



Goal of this lecture note

- Bitcoin and Ethereum
- Problems of PoW
- Trilemma vs. DeSecure Strategy
- DeSecure Blockchains
- ECCPoW
- Open Source DeSecure Project
- Impact of DeSecure Blockchains

1 Bitcoin and Ethereum

- Bitcoin's Ideals
 - BTC is the first global digital currency of people which works beyond national boundaries.
 - Ideals around BTC are
 - Decentralization
 - Reforming Wall street
 - Unbundling big corporations
 - Reduction of inequality

1 Bitcoin and Ethereum

- Ethereum's Ideals
 - ETH is a world decentralized computing platform.
 - Programming smart contracts is easier.
 - One can make DApps.
 - One can create tokens in 20 minutes.
 - People can make Decentralized Autonomous Organizations (DAO).

2 Problems of PoW

*PoW is fundamental.
But there are problems.
Let us fix its problems and use it.*

2 Problems of PoW

- Complaints today
 - PoW based blockchains are most secure;

But they are ...

- Spending too much energy in mining
- Re-centralized
- Said to be too slow, not supporting speedy transactions

3 Trilemma vs. DeSecure Strategy

- Blockchain Trilemma?

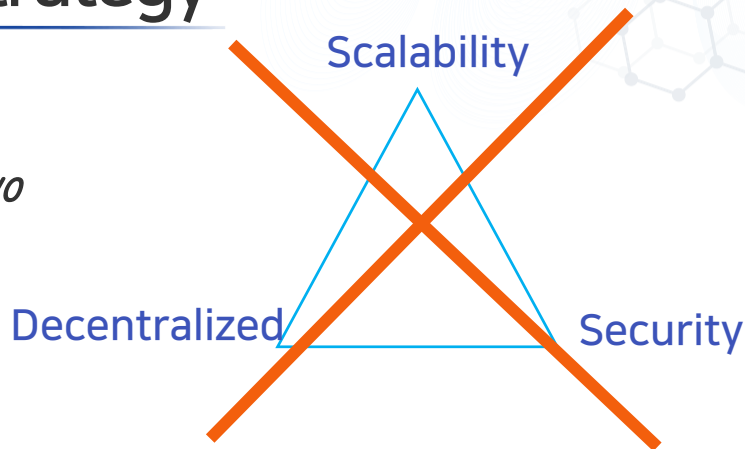
“blockchain systems can only at most have two of the following three properties”

- Vitalik Buterin

Wrong approach!

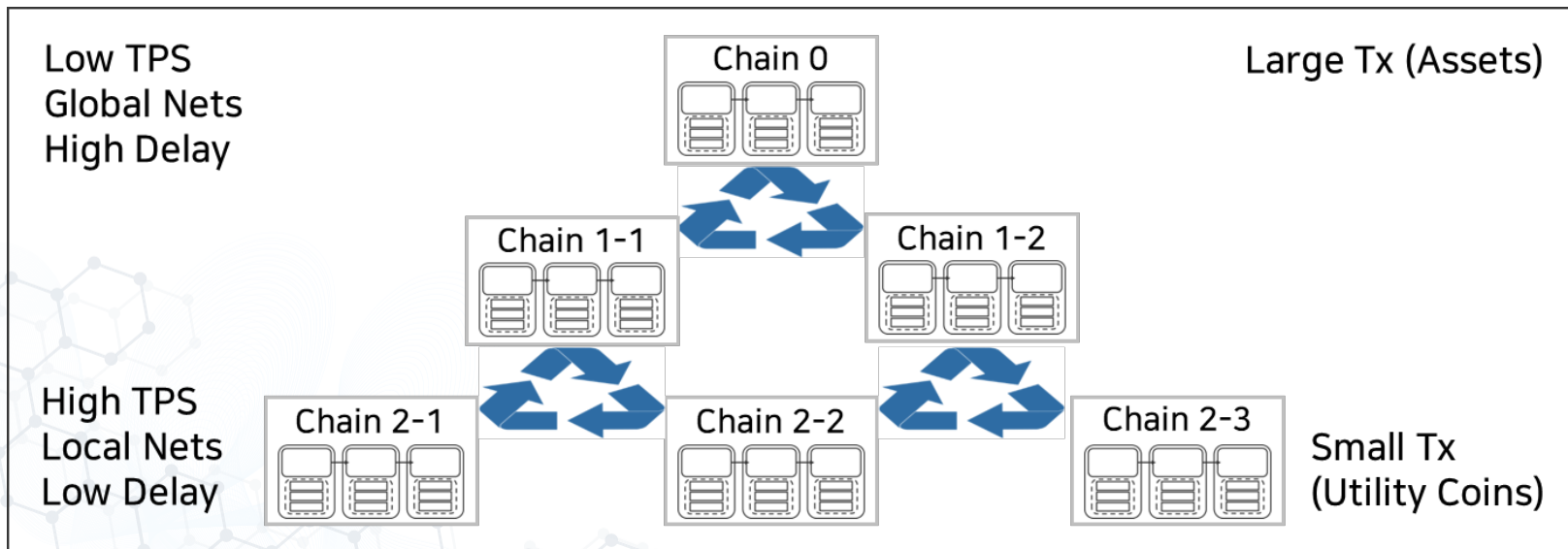
- Not in a single blockchain, can it be achieved!
- We shall promote many decentralized secure (DeSecure) blockchains to achieve scalability!

출처: <https://github.com/ethereum/wiki/wiki/Sharding-FAQ>



3 Trilemma vs. DeSecure Strategy

- Provision of DeSecure chains is to solve Scalability issue!
 - Global chains → national chains → local chains → diff. applications







4 DeSecure Blockchains

- We aim to approach these two issues with DeSecure blockchains.
 - Anti-ASIC ECC PoW
 - Ecosystem of DeSecure blockchains
- DeSecure blockchains use novel **Error-Correction Code PoW**.
- We aim to provide two DeSecure blockchains, ETH-ECC and BTC-ECC.



4 DeSecure Blockchains

- They Have Sought Alternatives to PoW, BUT

	Pros	Cons	Coins within top 50 rank
PoW (Proof-of-Work)	<ul style="list-style-type: none"> • Strong security <ul style="list-style-type: none"> - Difficult to produce - Easy to verify 	<ul style="list-style-type: none"> • Extreme computing power • 51% attacks • Transaction speed / Transaction throughput 	 Bitcoin  Ethereum
PoS (Proof-of-Stake)	<ul style="list-style-type: none"> • Energy & hardware efficiency • Much more expensive • 51% attacks 	<ul style="list-style-type: none"> • Recentralization • The rich-get-richer • "Nothing at stake" problem 	 Qtum  Stratis

4 DeSecure Blockchains

- They Have Sought Alternatives to PoW, BUT

	Pros	Cons	Coins within top 50 rank
DPoS (Delegated PoS)	<ul style="list-style-type: none"> • Scalability and speed • Energy & hardware efficiency • Encouraging good behavior by realtime voting 	<ul style="list-style-type: none"> • Recentralization • DDoS attacks • Double Spending 	
PoA (Proof-of-Activity)	<ul style="list-style-type: none"> • Decentralization - Validators are randomly selected 	<ul style="list-style-type: none"> • Computing power • Recentralization • The rich-get-richer 	

4 DeSecure Blockchains

- Existing Scalability Solutions

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

Type	DeSecure	Bitcoin		Ethereum	
Name	Multi-level, multiple chains	Seg-Wit	Lightning Network	Plasma	Sharding
구현	ECCPoW 기반 독립체인들을 여러 계층으로 묶음	블록 데이터 구조를 변경하여 구현	오프체인 거래 진행 최종 결과값을 메인 블록체인에 기록	하부 체인 생성 거래 진행 후 최소한의 기록만 메인 블록체인 기록	블록체인의 DB에 해당하는 스테이트를 여러 샤드로 분할, 분리 처리

4 DeSecure Blockchains

- Existing Scalability Solutions

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

Type	DeSecure	Bitcoin		Ethereum	
Name	Multi-level, multiple chains	Seg-Wit	Lightning Network	Plasma	Sharding
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

4 DeSecure Blockchains

- Existing Scalability Solutions
 - DeSecure Blockchain aims to resolve the re-centralization problem without sacrificing the secureness!*

Type	DeSecure	Bitcoin		Ethereum	
Name	Multi-level, multiple chains	Seg-Wit	Lightning Network	Plasma	Sharding
단점	No single chain solution/ 생태계필요	트랜잭션 처리속도 증가 효과 미비	오프체인 거래기록 없음	Full노드 만 플라즈마 사용 가능	S/W 복잡도 상승

5 ECCPoW

- We aim to Replacing SHA-PoW with ECC-PoW!

Three key parts

1. Web server interface n

- Node registration, get
- Full node or light node
- Communication amon

2. Wallet for TX generati

- Make private and publ
- neighbor, check to see

3. Consensus Mechanism

- **Data**: Genesis block +
- **Protocol**: consensus, l
- **Mining**: Get the longe
- mempool and form a l
- block header, and atta

Program Suite

- C++, Python, Go, Java, Fi
- Download and run, then you have

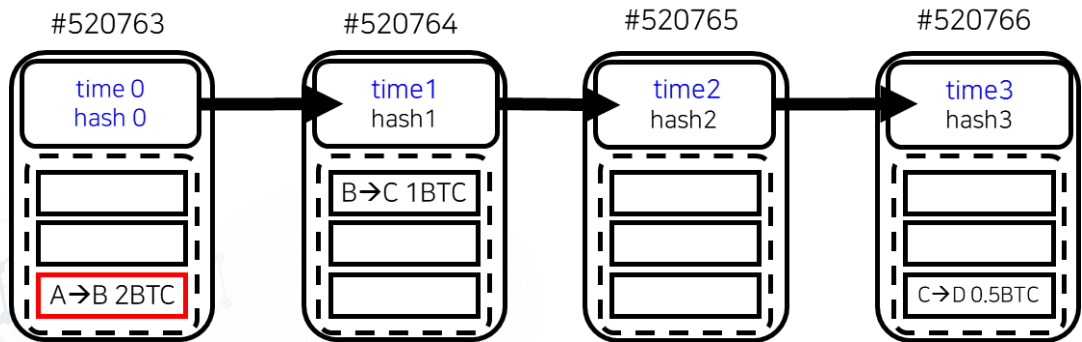
3. Consensus Mechanism

- **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.

Consensus Engine

5 ECCPoW

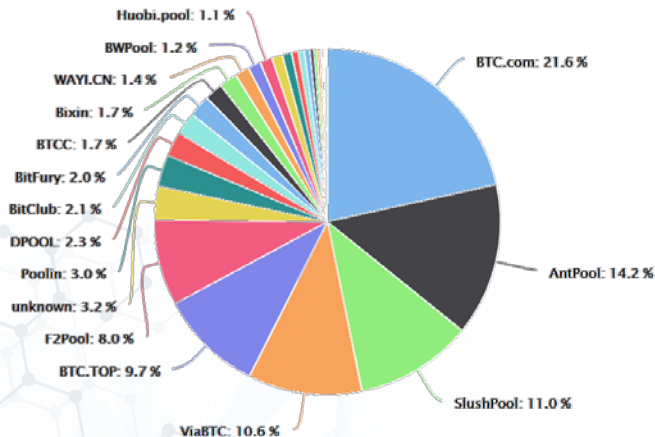
- Pow is fundamental to OPEN blockchains.
 - What happens when any alteration is made?



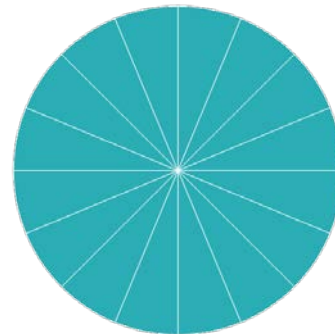
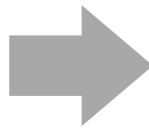
5 ECCPoW

- ECC-PoW aims to resolve Recentralization Issue.
 - ASIC → Mining Moguls → Discourage Average Miners
 - Prone to Collusion, Censorship

Decentralized again



Recentralized



1. ASIC resistant
2. Vulnerability to DS attacks reduced

5 ECCPoW

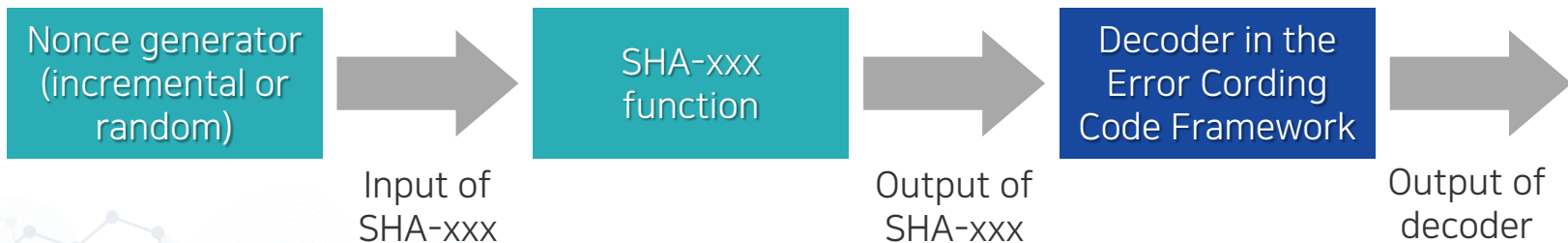
- Item to consider a new PoW!
 - A new puzzle generation system is capable of varying puzzles from block to block with the following properties:
 - P1: Easy to verify but difficult to prove
 - P2: Robust to detect block modification attacks
 - P3: Controllable in changing the difficulty level
 - P4: Open to anyone with a CPU
 - **P5: Unfixed and changeable from block to block**
 - The re-centralized problem can be resolved thanks to P5.

5 ECCPoW

- Novel Error Correction Codes PoW (ECCPoW)
 - There are many one-way functions in inverse problems
 - Error Correction Codes
 - Sparse-Signal Recovery
 - Space-Time Coding
 - Sphere-Decoding
 - In these problems, encoding is easy but decoding is controllably time-consuming!

5 ECCPoW

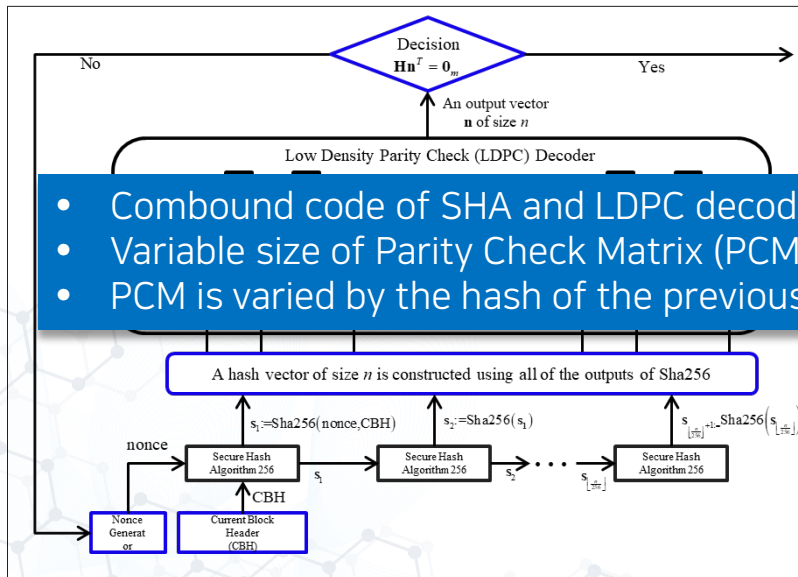
- Novel Error Correction Codes PoW (ECCPoW)
 - We combine a Error Correcting Code framework with SHA-xxx.



- The decision of mining success is made with the output of the above decoder.

5 ECCPoW

- Novel ECCPoW Consensus is proposed!
- ECCPoW 합의 엔진



- Compound code of SHA and LDPC decoder.
- Variable size of Parity Check Matrix (PCM) → Amt of resource (mem, comp) varies.
- PCM is varied by the hash of the previous block.

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, 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

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

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

5 ECCPoW

- Error Correction Code
 - Transmitter and receiver uses a codebook.
 - In a codebook, there are codewords.
 - Transmitter sends a message.
 - Message goes through channel.
 - Errors are induced.
 - Receiver gets the erroneous message.
 - Decoder aims to find a nearest codeword.
- Decoder uses memory and computer to run and find a codeword.

5 ECCPoW

- Block code, encoder and decoder

$$\begin{bmatrix} \mathbf{s} \end{bmatrix} = \begin{bmatrix} \mathbf{F} \end{bmatrix} \begin{bmatrix} \mathbf{e} \end{bmatrix}$$
$$\begin{aligned} \mathbf{S} &\in GF(q)^{M \times 1} \\ \mathbf{F} &\in GF(q)^{M \times N} \\ \mathbf{e} &\in GF(q)^{N \times 1} \end{aligned}$$

Decoder: Given \mathbf{e} , find $\hat{\mathbf{e}} = DEC(\mathbf{s} = 0, \mathbf{F})$

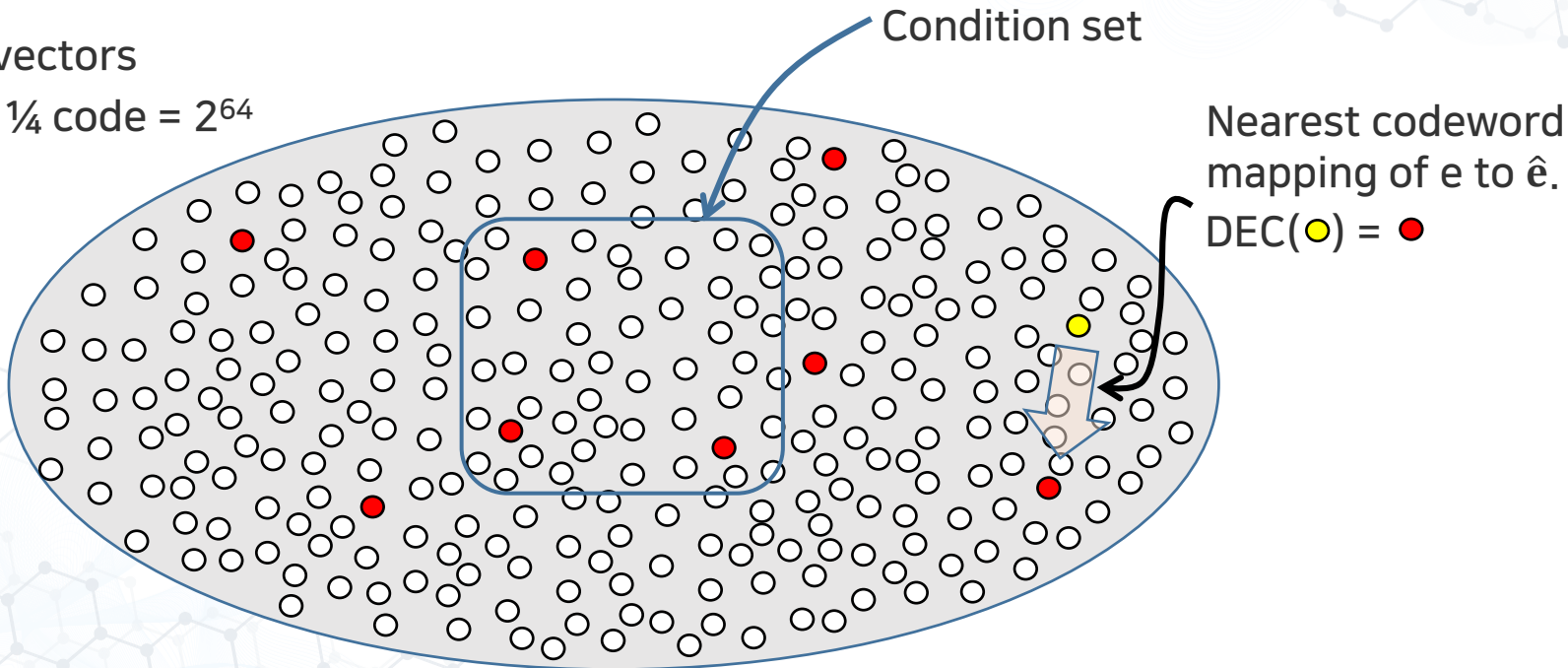
5 ECCPoW

- Decoder
 - SHA output is input to the decoder.
 - Decoder treats it as erroneous message and produces either a codeword or non-codeword.
 - We use the low-density parity-check (LDPC) code and its message passing decoder.
 - We change the matrix F to change the puzzle.

5 ECCPoW

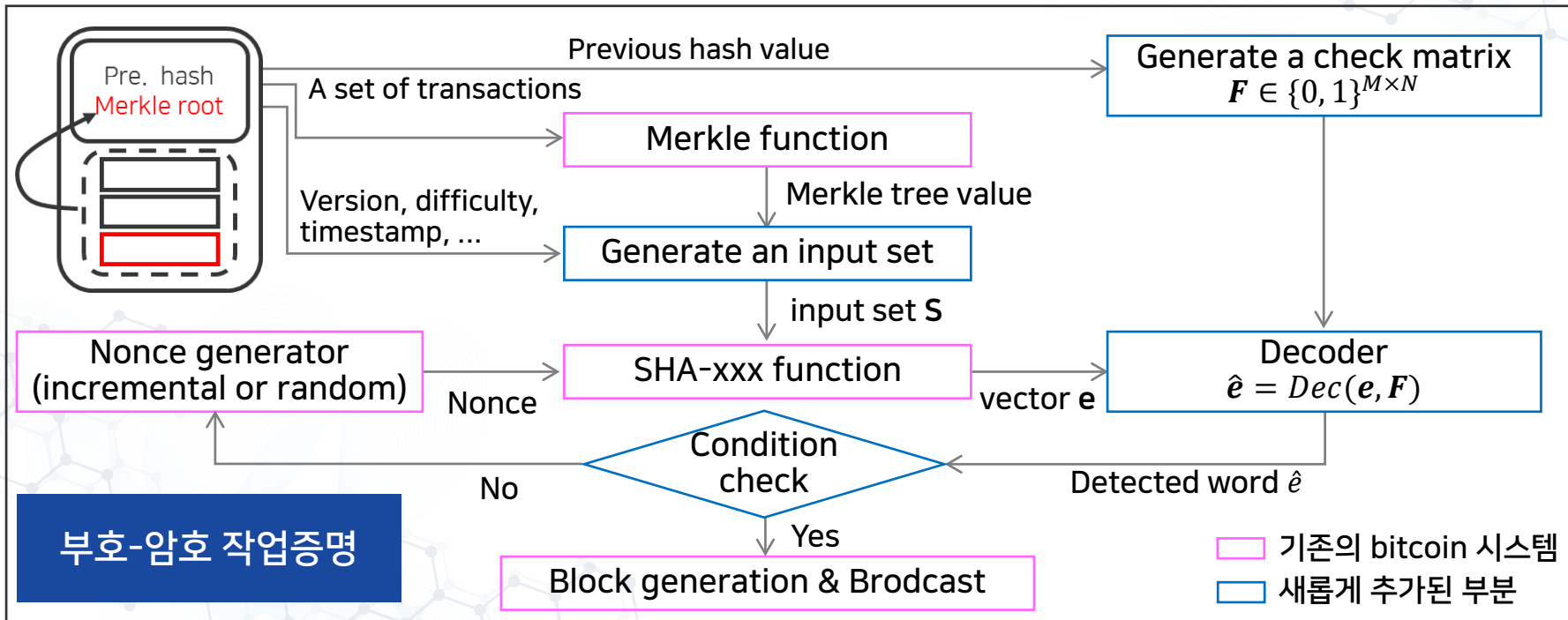
• Geometrical Explanation

- 2^{256} vectors
- Rate $\frac{1}{4}$ code = 2^{64}



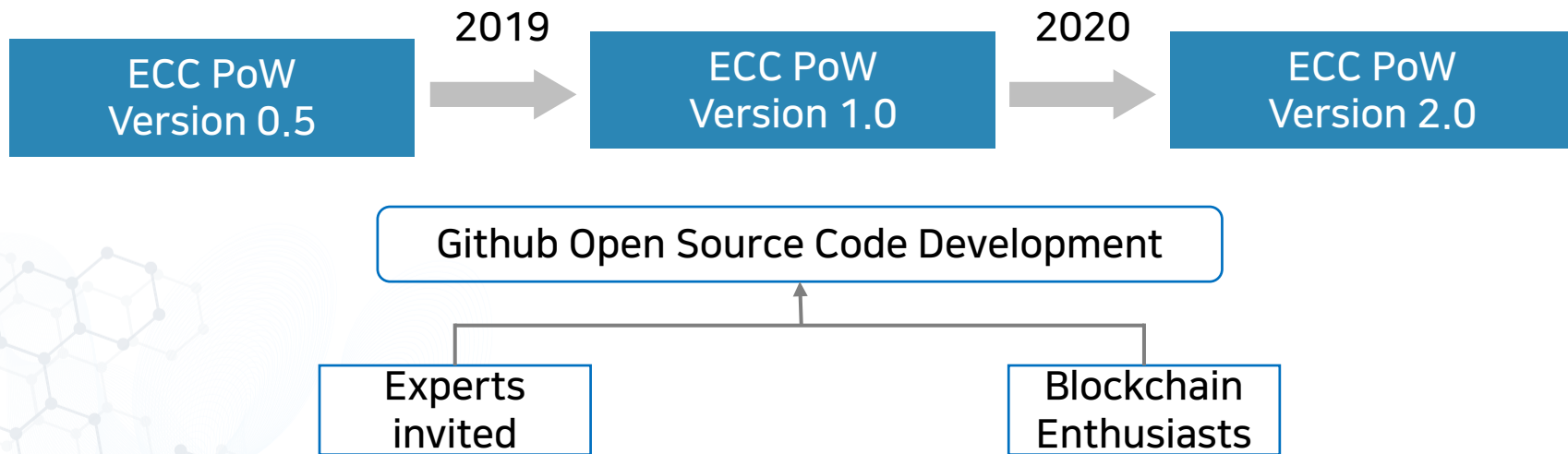
5 ECCPoW

• Diagram of ECCPoW



6 Open Source DeSecure Project

- DeSecure Blockchain Release Plan



6 Open Source DeSecure Project

- DeSecure is Open Project.
 - HP in prep: <https://dsecure.org/>
 - BTC-ECC explorer: <http://13.209.74.13/blocks> (AWS node)
 - BTC-ECC Github: https://github.com/cryptoecc/bitcoin_ECC
 - ETH-ECC: https://github.com/cryptoecc/go-ethereum_ECC/tree/eccpow-1.9
 - List of papers on DeSecure Blockchain
https://infonet.gist.ac.kr/?page_id=6832

7 Impact of DeSecure Blockchains

- Impact on **Safe Start**

It is **easier to start a new** blockchain network.

- Today there are mining equipment renting sites.
- A new borne blockchain network needs to grow, but a newbie is much more vulnerable to 51% attacks.
- New blockchain networks with ECCPoW do not suffer from such problems since there are no mining equipment available for ECCPoW.

7 Impact of DeSecure Blockchains

- Impact on **Standardization**

One can make multiple blockchain networks

- Make the first blockchain network by running ETH-ECC over a network (**Pusan ETH**)
- Make the second blockchain network by running BIT-ECC over other network (**Gwangju BIT**)
- Make the third blockchain network by running ETH-ECC over another network (**Seoul ETH**)
- Make the fourth blockchain network by running BIT-ECC over yet another network (**Global BIT**)

7 Impact of DeSecure Blockchains

- Impact on **Standardization**

One can make multiple blockchain networks

- Each cryptocurrency is independent with its own genesis block and random starting seed and can be **adjusted sufficiently strong for its regional requirement** in the sense of scalability, security and decentralization.
- These blockchains are **inter-connected** at the local, regional, and national, transnational level.

7 Impact of DeSecure Blockchains

- Impact on **Resolving the Scalability Trilemma**
 - Each DeSecure blockchain is already very strong in decentralization.
 - Each DS blockchain is flexible enough to provide various settings of transaction speeds and security levels.
 - **Regional DeSecure** networks can be set to work **very fast**, i.e. allowing up to 10s of thousands of TXs per sec.
 - **National** DeSecure networks can be set sufficiently **fast** for covering inter-regional transactions.
 - **Transnational** DeSecure networks shall be set to work **slow** due to large delays.

7 Impact of DeSecure Blockchains

- Impact on **Resolving the Scalability Trilemma**
 - All these blockchains started up with its own seed and decentralized levels are mutually independent and each one can be **set to work at the required level of security and speed to serve its purpose.**
 - All these **DeSecure blockchains** can be **inter-connected** via distributed value-exchange networks.

7 Impact of DeSecure Blockchains

- Impact : **New PoW**

PoW is problem. Yes.

But it is not the inherent to PoW.

It is the fixedness and simplicity of the PoW puzzle.

ECCPoW is time-varying and grow very complex.

7 Impact of DeSecure Blockchains

- Impact on **Deterrence to ASICs**:

The complexity of ECCPoW puzzles can be set to grow very large.

- ECCPoW is a computer algorithm!
- Thus it is **not impossible** to find a **hardware acceleration** solution for it.
- But **it comes with boundless cost** to memory and computing resource.

7 Impact of DeSecure Blockchains

- Impact on **Energy Spending**:

- Deterrence to hardware acceleration offers a blockchain network with small hash rate requirement.
- Ordinary people can join.
- One-cpu one-vote possible again