimit))
        return result;

    int level = GetLevelfromnBits(block.nBits);
    LDPC *ldpc = new LDPC;
    ldpc->set_difficulty(level);
    ldpc->initialization();
    ldpc->generate_seeds(UintToArith256(block.hashPrevBlock).GetLow64());
    ldpc->generate_H();
    ldpc->generate_Q();
    ldpc->generate_hv((unsigned char*)block.GetHash().ToString().c_str());
    ldpc->decoding();
    if (ldpc->decision())
        result = true;

    delete ldpc;
    return result;
```

01 nBits의 유효성 검사

02 암호 퍼즐 난이도 결정

03 암호 퍼즐 생성 및 검증

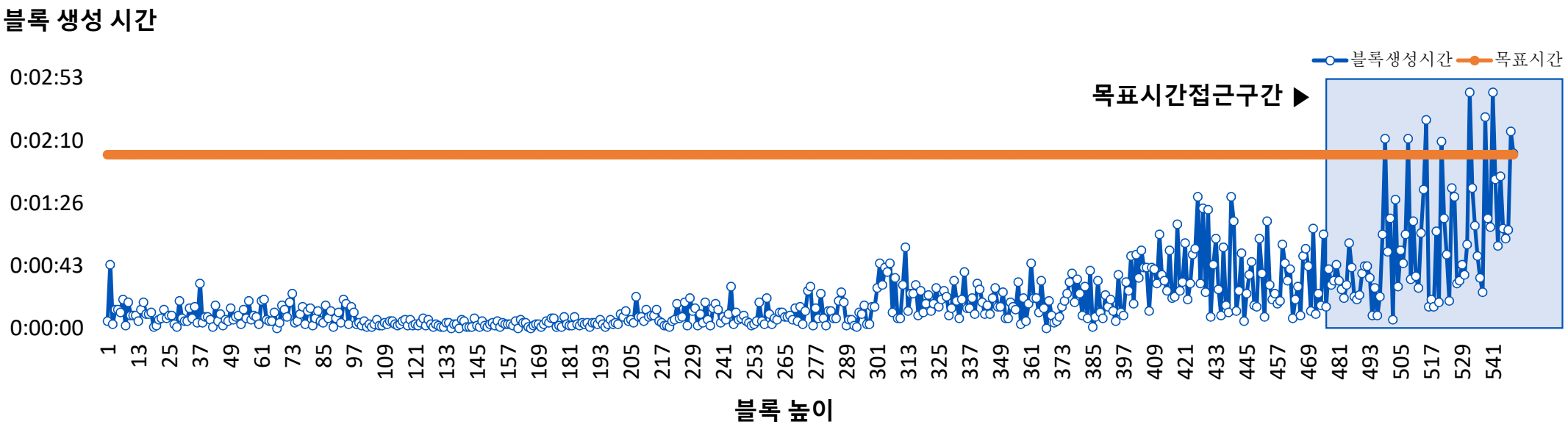
BTCECC 블록 탐색기



* 블록체인 탐색기(http://15.164.244.139/blocks)에서 확인 가능

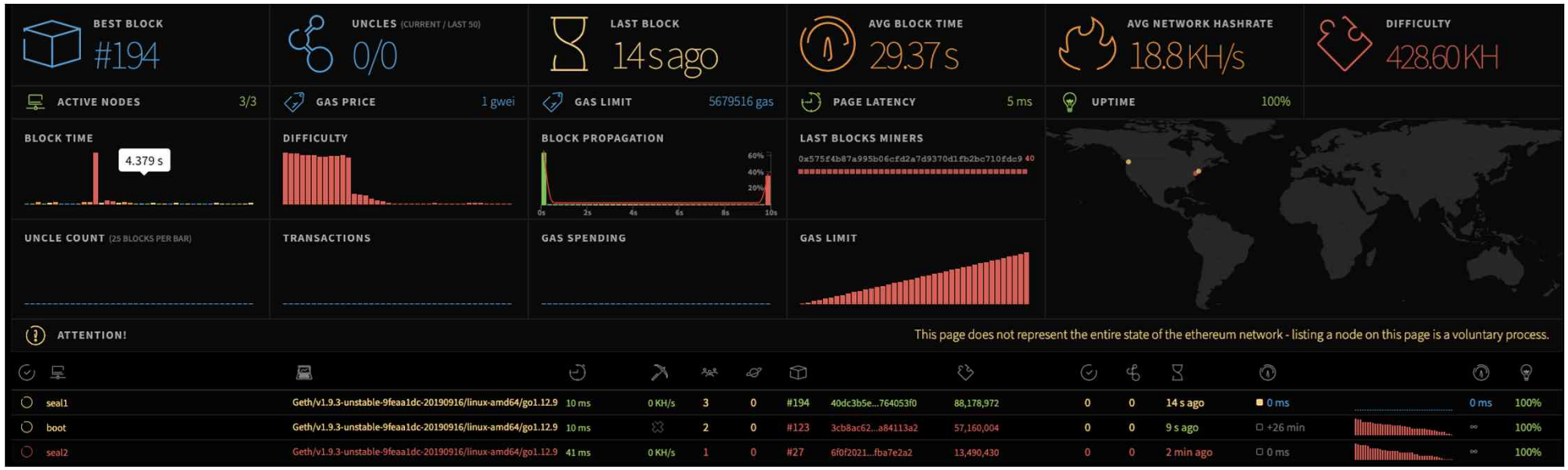
BTCECC 난이도 조절 기능 검증

<블록생성시간-블록높이 그래프(블록 생성 목표시간 2분)>



- 난이도 변경 높이 이전의 총 블록 생성시간을 계산하여 생성시간이 빠르면 난이도를 증가시키고 낮으면 난이도를 감소시킴
- 난이도 증감을 통해 목표 시간 접근 구간 확인 가능
- 위의 그래프는 블록체인 탐색기(http://13.209.74.13/blocks)를 통해 확인 가능

puppeth를 이용하여 배포된 프라이빗 네트워크



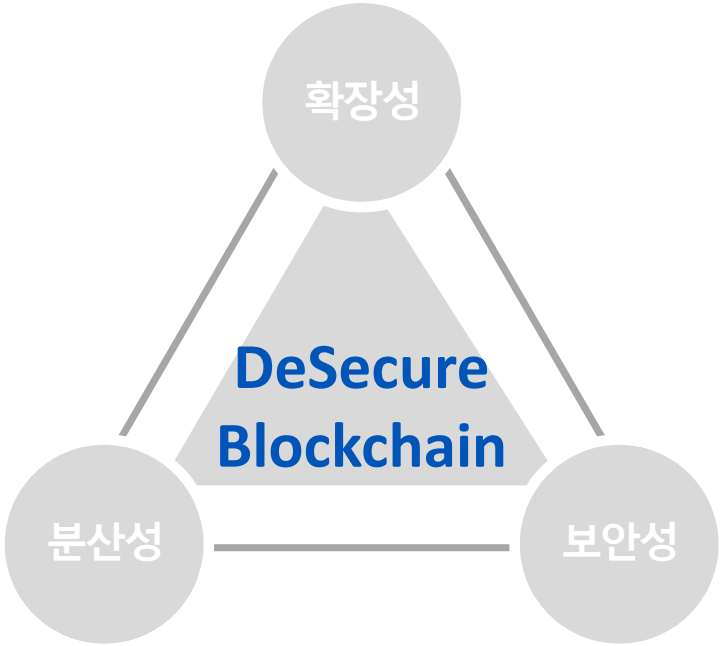
- puppeth를 통해 배포된 ETHECC의 대시보드
- 평균 블록 생성시간 현재 블록 넘버, 마지막 블록 생성 후 경과한 시간 등을 확인 가능
- 대시보드와 통신하고 있는 여러 노드들의 상태를 한번에 관찰 가능
- 노드숫자 4대, 네트워크 생성초기라 29.37초이며 시간에 지남에따라 10~15초 형성

06

2단계 연구계획

2단계 연구 계획

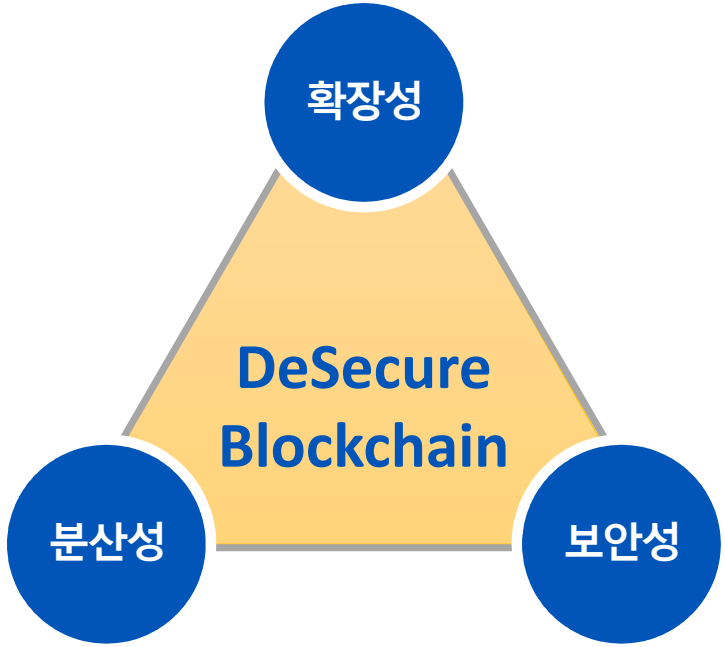
블록체인 하드포크 (비트코인, 이더리움)



ECCPoW 1.0 **작업증명 보안성 수준**

1단계 연구

다중 복합구조 블록체인, 플라즈마



ECCPoW 2.0 **이중지불공격 방지**

2단계 연구

2단계 연구 계획 요약

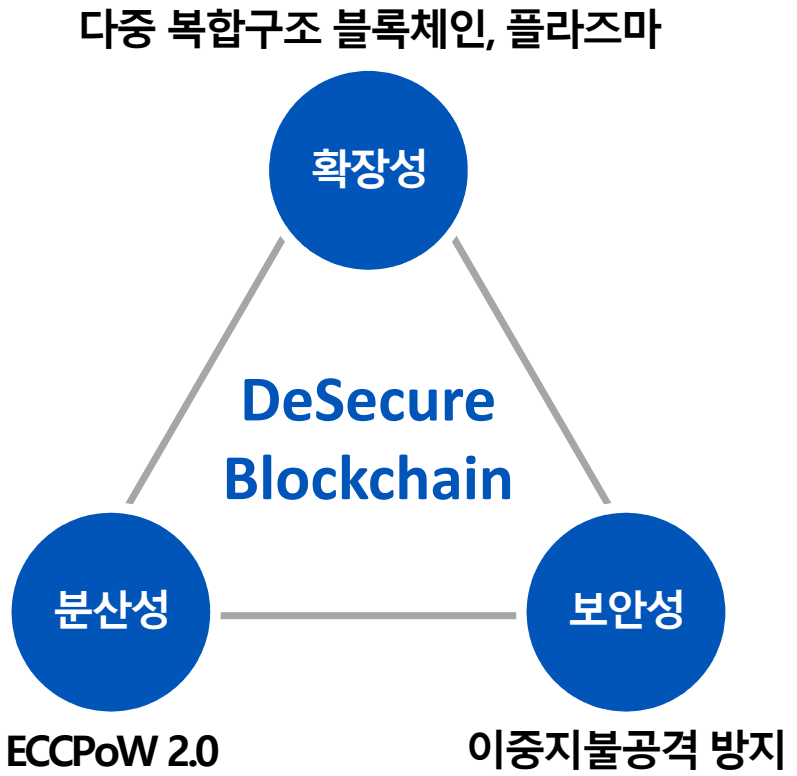
확장성 강화
다중 복합구조 블록체인 연구

보안성 강화
거래검증횟수 최적화 알고리즘 개발

유연성 확대
플라즈마 모델 연구, 개발 및
DeSecure 블록체인에 적용

보안성 강화
플라즈마의 데이터 가용성
문제 개선에 관한 연구 및 개발

ECCPoW 코어 2.0 개발
블록생성 제어 방법 고도화



2단계 연구 계획 목표

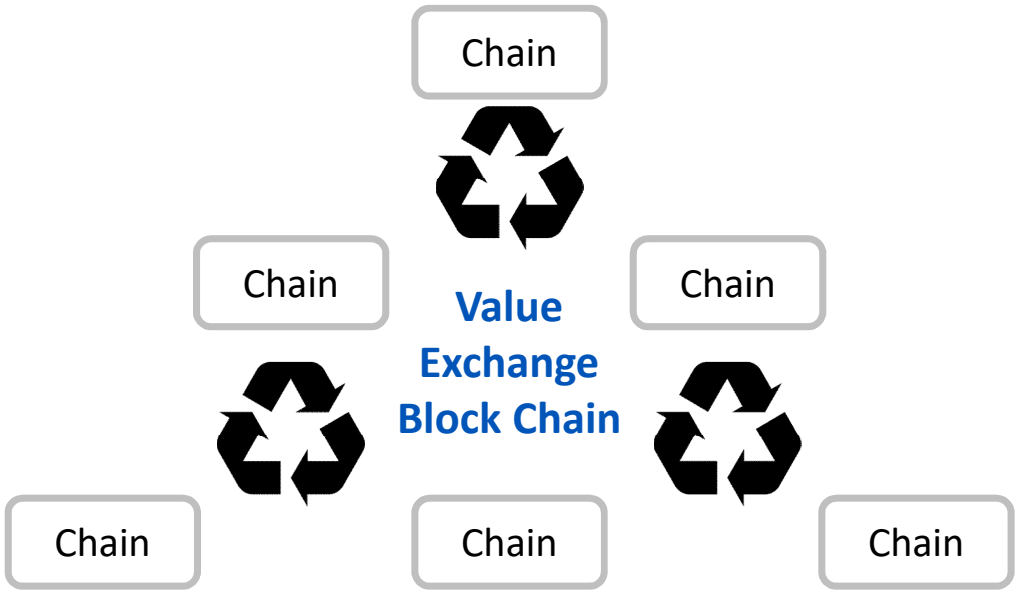
세부 연구 목표		연구개발 수행 내용	담당
분산성	**ECCPoW 코어 2.0 개발**	▪ 블록생성주기 및 난이도제어 고도화 ▪ 난이도별 블록생성 확률 분석 ▪ 난이도 조절 규칙 연구	주관 기관
확장성	**다중 복합구조 블록체인 연구**	▪ 다중 복합구조 블록체인 설계 ▪ 트랜잭션의 용도별 블록체인 파라미터 최적화 ▪ 다중 블록체인간 정보교환 프로토콜 연구	
보안성	**거래 검증 횟수 최적화 알고리즘 개발**	▪ 이윤발생 (Profitable) 이중 지불 공격을 방지하는 동시에 빠른 거래완료 속도를 달성하기 위한 조건 연구 ▪ 트랜잭션의 용도별 검증 횟수 최적화 알고리즘 개발	
유연성	**플라즈마 모델 개발**	▪ 이더리움의 레이어2 솔루션인 플라즈마 모델을 개발하여 DeSecure 블록체인에 적용 ▪ 부적절 거래 방지를 위한 플라즈마 데이터 가용성 개선 알고리즘 개발	참여 기관

확장성 강화 연구

- Evolutionary Space에서 DeSecure 블록체인을 용도에 따라 특화
- 용도별 특화 블록체인들을 연결하여 다중 복합구조 DeSecure 블록체인 형성

Low TPS
Global Nets
High Delay

Large Tx (Assets)



High TPS
Local Nets
Low Delay

Small Tx
(Utility Coins)

<용도에 따라 세분화된 다중 복합구조 블록체인>

확장성 강화 연구

- 사용 용도에 따라 블록전파지연시간과 참여 노드 수가 다르므로 용도에 따른 파라미터 최적화를 연구함
- **Enterprise DeSecure Blockchain**은,
  Private Consortium으로 구성되어 기업간의 정보를 공유하는데 사용될 수 있음
  - Enterprise와 지역규모 DeSecure Blockchain들은 빠른 거래 처리속도 (TPS)에 집중하여 채굴난이도를 낮은 수준으로 설정함
  - 동시에 이중 지불 공격 방지 및 이상 행위 퇴출을 위해 멤버십 제도와 같은 Off-Chain Policy를 적용함
- **지역규모 DeSecure Blockchain**은 시/구/군 규모의 블록체인으로 작은 규모의 거래가 주를 이룸
- **국가규모와 국제규모 DeSecure Blockchain**은,
  각각 지역 간, 그리고 국가 간의 거래를 기록하며, 거래의 규모가 큼
  - 국가규모와 국제규모 DeSecure 블록체인들은 거래의 규모가 큰 만큼 거래 처리속도 보다 보안성 제고를 위해 채굴난이도를 높은 수준으로 설정함

확장성 강화 연구

피라미터/용도	Enterprise / Consortium	지역 규모	국가규모	국제규모
네트워크 전파시간	<1초	<10ms	<100ms	<1초
블록생성 시간	<0.1초	1분	5분	10분
채굴난이도	최소	하	중	상
Off-chain 정책	O	O	X	X
참여 노드 수	허가된 소수 (10개 내외)	<100개	<1000개	<10000개
보안성	낮음	낮음	중간	높음
TPS	>42000	<70	<14	<7

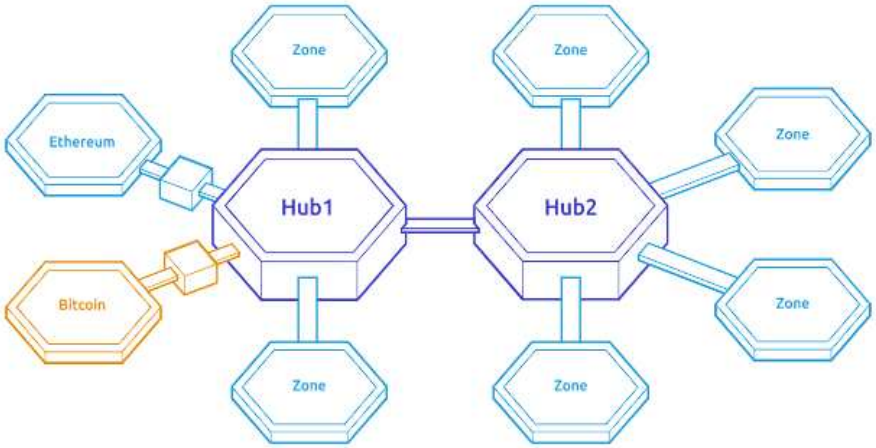
※ TPS 계산 기준 : 1MB 블록 사이즈, 0.24KB 트랜잭션 사이즈

확장성 강화 연구

- **DeSecure 다중 복합구조 블록체인은 용도에 따른 최적화만으로도, PoS/DPoS/BFT 등보다 유연하게 작동할 수 있음**
  - PoS/DPoS/BFT 등의 합의방식은 노드의 Generic ID가 완벽히 신뢰할 수 있거나, 네트워크 규모가 아주 작을 때 정상적으로 작동함
  - 노드의 Generic ID가 완벽하지 않다면 소수의 노드가 많은 ID를 보유하여 네트워크에 큰 영향력을 행사하는 Sybil Attack이 가능함
  - Generic ID기술 중 하나인 PUF의 경우, 하나의 전자장비로 여러 개의 ID를 만들어 낼 수 있음
  - 또 다른 기술인 SSID의 경우 중앙 시스템 (정부 혹은 플랫폼 제공 기업)에 의해 통제되기 때문에, 안전하지 않음
- 반면 ECCPoW를 사용하는 **DeSecure 블록체인**은 Generic ID에 의존하지 않기 때문에 **상기 보안 문제로부터 자유로움**
- 이뿐만 아니라, **DeSecure 블록체인**을 다중 복합구조로 설계함으로써 PoS/DPoS/BFT가 가지는 장점인 **빠른 거래처리 속도까지 확보할 수 있음**

확장성 강화 연구

- **다중 복합구조 DeSecure 블록체인 간의 통신 프로토콜 연구**
  - 용도별 DeSecure 블록체인간의 가치 및 정보교환을 위한 통신 프로토콜을 연구함
  - 다중 복합구조 DeSecure 블록체인들은 모두 같은 합의 알고리즘을 탑재하고 있으므로 블록체인 간 통신이 용이함
  - Sidechain의 개념으로 다중 구조 블록체인을 제안한 Polkadot과 Cosmos와 같이 통신의 Hub Station 역할을 해주는 블록체인을 도입하는 방법도 적용 가능함



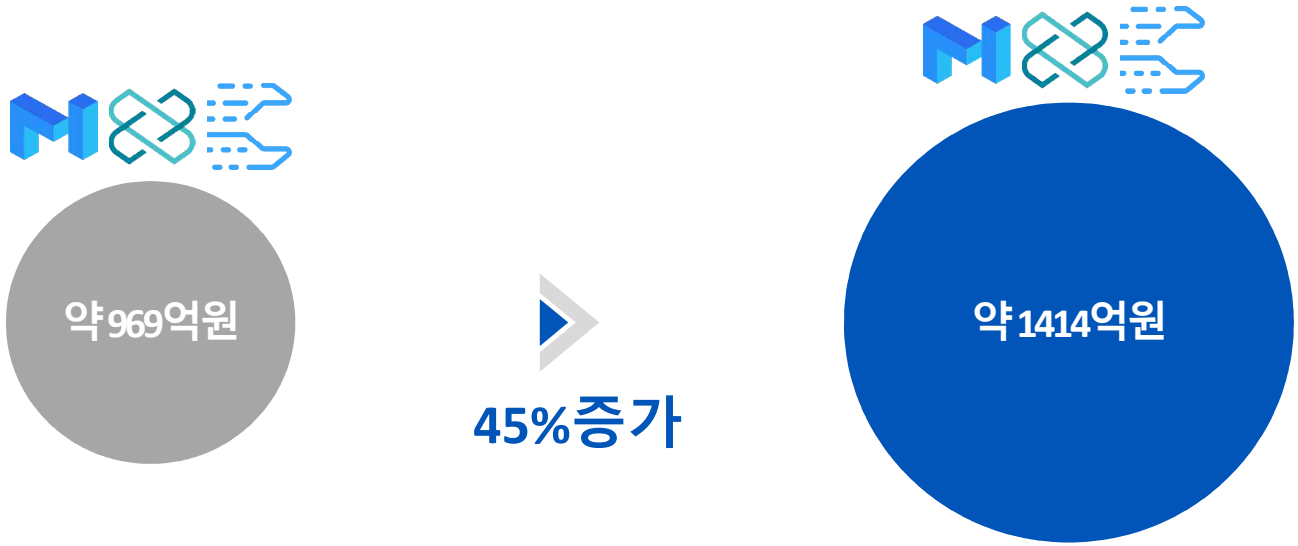
<Polkadot의 블록체인 간의 연결 구상도>

ECCPoW와 다른 확장성 방법과 비교

- DeSecure Blockchain aims to resolve the re-centralization problem without sacrificing the secureness!

체인 이름	DeSecure	Bitcoin		Ethereum	
방법	다층멀티체인 ECCPoW	세그윗	라이트닝 네트워크	플라즈마	샤딩
구현	ECCPoW 기반 독립체인들을 여러 계층으로 묶음	블록 데이터 구조를 변경하여 구현	오프체인 거래 진행, 최종 결과값을 메인 블록체인 기록	하부 체인 생성, 거래 진행 후 최소한의 기록만 메인 블록체인 기록	블록체인의 DB에 해당하는 스테이트를 여러 샤드로 분할, 트랜잭션 별 분리 처리
장점	서로 다른 블록체인 연결해 다양한 기능과 역할 구현	쉽게 구현이 가능함	결제 속도 제고, 즉각적인 완결성, 수수료 절감	수수료 절감	트랜잭션 처리 속도 증가
단점	No single chain solution/생태계필요	트랜잭션 처리속도 증가 효과 미비	오프체인 거래기록 없음	Full노드 만 플라즈마 사용 가능	S/W 복잡도 상승

주요 Layer2 프로젝트 규모 증가



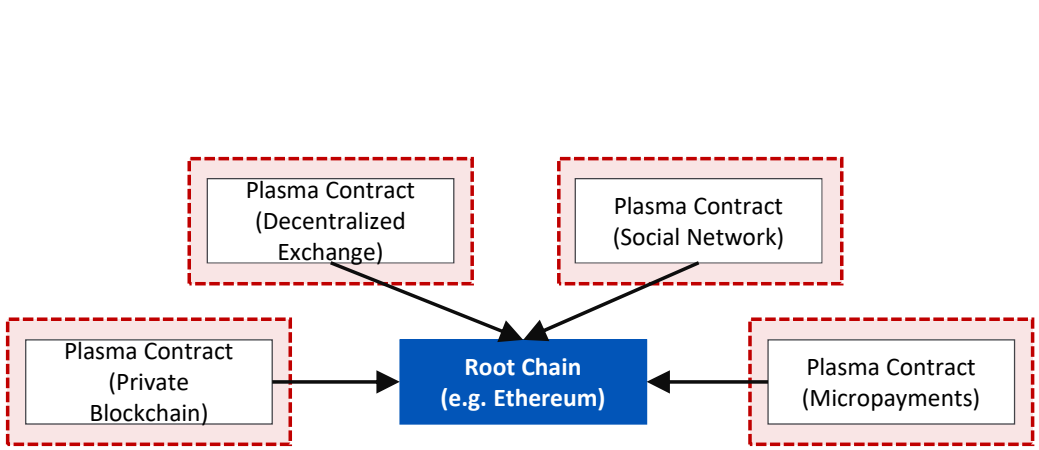
- 주요 layer2 프로젝트의 시가총액의 합은 2019년초 약 969억원 대비 2019년 12월 현재 약 1414억원으로 약 45% 성장
- 다른 프로젝트의 시가 총액이 감소, layer2 솔루션의 성장으로 기대와 전망을 확인할 수 있음

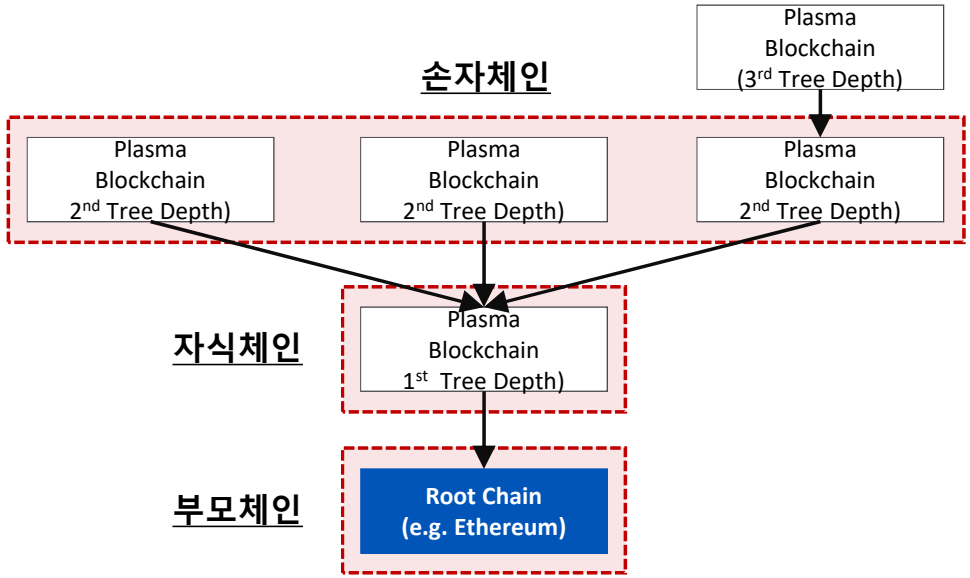
유연성 강화를 위한 플라즈마 도입

- **플라즈마**
  - 스마트 계약(이하 플라즈마 컨트랙)의 인센티브 및 강제 실행(incentiveized and enforced execution)을 위한 프레임워크로 초당 상당한 양의 상태 업데이트(잠재적으로 수십억 개)로 확장 가능하여, 블록체인(별도의 플라즈마 체인)이 전세계적으로 상당한 양의 분산형 금융 애플리케이션 구동을 가능하게함

  - 스마트 계약은 네트워크 거래 수수료를 통해 자율적으로(autonomously) 운영을 지속하도록 유도되며, 이는 궁극적으로 트랜잭션 상태 전환을 강제(enforce)하기 위해 메인 체인(예: Ethereum)에 의존함

유연성 확보를 위한 플라즈마 도입





- 플라즈마를 도입 했을때 DeSecure체인을 부모체인으로 하는 다수의 체인을 생성할 수 있음
- 각 체인은 **목적에 맞는 스펙**을 가질 수 있으며 필요에 따라 언제든지 체인을 열고 닫을 수 있음
- 또한, 자식체인이 손자/손녀 체인들의 부모 체인이 되는 **계층적 구조로 확장**할 수 있기 때문에 이론상으로는 무한대의 확장성 또한 확보 가능

플라즈마 체인의 보안성 강화 연구

플라즈마 체인의 보안성 문제 정의

- 자식체인의 상태 강제를 위해서 진실에 공판에 올라갈 증거가 필요함
- 플라즈마 체인의 운영자(Operator)가 블록의 내용을 내어주지 않을 가능성이 존재
- 증거(Proof)가 없으면 앞에서 언급된 어떠한 검증장치들도 작동하지 못함
- 이러한 문제를 데이터 가용성(Data Availability, 이하 DA) 문제라고 함

더 큰 문제는 이 문제가 상당히 주관적(Subjective) 특징을 지님

- 데이터를 받았다는 것을 증명하는 것은 쉬우나, 데이터의 내용을 모르는 상태에서 데이터를 받지 않았다는 것을 증명하는 것은 **상당히 어려움**
- 받았음에도, 받지 않았다고 주장할 수도 있기 때문에 데이터 인질이 있는지 없는지 여부에 대한 판단은 매우 **주관적**이 될 수밖에 없음

플라즈마 체인의 보안성 강화 연구

플라즈마 체인의 보안성에 대해 보유한 연구 성과

[Solevm] – 스마트 컨트랙트 EVM

- 연산 챌린지를 위해서는 EVM의 런타임에 대한 검증게임이 이뤄져야 함
- 그래서, EVM자체를 스마트 컨트랙트로 구현하는 것이 매우 중요함
- 이는 마치 파이썬으로 만든 파이썬, 자바로 만든 자바와 같음
  → 다만 커스텀한 체인의 실행모델이라면, 그 환경에 맞춰진 변형된 EVM 컨트랙트 코딩이 필요함

[Continuous Rebase] – 플라즈마 체인 적용 핵심기술

- Continuous Rebase 모델은 플라즈마 체인의 정상적인 작동과정에 Rebase를 포함시킴.따라서 지속적이고 주기적인 Rebase를 통해 사용자들의 Escape Request를 반영
  (Rebase : 기존 블록을 다른 블록 기준으로 마이닝)
- 이를 통해 사용자들은 DA문제가 있을 경우 Escape Request를 제출하여 안전하게 탈출 가능. 또한 제출된 블록이 올바르지 않을 경우 연산 챌린지를 통해 해당 블록들이 Finalize 되는 것을 막을 수 있음

보안성 강화 연구

보안성 문제 정의

- 거래검증 횟수가 많을수록 거래처리속도는 느려지나, 이중 지불(DS) 공격에 강인해짐
- 지금까지는 거래검증 횟수의 설정 효과가 수치화 되어 있지 않음

※ 거래검증 횟수 : Block confirmation number

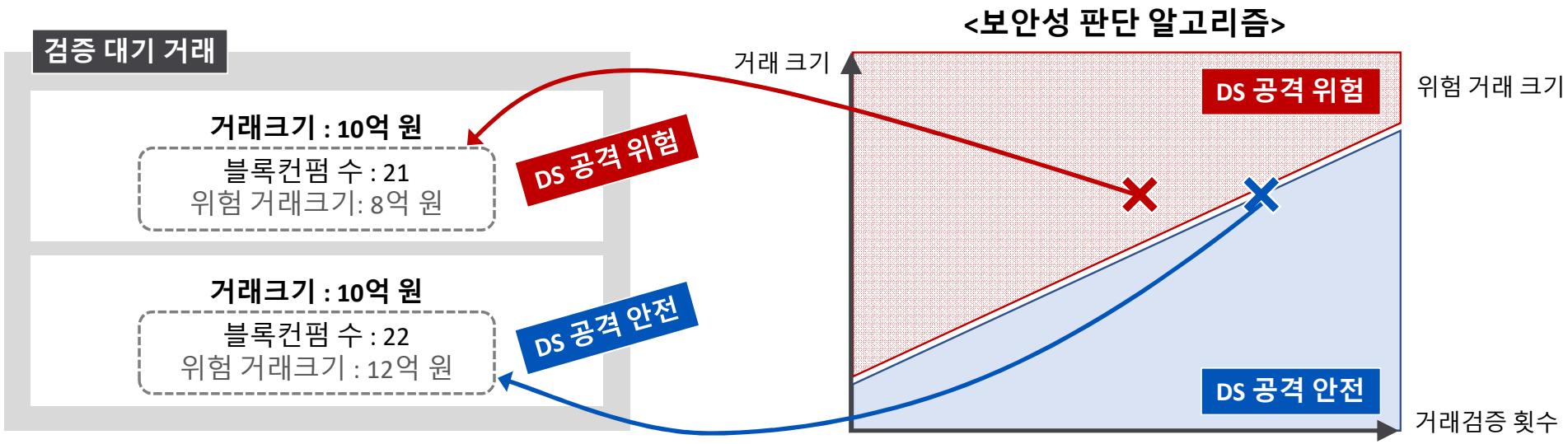
보안성 분석 보유 연구성과

- Satoshi Nakamoto의 백서를 포함한 기존 연구는 대규모 (50% 이상)컴퓨팅파워 확보에 의한 DS 공격의 위험성에 초점을 맞추었음
- 소규모 (50%미만) 컴퓨팅 파워 확보로도 위협적인 DS 공격이 가능함을 수학적으로 밝힘
- **DS공격의 수익(Profit)과 공격목표 거래규모, 거래검증 횟수와의 상관관계를 제시함**
- 연구 성과를 논문으로 작성하여 국제 학술지에 제출

보안성 강화 연구

보유 연구성과 활용 방안

- 거래 별로 DS공격의 위험성을 평가하여 사용자가 보안위험 자각 및 대처 가능
- 거래검증 횟수와 거래크기가 DS 공격자에게 이윤을 발생시키는지를 거래 별로 평가 가능

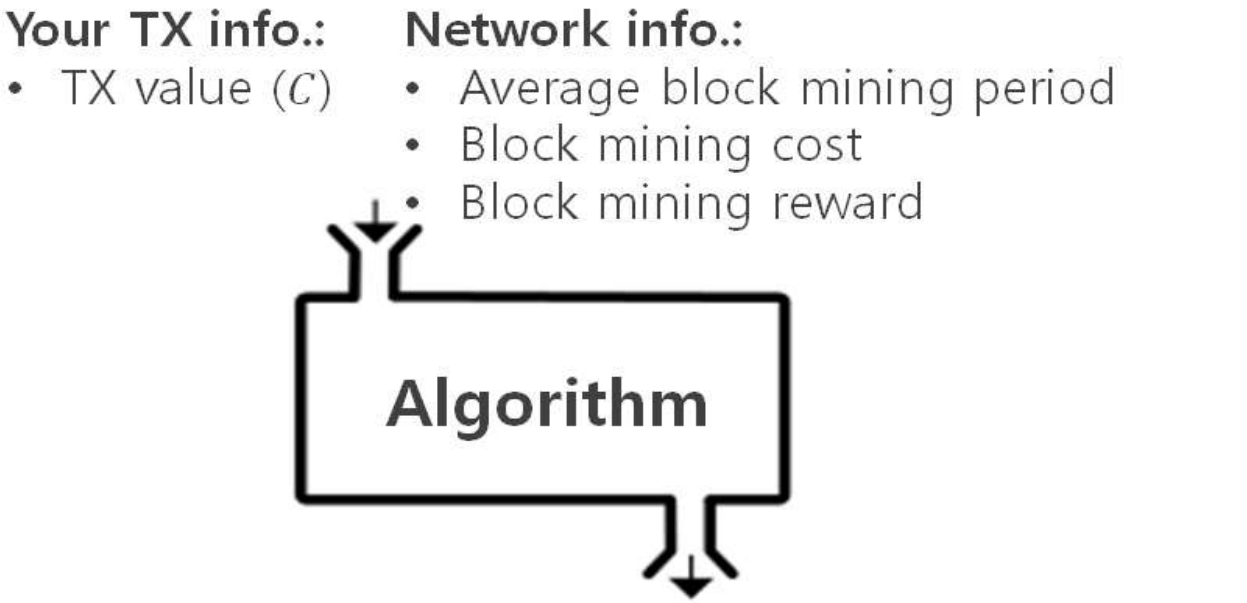


보안성 강화 연구

거래 검증횟수 최적화 알고리즘 개발

- **거래 용도에 따라 최적의 검증 횟수를 결정해주는 알고리즘을 개발함**
- 최적의 검증횟수란 DS 공격을 방지하는 동시에 거래 완료에 걸리는 시간을 최소화하는 검증 횟수임
  - 거래금액에 따라 공격자의 이윤 발생을 방지하는 검증 횟수가 존재함
- **최대 거래 속도(확장성)가 거래의 용도에 따라 유동적으로 결정되도록 함**
  - 소액 거래일 때는 공격자가 DS 공격을 통한 이윤을 기대하기 어려우므로 보안성보다 확장성을 위한 작은 검증횟수가 적절함
  - 고액 거래일 때는 이중 지불 공격의 목표가 될 가능성이 있으므로 큰 검증횟수를 설정해 보안성을 유지함
- 거래 검증 횟수 최적화 알고리즘을 지갑에 탑재하여 거래를 생성할 때마다 자동 실행되도록 함

보안성 강화 연구



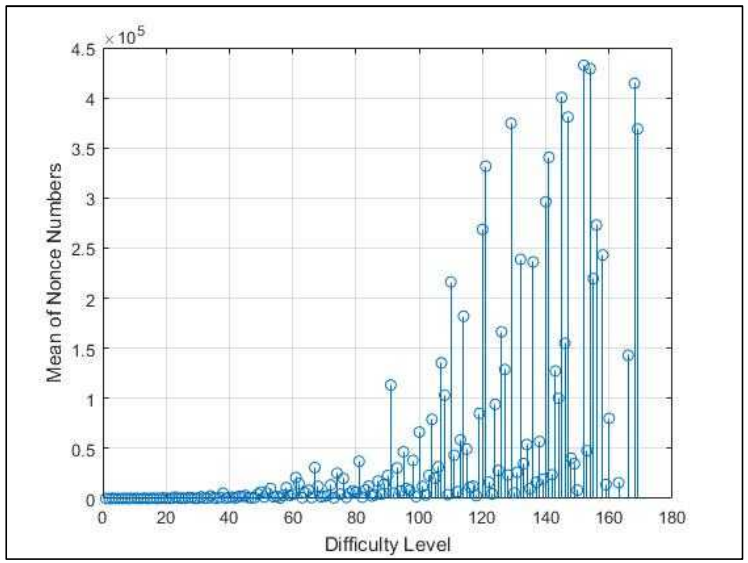
<검증횟수 최적화 알고리즘>

ECCPoW 코어 2.0 개발

1단계에서 확보한 연구 성과

Level	Length	wc (the number of ones	wr (the number of ones	from	to	type	Prob. Calculated	Average Nonce Measured
1	32	3	4	10	22	2	3.08E-05	20.46
2	32	3	4	10	16	2	2.02E-05	30.51
3	32	3	4	16	16	1	9.68E-06	66.24
4	32	3	4	14	14	1	6.78E-06	97.22
5	36	3	4	12	24	2	4.83E-06	29.40
6	36	3	4	12	18	2	3.13E-06	44.19
7	32	3	4	12	12	1	2.86E-06	222.73
8	44	3	4	14	30	2	1.64E-06	62.10
9	36	3	4	18	18	1	1.42E-06	103.60
10	36	3	4	16	16	1	1.05E-06	141.06

<채굴 난이도별 설정방법>



<채굴 난이도별 블록생성 시도 횟수 측정 값>

ECCPoW 코어 2.0 개발 – 연구문제의 도전성 및 중요성

블록생성 확률 계산의 도전성

- 1단계 연구에서 블록생성 확률의 상한과 하한 값을 찾음
- 기존 작업증명 알고리즘은 그 원리가 단순하여 블록생성 확률 계산이 쉬움
- Anti-ASIC 특성을 확보하기 위해 ECC라는 고도화된 알고리즘을 활용하므로 확률 계산이 도전적임

블록생성 주기 제어 고도화의 중요성

- 네트워크 총 계산 량의 변동에 따른 블록생성 주기의 안정화 시간 (settling time)을 더욱 단축
- 급격한 계산 량 변동을 유도하여 부당 이득을 취하려는 공격 시도를 억제 할 수 있음

ECCPoW 코어 2.0 개발 – 연구문제의 해결 전략

블록생성 확률 계산

- ECC에서 사용되는 LDPC 행렬의 특성과 확률 분포에 관한 연구 문헌을 조사하여 정확한 확률을 계산 가능
- 많은 양의 실험을 통해 난이도별 블록생성 통계를 측정하여 활용 가능

계산 량의 변동에 따른 난이도 설정 규칙 정의

- 비트코인과 이더리움은 각각 자체 정의한 난이도 설정 규칙을 적용함
- 두 규칙은 오랜 기간 사용되어 왔으며 그 안정성이 실증되었음
- 블록생성 확률을 정확하게 계산 할 수 있다면, 기존의 두 규칙을 활용 가능함

$$D_{next} = D_{prev} \times \frac{2 \text{ weeks (20160 minutes)}}{\text{Time spent for mining 2016 blocks}}$$

<비트코인의 난이도 설정 규칙>

$$D(H) \equiv \begin{cases} D_0 & \text{if} \quad H_i = 0 \\ \max\left(D_0, P(H)_{H_d} + x \times \varsigma_2 + \epsilon\right) & \text{otherwise} \end{cases}$$

<이더리움의 난이도 설정 규칙>

공인 인증 평가 목적

세계 최고 수준의 블록체인인 비트코인, 이더리움과 비교 평가함
동일한 평가 환경(난이도 변경 주기, 목표 블록 생성시간,
23개의 Instance 등)에서 비교

[평가의 객관성]
평가 데이터와 블록체인 소스코드를 Github에 공개하여 평가 결과는
누구나 검증 가능함

Bitcoin 평가 데이터 : https://github.com/paaabx3/BTCBGT3-2
Bitcoin 평가 데이터 : https://github.com/paaabx3/BTCeccBGT3
ECCPoW 블록체인 탐색기 : http://13.125.223.181/blocks
ECCPoW 블록체인 탐색기 : http://15.164.244.139/blocks

1차년도 공인 인증 평가 요소

01

분산성

각 채굴 노드들이 전체 채굴량에 대해 일정하게 채굴하는 정도를 의미함.
분산성 수치가 100%에 가까울 수록 각 채굴자들의 채굴 확률이 균등하게 분포 된 것을 뜻함.

02

보안성

이중 지불 공격의 원인인 고아 블록의 출현을 방지하고 이를 보안을 유지할 수 있는 것을 의미함
즉, 고아 블록 비율이 낮으면 보안성이 좋다고 할 수 있음

03

확장성

블록체인 환경에서의 처리할 수 있는 트랜잭션 (TPS)을 증가시킬 수 있음을 의미함.
동일한 환경에서 비트코인/이더리움과 ECCPoW의 TPS를 비교는 확장성을 비교할 수 있음

공인 인증 평가 결과

- 국제 공인인증 기관인 "한국시험인증원"으로부터 기술력을 인정 받음

평가 항목 (주요성능 Spec)	단위 (%)	전체 항목에서 차지하는 비중 (%)	세계최고 수준 보유기업 (비트코인, 이더리움)	연구개발 전 국내수준	목표		실적	평가방법
			성능수준	성능수준	최종목표	당해년도	당해년도	
① 분산성	채굴성공률 분포도	35%	40% (추정 값) (기준 : 비트코인, 2018년 10~12월)	40%	80%	60%	**92.22%**	공인인증기관
② 보안성	비트코인 대비 보안성	35%	100% (기준: 비트코인)	100%	200%	100%	**100%**	공인인증기관
③ 확장성	비트코인 대비 확장성	15%	100% (기준: 비트코인)	100%	200%	100%	**98.95%**	공인인증기관
④ 확장성	이더리움 대비 확장성	15%	100% (기준: 이더리움)	100%	200%	100%	**102.97%**	공인인증기관

① 분산성 : 당해 년도 목표 대비 **+32.22%**
② 보안성 : 당해 년도 목표 대비 **0%**
③ 확장성(BTCECC) : 당해 년도 목표 대비 **-1.05%**
④ 확장성(ETHECC) : 당해 년도 목표 대비 **+2.97%**

2차년도 공인 인증 평가 요소

01

분산성

각 채굴 노드들이 전체 채굴량에 대해 일정하게 채굴하는 정도를 의미함.

분산성 수치가 100%에 가까울 수록 각 채굴자들의 채굴 확률이 균등하게 분포 된 것을 뜻함.

02

보안성

동일한 환경의 비트코인과 DeSecure 블록체인에 이중지불 공격 모의 실험을 수행하여 피해 금액을 측정함.

피해 금액이 적을수록 보안성이 우수함.

두 블록체인의 피해 금액을 비교하여 보안성을 상대 평가함.

03

확장성

블록체인 환경에서의 처리할 수 있는 트랜잭션(TPS)을 증가시킬 수 있음을 의미함.

동일한 환경에서 비트코인/이더리움과 ECCPoW의 TPS를 비교는 확장성을 비교할 수 있음

감사합니다