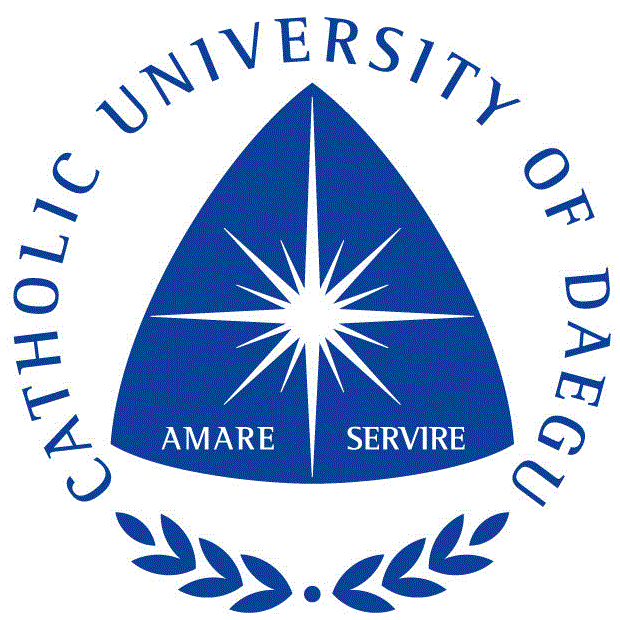
SUMMARY

대구가톨릭대학교 18학번 김성학



|  |  |
| --- | --- |
| **학과** | 컴퓨터공학전공 |
| **학번** | 18113699 |
| **이름** | 김성학 |
| **담당 교수** | 김기성 교수님 |

블록체인의 본질이 무엇인지, 실제로 가치가 있는지에 대한 가치 판달을 할 수 있게 하는 목적으로 작성하였음.

※ 본 내용은 개인적으로 공부하며 정리하는 내용이라 틀릴 수 있습니다.

**블록체인 개념 정리 v0.1**

**대구가톨릭대학교 18학번 김성학**

블록체인 기본 매커니즘에 관한 부가 설명

1. 개별 거래(Transaction)는 암호화(Cryptography) 매커니즘으로 거래 상대방을 확인

예를 들어서 A가 B에게 10코인만큼을 줬다는 경우,

B입장) 실제 A가 맞는지, 다른사람이 A인 척 하는것이 아닌지, 코인을 준 척 그에 상응하는 현금을 주라는 것이 아닌지에 대해 확인하는 방식 (공개키 / 비밀키)

2. 장부(Ledger)는 소유주 변동 상황을 기록

3. 일정한 주기로 일정 수(가령, 2400건)의 새로운 거래를 포함한 새로운 장부를 작성

4. 누구나 새로운 장부를 작성하고, 발표(Publish)

※ 누구나 장부 작성 시, 가짜 장부 발생 40코인 -> 400코인

5. 새로운 장부로부터 제일 먼저 SHA256 코드를 발굴한 사람(Miner)이 일정수의 코인을 획득

6. 장부 그 자체가 코인

public key 누구나 알려주는 키 : **pk**

private(secret) key 숨기는 키 : **sk**

A give 10 to B : Message

시행 과정

1. 상대방이 진짜 자신이 주장하는 사람인가? Identity

2. 정말 그러한 자산을 가지고 있는가? Ownership

A(송신자)일 경우,

**Sign(Message, sk) {**

**...**

**return Signature, Encrypted Message }**

==> 위의 메시지랑 비밀키를 이용하여 리턴값을 구한다.

리턴되는 값: 전자서명과 암호화된 메시지

-> Signature, Encrypted Message 전송

B(수신자)일 경우,

**Verify(Encrypted Message, Signature, A\_pk) {**

**...**

**return Message }**

==> 암호화된 메시지, 전자서명과 A의 공개키를 이용하여 리턴값을 구한다.

리턴되는 값: 복호화된 메시지

문제점 발생 : A의 전자서명(Signature)을 복사하여 사용.

결론은 불가능.

Message가 조금만 바껴도 Signature이 달라지기 때문에 A의 전자서명을 복사해서 재사용하는 것이 불가능하다.