2019 Australia-Korea FinTech Symposium

Feb. 22nd, 2019
UTS Business School Dr Chau Chak Wing Building
Sydney Technology University

Blockchain Technology and Regulations

Heung-No Lee, GIST, South Korea
Home page: http://infonet.gist.ac.kr
Publication ID/facebook ID: Heung-No Lee

Sponsored by:

Australian Government

Australia-Korea FOUNDATION

Preliminary Program

Date: 22nd February 2019

Venue: UTS Business School Dr Chau Chak Wing Building

Start	Finish	Description	Topic	Speaker(s)
8:30:00 AM	8:40:00 AM	Welcome	Welcome Address	Ashish Sinha (UTS)
8:40:00 AM	9:20:00 AM	Session 1	Blockchain Standards to support FinTech Innovation	Pip Ryan (UTS)
9:20:00 AM	10:00:00 AM	Session 2	Blockchain Technology	HeungNo Lee (BIEC)
10:00:00 AM	10:20:00 AM	Morning Tea		
10:20:00 AM	11:00:00 AM	Session 3	ASX Blockchain Registry	Cliff Richards (ASX)
11:00:00 AM	11:45:00 AM	Keynote	TBA	YooShin Jung (Korea Fintech Center)
11:45:00 AM	12:30:00 PM	Panel 1	Blockchain Regulation: How to Regulate a Self Regulating System?	(Financial Services Commission), SoonHyuck (Kenneth) Jung (CCET Project), (ASIC), Pip Ryan (UTS) Host: Elvira Sojli (UNSW)
12:30:00 PM	1:15:00 PM	Lunch		
1:15:00 PM	1:55:00 PM	Session 4	Fintech Regulation	(ASIC)
1:55:00 PM	2:35:00 PM	Session 5	(TBA)	Michelle East (Certainty Compliance)
2:35:00 PM	2:55:00 PM	Afternoon Tea		
2:55:00 PM	3:35:00 PM	Session 6	Cryptocurrency: Tax Issues	SangWha Shin (Korea Institute of Public Finance)
3:35:00 PM	4:15:00 PM	Session 7	Blockchain and Law	YoungMi Ko (Soongsil Uni)
4:15:00 PM	4:55:00 PM	Panel 2	Digital Payments: Regulation to Drive Innovation?	KiHoon Hong (Hongik Uni), JungHoon Kim (FSS), Karen Parkes (AUSTRAC), Ed Tellez(RBA) Host: Sean Foley (Sydney Uni)
4:55:00 PM	5:00:00 PM	Closing Address		Adrian Lee (UTS)

Abstract of the Talk

In the year 2018, we have witnessed the surge and the fall of crypto-currencies. With the surge, blockchain the new technology behind cryptocurrencies, and its idealistic footprint of advanced thoughts, blockchainism it can be perhaps called, came to enthrall our minds. Thousands of new ambitious projects have been conceived and fast activated with the worldwide frenzy of new funding through initial coin offerings a novel funding mechanism in the blockchain world. Decentralized societies, equal accesses to valuable resources, reducing the cost of middleman, freed individuals from hierarchical organizations, and reducing the spread in inequalities are some of those advanced thoughts. But the fall came; the market value for Bitcoin has collapsed more than 7 times from its peak-value; that of Ethereum has plummeted more than 12 times. These two power houses which have supported those progressive projects are now torn apart. Recent New York Times report reads, “Blockchain: What’s it good for? Absolutely nothing, report finds.” Another one reads, The Blockchain Is a Reminder of the Internet’s Failure. The same utopian promises that bloomed during the Internet’s early days are back. Be afraid.“ Should this be the end of our pursue to change and make a better world with blockchains? Obviously not. In this presentation, I would like to talk about the reality of blockchain technology and how distant it is from the ideals. With this assessment, I would like to present some of novel research progresses we made in year 2018 and talk about further research ideas to pursue in year 2019. Finally, regulations around the world are presented in comparison with them in Korea and how innovative work can be put together into a business and creating of new businesses soaring through the firm ceiling of Korean regulation.

Short Bio of Dr. Heung-No Lee

Heung-No Lee graduated from University of California, Los Angeles (UCLA), U.S.A. with Ph.D., M.S., and B.S. degrees all in Electrical Engineering, 1999, 1994 and 1993 respectively. He has written more than 70 international journal publications and a hundred international conferences and workshop papers. He worked at HRL Laboratory, Malibu, California, U.S.A., as Research Staff Member from 1999 to 2002. He worked as Assistant Professor at the University of Pittsburgh, Pittsburgh, Pennsylvania, U.S.A. from 2002 to 2008. He then moved to Gwangju Institute of Science and Technology (GIST), Republic of Korea, in 2009 where he is currently tenured full professor. His research lies in the areas of Information Theory, Signal Processing Theory, and Communications Theory, and their application to Communications and Networking systems, Biomedical systems, and Signal Processing systems. Awards he has received recently include Top 50 R&D Achievements of Fundamental Research in 2013 (National Research Foundation), Top 100 National R&D Research Award in 2012 (the Ministry of Science, ICT and Future Planning) and This Month Scientist/Engineer Award (National Research Foundation) in January 2014. He was the Director of Electrical Engineering and Computer Science within GIST College in 2014. Administrative positions he has held at GIST include the Dean of Research and the Director of GIST Research Institute.

Disclaimer: An extended version of this lecture was presented as Plenary Talk at ICEIC 2019, Jan. 23rd, 2019, Auckland, New Zealand.

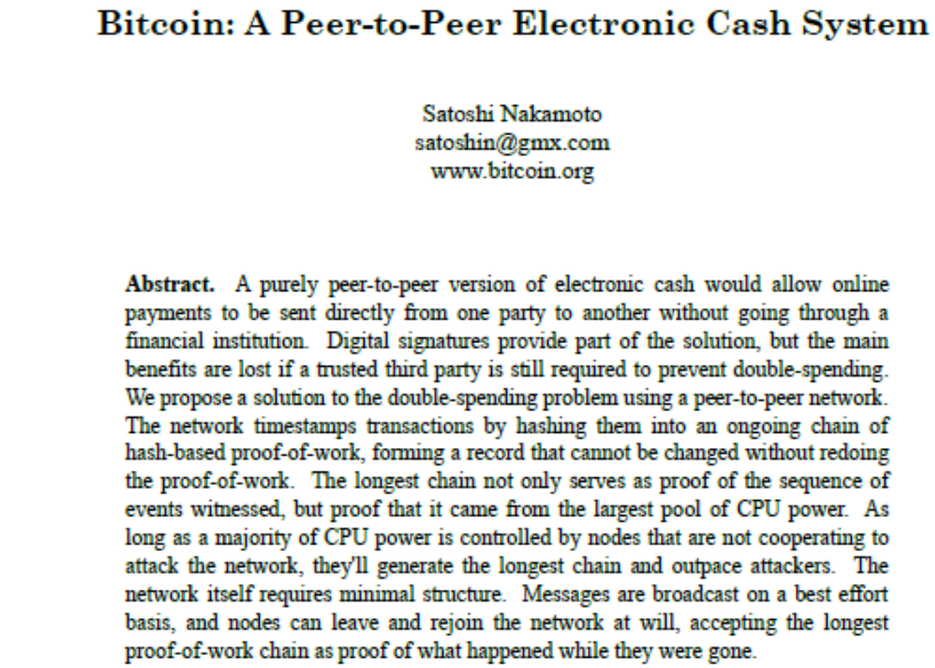
Talk today

- This talk shall focus on the open public blockchains but not on the private blockchains.

- Blockchain Ideals
- Reality
- Future
- Regulations
- Summary

Bitcoin, What it is?

- Year 2019 is the 10th anniversary of the birth of Bitcoin.
- Today, it has grown into a global computer network which mints coins every 10 minute.



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bitcoin’s Ideals

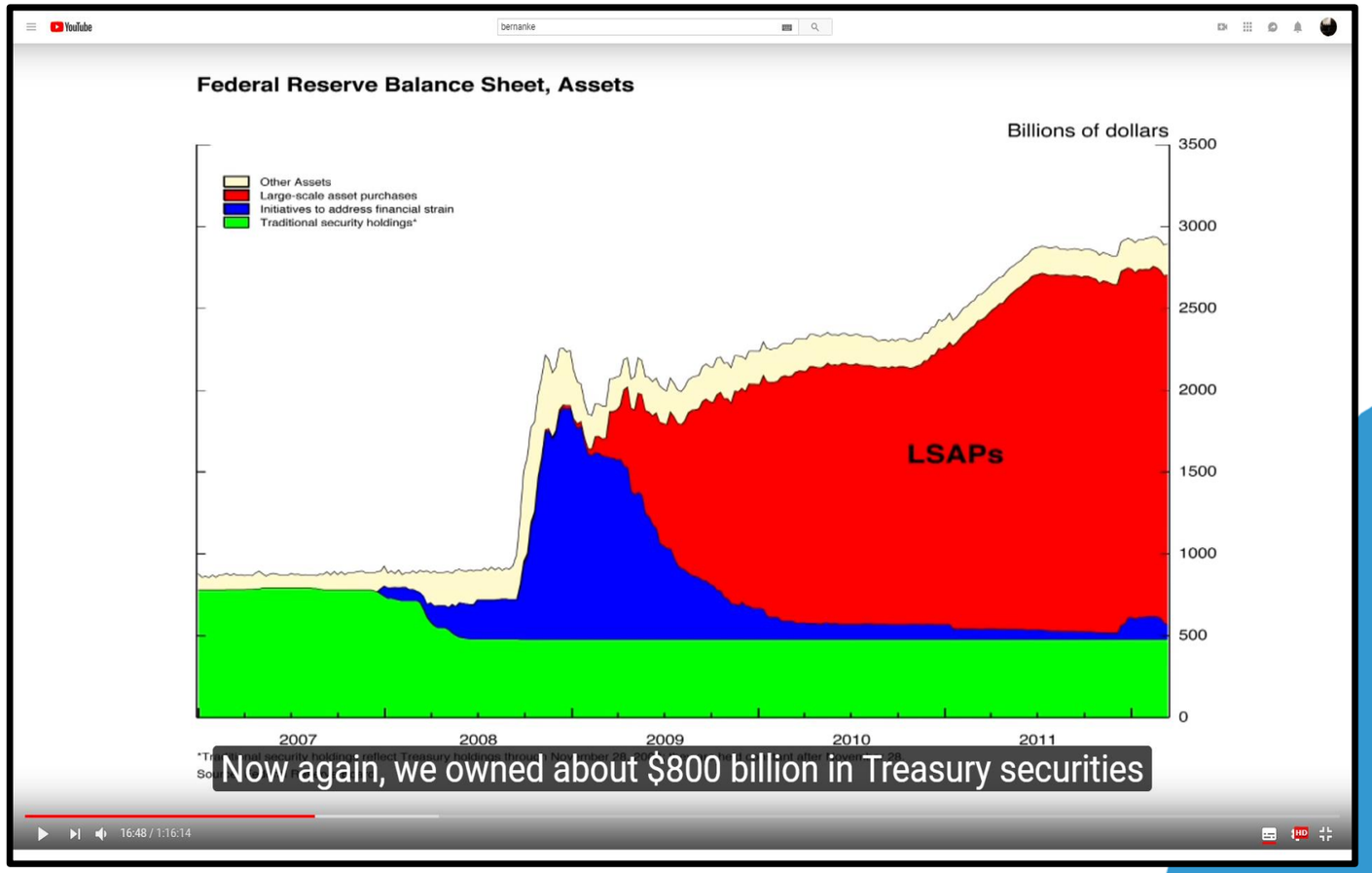
- Since birth in 2009, Bitcoin has never stopped breathing and alive currency system.
- It is a global digital currency which works beyond national boundaries.
- It was the time when trust on the banks and governments were severely degraded.
- Ideals around bitcoin are
  - Decentralization
  - Reforming Wall street
  - Unbundling big corporations
  - Reduction of inequality

FED and LSAPs

Large Scale Asset Purchase (QE)

Control the supply of long-term securities.

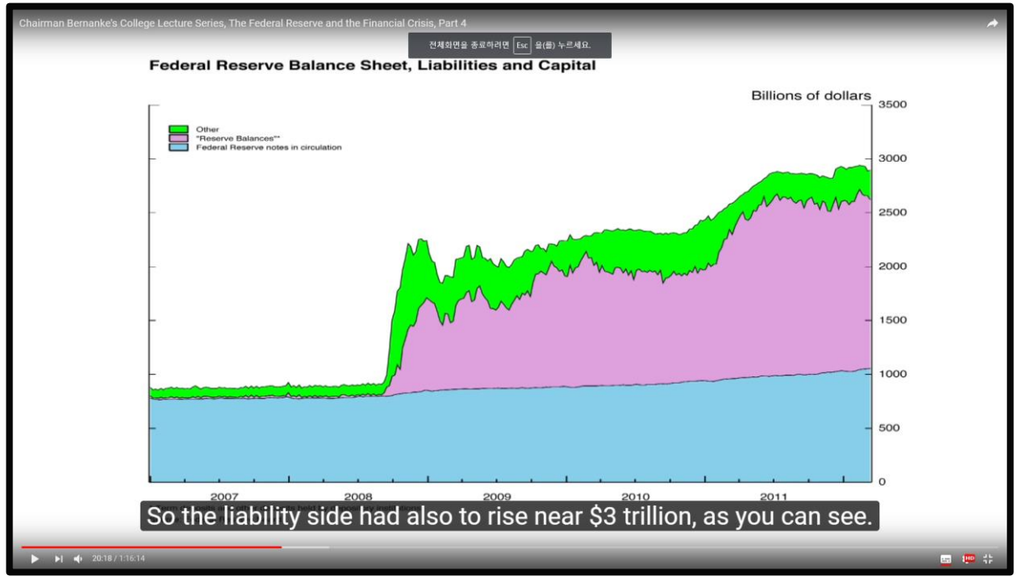
Lowered the long term interest rate.



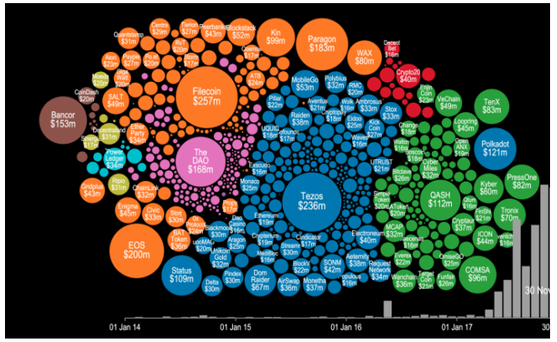
How to pay for LSAPs?

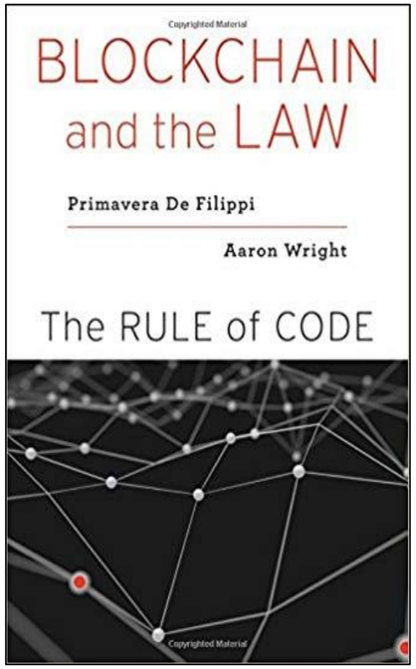
the liability side had also to rise near $3 trillion… But as a literal fact, the Fed is not printing money to acquire these securities. The amount of currency in circulation has not been affected by these activities. What has been affected is the purple area. Those are the accounts that banks, commercial bank, holds with the FED. They are part of what's called the monetary base. But again, they are not – they certainly aren't cash.

Watch for yourself right here.

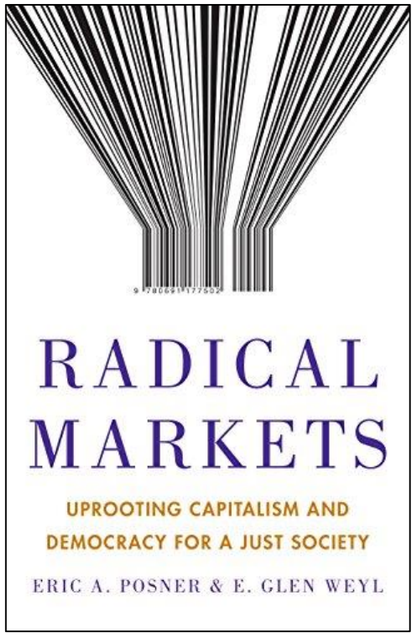


Ethereum's Ideals





- Ethereum network allows not only coin TXs, but also doc files and computer codes.
- A *decentralized* app (Dapp) runs a front end code; a backend code runs in *the Eth Net*.
  - ✓ cf) For an ordinary app, the backend code is running on *a centralized server*.
- Smart contracts
  - ✓ A computer code can be executed and advanced to the next stage each time a contractual term matures.
- Decentralized autonomous organization has its bylaw written in smart contracts.
  - ✓ The organization spends tokens and makes governance decisions w.r.t. smart contracts.
- *Lex Cryptographia!*
- *Uprooting capitalism and democracy for a just society!*
- *Sharing Economy!*



Reality

Blockchain Core (Program Suite)

Network of peers

- Node registration, get-address, give-address
- Full nodes, light nodes, wallet nodes

Wallets for TX generations

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

Miners guarding the blockchain

- Data: Genesis block and regular blocks, one block every 10 minute, 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.

Web server interface

- Means of communication among nodes, wallets and miners

Program Suite

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

Blockchain after-all is just a computer server network.

- A digital ledger in which the content of TXs is recorded right away as soon as each occurs.
- A technology which keeps what's recorded in its original form.

- What are those recorded in the distributed ledger?

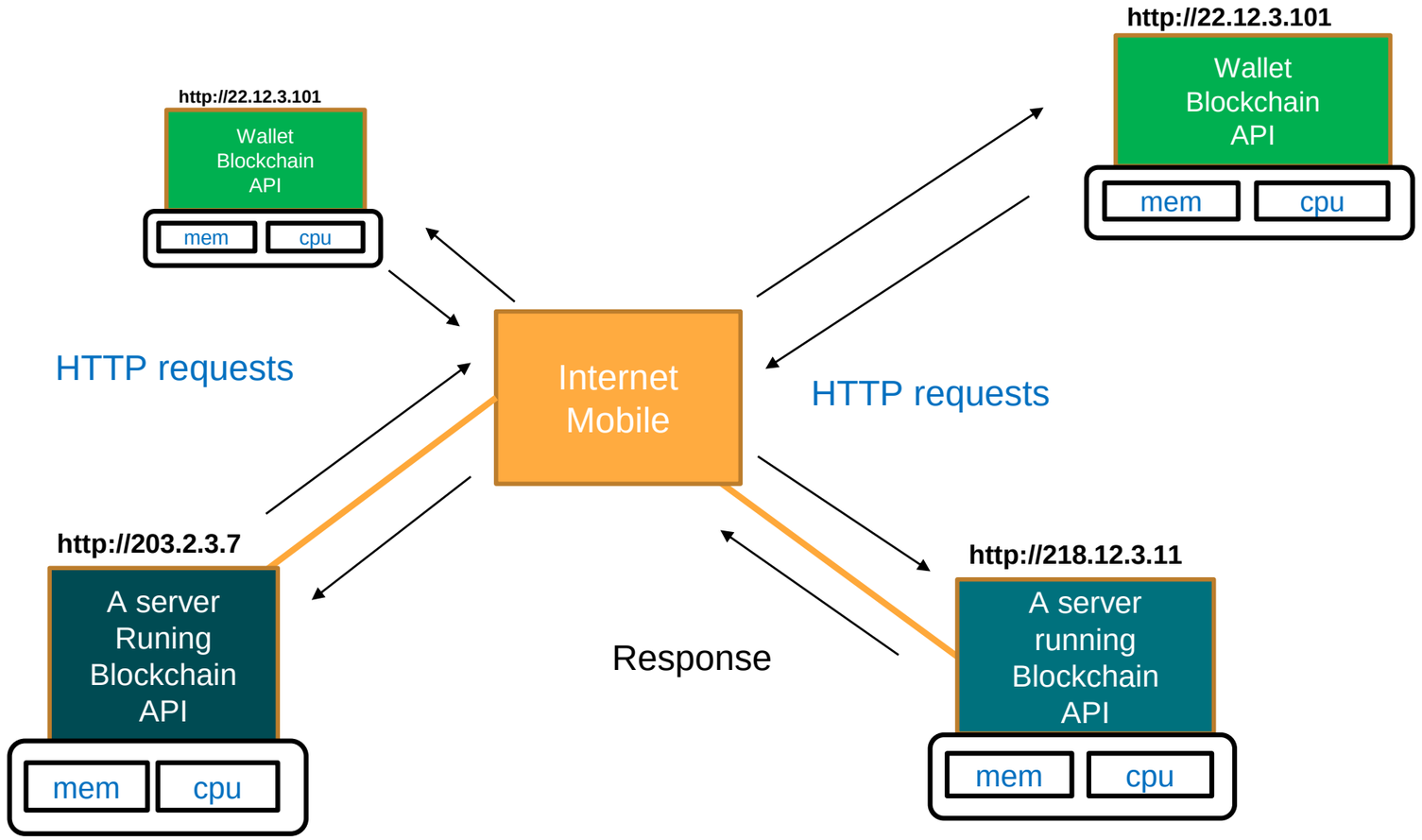
  - Coin transactions (Bitcoin) → crypto currencies and tokens
  - Important content → open public record house
  - Computer code and execution → contract executing computer

- Decentralization: Getting rid of middleman → But we all need to contribute!

- Incentivisation with cryptocurrencies
  - People often get greedy and aim to take over the power!

Anybody who downloads and runs the Blockchain.core can become a member of

a blockchain internet



Reality (1)

- Middleman → computer network → Owners of computer networks
- Re-centralized: a few mining sites dominate!
- Scalability Trilemma: if aiming to increase TSP, you shall give up either security or decentralization!
- Not even just: a few people are predominant in share of coins.
- No killer DApps as of yet, why?
- 98% of ICOs in 2018 ~ scams or at least did not deliver what's promised!
- Crypto-exchanges are full of pump&dump practices and insider trades!
- Smart contracts is one and a lawful contract is another!

Reality (2)

- White papers are not peer reviewed nor validated are the ideas!
- No more easy funding only with white papers!
- Blockchains are after all games of gathering autonomous people with a common interest who are willing to give their funds, talents, computing power and time for making the society a better place to live than before.

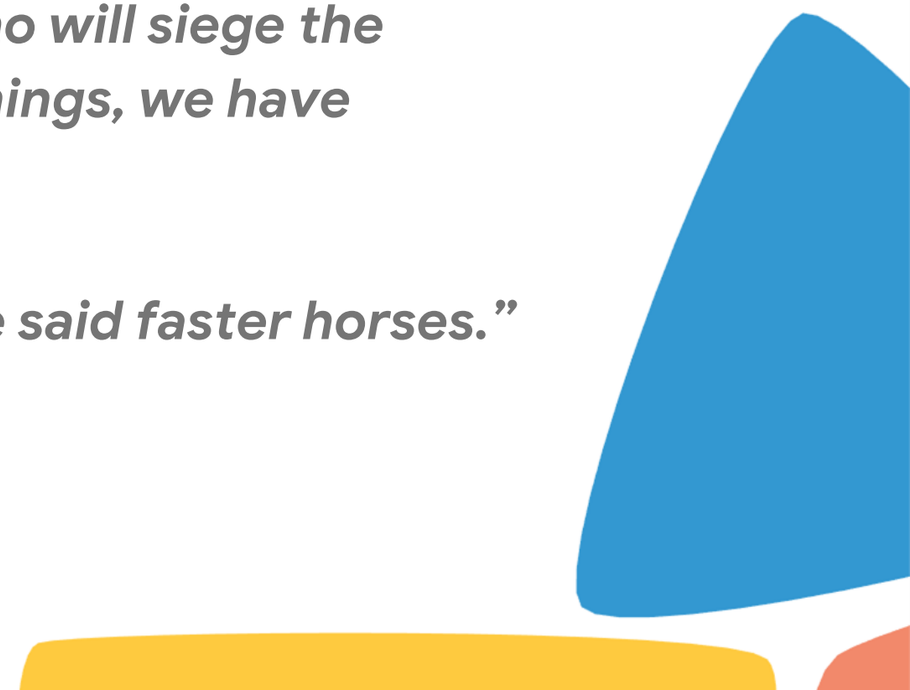
Future

Idealists, Realists, Innovators

- *Can we make the world functional with little-to-no government intervention?*
  ~ Cyberpunk philosophy

- *Bitcoin is a toy of engineers with no real use at all. Decentralization is a goal that cannot be achieved. There is always a strong man who will siege the power and wield it for his own benefit. To prevent such things, we have governments. ~ Famous Korean Politician SM Yoo*

- *“If I had asked people what they wanted, they would have said faster horses.”*
  ~Henry Ford



Facts

Bitcoin

- It is **the first working transnational digital currency**.
- **Any government cannot ban it or control it**.
- For the first time in history, **average person can mint currency**.
- Bitcoin's blockchain gives **confidence** that **double spending problem can be resolved** without a center. (**immutability of blockchain; trust without a trusted party**)
- It shows that **such confidence** can be used to build an **autonomous** global **currency system**.

Ethereum

- **Showcased the possibility of blockchain computer network which can support various applications.**
- **Made it very easy to create DApps with token minting capability.**

Investors

- There are many investors who still believe in the potentials of blockchains and cryptocurrencies.

Innovation

- *Locate problems of the current solutions.*
  - ***RE-CENTRALIZATION***
  - ***SCALABILITY TRILEMMA (Scalability, Security, Decentralization)***
- *Find a way to resolve the problem (innovation)*
- *Walk toward achieving the goal, one robust step at a time.*

Novel approaches to resolve Re-centralization and Trilemma!

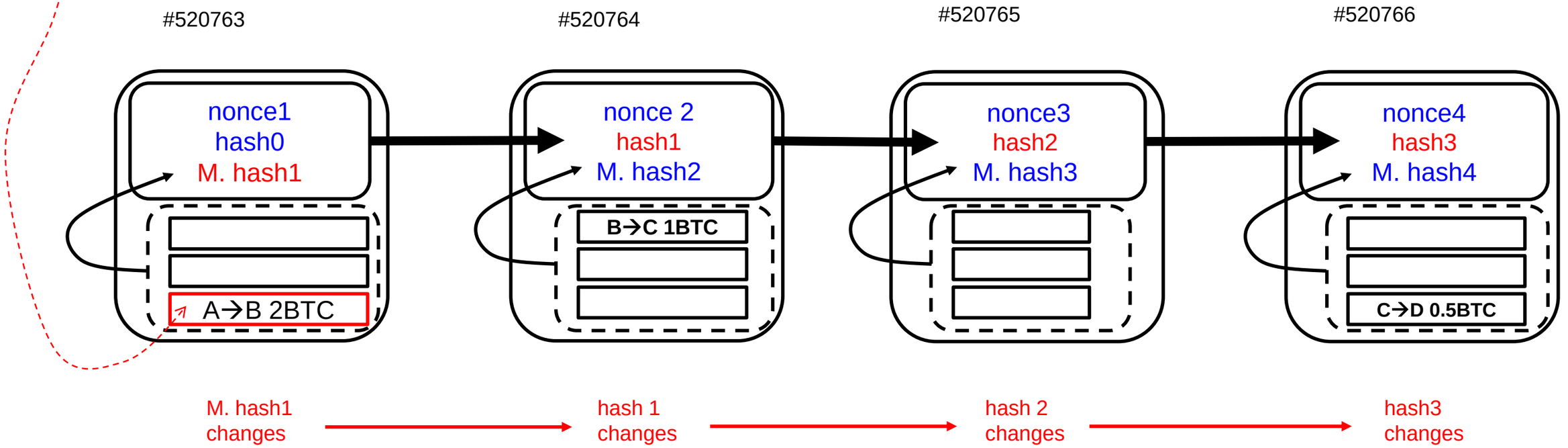
- **Error-Correction Code base Proof-of-Work**
  - This is to have the re-centralized blockchain networks decentralized again!
- **Profitable double spending (DS) attack**
  - It is well known that one needs to have at least 51% of whole network's computing power for launching a successful DS attack.
  - Our analysis shows that DS attacks are possible even under 50% computing power.

ECC PoW aims at resolving Re-centralization and Trilemma

Blockchain Immutability? Where is it from?

- What is blockchain?
  Series of blocks containing Txs and time-stamp?

- What happens when any alteration is made?
- What if there is no Proof-of-Work (PoW) attached?



Properties of Proof-of-Work (PoW)

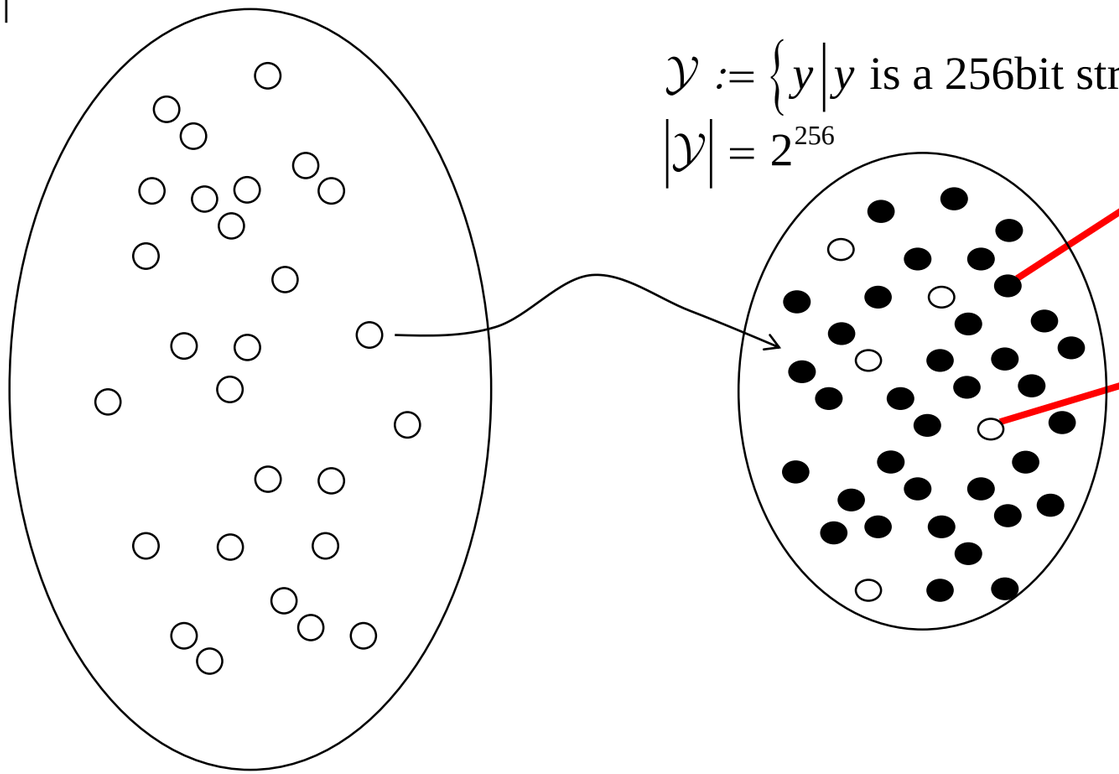
- The proof of work is used to keep the ledger unalterable. It is the proof that all the computers in the network worked together to connect the pertinent block to the chain. For one to redo all the work done, one shall apply the same total amount of time all the computers in the network have spent to make the connection.

- Properties of proof-of-work
  P1: Easy to verify but difficult to prove
  P2: Robust to detecting block modification attacks
  P3: Controllable in changing the difficulty level
  P4: Open to anyone with a CPU

Probability, a cpu solves the PoW puzzle in a single cycle?

$$\mathcal{X} := \{x \mid x \text{ is a message up to 1 Mbyte in size}\}$$
$$|\mathcal{X}| = 2^{8,000,000}$$

$$\mathcal{Y} := \{y \mid y \text{ is a 256bit string}\}$$
$$|\mathcal{Y}| = 2^{256}$$



- An ordinary hash value (hex)
  2d711642b726b04401627ca9fbac32f5c8
  530fb1903cc4db02258717921a4881
- A hash value with the first four 0s
  0000f727854b50bb95c054b39c1fe5c9
  2e5ebcfa4bcd5dc279f56aa96a365e5a

c = the set of all hash values
$= 2^{256}$

a = the set of wanted hash values
$= 2^{(256-16)} = 2^{240}$

P1 = a/c = 2^{-16}
$= 1/2^{16} \sim 1/64000$

PoW is fundamental to data immutability of blockchain.

- How long does it take to mine a single block alone?
  For a single AntMiner machine, it would take 16 years.
  But, for a network of more than 1 million miners working together, it takes only 10 minute on the average.

- Each nonce is thus a proof that the network of 1 million miners have worked together to mold a block.

- Thus, the content is scribed into the blockchain and cannot be altered.

But the current bitcoin network is re-centralized.

- Today, mining mogules investing heavily on state-of-the art ASIC miners appear.
- The bitcoin network is left with only handful of these mogules.
- This shows the current bitcoin network is centralized, leading to that the immuntability of the blockchain lies at the hand of a few people.
- Public trust established and granted to blockchain has eroded.

Proof-of-XXX, many 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	• Centralization • DDoS attacks	EOS, NEO smart economy
PoA (Proof-of-Activity)	• Much more expensive 51% attacks • Decentralization - Validators are randomly selected.	• Centralization • Extreme computing power • The rich-get-richer	decred

Current PoWs have no ASIC resistance.

- PoWs below are proposed to prevent the advent of the devices.
  1. Ethash algorithm which uses directed acyclic graphs (DAG).
  2. Both X1n and Scripts use multiple SHA functions.

- They were effective in the past, but failed to prevent ASIC devices. This failure is due to no enough variations on crypto puzzles.

Needs new time-variant PoWs

- ASICs are useful when crypto puzzles are not changeable.
- To make ASICs improvable solutions, our approach is to make crypto puzzles time-variant!.
- We call our solution ECCPoW because it is a result of applying Error Correction Coding (ECC) to PoW puzzle making problems.

Add time-variant property to PoW properties!

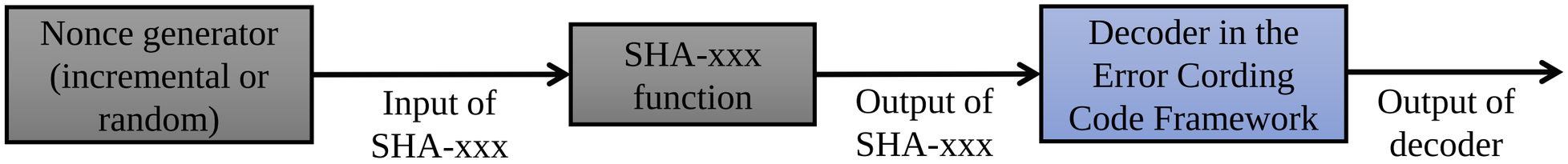
- A new puzzle generation system is capable of varying puzzles from block to block with the following properties:

  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.

Proposed Error Correction Codes PoW (ECCPoW)

- There are many one-way functions in Inverse Problems such as Error Correction Codes, Sparse-Signal Recovery, Space-Time Coding, Sphere-Decoding, Digital Communications Receiver algorithms.
- In these problems, encoding is easy but decoding is time-consuming!
- We combine a Error Correcting Code framework with SHA-xxx.



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

The Proposed Invention

- There are many inverse problems which can be used in cryptocurrency mining problems.
- In the context of **Error Correction Coding**, there is an encoder-decoder pair separated by a channel.
  Encoding is easily made with relatively little computation.
  Decoding is typically time-consuming with more computation.
- There are various ways to control the difficulty level.
- For example, the difficulty level of decoding can be varied by the size of the block code, the rate of the code, and the constraints on the decoded output.

Block Code

- A block code C(N, Rate, **G**, **F**, ENC, DEC, GF(q)) is well defined as a collection of codewords. When, q = 2, it is a binary system.
- N is the dimension of the code (e.g. N = 512)
- Rate = (N – M)/N is the rate of the code, where M < N.
- For example, with N = 1024 and M = 256, Rate = 3/4.

- **G** is the Generator matrix with dimension $N \times (N - M)$.
- **F** is the Check matrix with dimension, $M \times N$.
- **G** and F are orthogonal to each other, i.e., **FG** = **0**.

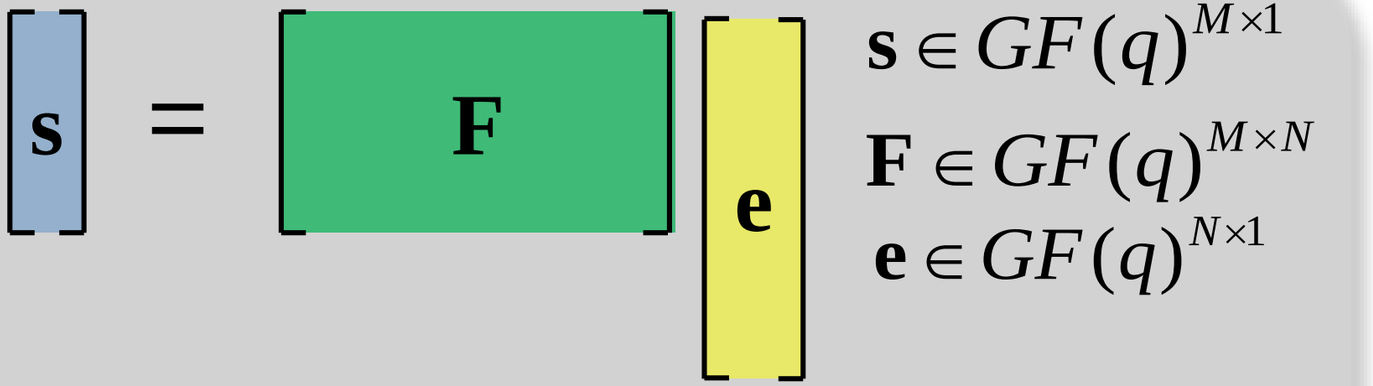
- A message vector m is an (N – M) × 1 vector.
- A codeword **c**, an N x 1 vector, is an element of the code and can be generated by multiplying a message vector m to the Generator matrix **G**, i.e., **c** = **Gm**.

- Galois Field of size q, GF(q), is used for addition and multiplication operations and storage of numbers in the system.

Block code, Encoder and Decoder

- ENC implies the encoder function, i.e., ENC takes the message vector **m** as the input and produces a codeword vector corresponding to it, e.g. **c** = ENC(**G**, **m**).

- DEC implies the decoding function; DEC takes an arbitrary vector e and returns a closest codeword $\hat{\mathbf{c}}$, i.e., $\hat{\mathbf{c}}$ = DEC(**F**, **e**).



$$\mathbf{s} \in GF(q)^{M\times 1}$$

$$\mathbf{F} \in GF(q)^{M\times N}$$

$$\mathbf{e} \in GF(q)^{N\times 1}$$

$$M < N$$

$$\text{Encoder : Given } \mathbf{e},\ \text{find } \mathbf{s} = Enc(\mathbf{e}, \mathbf{G})$$

$$\text{Decoder : Given } \mathbf{s},\ \text{find } \hat{\mathbf{c}} = Dec(\mathbf{s}, \mathbf{F})$$

Decoder

- DEC is to find a codeword $\hat{\mathbf{c}}$ most close to the input word **e**.
- For the concept of distance, the Hamming distance can be used.
  For example, $DH(\mathbf{e}, \hat{\mathbf{c}}) = \|\mathbf{e} - \hat{\mathbf{c}}\|_0$ is the number of non-zero values in the $(\mathbf{e} - \hat{\mathbf{c}})$ vector.

- There are many ways to find $\hat{\mathbf{c}}$ satisfying $\mathbf{F}\hat{\mathbf{c}} = \mathbf{0}$.

- We propose to use the message passing graph decoder for its excellency in accuracy and superiority in decoding speed.
  This is to prevent a cheating attack in which a smart miner comes up with a new decoder algorithm of his own developed and aims to outpace regular miners using the designated decoder. If this is allowed, a hidden advantage goes to the smart miner.

Geometrical Explanation

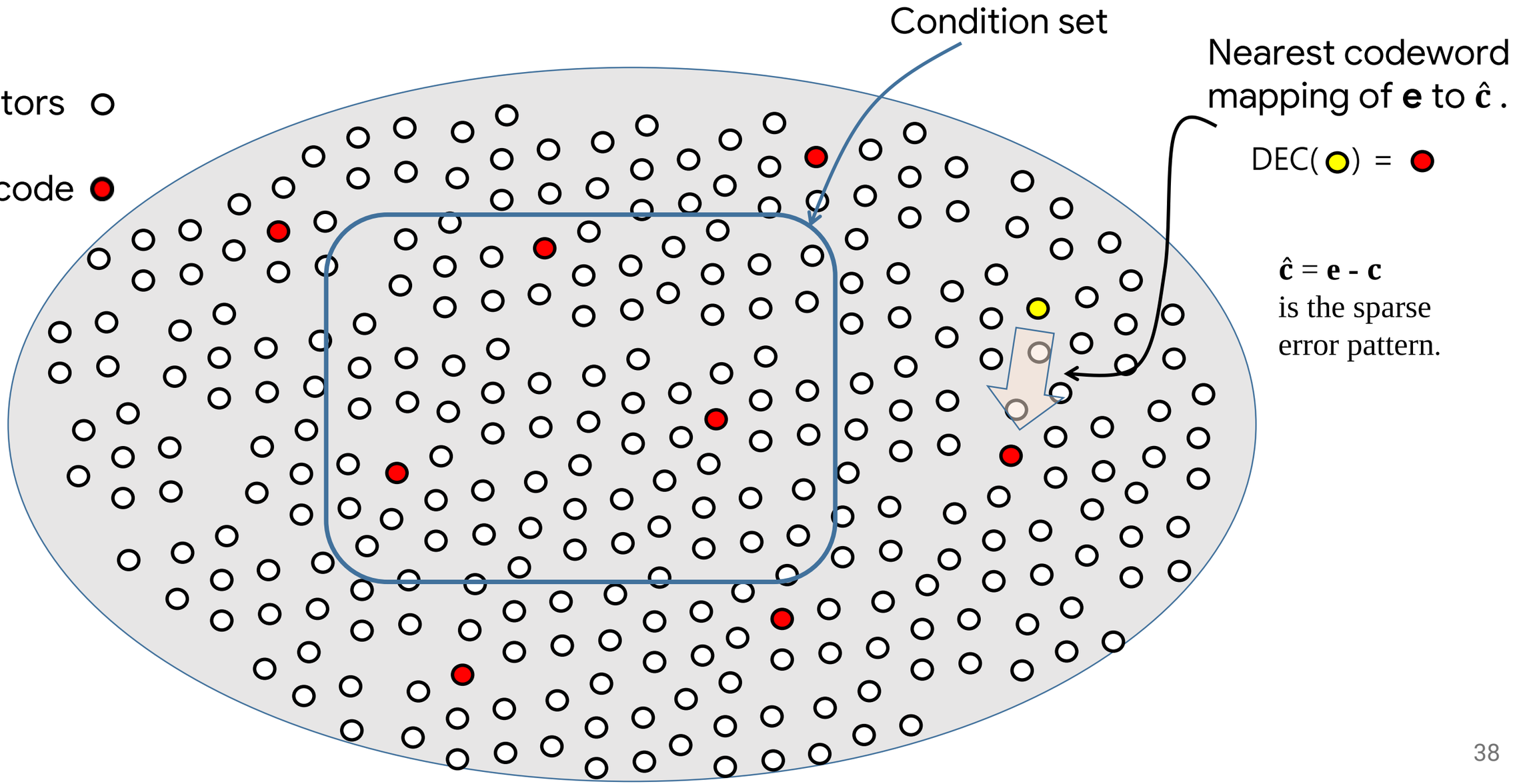
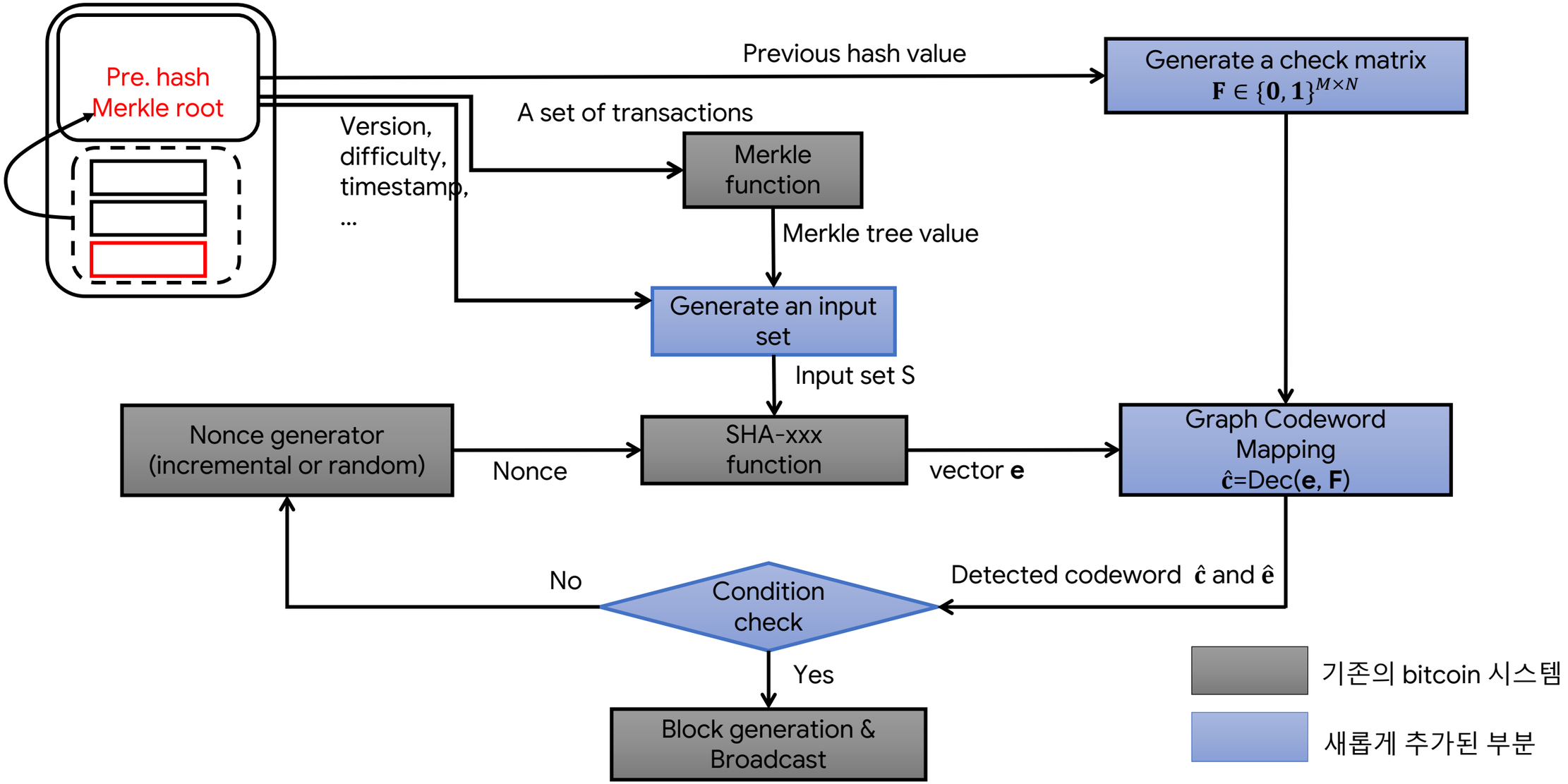
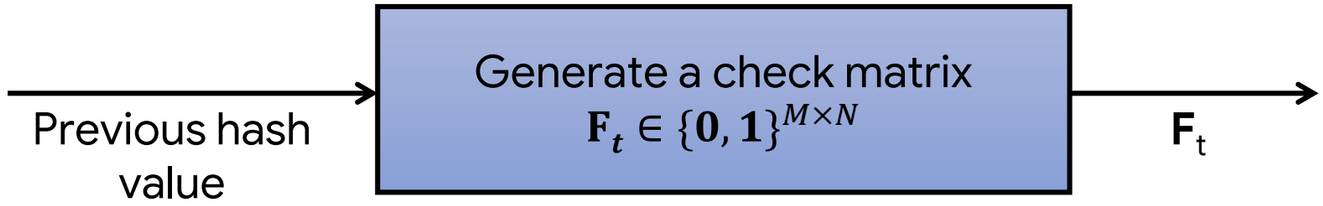


Diagram of ECCPoW



Generate a Check Matrix

- Parameter set S_t = {h_t-1, *code parameters*};
- GenCheckMatrix(S_t) = $\mathbf{F}_t$
- Generate a check matrix $\mathbf{F}_t$ w.r.t. previous hash h_t-1.
- Takes the previous hash h_t-1 as the input to this routine.
- That is, $\mathbf{F}_t$ changes from block to block.



New Functions in ECCPoW

- New functions
  1. int **H = GenCheckMatrix(int n, int w_c, int w_r, int seed);
  2. bool DEC(int **H, int *e, int n, int w_c, int w_r, int *c);
  3. void Dec_Difficulty(int &n, int &wc, int &wr, int level);

- These functions are the key parts of the proposed solution.
  1. They are implemented in C++.
  2. They are used to implement a mining routine

- An example of mining

1. generate block header with zero nonce.
2. Dec_Difficulty(&n,&wc,&wr,difficulty)
3. Seed = f(phv)
4. H = GenCheckMatrix(n, wc, wr, seed)
5. nonce = nonce + 1
6. e = SHA256(version, time, difficulty, nonce, mtv)
7. flag = DEC(H,e,n,wc,wr)
8. If flag == 0; go to step 4
9. Update chv and nonce.
10. Generate block and broadcast.

ECCPoW Hardfork

- New ECCPoW

  A new structure of the block header has been introduced and,

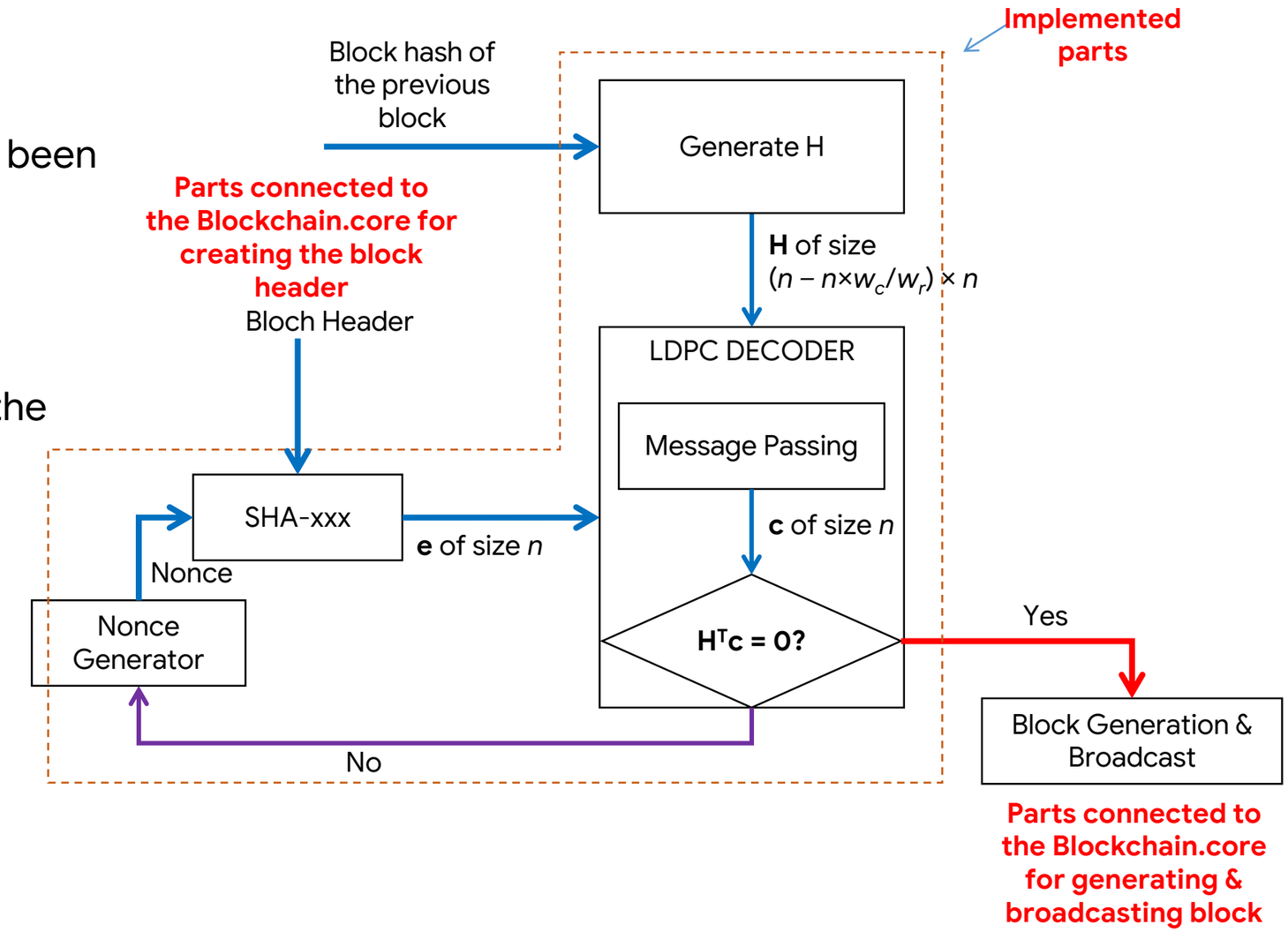
  three new functions are also have been introduced.

- We aim to link these functions to existing the blockchain. For example,

  mining function,

  chain validation function,

  consensus function and so on.



Impact of ECCPoW 1:
It is easier to start a new blockchain network.

- A large blockchain network is stable and not easy to disrupt.

- Today there are mining equipment renting sites.
- A new borne blockchain network needs to grow, but newbies are 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.

Impact of ECCPoW 2:
One can make multiple blockchain networks.

- It is easy to make a new blockchain with ECCPoW.

- Suppose hardforking a Bitcoin and an Ethereum with ECCPoW.
- Let us call them BitECC and EhterECC protocols.

- Make the first blockchain network by running EtherECC over a network (Pusan coin).
- Make the second blockchain network by running BitECC over other network (Gwangju coin).
- Make the third blockchain network by running EtherECC over another network (Seoul coin).
- Make the fourth blockchain network by running BitECC over yet another network (Korea coin).

- Each cryptocurrency is independent with its own genesis block and random starting seed;
- Each can be adjusted 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.

Impact of ECCPoW 3:
Resolving the Scalability Trilemma.

- Trilemma by V. Buterin is well known: Only up to **two out of the three** virtues such as Scalability, Decentralization and Security **can be achieved simultaneously**.

- With ECC, each blockchain is already very strong in decentralization.
- Each EEC blockchain is flexible enough to provide various settings of transaction speeds and security levels.
  - Campus ECC blockchain networks can be set to work very fast allowing up to 100s of thousands of TXs per second since the delay of the underlying communications network is very small.
  - Regional ECC blockchain networks can be set to work fast, i.e. allowing up to 10s of thousands of TXs per sec.
  - National ECC blockchain networks can be set sufficiently fast for covering inter-regional transactions.
  - Transnational ECC blockchain networks shall be set to work slow due to large delays.

- Each of these blockchains started up with its own seed and decentralized level is mutually independent and each one can be set to work at the required level of security and speed to serve its purpose.
- All these ECC blockchains can be inter-connected via *distributed value-exchange* networks.
- The connected ECC blockchains can be named the ECC Blockchain International.
- *ECC Blockchain International* as a whole can resolve the Scalability Trilemma.

Impact of ECCPoW 4:
It is safe to use a time-proven blockchain protocol.

- Bitcoin protocol has withstood the tough test of time.
- Thus, the networking part and the wallet part are robust enough.

- PoW is problem. Yes.
- But it is not the problem of PoW.
- It is the **fixedness** of the PoW puzzle.

- ECCPoW puzzles can be made to vary over time, from block to block.

- The problematic consensus with a fixed PoW can be replaced with a new consensus enabled by ECC PoW.

Impact of ECCPoW 5:
The complexity of ECCPoW puzzles can be set to grow very large; thus the cost for hardware acceleration is boundless.

- ECCPoW is a computer algorithm!
- Thus it is not impossible to find a hardware acceleration solution for it.

- ECCPoW puzzle can be represented as a randomly connected bipartite graph.
- In order to parallelize the algorithm, more memory and computation resource need to be allocated.
- The size of ECCPoW puzzle can grow very large.
- As the size of the puzzle grows, the more needed is the memory and computation resource.
- With ECCPoW puzzles, therefore, one can easily deter the emergence of hardware acceleration solution.

- Deterrence to hardware acceleration offers a blockchain network with small power consumption requirement.

Development Schedule

- Open research platform
  - Source codes github uploaded
  - Open development
- 2019 plan
  - ECCPoW 0.5 Version
  - Ethereum and Bitcoin Hardforks with ECCPoW 0.5v
  - Develop them into Ethereum ECCPoW 1.0v and Bitcoin ECCPow 1.0v
- 2020 plan
  - Network growth at least by 10,000 nodes worldwide
  - Co-working with Bitcoin and Ethereum communities

Cryptocurrency Regulations Worldwide and Perspective to Korean Regulations

Current Cryptocurrency Regulation of Major Countries

- The central government and tax department classify cryptocurrencies as a financial asset making sure it is subject to taxation.

By	Countries	Regulations
Central Bank	Belarus	(2018) National Bank of the Republic of Belarus (NBRB) proposed rigorous requirements for investors to participate in the ICO.
	Iran	(2018) Central Bank of Iran (CBI) prohibits the handling of cryptocurrencies by all financial institutions including banks and lenders.
	Israel	(2018) Bank of Israel treat cryptocurrencies as a financial asset.

Current Cryptocurrency Regulation of Major Countries

By	Countries	Regulations
Tax Department	Argentina	(2017) Treat profits from the sale of cryptocurrency as income from stocks/ bonds and impose tax on.
	Iceland	(2017) The National Tax Service issued an income tax reporting guideline which classifies cryptocurrencies as other assets..
	Belarus	(2018) Enacted an ordinance to legalize cryptocurrency, ICO, and smart contracts and exempt related taxes for five years.
	Brazil	(2018) Published a tax draft about cryptocurrency. It is mandatory that exchanges should submit a monthly report and the individual/ institutional investors declare if they trade more than a certain amount on a foreign cryptocurrency exchange.
	China	(2018) Cyberspace Administration of China (CAC) announced policy draft for blockchain information service management.
	Israel	(2018) The tax authority treated the use of cryptocurrencies as a method of virtual payment and subject to taxation.
	Japan	(2018) Confirmed that cryptocurrency is subject to property reporting.

Current Cryptocurrency Regulation of Major Countries

- Countries regulate the definition of the cryptocurrency, ICO guidelines, and income tax for the cryptocurrency transaction through legislation

By	Countries	Regulation
Department of Justice	Canada	(2014) Stated that cryptocurrencies are subject to anti-money laundering and anti-terrorism-financing laws. (2018) The House Finance Committee defines all processes of purchasing cryptocurrency with legal currency as a currency service business.
	France	(2018) allowed the ICO and suggested guidelines .
Legislature	Australia	(2017) The Senate committee implements the obligation to register a cryptocurrency operator and to report suspicious transactions.
	France	(2018) The National Assembly passed an amendment to reduce cryptocurrency transfer income tax from 36% to 30%.

Current Cryptocurrency Regulation of Major Countries

- Regulations on the Cryptocurrency of the Financial Committee by County

Countries	Regulation
Argentina	(2014) Businesses running on virtual currency need to report on suspicious transactions, including money laundering or terrorist financing.
United States of America	(2017) The Securities and Exchange Commission (SEC) has issued guidelines to provide guidance on ICO, blockchain technology, ICO investment appraisal, and rights. (2018) The SEC announced that it would strengthen the application of securities laws to ICOs.
Switzerland	(2018) Swiss Financial Market Supervisory Authority (FINMA) announces cryptocurrency ICO guidelines.
Australia	(2018) The Australian Transaction Reports and Analysis Centre (AUSTRAC) has enacted legislation to prevent money laundering and funding of terrorist organizations for Australian cryptocurrency exchanges.
Canada	(2018) The Canadian Standards Association (CSA) provided requirements for securities laws application to cryptocurrency disclosure (ICO), token disclosure (ITO), cryptocurrency investment funds, and exchanges.

Current Cryptocurrency Regulation of Major Countries

Countries	Regulation
Gibraltar	(2018) The Gibraltar Financial Services Commission (GFSC) and the government established regulations for token promotion, sales and distribution of individuals/ organizations and announced token regulatory guidelines.
Israel	(2018) The Israel Securities Authority (ISA) introduced blockchain for cyber security of the message system.
Japan	(2018) Japan's Financial Services Agency (FSA) has announced that the Japan Virtual Currency Exchange Association (JVCEA) will serve as a self-regulating body for cryptocurrency.
Jersey	(2018) The Jersey Financial Services Commission (JFSC) announced ICO Investment Protection Guidelines.
Switzerland	(2018) The Capital Markets and Technology Association (CMTA) announced anti-money laundering standards applicable to cryptocurrency.

Current Cryptocurrency Regulation of South Korea

- The Korean government announced a complete ban on the ICOs using cryptocurrencies.
- Since then, the government has been watching the market for cryptocurrency without taking any concrete follow up action for legalization.

By	Regulations
Government – Complete ban on all ICO activities (2017.9.29.)	- Announced the prohibition of all ICO activities including securities issuance. - Announced the prohibition of credit offering including money lending and coin margin transaction and the complete ban on related sales and alliances with financial companies. - Announced the goal of establishing a joint inspection system for customer information leakage investigation and virtual currency handling business.
Blockchain Association – Self-regulating guidelines for cryptocurrency exchange (2018.1)	- Established the standards for creating sound cryptocurrency exchanges. - Prevention of money laundering activities (personal identification process, 5-year retention of transaction records, etc.), introduction of abnormal transaction detection system, protection of users in cryptocurrency listing (disclosure of information necessary for user protection, such as white paper, overseas transaction price), proof of financial soundness (equity capital of more than KRW 2billion, submission of corporate governance and financial data, etc.), enactment of ethics charter, made mandatory.

Current Cryptocurrency Regulation of South Korea

By	Regulations
Financial Services Commission (2018.6.27.)	- In association with cryptocurrency-related financial transaction, ① clarified matters necessary for the enforcement of the Act On Reporting And Using Specified Financial Transaction Information and its subordinate laws and ② stipulates matters requiring compliance with financial companies to ensure effective prevention of money laundering and public intimidation fundraising activities.
Court (2018.10.29.) Bank's cryptocurrency deposit suspension is an unfair judgement (2018.10.29.)	- The court ruled in favor of a cryptocurrency exchange (Coinis) in a complaint filed by the exchange with the court seeking to prohibit the bank from suspending its transactions. It was considered illegal for the bank to suspend the exchange's transactions based solely on the FSC guidelines which is not a related laws.
Blockchain Start-up Association - IEO Guidelines (2018.11.01.)	- Guidelines include ① MVP (Minimal Visible Product) ② Self-check list and ③ Initial price. - A firm can raise business fund for a cryptocurrency only if the firm has developed an MVP. For example, a working Dapp or a live mainnet realizing a proof-of-concept can serve as an MVP.
Korea Blockchain Association (2018.11.16.)	(Blockchain Analysis and Evaluation Guideline 2.0) The items for blockchain analysis and evaluation were derived from four areas: token structure evaluation, BM evaluation, organizational evaluation, and technology evaluation.

Concluding Remarks

- ECCPoW blockchains can play a crucial role in ushering in the ideals of blockchains and advance our society to the next level!

- Global collaboration is needed advancing the new technology, fostering continued innovation and forming a transnational community. It can move us to go beyond national boundaries and bring us to come closer to a desired future.

References

- [Fed-1] Ben Bernanke, College Lecture Series, The Fed and financial crisis, https://www.federalreserve.gov/aboutthefed/educational-tools/lecture-series-the-aftermath-of-the-crisis.htm.
- [ECC] Error correctin code in Wikipedia, https://en.wikipedia.org/wiki/Error_detection_and_correction.
- [LDPC codes] Robert Gallager, 1963 Thesis on LDPC codes, https://web.stanford.edu/class/ee388/papers/ldpc.pdf.
- [Bitcoin] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf.
- [Lee19-1] J. Jang and Heung-No Lee, "Profitable Double-Spending Attacks, Submitted to IEEE Trans. on Communications.
- [Lee19-2] S.J. Park, H.U. Choi and Heung-No Lee, "Channel-Code Consensus," Preparation for submission to IEEE Trans. on Communications. Korean Patent No: P181403KR01, Date: 2018. 7. 18. Claim of Priority to US, Application No. 62/669751.
- [Lee19-3] H.J. Jung and Heung-No Lee, "Cryptocurrency Investment and Regulations," Communications of the Korean Institute of Information Scientists and Engineers, Vol. 36, No. 12, pp. 48~56.

- **Thank you!**
- **Q&A**
- **We are looking for people to join us.**