Scalable DeSecure ECCPoW Blockchains

이 흥 노 교수

JCCI 2019 특별세션
강릉세인트존스 호텔

May 1st 2019

heungno@gist.ac.kr
facebook ID: Heung-No Lee
https://infonet.gist.ac.kr

http://jcci.kr/sub/spe_program.asp

JCCI 2019 강릉 세인트존스 호텔

May 1st ~ 3rd, 2019

목차

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

▣ 특허

특허	출원인	출원번호/등록일	핵심기술
부호-암호 화폐 시스템	이흥노 외 3인	10-2018-0097677 / 2018.08.21	블록체인의 재중앙화 문제 해결을 위한 핵심 기술
유한체의 희소신호 복구방법, 유한체의 희소신호 복구장치, 및 이 방법을 기록되는 기록매체	이흥노 외 1인	Japan patent number: 5914755 /2016.4.8	ECCPoW의 LDPC decoder 구현 특허
Method and apparatus for sparse signal transmission, method and apparatus for sparse signal recovery	이흥노 외 2인	application number: 13/420176 /2012.3.14	ECCPoW의 LDPC decoder 구현 특허

▣ GIST (주관기관) 와 ㈜온더 (참여기관) 과기부 IITP과제 참여 중

기술개발의 필요성

국내외 현황 및 연구 필요성

- 블록체인 (Blockchain) : 위·변조가 어려운 분산 거래 장부
  - 세계 블록체인 시장은 향후 5년간 10배 이상 성장 전망('16 WEF, '17 가트너)
  - 금융, 의료, 콘텐츠, 공공, 물류, 에너지 등 다양한 산업과 결합하여 효율성 및 신뢰성을 높이고, 새로운 경제적 가치 창출 가능
  - 선진국 대비 블록체인 코어 기술 경쟁력 취약
  - 전문연구 인력 부족

('18 블록체인 기술 발전전략, 과학기술정보통신부)

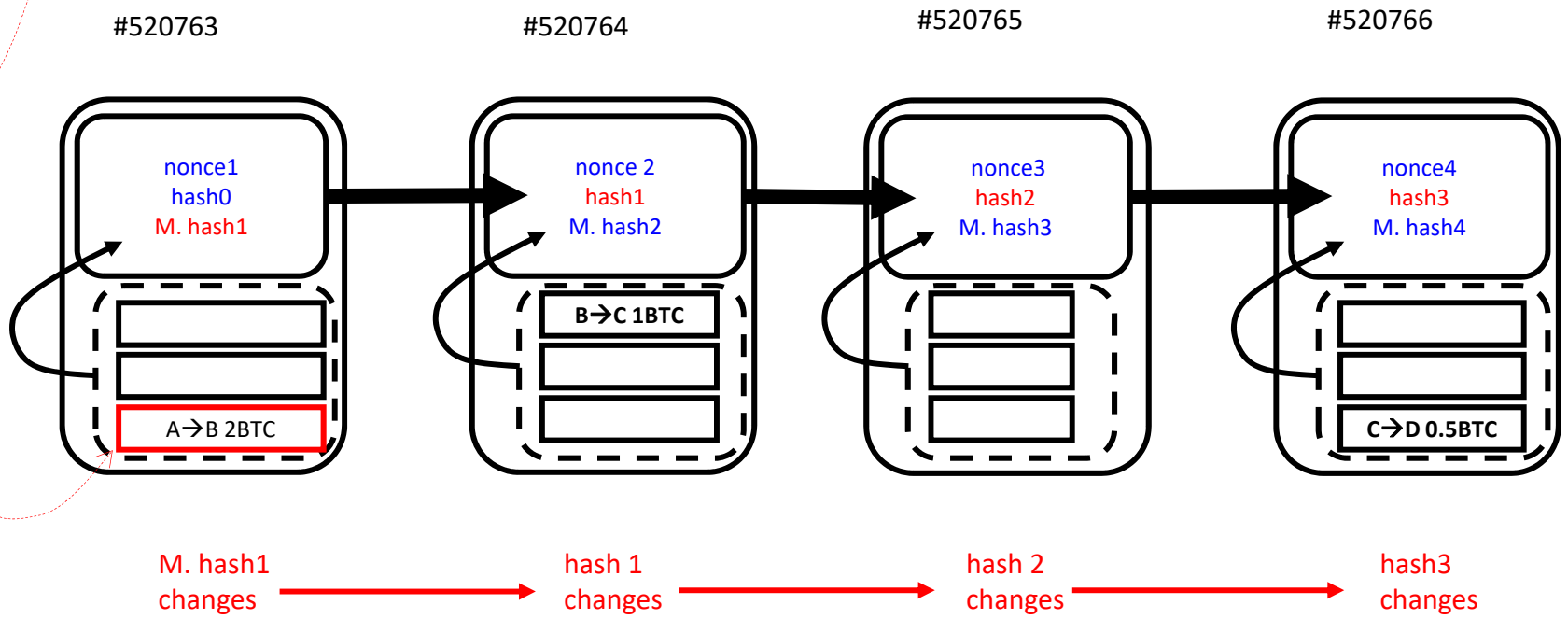
구분	1세대 (2009 ~ 2014)	2세대 (2015 ~ 현재)	3세대
주요 특징	• 가상통화 • 자산거래	• 스마트계약 • 분산 앱 (D-App)	• 확장성 (Scalability) • IoT 지원
대표 사례	• 비트코인	• 이더리움, 하이퍼레저	• 다양한 블록체인 플랫폼 개발 중
개발 수준	도입기	확산기	성숙기

기술 개발 개요

- DeSecure 블록체인 엔진 개발
  - 블록체인의 재중앙화 문제 해결을 위한 부호-암호 기반의 작업증명 방식 연구
  - 출원한 암호-부호 작업증명 특허(GIST IP)를 기반으로 DeSecure 엔진 개발
  - DeSecure 합의엔진을 기존 블록체인 BTC, ETH 틀에 탑재 및 확산

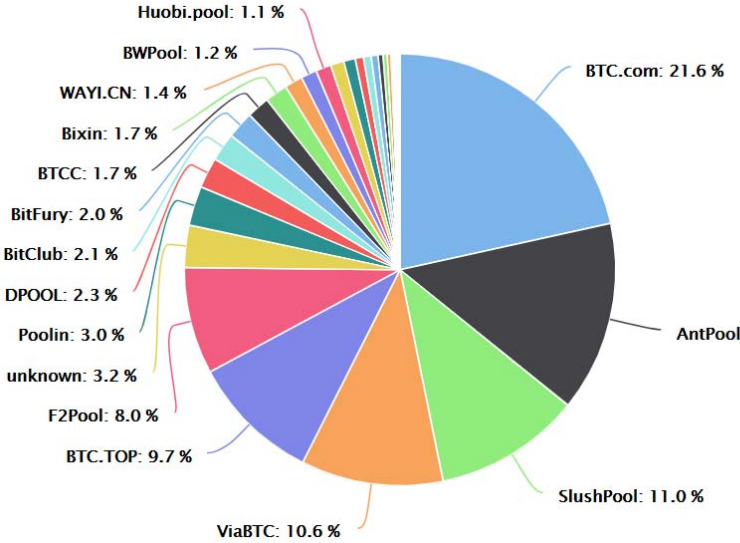
Blockchain & Proof-of-Work (PoW)

- 블록체인의 블록들은 Hash값으로 연결
- 기록된 거래 변경, Hash값의 연쇄변화 발생, 들통남
- 처음부터 끝까지 모두 변경 후 제시하면 거래변경 성공
- PoW를 무겁게 하여 쉽게 변경할 수 없도록 함

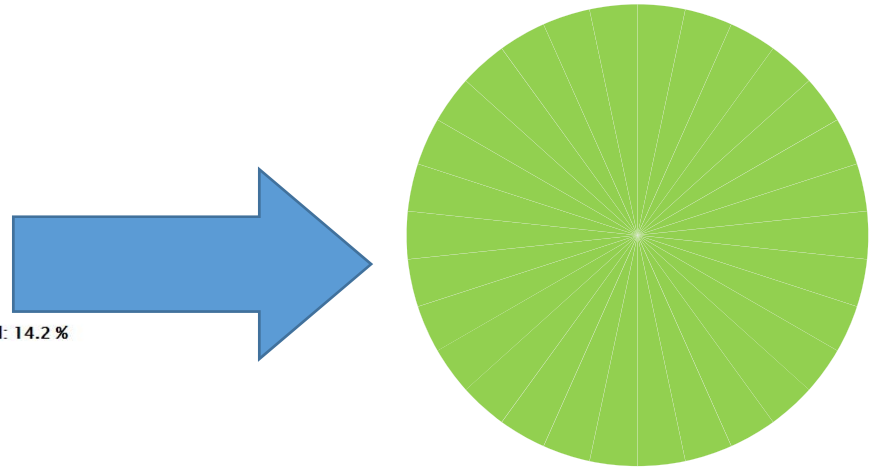


PoW 문제점을 해결, 제안기술의 도전성, 혁신성

- 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



중앙화된 블록체인 네트워크



탈 중앙화된 블록체인 네트워크

1. ASIC 저항성 증가
2. 블록체인 위변조 위험 감소

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 • "Noting 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

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

기술개발의 목표

기술개발의 목표

▣ 문제 : 부호-암호 합의알고리즘을 탑재한 탈중앙 BTC/ETH 블록체인 개발

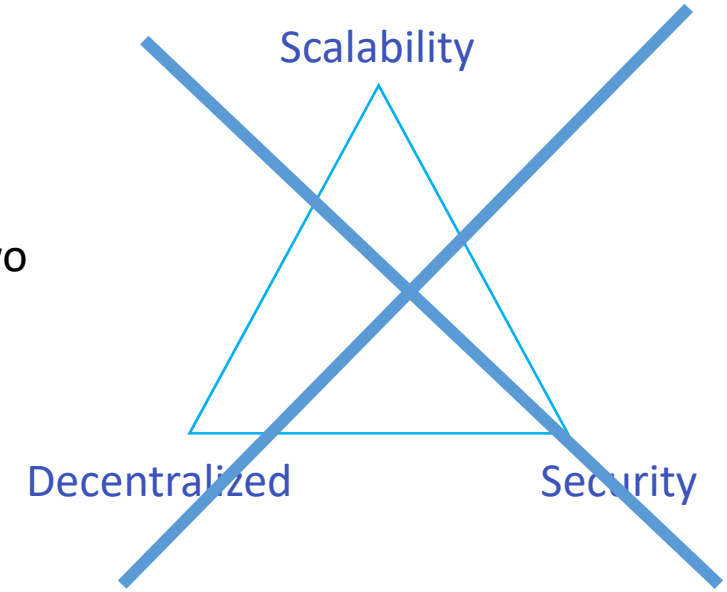
- 거래속도, 확장성, 보안성, 지역성 등 다양한 서비스 목표를 수용할 수 있는 표준형 Decentralized Secure (DeSecure) ECCPoW 블록체인 합의알고리즘 개발 목표

▣ 기술개발의 최종목표

연구 범위	최종목표
2019	• ECCPoW 버전 1.0 개발 및 배포 • ECCPoW 개발 및 비트코인에 적용 BIT-ECC 개발 • ECCPoW 개발 및 이더리움에 적용 ETH-ECC개발
2020	• ECCPoW 버전 2.0 개발 및 배포 목표 (작업증명 보안성 및 유연성 고도화) • 확장성 문제 해결을 위하여 국제 공동 연구 참여 및 ETH-ECC 플라즈마 개발

트릴레마, Single 블록체인으로 해결 가능?

Blockchain Trilemma?



“ blockchain systems can only at most have two of the following three properties

- Vitalik Buterin, Sharding FAQ
https://github.com/ethereum/wiki/wiki/Sharding-FAQ

”

- Wrong approach!
- Not in a single blockchain, can it be achieved!
- *We shall promote many decentralized secure (DeSecure) blockchains to achieve scalability!*

기술개발 내용

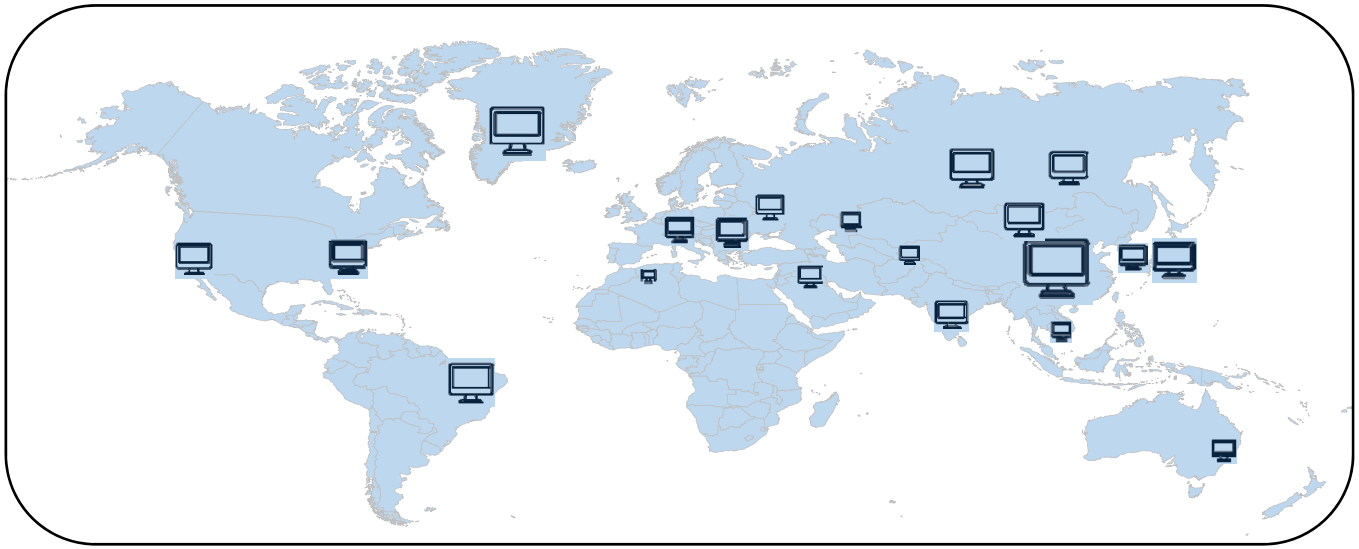
어떻게 ECCPoW가 분산성을 개선하는가?

▣ 분산성 문제 정의

- ASIC 채굴 장비 개발, 채굴칩 다량 보유 노드 채굴권 독점
- 난이도 증가, 채굴전기 소모량 극대화, 일반 노드 채굴 참여 의욕 저하

▣ 분산성 해결 방향

- *ASIC Resistant PoW개발*, 채굴능력 평준화, 보다 많은 노드 참여 유도



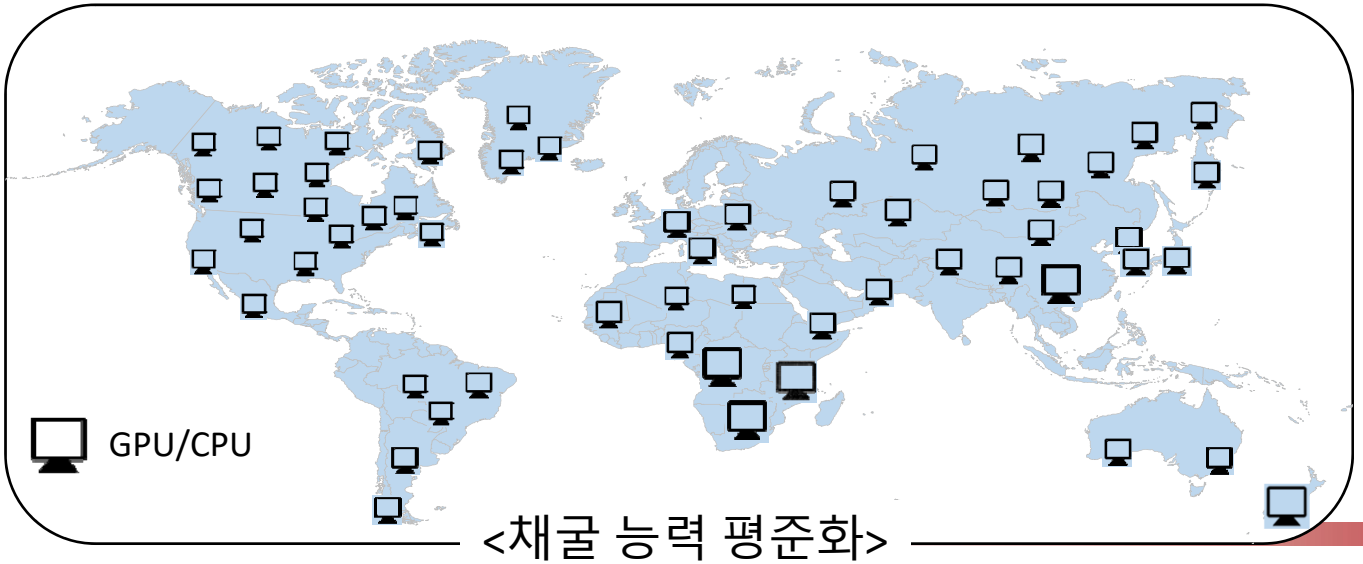
<ASIC 채굴장비에 의한 채굴능력 격차>

Concept of ECCPoW

▣ 부호-암호 작업증명 (ECCPoW) 목표

- 부호-암호 작업증명은 다음 요건들을 만족시켜야 함
  1. 암호 퍼즐은 풀기 어려우나, *증명과 검증은 쉬워야 함*
  2. 암호 퍼즐은 외부 *공격*으로부터 견고한 *저항성*을 가져야 함
  3. 풀린 암호 퍼즐의 정답은 재사용되지 않아야 함
  4. 암호 퍼즐의 난이도는 조절 가능해야 함
  5. CPU를 갖고 있으면 *누구든지 작업 증명에 참여*할 수 있어야 함
  6. 작업증명에 쓰이는 함수는 *매 블록마다 변화*하여 바꿀 수 있어야 함

▣ ECCPoW는 ASIC 채굴장비 출현 억제, 채굴능력 평준화도 개선



<채굴 능력 평준화>

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.

3. Consensus Mechanism

합의엔진

- 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.

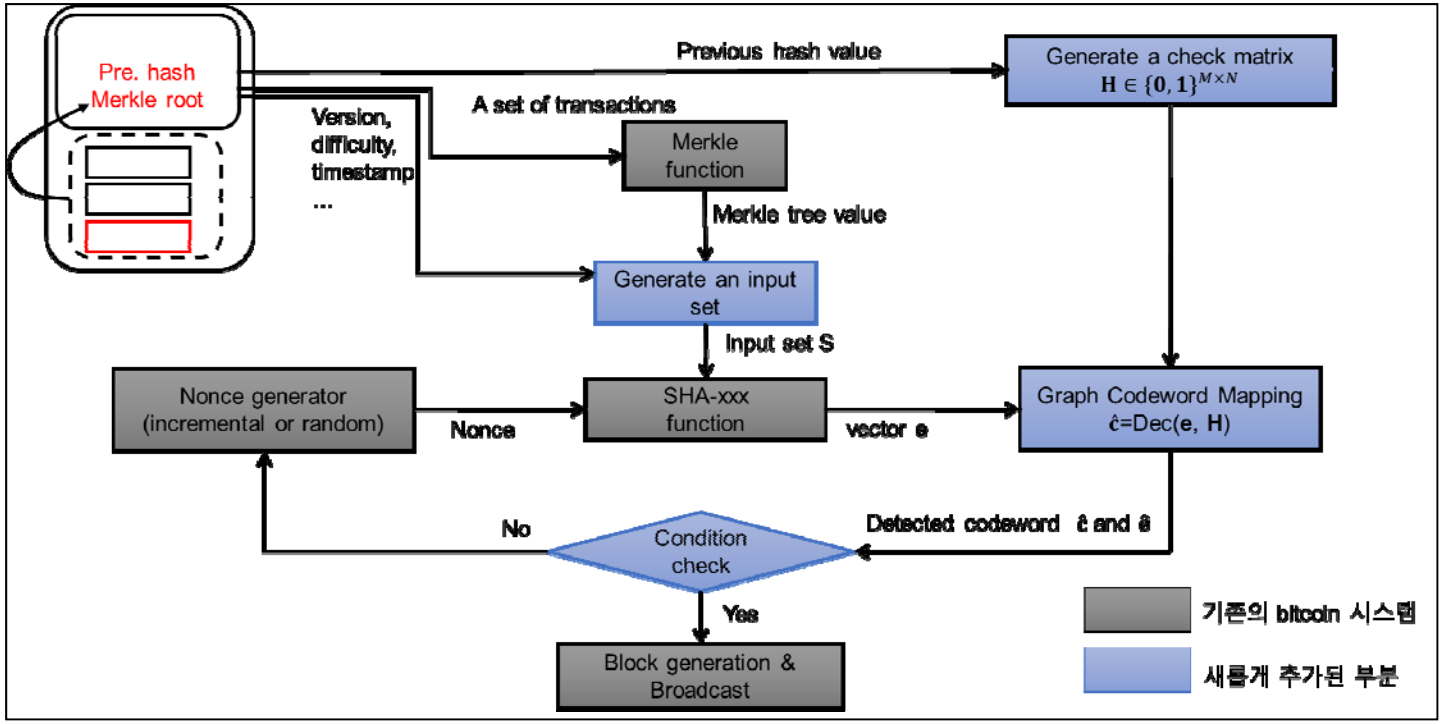
Program Suite

- **C++, Python, Go, Java, Flask, http**
- **Download and run, then you have a blockchain server.**

ECCPoW Consensus의 원리 및 구조

▣ ECCPoW의 원리: 매 블록마다 변화하는 암호 퍼즐 디코더

- Bitcoin의 PoW: SHA함수 대입문제를 반복적으로 풀어 원하는 답 찾기
- 새로운 ECCPoW: LDPC 부호의 역문제를 풀어 원하는 답 찾기 (작업증명 *난이도 조절능력*)
- 블록에 기록된 해쉬값을 활용하여 *매 블록마다 새로운 LDPC 행렬 생성 (ASIC Resistance)*
- LDPC행렬을 매 블록마다 바꾸어 *역문제를 매 블록마다 바꿈 (ASIC Resistance)*
- *SHA함수 Output을 여러 개 묶어 LDPC 부호의 길이를 크게 할 수 있음 (ASIC Resistance)*

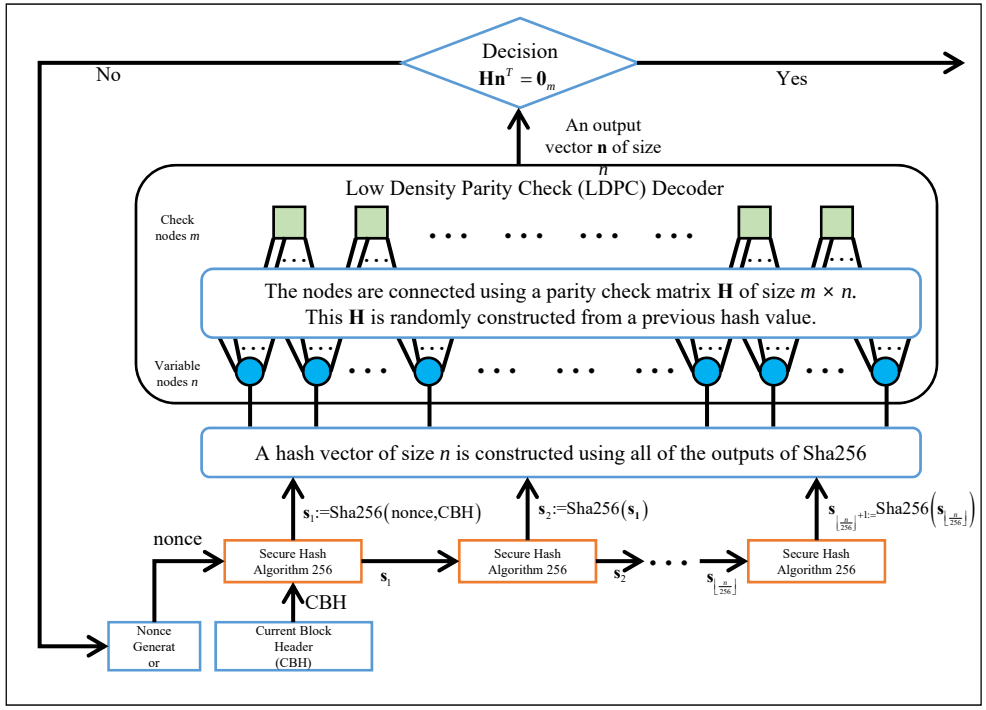


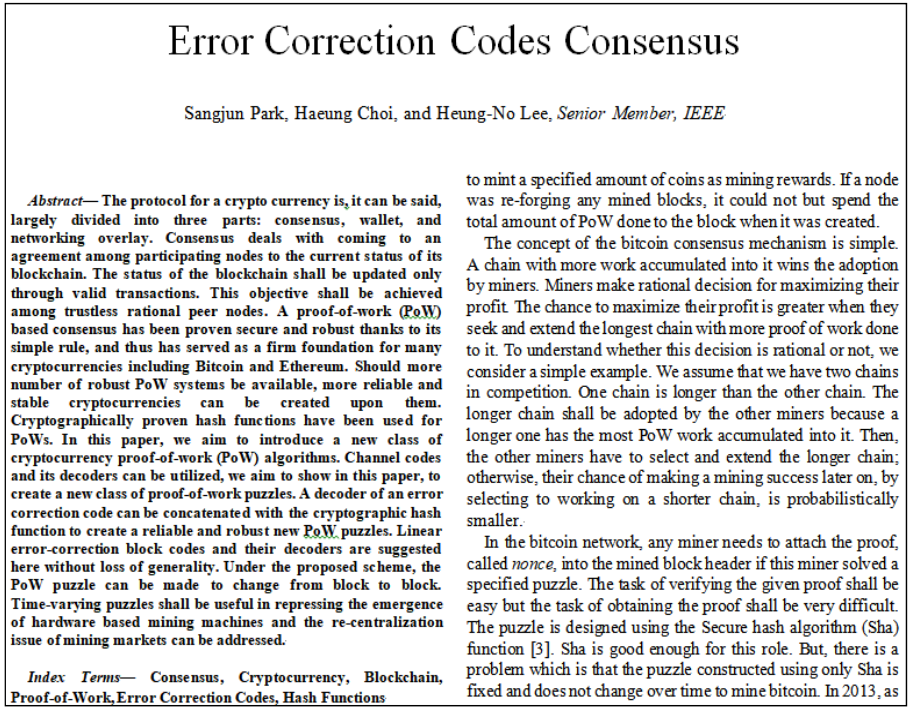
<부호-암호 작업증명>

ECCPoW 합의 엔진 개념도

▣ ECCPoW 합의 엔진

- SHA와 LDPC Decoder의 합성함수 개발
- Parity Check Matrix (PCM) 크기 변경, 필요한 자원(mem, comp)량 변경
- PCM은 이전 블록의 hash 값을 입력하여 블록마다 변경 가능





Error Correction Codes Consensus

Sangjun Park, Haeung Choi, and Heung-No Lee, *Senior Member, IEEE*

***Abstract*— The protocol for a crypto currency is, it can be said, largely divided into three parts: consensus, wallet, and networking overlay. Consensus deals with coming to an agreement among participating nodes to the current status of its blockchain. The status of the blockchain shall be updated only through valid transactions. This objective shall be achieved among trustless rational peer nodes. A proof-of-work (PoW) based consensus has been proven secure and robust thanks to its simple rule, and thus has served as a firm foundation for many cryptocurrencies including Bitcoin and Ethereum. Should more number of robust PoW systems be available, more reliable and stable cryptocurrencies can be created upon them. Cryptographically proven hash functions have been used for PoWs. In this paper, we aim to introduce a new class of cryptocurrency proof-of-work (PoW) algorithms. Channel codes and its decoders can be utilized, we aim to show in this paper, to create a new class of proof-of-work puzzles. A decoder of an error correction code can be concatenated with the cryptographic hash function to create a reliable and robust new PoW puzzles. Linear error-correction block codes and their decoders are suggested here without loss of generality. Under the proposed scheme, the PoW puzzle can be made to change from block to block. Time-varying puzzles shall be useful in repressing the emergence of hardware based mining machines and the re-centralization issue of mining markets can be addressed.**

***Index Terms*— Consensus, Cryptocurrency, Blockchain, Proof-of-Work, Error Correction Codes, Hash Functions**

to mint a specified amount of coins as mining rewards. If a node was re-forging any mined blocks, it could not but spend the total amount of PoW done to the block when it was created.

The concept of the bitcoin consensus mechanism is simple. A chain with more work accumulated into it wins the adoption by miners. Miners make rational decision for maximizing their profit. The chance to maximize their profit is greater when they seek and extend the longest chain with more proof of work done to it. To understand whether this decision is rational or not, we consider a simple example. We assume that we have two chains in competition. One chain is longer than the other chain. The longer chain shall be adopted by the other miners because a longer one has the most PoW work accumulated into it. Then, the other miners have to select and extend the longer chain; otherwise, their chance of making a mining success later on, by selecting to working on a shorter chain, is probabilistically smaller.

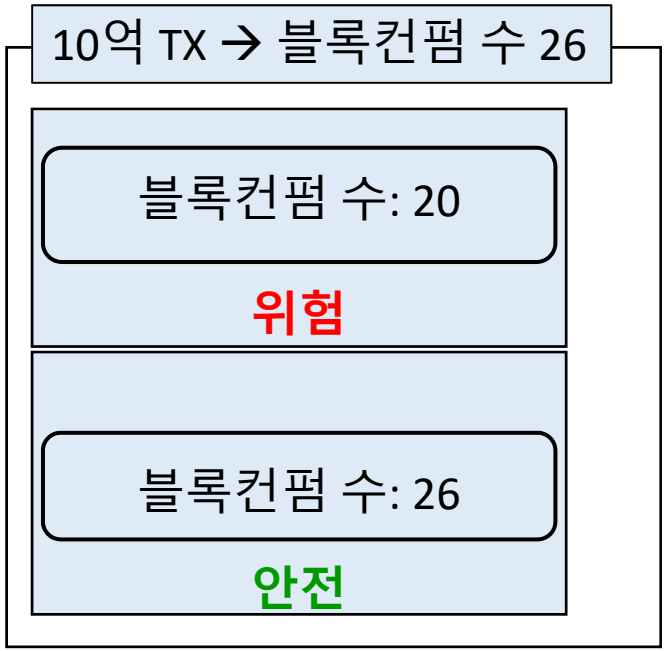
In the bitcoin network, any miner needs to attach the proof, called *nonce*, into the mined block header if this miner solved a specified puzzle. The task of verifying the given proof shall be easy but the task of obtaining the proof shall be very difficult. The puzzle is designed using the Secure hash algorithm (Sha) function [3]. Sha is good enough for this role. But, there is a problem which is that the puzzle constructed using only Sha is fixed and does not change over time to mine bitcoin. In 2013, as

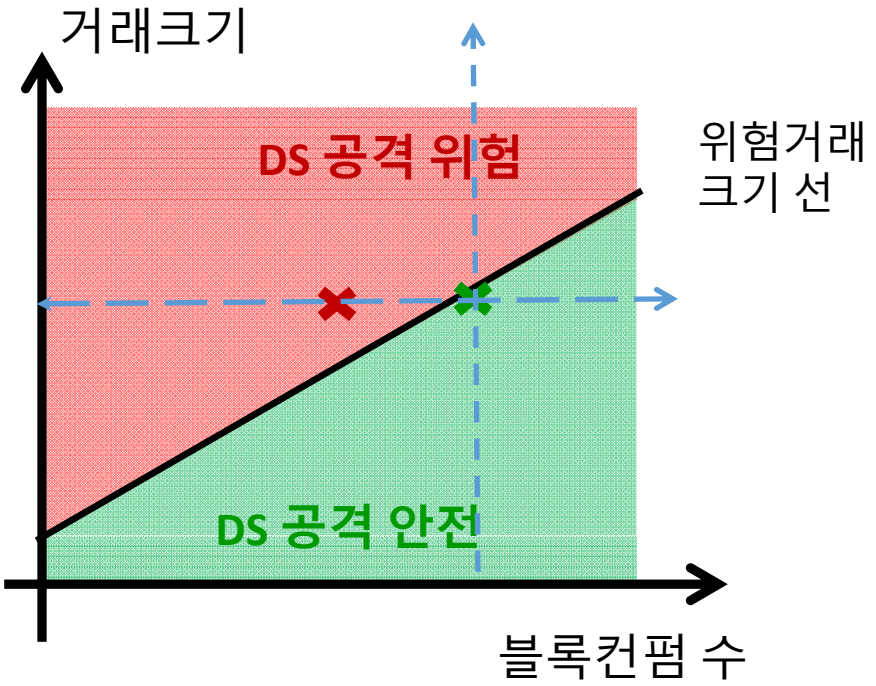
※ 국제 학술지 IEEE trans. Information Forensics and Security에 제출예정

보안성 개선 - DS 공격 위험성 평가 알고리즘

▣ DS 공격 위험성 평가 알고리즘의 목표

- *거래 별로 DS공격의 위험성을 평가, 사용자에게 자가 보안위험 대처 능력 부여*
- 보유 연구성과를 바탕으로 블록컨펌 수와 거래크기가 DS 공격자에게 이윤을 발생시키는지를 거래 별로 평가 가능
- 보안성 점수를 수치화하여 사용자에게 제공 가능





<보안성 판단 알고리즘>

보안성 개선 - DS 공격 위험성 평가 알고리즘

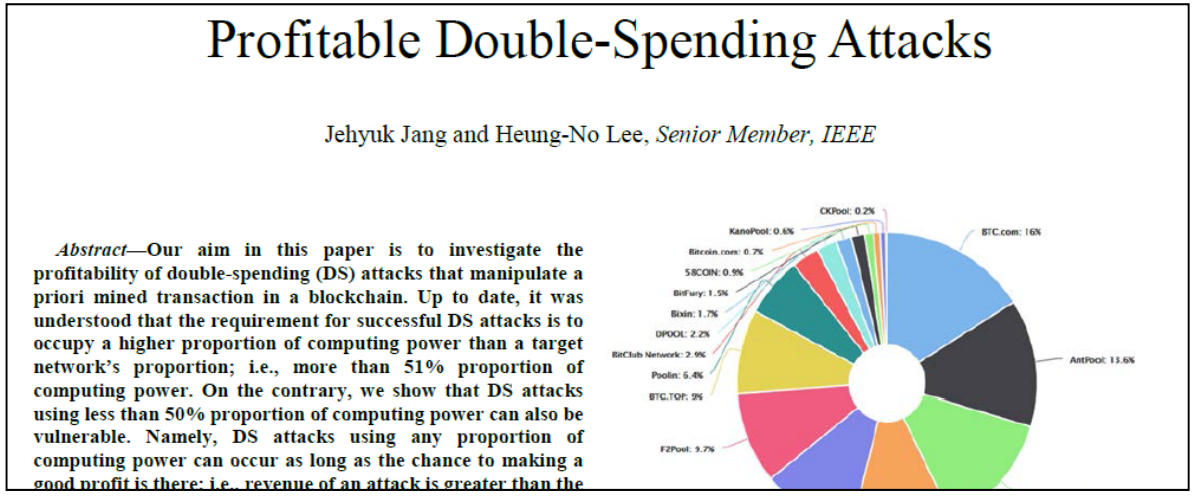
▣ 보안성 문제 정의

- 블록컨펌 수가 클수록 거래처리속도는 느려지나, DS공격에 강인해짐
- 지금까지는 블록컨펌 수의 설정 효과가 수치화 되어 있지 않음

※ 블록컨펌 수: 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)* 컴퓨팅파워 확보로도 위협적인 DS 공격이 가능함을 수학적으로 밝힘
- DS공격 수익(Profit), 거래규모, 블록컨펌 수와의 상관관계를 제시함



Profitable Double-Spending Attacks

Jehyuk Jang and Heung-No Lee, *Senior Member, IEEE*

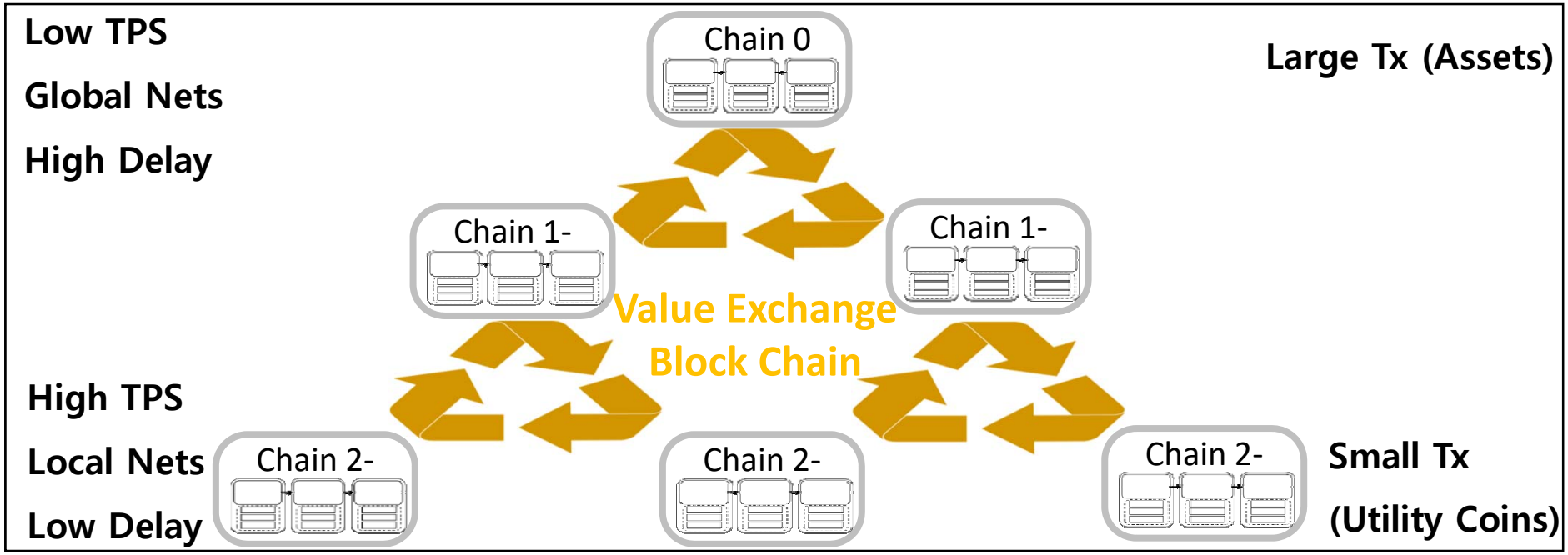
***Abstract*—Our aim in this paper is to investigate the profitability of double-spending (DS) attacks that manipulate a priori mined transaction in a blockchain. Up to date, it was understood that the requirement for successful DS attacks is to occupy a higher proportion of computing power than a target network's proportion; i.e., more than 51% proportion of computing power. On the contrary, we show that DS attacks using less than 50% proportion of computing power can also be vulnerable. Namely, DS attacks using any proportion of computing power can occur as long as the chance to making a good profit is there: i.e., revenue of an attack is greater than the**

※ 국제 학술지 IEEE trans. Information Forensics and Security에 제출됨

DeSecure 표준체인 사용 확대, 확장성 해결

▣ 다층 복합구조 블록체인, 코인가치교환 블록체인

- 현재 비트코인, 이더리움의 초당 처리속도는 수십 건 내외임
- ECCPoW 비트코인에서 확장성 개선을 위해 다층 복합구조 블록체인 제안
- 다 계층 블록체인 간 가교 역할을 담당할 아토믹스왑 기술 적용 가능



<다층 복합구조 블록체인>

검증 및 평가

▣ DeSecure 블록체인 시스템 검증 시나리오

- ECCPoW 비트코인과 ECCPoW 이더리움을 테스트
- 단일 노드 시나리오: 블록작성 검증, 체인형성 검증
- 복수 노드 시나리오: 블록작성 검증, 체인형성 검증, 난이도 조절 검증, 블록 동기화 검증, 합의 검증 및 거래 검증

▣ 시스템 검증 항목

- 블록작성 검증: 블록헤더가 주어졌을 때 올바른 블록이 작성되는지 검증
- 체인형성 검증: 주어진 길이 이상의 체인을 정상적으로 생성할 수 있는지 검증
- 난이도 조절 검증: 참여하는 채굴노드의 숫자에 따라 암호 퍼즐의 난이도가 변경되어 블록 생성 속도가 예측 가능하게 유지 되는지 검증
- 합의방식 작동 검증: 블록체인의 합의 방식(longest chain)이 작동하는지 검증
- 거래 검증: 발생한 거래들이 정상적으로 블록에 기록되는지 검증

검증 및 평가

▣ 시스템 성능 평가

- **테스트베드 평가**: 1차년도 연구 결과를 일정 수의 채굴 노드 확보를 통해 테스트 후 개발 목표치 달성 여부 평가
- **배포 평가**: 2차년도 연구 결과를 배포하여 다수의 채굴 노드 확보 후 목표치 달성여부 평가

▣ 시스템 성능 평가 항목

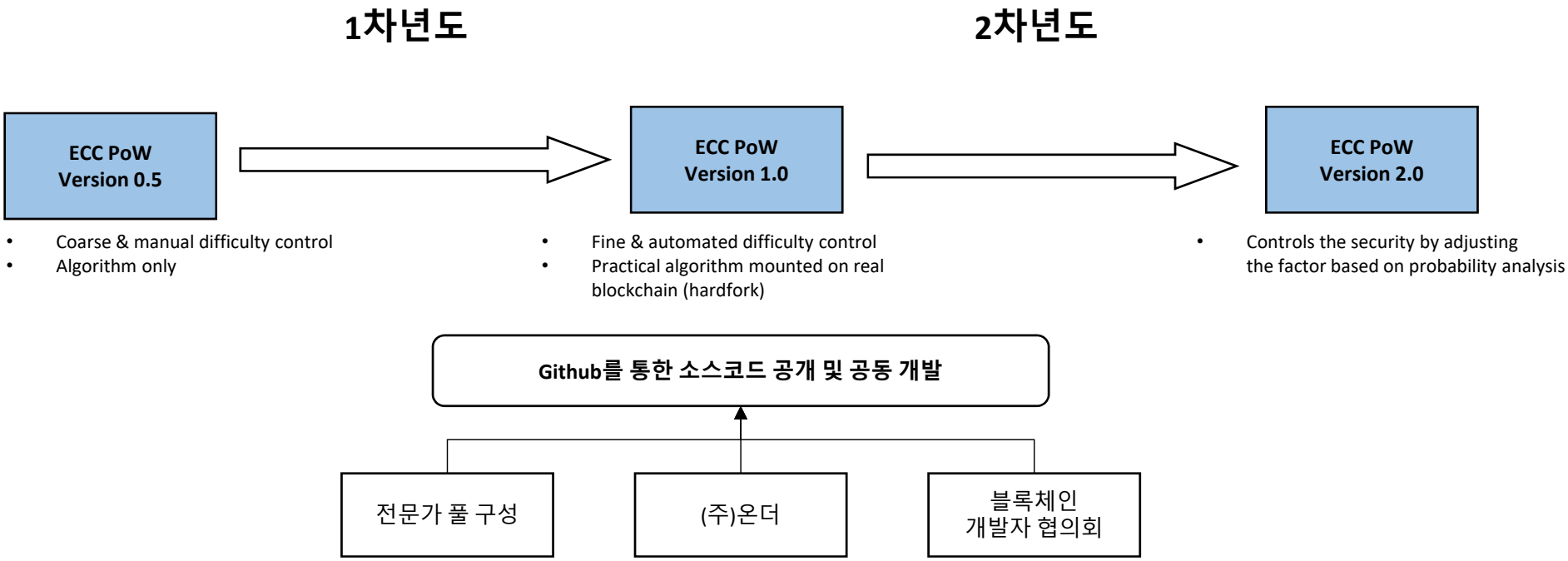
평가 항목	단위	세계최고 수준 보유기업 (비트코인, 이더리움)	개발 목표치		평가 방법
		성능수준	1차년도	2차년도	
1. 분산성	채굴성공률 분포도 (%)	40% (추정 값) (기준: 비트코인, 2018년 10~12월)	80%	80%	• 노드 채굴성공 확률의 평균과 분산을 측정 • 100%에 가까울수록 분산도가 적음
2. 보안성	비트코인 대비 보안성 (%)	100% (기준: 비트코인)	100%	200%	• 자체 정의한 보안성 평가지표로 계산 • 비트코인과 비교 평가
3. 확장성 (비트코인 하드포크)	비트코인 대비 확장성 (%)	100% (기준: 비트코인)	100%	200%	• 노드 수 증가대비 TPS 감소량 측정 • 비트코인과 비교평가
4. 확장성 (이더리움 하드포크)	이더리움 대비 확장성 (%)	100% (기준: 이더리움)	100%	200%	• 노드 수 증가대비 TPS 감소량 측정 • 이더리움과 비교평가

※ $\text{채굴성공률분포도}(\%) = \frac{(\text{채굴성공확률의 평균})}{\sqrt{(\text{채굴성공 확률의 분산}) + (\text{채굴성공 확률의 평균})^2}} \times 100$

기술개발의 추진전략, 방법 및 추진체계

연구 추진 전략

▣ DeSecure 블록체인 개발 추진 전략 및 일정



국내외 활동 계획

▣ 국제 학술대회 발표 계획

- University of Technology Sydney Conference (2월 22일, Sydney)
- Workshop on Cryptocurrencies and Blockchains for Distributed Systems, part of 2019 IEEE International Conference on Computer Communications (4월 29일, 프랑스 파리)
- IEEE/IFIP International Conference on Blockchain and Cryptocurrency (5월 17일, 서울)
- Crypto Valley Conference on Blockchain Techonology (6월 24일, 스위스 추크)
- 2nd IEEE International Conference on Blockchain (7월 14일, 미국 애틀랜타)

▣ 서울블록체인 밋업 공동조직자 및 이더리움 재단 개발자 모임 활동

- 이더리움 에드콘 (5월), 데브콘 (11월), 이더서울 (5월), 이더싱가폴 (연말)

▣ SCI 논문 게제 계획

- IEEE Transactions on Information Forensics and Security
- IEEE Transactions on Service Computing

▣ 블록체인 워크샵 "블록체인과 개인정보, 마이데이터" 개최 계획

- 2019년 9월 중 추진 예정

국내대학 및 협력사 연계

□ ECCPOW 블록체인 유저 확대 방안

- ✓ GIST 교내 블록체인 사업 확정
  - ▪ GTI 연구개발 사업
- ✓ 국내외 유수 대학에 연구용 DeSecure 블록체인 SW 보급

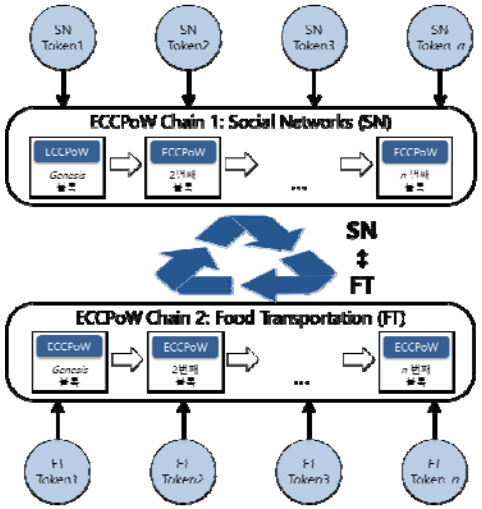
□ 기반 기술과 경험 활용 비즈니스 확장 전략

- ✓ 기 확보된 파트너사들의 비즈니스를 ECCPOW기반 솔루션 적용
- ✓ ECCPOW 블록체인 플랫폼 구축관련 컨설팅 및 교육
- ✓ 이더리움 dApp을 DeSecure ECCPoW 블록체인으로 탑재운용 유도

사업화 전략 – GIST 캠퍼스블록체인 추진

▣ GIST 블록체인 및 코인 활용방안

- GIST 캠퍼스 블록체인 개발 및 적용
- 연구노트, 상품권 코인, 성적표, 강의평가 등 시범 네트워크 구축
- GIST 스캔 서버 운용 (블록크기, 속도, TPS 등을 모니터링)
- (Living Lab.) 학내 구성원으로부터 GIST 캠퍼스 블록체인 평가를 수집하고 평가 결과를 반영하여 시스템을 고도화
- GIST 블록체인 Dapp 개발 경진대회 운용 (해커톤)



발표요약

- 핵심 연구, 개발 역량 확보
- 핵심 IP확보, 핵심 MoU 확보
- ECCPoW기술 활용 표준형 DeSecure 블록체인 개발
- DeSecure BTC-ECC, ETH-ECC 프로토콜 보급
- 다층형 멀티체인 생태계 추동
- 이더리움 개발자 협력 경험
- DeSecue Blockchain 교육, 연구, 창업 성과 창출 가능
- GIST캠퍼스BC, 리빙랩 운영
- 국내외 확산 사업화 전략 제시

heungno@gist.ac.kr
facebook ID: Heung-No Lee
https://infonet.gist.ac.kr