Information Security

#10: 블록체인에 대한 이론적 모델(simple version)

Howon Kim

2022.4

- 정보보호 및 사물지능(AIoT) 연구실 http://infosec.pusan.ac.kr
- 블록체인 플랫폼 연구센터 http://itrc.pusan.ac.kr
- 지능형 융합보안대학원 http://aisec.pusan.ac.kr

정보보호 및 사물지능 연구실
Information Security & AIoT (AI of Things)

블록체인 플랫폼 연구센터
BLOCKCHAIN PLATFORM RESEARCH CENTER

부산대학교 융합보안대학원
PNU GRADUATE SCHOOL OF CONVERGENCE SECURITY

Agenda

I. 블록체인의 이론적 모델

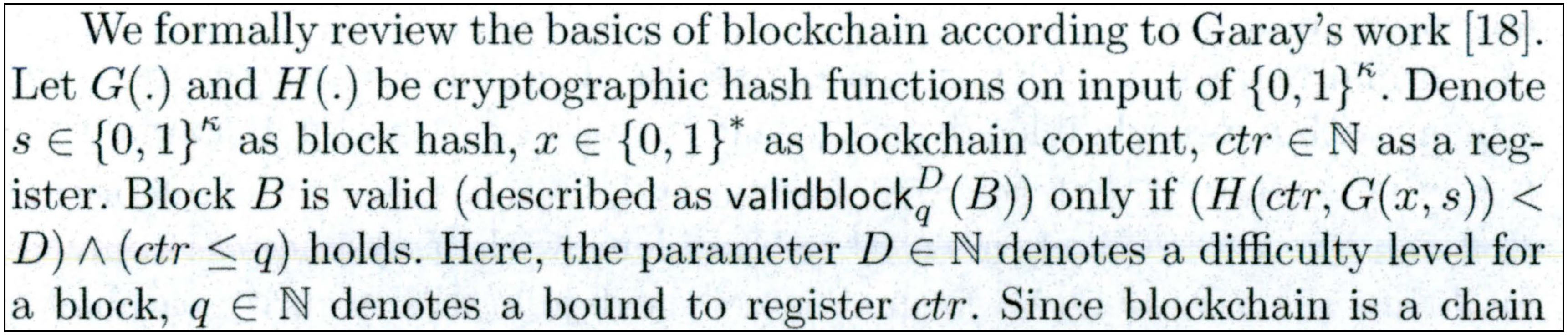
1. Defining Blockchain Model

참고문헌:

- (1) The Bitcoin Backbone Protocol: Analysis and Applications by Juan A. Garay, et.al.
- (2) Design and Analysis of Cryptographic Algorithms in Blockchain by Ke Huang, et.al

1. Defining Blockchain model

- Theoretical model of Blockchain (Garay's paper or CH2 at Ke Huang's book)

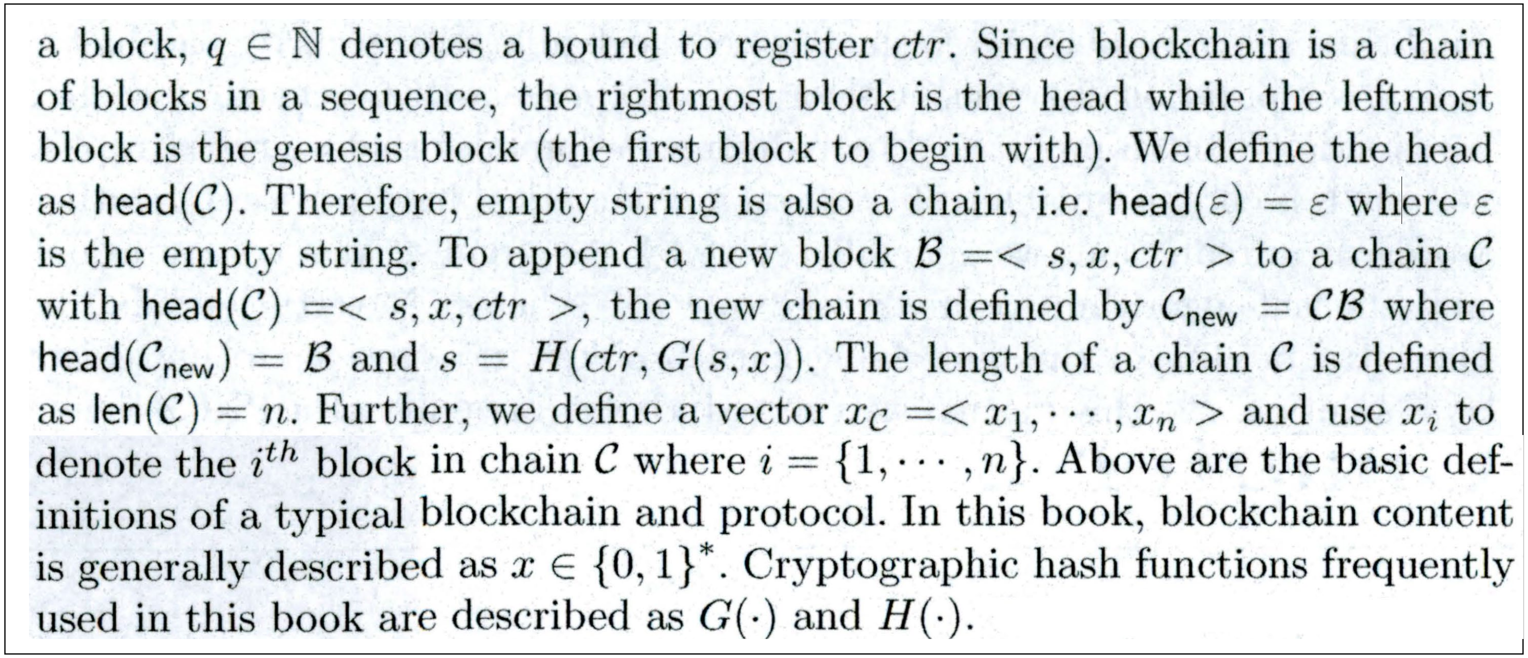


We formally review the basics of blockchain according to Garay's work [18]. Let $G(.)$ and $H(.)$ be cryptographic hash functions on input of $\{0,1\}^{\kappa}$. Denote $s \in \{0,1\}^{\kappa}$ as block hash, $x \in \{0,1\}^{*}$ as blockchain content, $ctr \in \mathbb{N}$ as a register. Block B is valid (described as $\mathsf{validblock}_q^D(B)$) only if $(H(ctr, G(x,s)) < D) \wedge (ctr \leq q)$ holds. Here, the parameter $D \in \mathbb{N}$ denotes a difficulty level for a block, $q \in \mathbb{N}$ denotes a bound to register ctr. Since blockchain is a chain

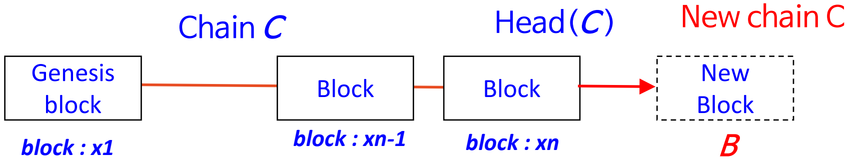
- G(.), H(.): k bit 입력 데이터를 갖는 hash 함수 (k bit?)
- x : 블록 contents, xi: i번째 블록
- s : 블록 해시값 (k bit)
- ctr : counter 값(블록체인의 nonce 값)
- Block의 유효성은 difficulty level보다 낮아야 만족됨(→ 해시값 특성)

1. Defining Blockchain model

- Theoretical model of Blockchain (Garay's paper or CH2 at Ke Huang's book)



a block, $q \in \mathbb{N}$ denotes a bound to register ctr. Since blockchain is a chain of blocks in a sequence, the rightmost block is the head while the leftmost block is the genesis block (the first block to begin with). We define the head as $\mathsf{head}(\mathcal{C})$. Therefore, empty string is also a chain, i.e. $\mathsf{head}(\varepsilon) = \varepsilon$ where ε is the empty string. To append a new block $\mathcal{B} =< s, x, ctr >$ to a chain $\mathcal{C}$ with $\mathsf{head}(\mathcal{C}) =< s, x, ctr >$, the new chain is defined by $\mathcal{C}_{\mathsf{new}} = \mathcal{C}\mathcal{B}$ where $\mathsf{head}(\mathcal{C}_{\mathsf{new}}) = \mathcal{B}$ and $s = H(ctr, G(s, x))$. The length of a chain $\mathcal{C}$ is defined as $\mathsf{len}(\mathcal{C}) = n$. Further, we define a vector $x_{\mathcal{C}} =< x_1, \cdots, x_n >$ and use x_i to denote the i^{th} block in chain $\mathcal{C}$ where $i = \{1, \cdots, n\}$. Above are the basic definitions of a typical blockchain and protocol. In this book, blockchain content is generally described as $x \in \{0, 1\}^*$. Cryptographic hash functions frequently used in this book are described as $G(\cdot)$ and $H(\cdot)$.

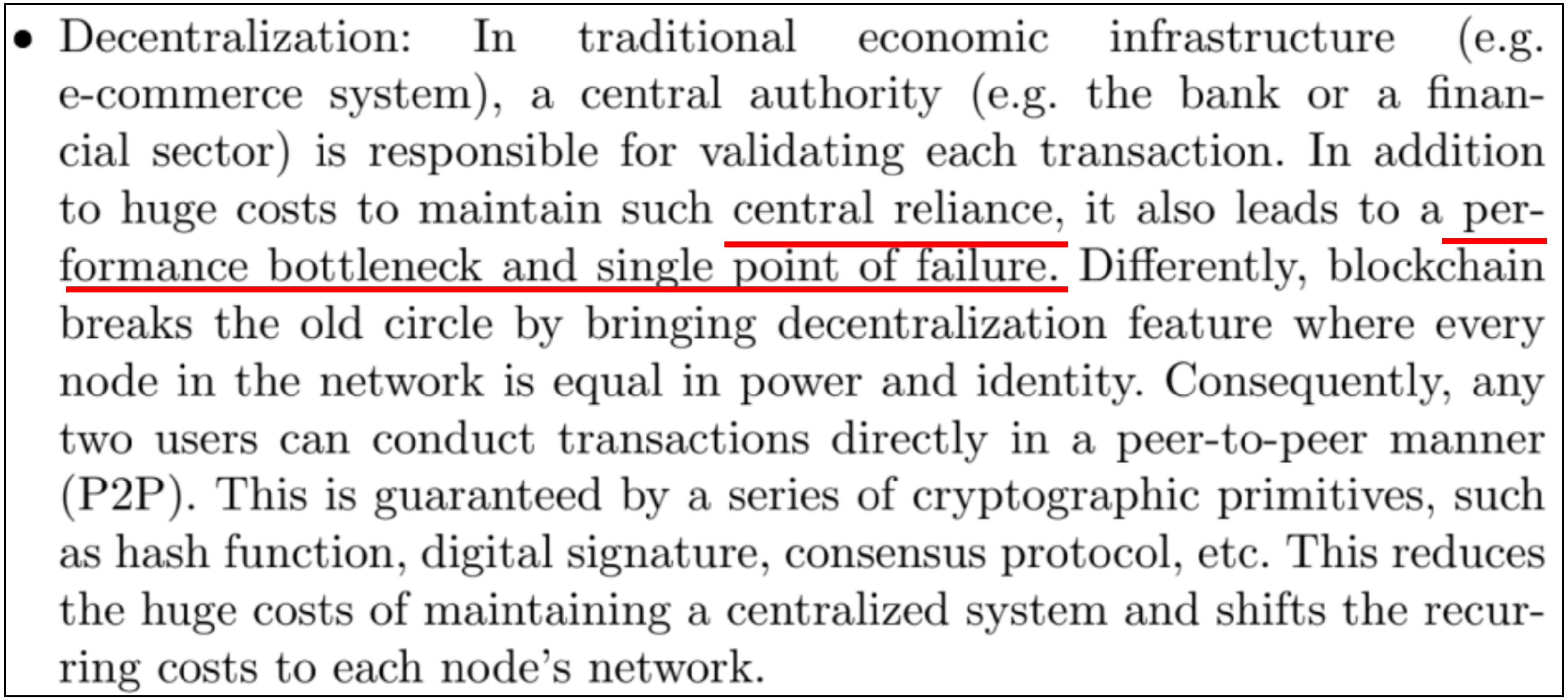


참고: x는 임의 길이를 갖는 블록 contents

(주의: xn은 n번째 block임. notation을 약간 헷갈리게 사용하고 있음)

2. Blockchain Introduction

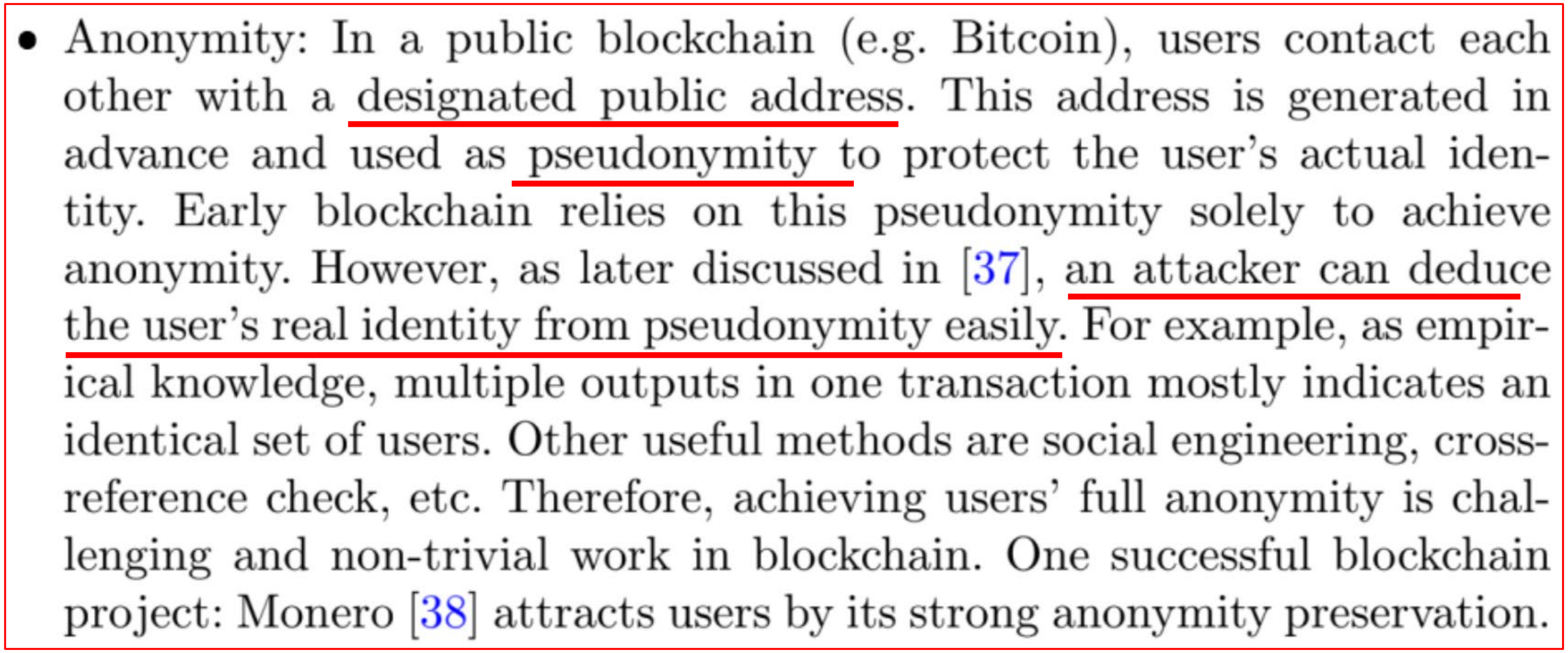
- Main characteristics of Blockchain – Decentralization(탈중앙화)



- Decentralization: In traditional economic infrastructure (e.g. e-commerce system), a central authority (e.g. the bank or a financial sector) is responsible for validating each transaction. In addition to huge costs to maintain such central reliance, it also leads to a performance bottleneck and single point of failure. Differently, blockchain breaks the old circle by bringing decentralization feature where every node in the network is equal in power and identity. Consequently, any two users can conduct transactions directly in a peer-to-peer manner (P2P). This is guaranteed by a series of cryptographic primitives, such as hash function, digital signature, consensus protocol, etc. This reduces the huge costs of maintaining a centralized system and shifts the recurring costs to each node's network.

2. Blockchain Introduction

- Main characteristics of Blockchain – Anonymity (익명성)

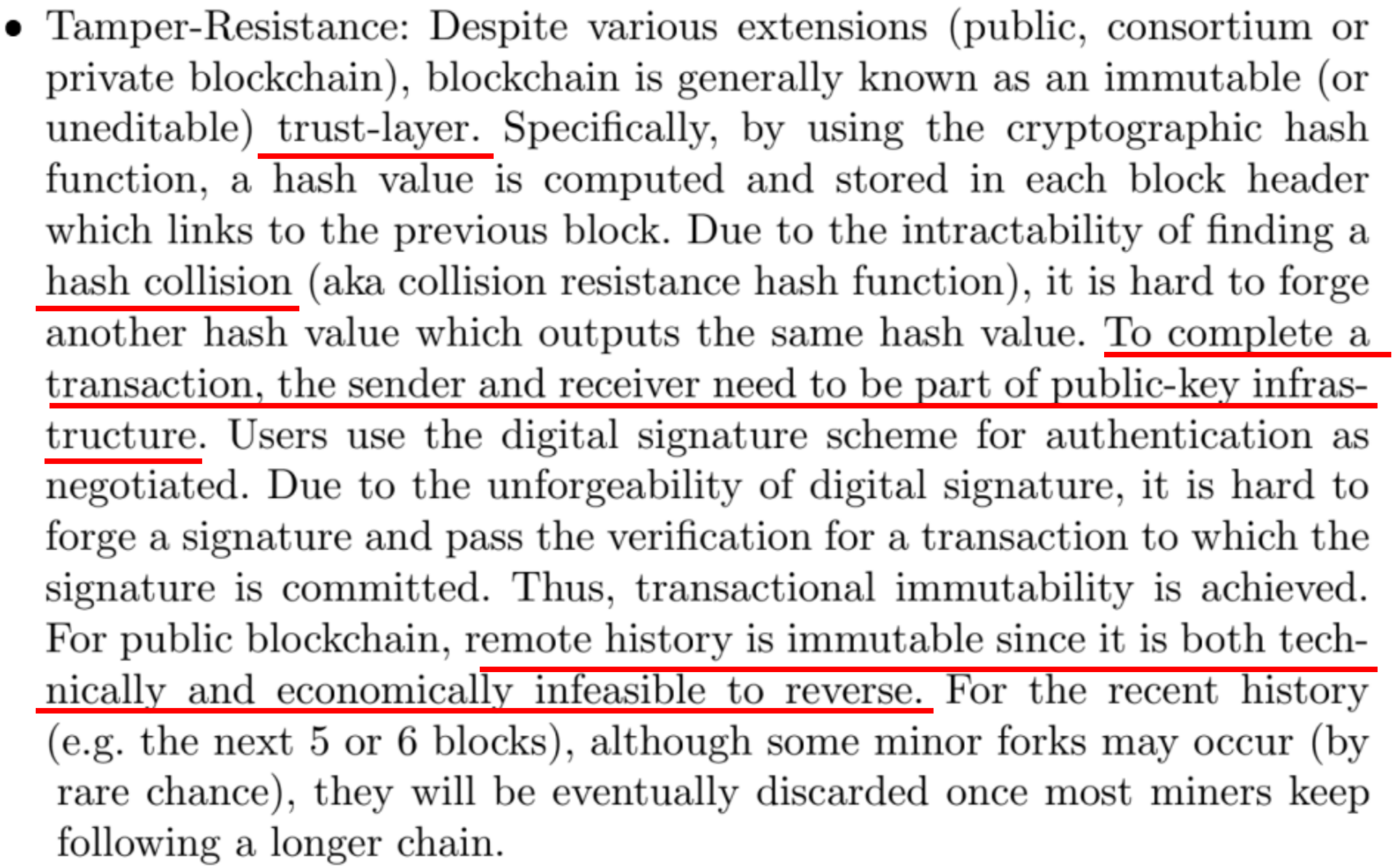


- Anonymity: In a public blockchain (e.g. Bitcoin), users contact each other with a designated public address. This address is generated in advance and used as pseudonymity to protect the user's actual identity. Early blockchain relies on this pseudonymity solely to achieve anonymity. However, as later discussed in [37], an attacker can deduce the user's real identity from pseudonymity easily. For example, as empirical knowledge, multiple outputs in one transaction mostly indicates an identical set of users. Other useful methods are social engineering, cross-reference check, etc. Therefore, achieving users' full anonymity is challenging and non-trivial work in blockchain. One successful blockchain project: Monero [38] attracts users by its strong anonymity preservation.

- **하지만 !!** Pseudonymity도 추적 가능함
- 더욱이, 최근에는 금융권의 KYC와 Travel Rule 때문에 더더욱 신원 익명성 보장은 어려워지고 있음 (기존 CEX에서는..)
- CEX : Centralized Exchange (참고: DEX: Decentralized Exchange)

2. Blockchain Introduction

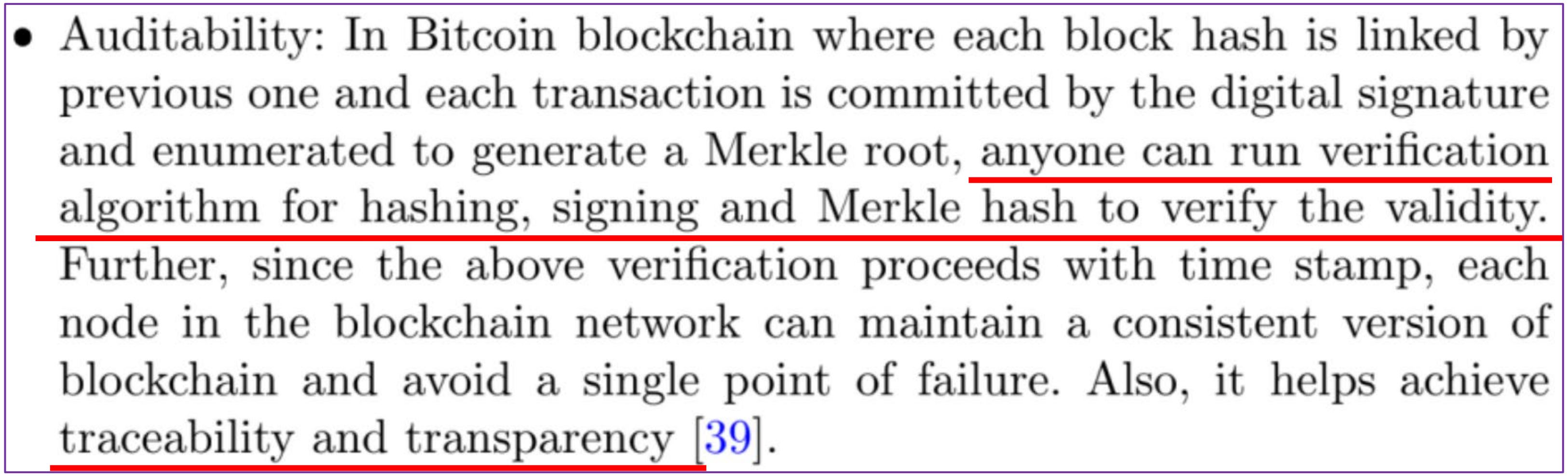
Main characteristics of Blockchain – Tamper Reisistance (탬퍼 저항성)



- Tamper-Resistance: Despite various extensions (public, consortium or private blockchain), blockchain is generally known as an immutable (or uneditable) trust-layer. Specifically, by using the cryptographic hash function, a hash value is computed and stored in each block header which links to the previous block. Due to the intractability of finding a hash collision (aka collision resistance hash function), it is hard to forge another hash value which outputs the same hash value. To complete a transaction, the sender and receiver need to be part of public-key infrastructure. Users use the digital signature scheme for authentication as negotiated. Due to the unforgeability of digital signature, it is hard to forge a signature and pass the verification for a transaction to which the signature is committed. Thus, transactional immutability is achieved. For public blockchain, remote history is immutable since it is both technically and economically infeasible to reverse. For the recent history (e.g. the next 5 or 6 blocks), although some minor forks may occur (by rare chance), they will be eventually discarded once most miners keep following a longer chain.

2. Blockchain Introduction

- Main characteristics of Blockchain – Auditability (감사특성)



- Auditability: In Bitcoin blockchain where each block hash is linked by previous one and each transaction is committed by the digital signature and enumerated to generate a Merkle root, anyone can run verification algorithm for hashing, signing and Merkle hash to verify the validity. Further, since the above verification proceeds with time stamp, each node in the blockchain network can maintain a consistent version of blockchain and avoid a single point of failure. Also, it helps achieve traceability and transparency [39].

Q&A