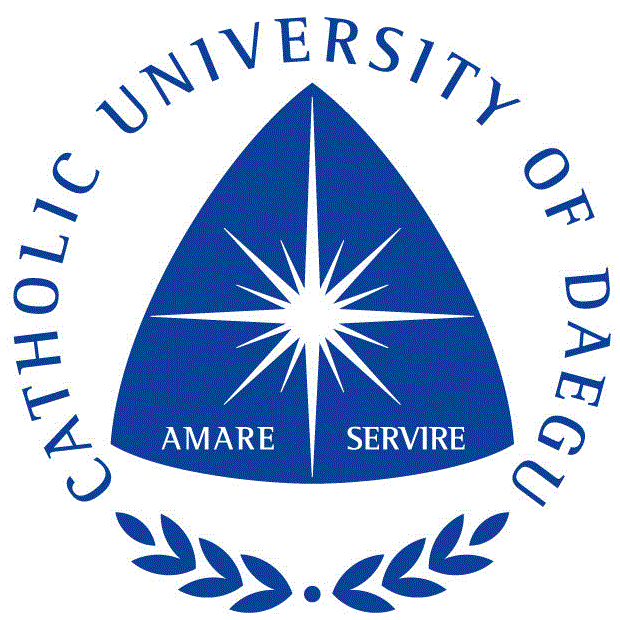
SUMMARY

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**

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.

==============================이것으로 Identity 확인==================================

**2. 정말 그러한 자산을 가지고 있는가? Ownership**

1. Computational work = Proof of work 51% 공격

2. Cryptographic hash functions 해시함수

3. Data에 어떤 숫자를 추가해서, 가령 맨 앞에 0이 30개가 포함된 SHA256을 생성.

-- Mining은 그 “어떤 숫자”를 찾는 단순 반복 작업(삽질)

**\*\* 내역을 바꾸기 위해 엄청난 노력(삽질)이 필요.**

4. 오염된(Flaud) Data에 어떤 숫자를 추가해서, 맨 앞에 0이 30개가 포함된 SHA256을 생성한다면?

-- 그리고 그 장부를 발표(Publish)한다면?

**\*\* 사기 조직의 마이닝 자원이 전세계 자원보다 51% 커야 경쟁에서 이김.**

발행 코인의 수량

1. 첫 210,000 블럭의 Miner에게 50코인씩 지급, 매 210,000블록마다 지급 코인이 1/2로 감소

210,000(50+ 25 + 12.5 + ...) = 21,000,000 블록 또는 코인

2. 처음 시작한 사람(및 그룹)이 막대한 이득 => 새로운 코인의 등장(2017년 12월 현재 1500종 이상)

3. Miner(또는 거래소)에 수수료 지급

코인을 다 발굴한 뒤로 Miner들이 없어지는가? 몰?루 찾아봐야됨.

채굴 난이도 조절 매커니즘

=====================================================================================

from hashlib import sha256 as sha

def hashcash(msg, difficulty):

nonce = 0

while True:

target = '%s%d' %(msg, nonce)

ret = sha(target.encode()).hexdigest()

*#if ret[:difficulty] == '1'\*difficulty:*

if ret[:difficulty] == '000000':

print()

print('new hash value : ' + ret)

print('--> NONCE = %d' %nonce)

break

nonce += 1

if \_\_name\_\_ == '\_\_main\_\_':

msg = 'HI SHUNGHAK'

difficulty = 6

print("msg's hash value : "+ sha((msg.encode())).hexdigest())

hashcash(msg, difficulty)

=====================================================================================

\*\* 0의 갯수가 더 많으면 난이도가 더 높아진다 =>

0이 많아질수록, 고려해야 하는 경우의 수가 훨씬 많아지므로, 연산의 량이 급격하게 증가함!

1. Moving average method

하나의 값으로 계속 수렴하게 함.

기록 변조가 불가능 Irreversible

3일 전에 있는 장부를 바꿀려고 시도를 한다.

그럼 그 해당 SHA256값과 그 이후 값들을 싹 다 바꿔야한다.

비트코인으로 비교하면 10분당 1블록, 대략 4000개의 블록을 싹 다 채굴해야된다.

-> 그러므로 실패!!

만약 20분 전 블록을 바꾼다고 하면, 2개의 블록이겠지만

51% 노드들이 합의를 통해 실패!!