

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. Some nodes are highlighted with blue circles, and others with blue dots. The diagram is rendered in a light gray color.

이더리움 네트워크 기초

비트코인

- ◎ 2008년 8월 bitcoin.org 도메인 등록됨
- ◎ 2008년 10월 31일 사토시 나카모토라는 가명의 사람이 제안(최초의 백서)
 - “Bitcoin : A Peer-to-peer Electronic Cash System”
 - 약 3850개의 피인용수
 - “완전히 분산화”된 형태의 최초의 가상(암호) 화폐
- ◎ 2009년 1월 최초의 비트코인 블록 생성 및 코드 공개
- ◎ 2010년 5월 유명한 10,000비트코인 피자 거래
 - 약 800억 규모
 - a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d *
- ◎ Proof Of Work 알고리즘 : 분산시스템에 적용
 - Slow to compute
 - Fast to verify



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshi@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.

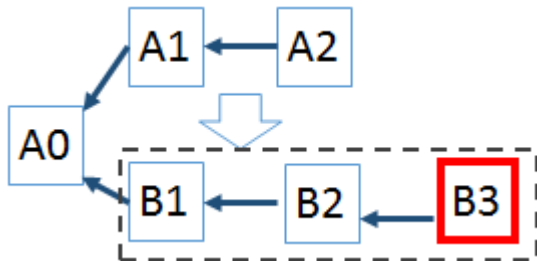
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

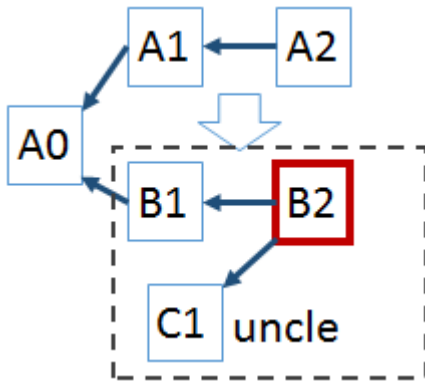
What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

이더리움

- ◎ 2013년 비탈릭 부테린(Vitalik Buterin)에 의해 고안됨
- ◎ 프로그래밍이 가능한 블록체인을 구현한 웹 프레임워크
- ◎ 비트코인 구조와 유사
 - 블록 번호, 해시 트리, 트랜잭션 정보, 년스 등을 포함
 - 추가적으로 잉클블록과 연료(Gas) 등의 개념이 추가됨



비트코인



이더리움

Block #0		Home
Overview		Comments (8)
Block Information		
Height:	0	
TimeStamp:	1132 days 15 hrs ago (Jul-30-2015 03:26:13 PM +UTC)	
Transactions:	8893 transactions and 0 contract internal transactions in this block	
Hash:	0xd4e56740f876aef8c010b86a40d5f56745a118d0906a34e69aec8c0db1cb8fa3	
Parent Hash:	0x00	
Sha3Uncles:	0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347	
Mined By:	0x00 in 15 secs	

이더리움의 첫번째 블록

이더, Ether

- ◎ 이더리움상에서 통용되는 화폐, ETH로 표기
- ◎ 비트코인과 유사
 - 송금(수수료 필요), 마이닝으로 보상은 동일
 - 발행의 제한이 없음
- ◎ 단위
 - 1 ETH = 1,000,000,000,000,000,000 wei (10^{18})
 - 모든 트랜잭션 및 이더리움 네트워크상에서는 wei 단위를 사용
- ◎ 거래액 및 시장 크기
 - 2016년 기준 약 1,100억원 규모
 - 현재 자산 가치 : \$56,296,388,182 (60조원), 비트코인 : 135조원
 - 삼성 시가 총액 346조 (대한민국 예산 400조)

Top 100 Cryptocurrencies by Market Capitalization						
Cryptocurrencies ▾		Watchlist		USD ▾		
▲#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Char
1	Bitcoin	\$126,388,046,312	\$7,406.17	\$4,685,170,000	17,065,237 BTC	
2	Ethereum	\$56,296,388,182	\$564.24	\$1,928,920,000	99,773,127 ETH	
3	Ripple	\$23,691,864,209	\$0.604539	\$272,614,000	39,189,968,239 XRP *	

스마트 컨트랙트

- ◎ 이더리움상에서 동작하는 프로그램 = 스마트 컨트랙트 = Dapp = 블록체인 어플리케이션
- ◎ 이더리움에 접속된 노드내의 EVM 전용 가상 머신에서 실행됨
- ◎ **Solidity**라는 언어로 스마트컨트랙트 개발
 - Javascript와 유사 (다른 언어도 있지만 Solidity가 현재 메인)
 - 튜링 완전 언어 (변수/상수/구조체/반복문/분기문 등 모두 포함)

```
/// @dev Assigns ownership of a specific Kitty to an address.  
function _transfer(address _from, address _to, uint256 _tokenId) internal {  
    // Since the number of kittens is capped to 2^32 we can't overflow this  
    ownershipTokenCount[_to]++;  
    // transfer ownership  
    kittyIndexToOwner[_tokenId] = _to;  
    // When creating new kittens _from is 0x0, but we can't account that address.  
    if (_from != address(0)) {  
        ownershipTokenCount[_from]--;  
        // once the kitten is transferred also clear sire allowances  
        delete sireAllowedToAddress[_tokenId];  
        // clear any previously approved ownership exchange  
        delete kittyIndexToApproved[_tokenId];  
    }  
    // Emit the transfer event.  
    Transfer(_from, _to, _tokenId);  
}
```

스마트 컨트랙트

스마트 컨트랙트 생성



스마트 계약 코드



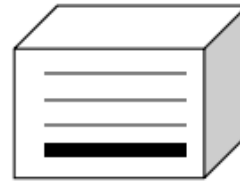
컴파일



바이트 코드



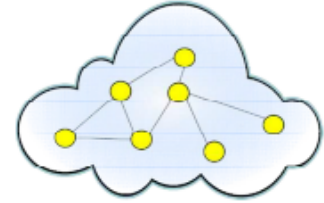
트랜잭션



블록에 삽입



배포



블록체인에 저장

스마트 컨트랙트 실행



사용자 주소

+



함수 주소

+



매개 변수



트랜잭션



블록에 삽입




실행




블록체인에
실행 결과 저장


어카운트 (account)

- ◎ 비트코인과 동일한 어카운트는 비밀키에 의해 표현됨
- ◎ **은행의 계좌번호**와 유사한 개념
- ◎ 어카운트 종류
 - **EOA**(Externally Owned Account) : 일반적으로 비트코인과 동일한 개념의 어카운트로 잔고 등을 볼 수 있음
 - **CA**(Contract Account) : 스마트컨트랙트의 주소, EOA와 동일하게 잔고 확인이 가능함, 하지만 EOA와 다르게 비밀키를 가지고 있지 않음, EOA에 의해 작동됨

 Address 0x5C6578866F382C8DD3FCc665e5596ea03C8B11b9 Home / Accounts / Address

Sponsored Link:  MoneyToken.Com - Roger Ver, founder of Bitcoin.Com, has joined the advisory board - [The Falling Market Protection Service](#).

Overview




Misc More Options

Balance: 30.00399 Ether

Ether Value: \$17,157.78 (@ \$571.85/ETH)

Transactions: 62 txns


Address Watch: Add To Watch List

Token Balances: View (\$0.00) 1 

Transactions

Token Transfers

Comments

 Latest 25 txns from a total Of 62 transactions View All

TxHash	Block	Age	From		To	Value	[TxFee]
0xfd549a110cc9530...	5706484	23 secs ago	0x5c6578866f382c8...	OUT	0x9f8646a35db0f46...	29.99979 Ether	0.00021
0x4b7122398a0bcd...	5701279	22 hrs 25 mins ago	0x1ff9ec542110ed9...	IN	0x5c6578866f382c8...	10 Ether	0.00105
0xd5b65727b9d253...	5689281	3 days 1 hr ago	0x1ff9ec542110ed9...	IN	0x5c6578866f382c8...	20 Ether	0.00105

어카운트 (account) 생성

1. ECDSA의 개인키 생성(랜덤)

- 256비트(32바이트)의 개인키 생성 (d)

2. 개인키로부터 공개키 생성

- 공개키 64바이트 생성 ($B=dA$)

3. 공개키로부터 어카운트 주소 생성

- $C = \text{Keccak256}(\text{pubKey})$
- C 의 마지막 20바이트(160비트)가 어카운트 주소임
- e.g. 0x27113019 85Fd072c 3c94b457 81d4897F 44C562d5

어카운트 주소(20바이트=160비트)

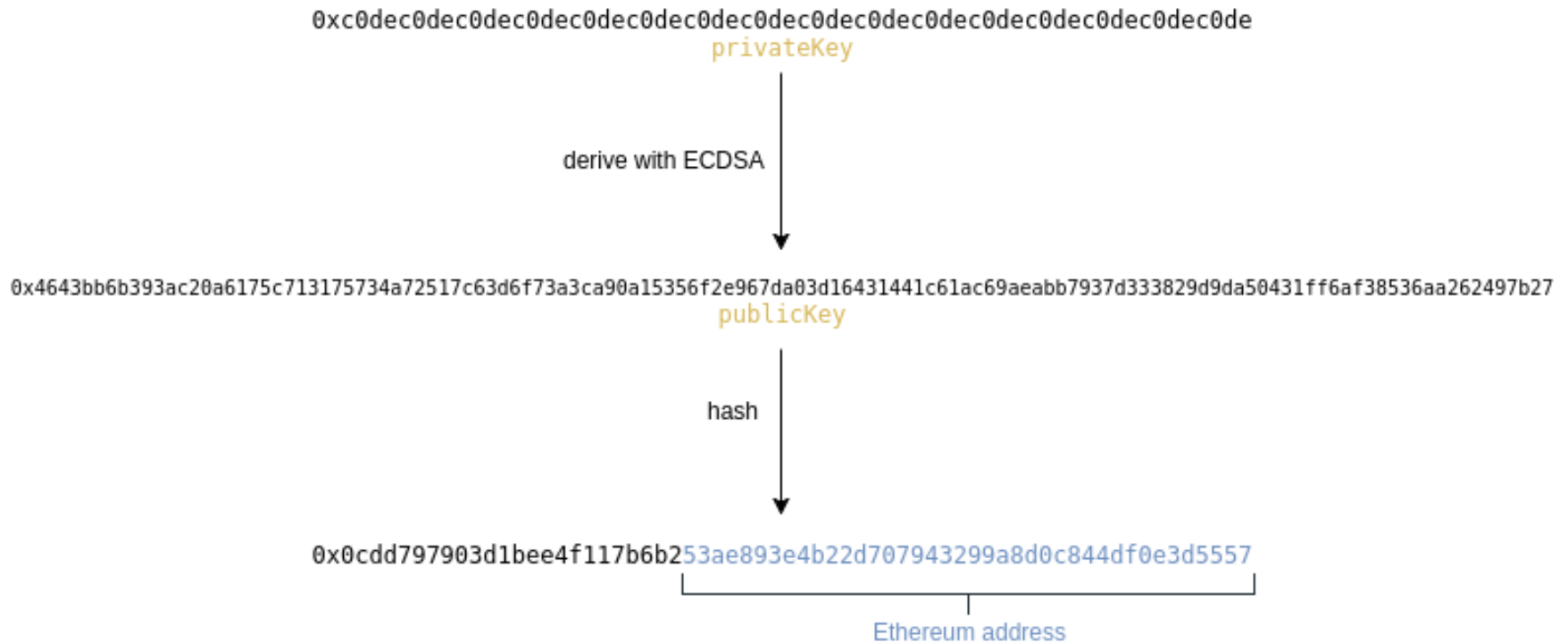
$C = 0xab5085Fd072c3c94b4572711301985Fd072c3c94b45781d4897F44C562d5$

For a given private key, p_r , the Ethereum address $A(p_r)$ (a 160-bit value) to which it corresponds is defined as the right most 160-bits of the Keccak hash of the corresponding ECDSA public key:

(213)

$$A(p_r) = \mathcal{B}_{96..255}(\text{KEC}(\text{ECDSAPUBKEY}(p_r)))$$

어카운트 (account) 생성

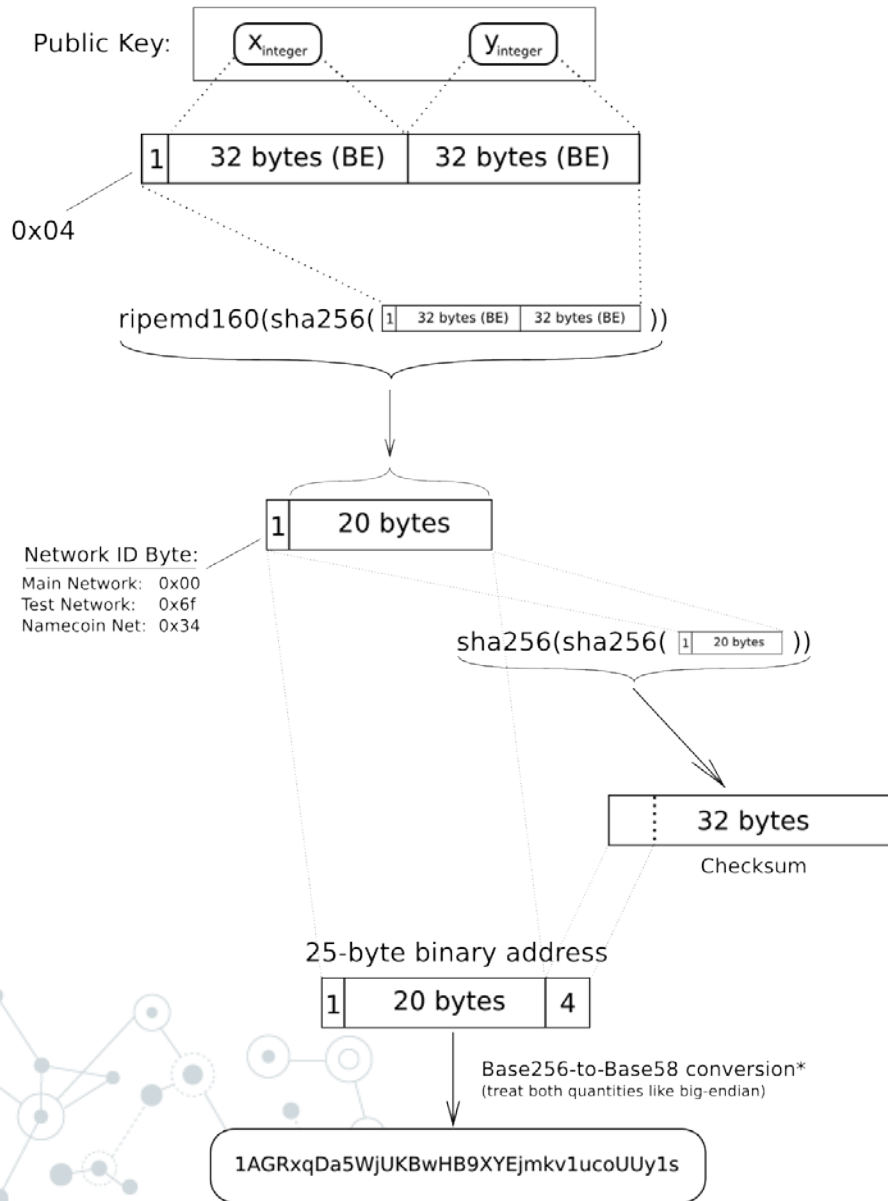


For a given private key, p_r , the Ethereum address $A(p_r)$ (a 160-bit value) to which it corresponds is defined as the right most 160-bits of the Keccak hash of the corresponding ECDSA public key:

(213)

$$A(p_r) = \mathcal{B}_{96..255}(\text{KEC}(\text{ECDSAPUBKEY}(p_r)))$$

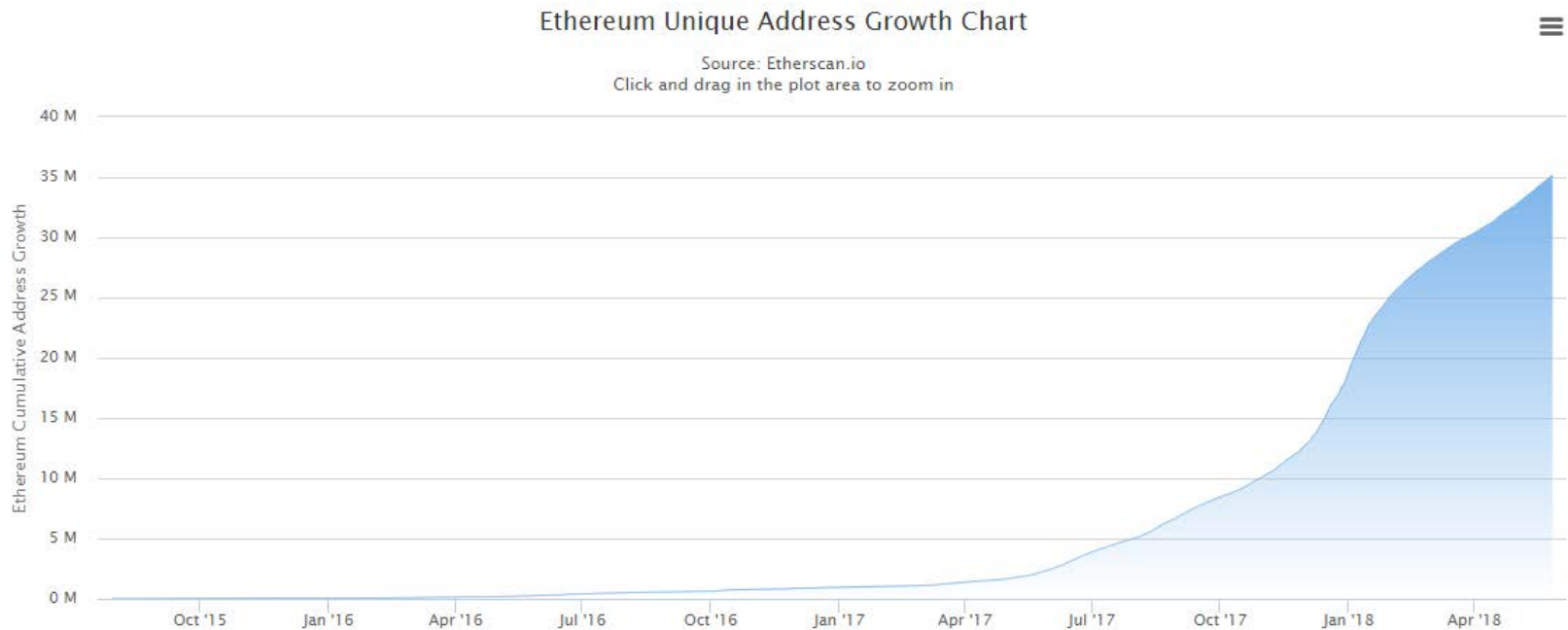
[참고] 비트코인 주소(addr) 생성 방법



- ◎ Base58
 - 0, O
 - 1, l
 - + / 를 Base64에서 제거한 포맷

동일한 어카운트 주소???

- ◎ 동일한 어카운트 주소가 생성되는 것은 극히 낮은 확율임
- ◎ 중앙에서 (은행 계좌번호) 발급 방식에 대해서는 기존 계좌번호 확인하여 중복이 안되게 발급이 가능
 - 하지만, 탈중앙화에서는 이러한 방식이 불가능함
- ◎ 현재, 35,154,536개의 어카운트 주소가 발급됨



발급된 어카운트 주소 개수

Birthday Attack

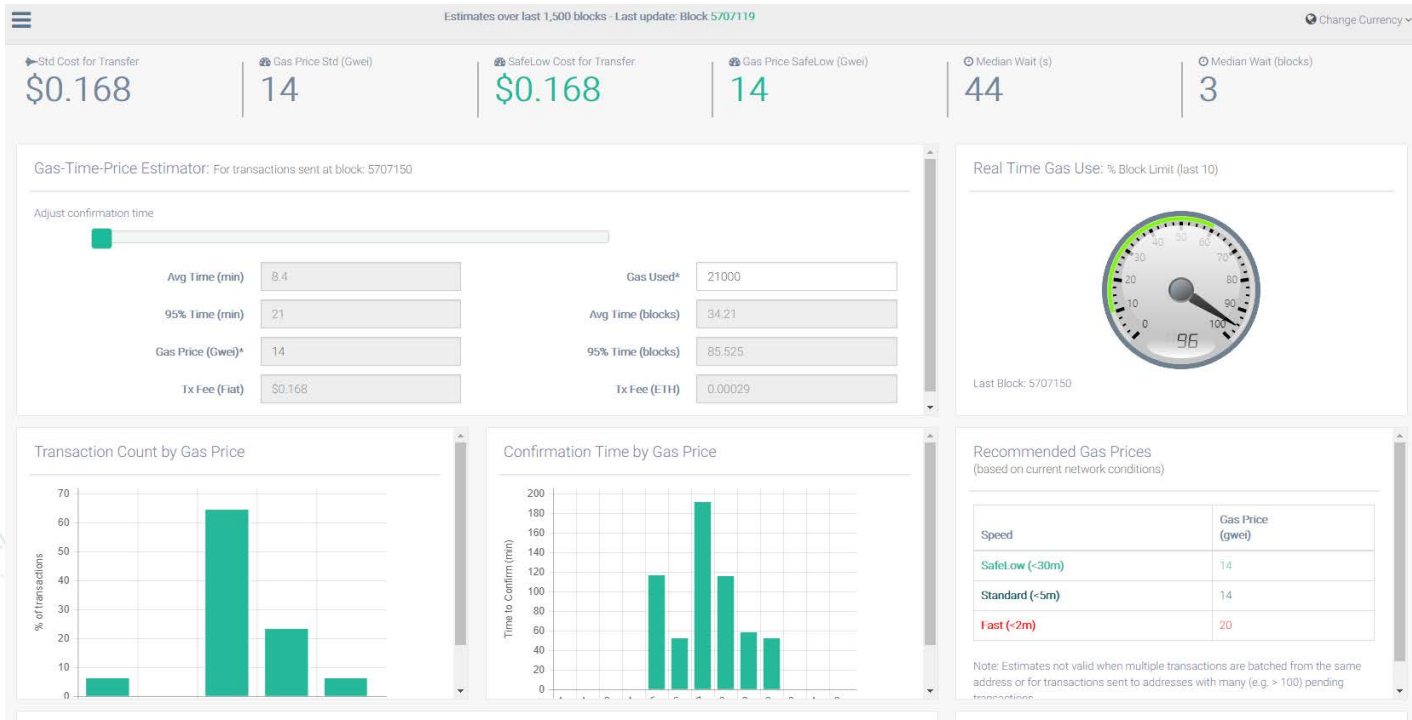
- ◎ 몇 명이 있으면 그 중에 생일이 같은 사람이 2명 이상이 있을 확률이 50% 이상인가?
- ◎ **Question : 50명이 있는 한 반에 생일이 같은 사람이 2명 이상 있을 확률?**
- ◎ **Answer : 약 97%**
 - 모두 생일이 다를 확률 $P_1 : \frac{364}{365} \cdot \frac{363}{365} \cdot \frac{362}{365} \cdots \frac{316}{365} \cdot \frac{315}{365} = \frac{365!}{365^{50}(365-50)!} \cong 0.0296$
 - $1 - 0.0296 = 0.97$, **97%**
- ◎ 50% 정도 확률일 경우 approximation : $\sqrt{m} = 365 \approx 19$

-
- ◎ Question : 어카운트의 주소가 같은 사람(지갑)이 2개 이상 있을 확률이 50% 이상이 되려면 몇 사람(지갑)이 있어야 하는지?

- ◎ Answer : 2^{80} 개의 사람(지갑)이 있어야 약 50%의 확률로 동일한 주소
현재 어카운트 비율 : $35,154,536 / 2^{80} = 2.9 \times 10^{-15}$
하루에 1개씩 생성된다고 했을 때에 약 3천년

Gas

- 모든 트랜잭션을 처리하는 데 필요한 수수료 (채굴자들의 보상)
- (실제 사용된 Gas) x (**Gas 단가**) = 수수료 Ether
 - $21000 \text{ Gas} \times 14 \times 10^9 \text{ wei/Gas} = 29,400 \times 10^9 \text{ wei} = 0.000294 \text{ ETH} (\$0.16)$
- <https://ethgasstation.info/>
 - 현재 이더리움 네트워크상의 Gas 단가 통계
 - $14 \text{ Gwei} = 14,000,000,000 \text{ Wei}$

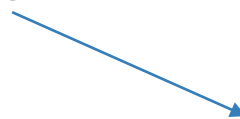


필요한 Gas의 양

The fee schedule G is a tuple of 31 scalar values corresponding to the relative costs, in gas, of a number of abstract operations that a transaction may effect.

Name	Value	Description*
G_{zero}	0	Nothing paid for operations of the set W_{zero} .
G_{base}	2	Amount of gas to pay for operations of the set W_{base} .
$G_{verylow}$	3	Amount of gas to pay for operations of the set $W_{verylow}$.
G_{low}	5	Amount of gas to pay for operations of the set W_{low} .
G_{mid}	8	Amount of gas to pay for operations of the set W_{mid} .
G_{high}	10	Amount of gas to pay for operations of the set W_{high} .
$G_{extcode}$	700	Amount of gas to pay for operations of the set $W_{extcode}$.
$G_{balance}$	400	Amount of gas to pay for a BALANCE operation.
G_{sload}	200	Paid for a SLOAD operation.
$G_{jumpdest}$	1	Paid for a JUMPDEST operation.
G_{sset}	20000	Paid for an SSTORE operation when the storage value is set to non-zero from zero.
G_{sreset}	5000	Paid for an SSTORE operation when the storage value's zeroness remains unchanged or is set to zero.
R_{sclear}	15000	Refund given (added into refund counter) when the storage value is set to zero from non-zero.
$R_{selfdestruct}$	24000	Refund given (added into refund counter) for self-destructing an account.
$G_{selfdestruct}$	5000	Amount of gas to pay for a SELFDESTRUCT operation.
G_{create}	32000	Paid for a CREATE operation.
$G_{codedeposit}$	200	Paid per byte for a CREATE operation to succeed in placing code into state.
G_{call}	700	Paid for a CALL operation.
$G_{callvalue}$	9000	Paid for a non-zero value transfer as part of the CALL operation.
$G_{callstipend}$	2300	A stipend for the called contract subtracted from $G_{callvalue}$ for a non-zero value transfer.
$G_{newaccount}$	25000	Paid for a CALL or SELFDESTRUCT operation which creates an account.
G_{exp}	10	Partial payment for an EXP operation.
$G_{expbyte}$	50	Partial payment when multiplied by $\lceil \log_{256}(exponent) \rceil$ for the EXP operation.
G_{memory}	3	Paid for every additional word when expanding memory.
$G_{txcreate}$	32000	Paid by all contract-creating transactions after the <i>Homestead</i> transition.
$G_{txdatazero}$	4	Paid for every zero byte of data or code for a transaction.
$G_{txdatanonzero}$	68	Paid for every non-zero byte of data or code for a transaction.
$G_{transaction}$	21000	Paid for every transaction.
G_{log}	375	Partial payment for a LOG operation.
$G_{logdata}$	8	Paid for each byte in a LOG operation's data.
$G_{logtopic}$	375	Paid for each topic of a LOG operation.
G_{sha3}	30	Paid for each SHA3 operation.
$G_{sha3word}$	6	Paid for each word (rounded up) for input data to a SHA3 operation.
G_{copy}	3	Partial payment for *COPY operations, multiplied by words copied, rounded up.
$G_{blockhash}$	20	Payment for BLOCKHASH operation.
$G_{quaddivisor}$	100	The quadratic coefficient of the input sizes of the exponentiation-over-modulo precompiled contract.

일반적인 트랜잭션(송금)에
필요한 Gas 양



필요한 Gas의 양

Overview		Comments
Transaction Information		
TxHash:	0x7aa93d01262b7fd8bf9c19b59fdc191ceacbeaa205a5e3947d1624440526746c	
TxReceipt Status:	Success	
Block Height:	5707184 (1 block confirmation)	
TimeStamp:	45 secs ago (May-31-2018 07:57:20 AM +UTC)	
From:	0x110793d66f7aa66b4805feb746faefbdb0996ae7	
To:	0xfeeb0a1b78408aa006d6750c09d2f87e919c91f7	
Value:	0.4 Ether (\$229.00)	
Gas Limit:	21000	
Gas Used By Txn:	21000	
Gas Price:	0.000000021 Ether (21 Gwei)	
Actual Tx Cost/Fee:	0.000441 Ether (\$0.25)	
Nonce & {Position}:	8 {200}	

송금 트랜잭션 Gas(Gas Limit 다 소진)

필요한 Gas의 양

Overview	Internal Transactions	Comments
Transaction Information ◀ ▶		
TxHash:	0xe31ab345da9640661059a2f1378fdf5cd1a35cbfc08e94ef135189913e9f1731	
TxReceipt Status:	Success	
Block Height:	5586916 (120276 block confirmations)	
TimeStamp:	21 days 5 hrs ago (May-10-2018 02:28:54 AM +UTC)	
From:	0x2670961315e98e9a5fa9e41a43998084bbc0c1eb	
To:	🔍 Contract 0x242960c81fd3ec2bb06c29233c44e284adb35ae2 ✔️ ... TRANSFER 2 Ether from 0x242960c81fd3ec2bb06c... to → 0x88ffc1c9c29f4b272e336...	
Value:	0 Ether (\$0.00)	
Gas Limit:	80401	
Gas Used By Txn:	48224	
Gas Price:	0.000000007 Ether (7 Gwei)	
Actual Tx Cost/Fee:	0.000337568 Ether (\$0.19)	
Nonce & {Position}:	6 {94}	

스마트 컨트랙트 함수 호출하기 위한 트랜잭션 (전체 소진하지 않음)

최대 Gas Limit은?

- ◎ DDOS 공격 및 스마트 컨트랙트 상의 무한 반복 실행 등으로 이더리움 네트워크의 부하를 줄이기 위한 목적
- ◎ **트랜잭션의 Gas Limit**
 - 각 트랜잭션에서 소모할 수 있는 Gas의 총량(e.g. 자동차에서 기름통)
- ◎ **블록의 Gas Limit**
 - 모든 트랜잭션의 소모된 Gas의 한계치
 - $8,000,000 / 21,000 = 380$ 개

to:	0x97b76ea01520545f206de1b11e34
Value:	5.273197 Ether (\$3,013.58)
Gas Limit:	90000
Gas Used By Txn:	21000
Gas Price:	0.000000022 Ether (22 Gwei)
Actual Tx Cost/Fee:	0.000462 Ether (\$0.26)
Nonce & {Position}:	435619 {121}
Input Data:	0x

트랜잭션의 Gas Limit

Total Difficulty:	4,513,173,066,178,540,738,044
Size:	36692 bytes
Gas Used:	7,979,206 (99.74%)
Gas Limit:	8,000,012
Nonce:	0x43b3c86007547bcf
Block Reward:	3.2342643808625 Ether (3 + 0.2342643808625)
Uncles Reward:	0
Extra Data:	七彩神仙鱼 (Hex:0xe4b883e5bda9e7a59ee4bb99e9b1bc)



블록의 Gas Limit

실제 송금하는 데 필요한 수수료

- ◎ 설정한 Gas Price에 따라 다름!!
 - 송금은 21,000의 Gas가 필요함
 - 1 Gas의 비용에 따라 필요한 이더가 다름

MetaMask Notification

CONFIRM TRANSACTION Private Network

MainMetamask
c33711...977d  >  1725Be...1D36
3.551 ETH
257.62 USD

Amount 0.00 ETH
0.00 USD

Gas Limit UNITS

Gas Price WEI

Max Transaction Fee 0.064000 ETH
4.64 USD

Max Total 0.064000 ETH
4.64 USD

Data included: 3460 bytes

RESET **ACCEPT** **REJECT**

Gas Price (eth/gas)

×

소모한 Gas양(gas)

×


이더리움 가격(\$/eth)

||


실제 필요한 수수료

Tx Gas Limit이 부족하면?

- ◎ 트랜잭션 Gas Limit을 매우 낮게 설정하면?
 - 단순 송금 트랜잭션의 경우 최소 Gas량으로 에러 메시지 표시
 - 스마트 컨트랙트 함수 호출 등의 트랜잭션의 경우 out of gas로 함수 호출이 실패
 - revert 처리(원래의 호출 전 상태로 되돌림)

 **CONFIRM TRANSACTION**

Account 5
267096...c1Eb
13.994 ETH
7976.84 USD



Account 2
C3C90C...e169

Amount

1.000 ETH
569.99 USD

Gas Limit

UNITS

Gas Limit Must Be Greater Than Or Equal To 21000 UNITS And Less Than Or Equal To 69891728 UNITS.

Max Transaction Fee

0.13 USD

Max Total

1.000 ETH
570.12 USD

Data included: 0 bytes

RESET

SUBMIT

REJECT

3844796 (117 block confirmations)

33 mins ago (Jun-09-2017 11:06:34 AM +UTC)

0xe7a3aa2509ec62386debd90f65a7d4f19199dc38

 Contract 0xf92f7c8012de01ae247a2523e6e3a086273ab03a 

 Warning! Error encountered during contract execution [Out of gas] ☹

1.71 Ether (\$451.27) - [CANCELLED]

59268

정리

- ◎ 이더의 트랜잭션을 위해서는 Gas가 필요
 - Gas X Gas가격 = 필요한 이더
- ◎ 스마트 컨트랙트도 이더리움상의 트랜잭션으로 Gas가 필요함
 - 실행하는 함수 등에 따라 Gas의 양이 달라짐
 - 최대 하나의 블록에 포함되는 Gas의 양은 정해져 있음
- ◎ 블록의 Gas Limit은 현재 800,000으로 일반 이더 송금을 위한 Gas로 치면 약 380개가 가능함

The screenshot shows a transaction configuration interface. At the top, 'Gas Limit' is set to 3200000 UNITS. Below it, 'Gas Price' is set to 20000000000 WEI, which is highlighted with a red rectangular box. Underneath, 'Max Transaction Fee' is displayed as 0.064000 ETH (4.64 USD). At the bottom, 'Max Total' is also shown as 0.064000 ETH (4.64 USD). Below these fields, it states 'Data included: 3460 bytes'. At the very bottom, there are three buttons: 'RESET' (orange), 'ACCEPT' (green), and 'REJECT' (red).

Gas Limit	3200000	UNITS
Gas Price	20000000000	WEI
Max Transaction Fee	0.064000	ETH 4.64 USD
Max Total	0.064000	ETH 4.64 USD

Data included: 3460 bytes

RESET ACCEPT REJECT

Gas Price를 높여야 트랜잭션이 빨리 처리됨