Key, Wallet

你的錢是不是你的錢？

加密貨幣 (自主管理)


要死掉了


鑰匙掉了

Key management

鑰匙掉了 ≅ 要死掉了

Key loss and vanish

- Controversial QuadrigaCX cryptocurrency exchange placed in bankruptcy
  - $190 million of funds got lost because the founder suddenly died in his trip. (April 8)
- Exit Scam? Dublin-Based Exchange Bitsane Vanishes With Users' Funds
  - Ireland-based cryptocurrency exchange Bitsane has apparently vanished, taking as many as 246,000 users' crypto deposits with it. The news was reported by Forbes on June 27.

Source: https://cointelegraph.com/news/exit-scam-dublin-based-exchange-bitsane-vanishes-with-users-funds

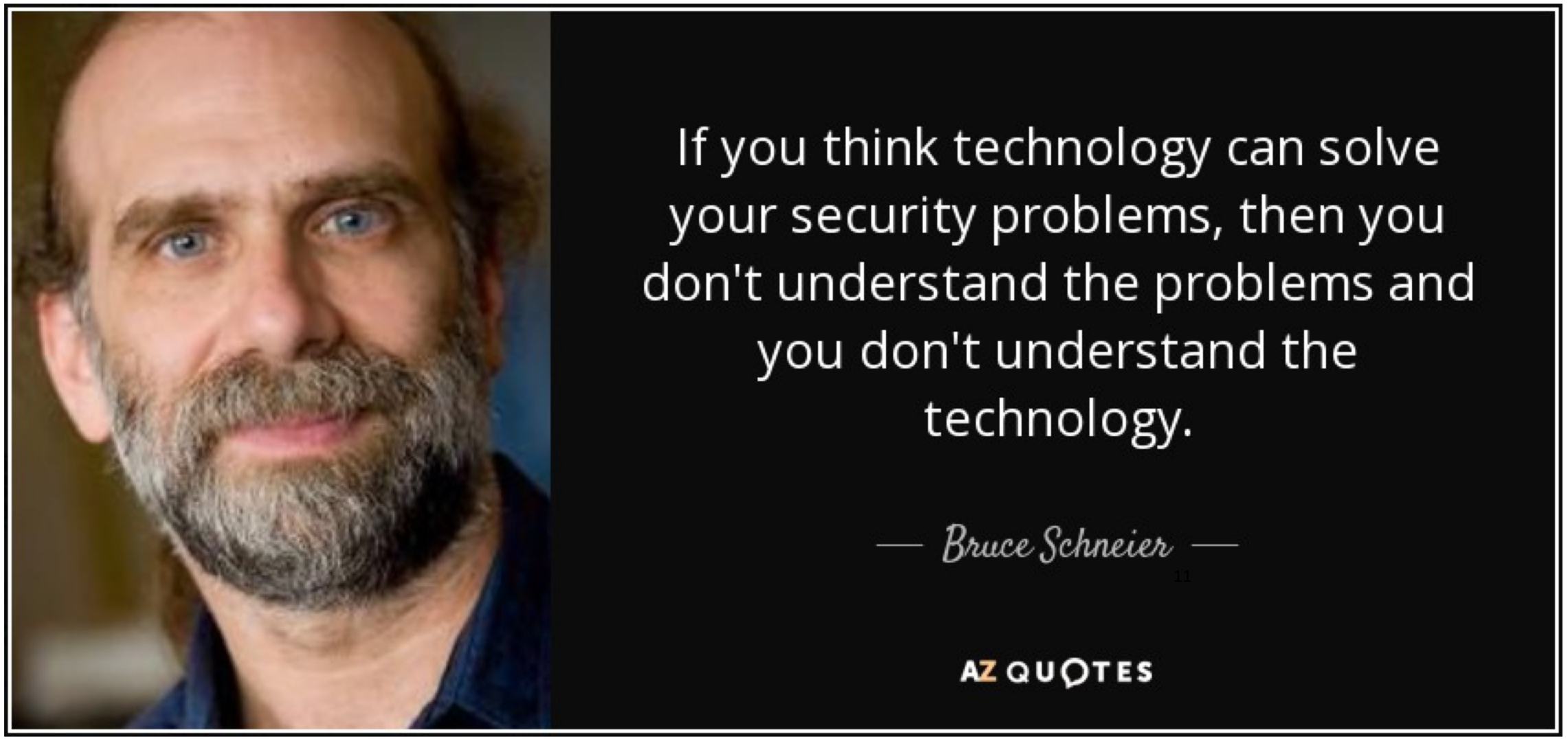
Hacked

- Singapore-Based Crypto Exchange DragonEx Has Been Hacked (Mar 26)
- Crypto Exchange Bithumb Hacked for $13 Million in Suspected Insider Job (Mar 30)

Source: https://thehackernews.com/2017/07/bitcoin-ethereum-cryptocurrency-exchange.html

Key management

- Centralized
  - Single Point of Failure (SPoF)
  - A lucrative target for hackers (ex: Binance)
- Decentralized
  - Ideal but
    - Self-sovereign (freedom)
    - Responsibility (Risk management)



Images from https://www.azquotes.com/quote/570040

All Ethereum Private Keys ! Home About **Donate:** 0x35e9Db3F1eaEdFB4aEbC7FFf4CB01DE22fdcA529

Private KEY e63d9444da54d04ec4eb6538e577842cdc6f5f025c2 Search

Back Random ;) Next

Page: 1 out of **463168356949264781694283940034751631413079938662562256157830336031652518559 8**

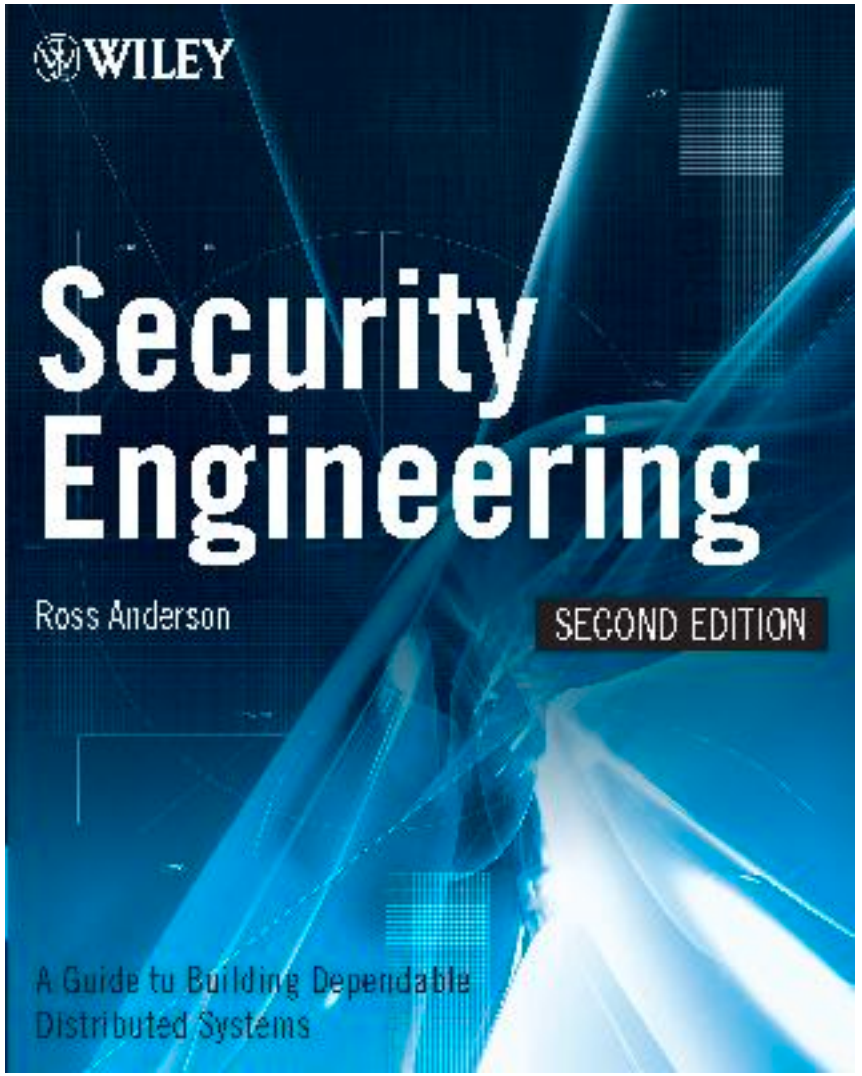
Private Key	Address	Balance
+ 0000000000000000000000000000000000000000000000000000000000000001	0x7E5F4552091A69125d5DfCb7b8C2659029395Bdf	0
+ 0000000000000000000000000000000000000000000000000000000000000002	0x2B5AD5c4795c026514f8317c7a215E218DcCD6cF	0
+ 0000000000000000000000000000000000000000000000000000000000000003	0x6813Eb9362372EEF6200f3b1dbC3f819671cBA69	0
+ 0000000000000000000000000000000000000000000000000000000000000004	0x1efF47bc3a10a45D4B230B5d10E37751FE6AA718	0
+ 0000000000000000000000000000000000000000000000000000000000000005	0xe1AB8145F7E55DC933d51a18c793F901A3A0b276	0
+ 0000000000000000000000000000000000000000000000000000000000000006	0xE57bFE9F44b819898F47BF37E5AF72a0783e1141	0
+ 0000000000000000000000000000000000000000000000000000000000000007	0xd41c057fd1c78805AAC12B0A94a405c0461A6FBb	0
+ 0000000000000000000000000000000000000000000000000000000000000008	0xF1F6619B38A98d6De0800F1DefC0a6399eB6d30C	0
+ 0000000000000000000000000000000000000000000000000000000000000009	0xF7Edc8FA1eCc32967F827C9043FcAe6ba73afA5c	0
+ 000000000000000000000000000000000000000000000000000000000000000a	0x4CCeBa2d7D2B4fdcE4304d3e09a1fea9fbEb1528	0
+ 000000000000000000000000000000000000000000000000000000000000000b	0x3DA8D322CB2435dA26E9C9fEE670f9fB7Fe74E49	0
+ 000000000000000000000000000000000000000000000000000000000000000c	0xDbc23AE43a150ff8884B02Cea117b22D1c3b9796	0
+ 000000000000000000000000000000000000000000000000000000000000000d	0x68E527780872cda0216Ba0d8fBD58b67a5D5e351	0
+ 000000000000000000000000000000000000000000000000000000000000000e	0x5A83529ff76Ac5723A87008c4D9B436AD4CA7d28	0

銀行內控

KYC, Freeze account

Security Engineering

- Chapter 10: Banking and Bookkeeping



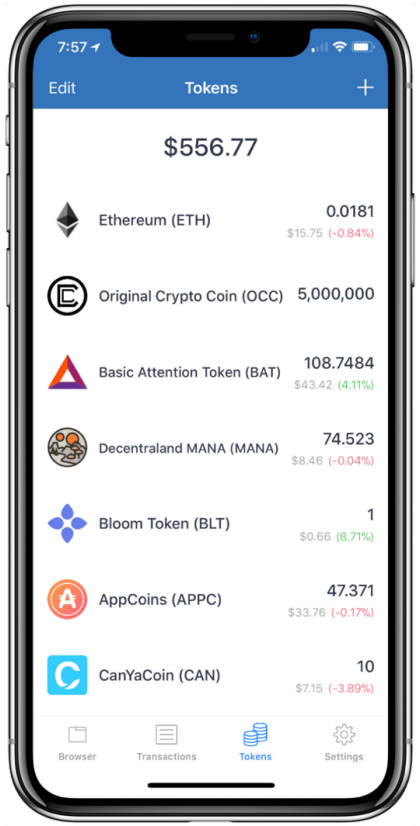
https://www.cl.cam.ac.uk/~rja14/book.html

虛擬貨幣 vs 銀行轉帳

- 私鑰掉了
- 交易地址填錯了
- 任意金額轉帳
- 驗證交易合法性
- 交易審查流程

- 密碼忘了
- 收款人賬戶號碼寫錯
- 任意金額轉帳 (約定轉帳)
- 驗證交易合法性 (證件)
- 交易審查流程 (行員蓋章)

Wallet (Risk)



20%

Hot wallet

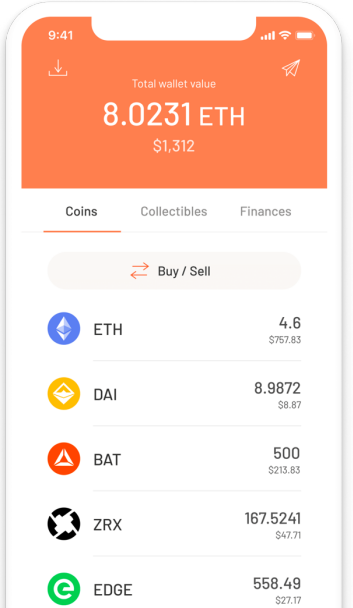
80%

Cold wallet

Source: https://vauban.io/custody-options-for-crypto-hedge-funds-3/

Hot Wallet

Argent



✗	MyEtherWallet / MyCrypto	· Website · Chrome browser extension	· Supports ETH and ERC20 tokens · Hardware wallet integration (Ledger & Trezor)
	Jaxx	· Android & iOS · OS X, Windows, Linux · Chrome browser extension	· Supports ETH and a limited set of ERC20 tokens · ShapeShift exchange integration
	ENJIN	· Android & iOS	· Supports ETH and ERC20 tokens · Part of the Enjin gaming network · Focus on security (e.g. via own custom keyboard)
	TRUST WALLET	· Android & iOS	· Supports ETH, ERC20 and ERC223 tokens · Includes a dApp browser
✗	METAMASK	· Chrome browser extension	· Supports ETH and ERC20 tokens · One of the most popular wallets (>1M users) · Quasi-standard for dApp interaction via web browsers
	imToken	· Android & iOS	· Supports ETH and ERC20 tokens · Includes a dApp browser · Focus on UX

https://media.consensys.net/how-to-store-digital-assets-on-ethereum-a2bfdcf66bd0

Cold Wallet

Ledger

keepkey

TREZOR

https://media.consensys.net/how-to-store-digital-assets-on-ethereum-a2bfdcf66bd0

Sign Tx with Cold Wallet

Prevent a Man-in-the-middle attack

1. Send raw Tx

2. Decode raw Tx, preview the Tx info
(2a) Send challenge to the wallet client
(Pick random character from TO address)
(2b) Challenge success

3. Sign raw Tx
4. Return signed Tx

5. Broadcast a signed Tx

Sign Tx with Cold Wallet

Software
- Electrum
- go-ethereum
- MyEtherWallet
- Ledger apps

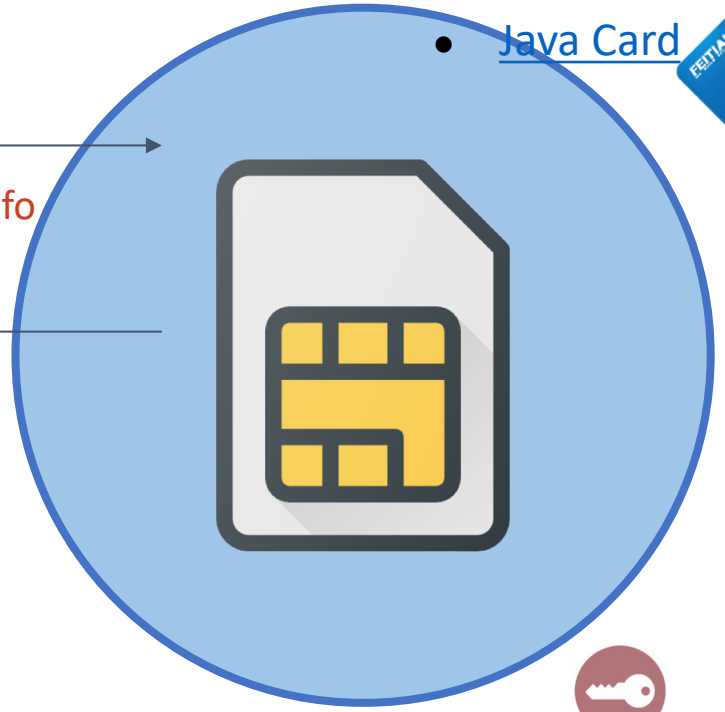
1. Send raw Tx
2. Decode raw Tx, preview the Tx info
3. Sign raw Tx
4. Return signed Tx

5. Broadcast a signed Tx

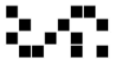
Software
- Electrum
- go-ethereum

Hardware Wallet
- Ledger Nano S
- TREZOR Wallet

Smart Card
- Java Card



Multisig Wallet

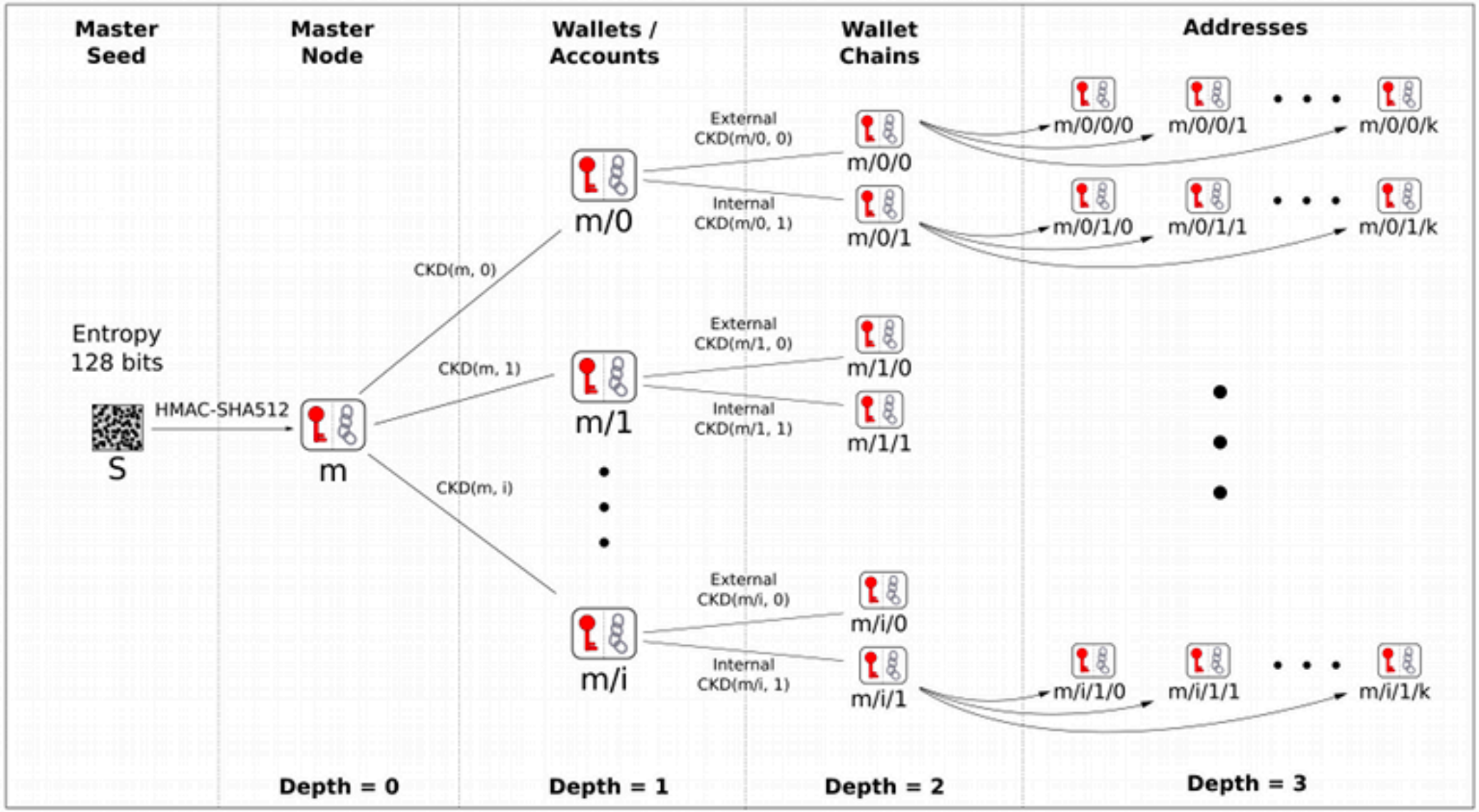
 Gnosis MultiSig Wallet	· Web and desktop user interface · Supports ETH and ERC20 tokens · Hardware wallet support (Ledger & Trezor) · Can add and remove members · Can set daily ETH limit · Used by a variety of companies and individuals to hold large amounts of crypto
 Ethereum MIST Wallet	· Desktop user interface · Supports ETH and ERC20 tokens · Official Ethereum wallet and dApp browser · Can add and remove members · Can set daily ETH limit · Not designed for contract interactions
 DappHub DSGroup Project	· No graphical user interface, command line only · All actions have an expiration · Cannot add or remove members
 Parity MultiSig Wallet	· Was built into Parity client · Experienced a major hack with high amounts of frozen funds · Development has discontinued

https://media.consensys.net/how-to-store-digital-assets-on-ethereum-a2bfdcf66bd0

BitGo

http://www.kudoscoin.org/

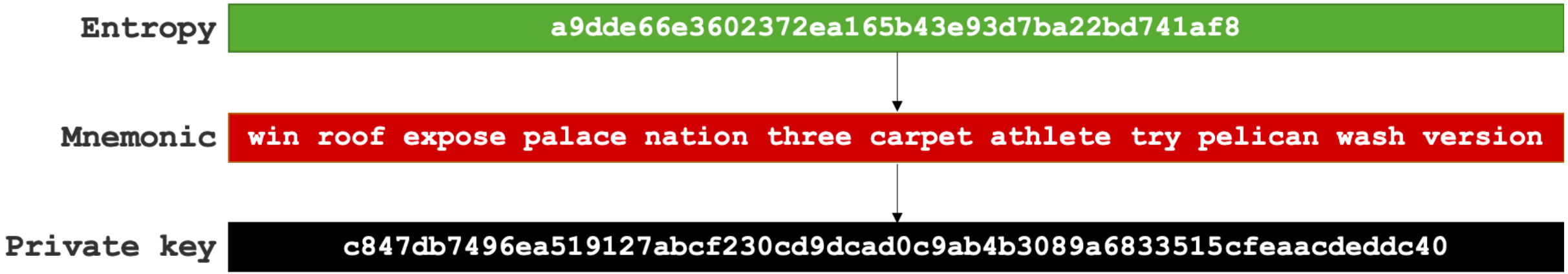
BIP 32 - Hierarchical Deterministic Wallets



Child Key Derivation Function ~ $CKD(x,n) = HMAC\text{-}SHA512(x_{Chain}, x_{PubKey} || n)$

https://iancoleman.io/bip39/

Mnemonic Phrase (BIP39)



1. Create a keypair of private/public key
2. public_key = ECDSA(private_key)
3. public_key_hash = Keccak-256(public_key)
4. address = '0x' + last 20 bytes of public_key_hash

BIP39

Mnemonic Language English 日本語 Español 中文(简体) 中文(繁體) Français Italiano 한국어

BIP39 Mnemonic

seat reform bulb nerve pool similar outside pulse net attitude gadget sugar guess manual vanish

BIP39 Passphrase (optional)

BIP39 Seed

e73b051b57efc020b3dfef59d588fe435795b33269c819ae7bded9e3aea6182065f9087960b74af2dcc00d578dceebc9884b16f5126f0c86bf577d2aa9b095f4

Coin

ETH - Ethereum

BIP32 Root Key

xprv9s21ZrQH143K3HFKduRfU483ZaZuMoCarBEvHc7omnQFFd1mEhqh1bEL3LpXkqyCyakfc4cFHewqp75AtL4W8uTde4RigrLWTjwijmWNaqr

https://iancoleman.io/bip39/

Derivation Path

BIP32 | BIP44 | BIP49 | BIP84 | BIP141

BIP32

For more info see the BIP32 spec

Client blockchain.info

BIP32 Derivation Path m/44'/0'/0'

Use hardened addresses

Bitcoin Core Use path `m/0'/0'` with hardened addresses.

For more info see the Bitcoin Core BIP32 implementation

Multibit Use path `m/0'/0`.

For more info see MultiBit HD

Block Explorers Use path `m/44'/0'/0'`. Only enter the `xpub` extended key into block explorer search fields, never the `xprv` key.

Can be used with: blockchain.info

BIP32 Extended Private Key

xprv9z73waDnLNVdypT42hVzLbcXDJQbVkMy54z34BckaPPWw4kkJWa3hJQyr3iFn65Cdiv9F1QXzj2HXB6nwWLbCQcpxvMQ4TLMG9T6bzMVZvD

BIP32 Extended Public Key

xpub6D6QM5kgAk3wCJXX8j2zhjZFmLF5uD5pSHudra2N8ivVos5tr3tJF6jThLJHz5RaEzKDAcN3rCJbZj3z5o5YtJTfWLpK6U9WB38iwNXFEkS

https://iancoleman.io/bip39/

Derivation Path

BIP32 | BIP44 | BIP49 | BIP84 | BIP141

BIP44

For more info see the BIP44 spec.

Purpose 44

Coin 60

Account 0

External / Internal 0

The account extended keys can be used for importing to most BIP44 compatible wallets, such as mycelium or electrum.

Account Extended Private Key
xprv9xfsN9Uft3MYRZZR8Byx8R3C5GvFNpStGFAA971Uip5sxLZtPTCGQrMbZWc4vyebhBYrCwpBDNU9eKVmuDxLfkfT6rGr73eDttNPbVBV2PG

Account Extended Public Key
xpub6BfDmf1ZiQuqe3dtEDWxVYyvdJkjnHAjdU5kwVR6H9crq8u2vzWWxeg5QnQX6z9iJFFtdwF3zJxg4Sm85ivjaJC4TCh1QuxtHWzxyxbQav5

The BIP32 derivation path and extended keys are the basis for the derived addresses.

BIP32 Derivation Path m/44'/60'/0'/0

BIP32 Extended Private Key
xprvA173rL9ZzsTq6rNu2WZtfbpipGnW1hTNGRJvsdApgU272mmb9S11UwpkS2vjj8RbCTsTLoPtUMaAvEpAUS3iBYtAC49DaGy42j4J75u7vuk

BIP32 Extended Public Key
xpub6E6QFqgTqF28KLTN8Y6u2jmTNJczRABDdeEXg1aSEoZ5ua6jgyKG2k9EHLB3BPZHz6kSVd5Yvx9idaF9cR2FdqysvZyYqmXQRJcFU6LvX7F

https://iancoleman.io/bip39/

Derivation Path

BIP44

BIP32 | BIP44 | BIP49 | BIP84 | BIP141

For more info see the BIP32 spec

Client Coinomi, Ledger

BIP32 Derivation Path m/44'/60'/0'

☐ **Use hardened addresses**

Bitcoin Core Use path `m/0'/0'` with hardened addresses.

For more info see the Bitcoin Core BIP32 implementation

Multibit Use path `m/0'/0`.

For more info see MultiBit HD

Block Explorers Use path `m/44'/0'/0'`. Only enter the `xpub` extended key into block explorer search fields, never the `xprv` key.

Can be used with: blockchain.info

BIP32 Extended Private Key

xprv9xfsN9Uft3MYRZZR8Byx8R3C5GvFNpStGFAA971Uip5sxLZtPTCGQrMbZWc4vyebhBYrCwpBDNU9eKVmuDxLfkfT6rGr73eDttNPbVBV2PG

BIP32 Extended Public Key

xpub6BfDmf1ZiQuqe3dtEDWxVYyvdJkjnHAjdU5kwVR6H9crq8u2vzWWxeg5QnQX6z9iJFFtdwF3zJxg4Sm85ivjaJC4TCh1QuxtHWzxyxbQav5

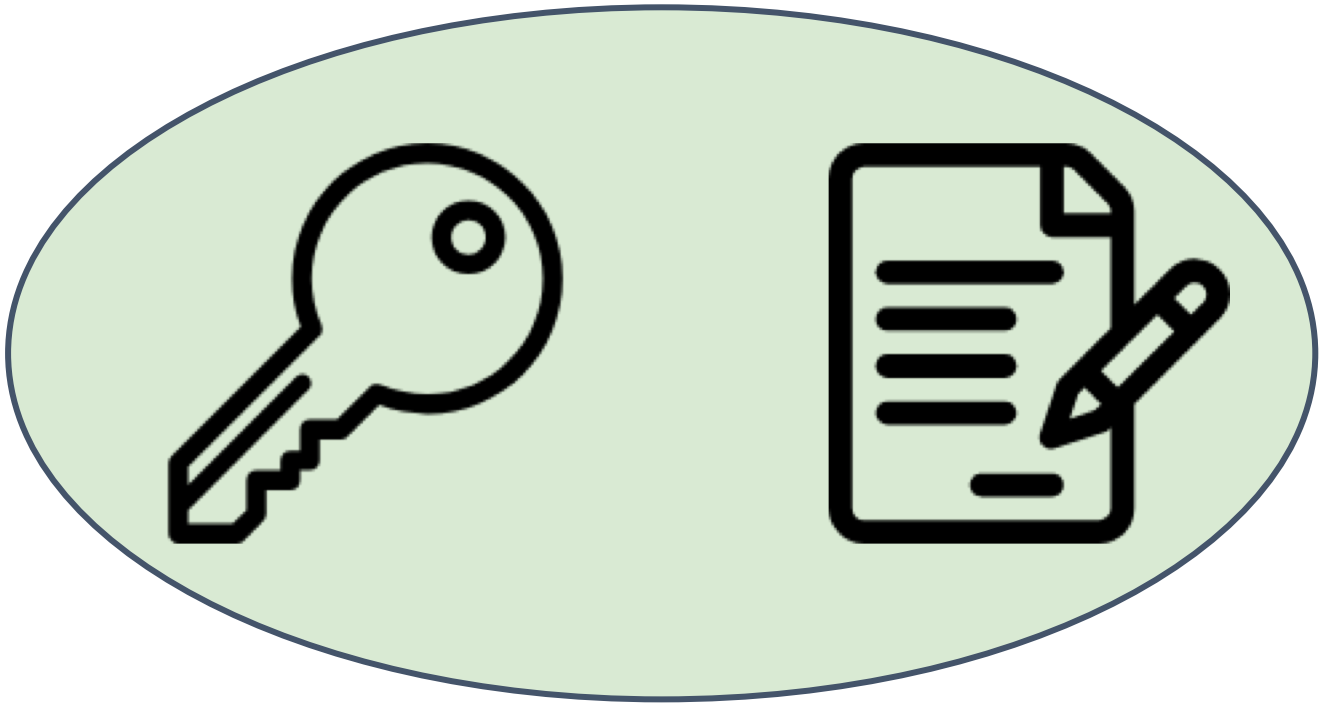
https://iancoleman.io/bip39/

Key import

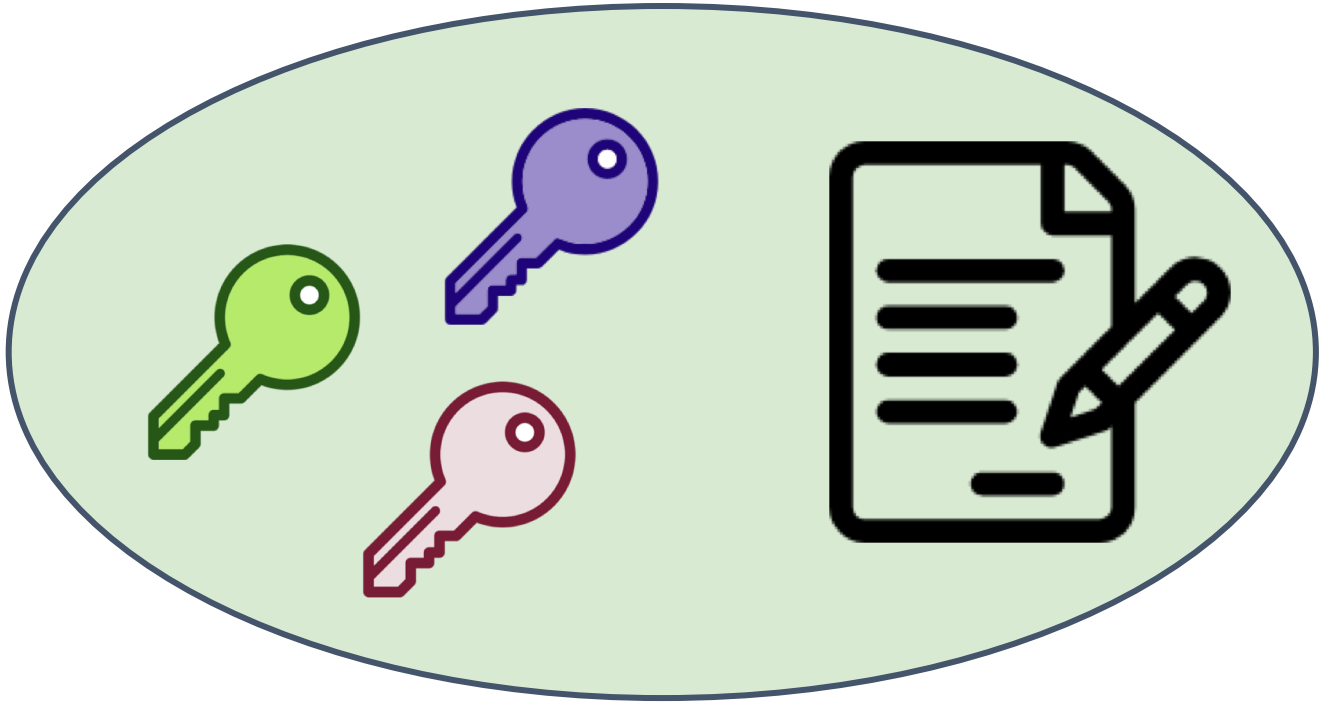
- Private key (!danger)
- Keystore
- Mnemonic Phrase

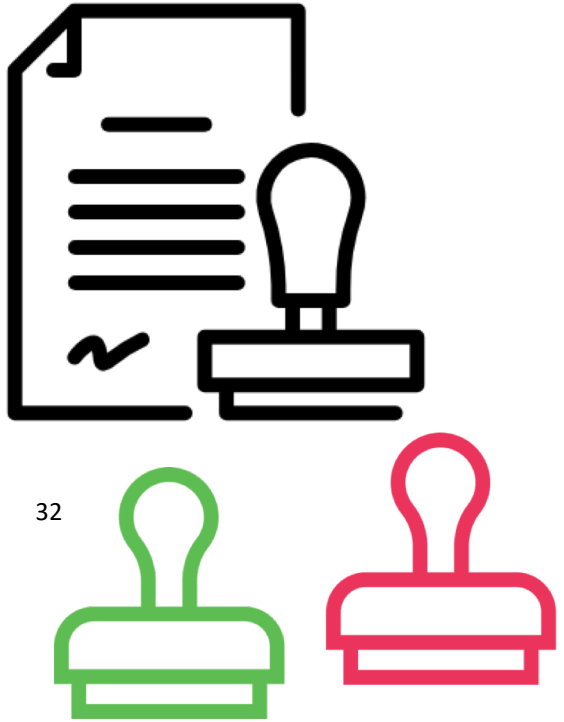

Mnemonic seed phrase:
begin fire hire matrix extend rude slim gauge cheese night crouch nerve
Private key:
99228c09a1320a7c7e43c290b1a8e032b4c4c2f4b91c97ee3a2cb99308943059
Public key:
e736055153ae191a7a782e07cd3389bbfe154621fb79bbe3eb5ab72ddc491299
2f87d629a4d10510a37e1ddd02d6918bbd00b0f0de2f7bd0cda280e4f15471e9
Ethereum address:
0xc1d237C49864CBDCe23fcdF6b191ad2661387CA6

What is a **valid** transaction?



Multisig transaction (m-of-n)



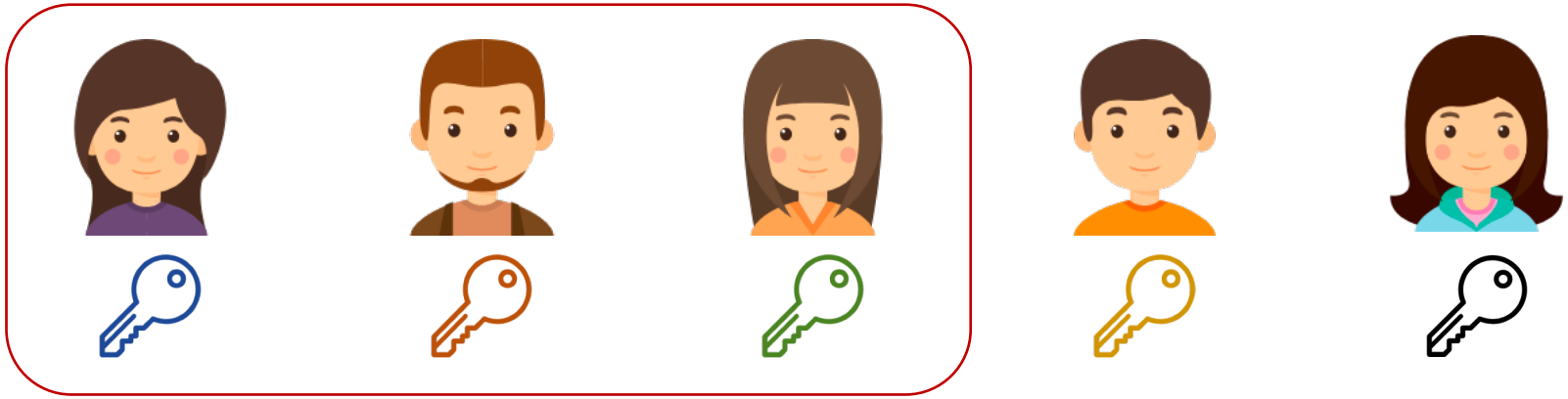


- Higher TX fee
- No privacy

Multi-Signature Transaction

1. Raw Tx generation

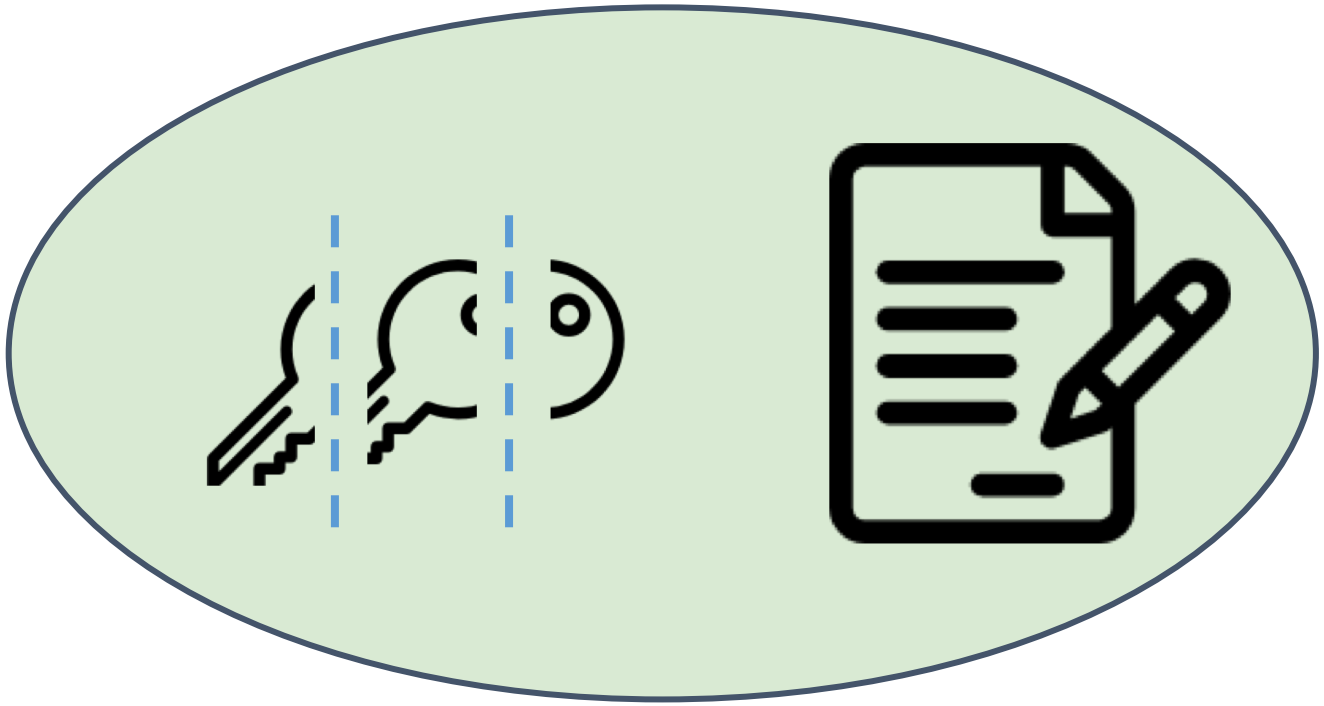
2. Sign Tx



3. Get enough signatures

- 俗稱的多簽交易
- 優點
  - 提供需要多簽的交易，避免單點故障或攻擊
  - 資產保管在自身
- 缺點
  - 以 BTC 來說，交易的大小會比較大，因為將多個簽名的長度一併算上去
    - 手續費高
    - 交易肥，也連帶影響區塊能裝的交易數目
  - 以 ETH 來說，因為實現在合約之中，所以轉帳必須透過 internal transfer 而非原生的交易
    - 需要耗費 gas
    - 某些交易所不支援 internal transfer 的入帳
  - 不論對 BTC 或 ETH 的使用者而言，都需要保管私鑰
  - 需要溝通的回合數多
  - 隱私性差，因為誰有參與都能夠從簽名辨識

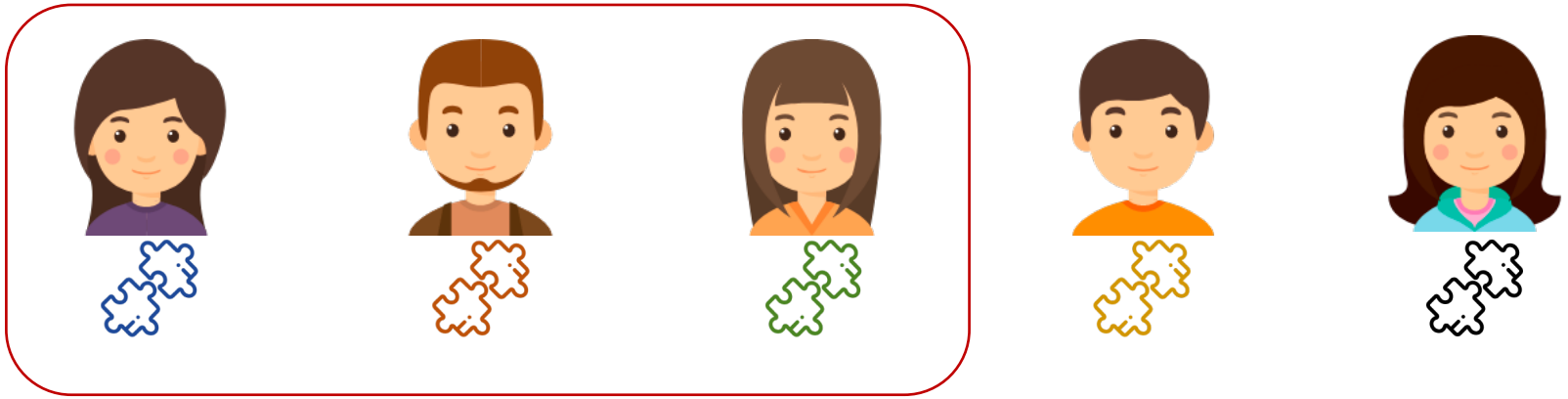
Threshold **key** sharing



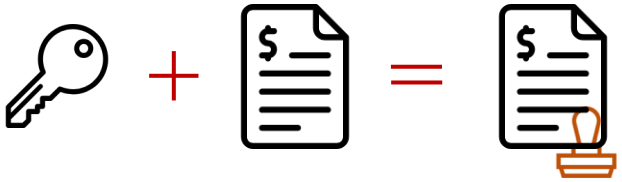
Threshold Key-Split Scheme

1. Raw Tx generation

2. Get enough shares to cerate the **key**

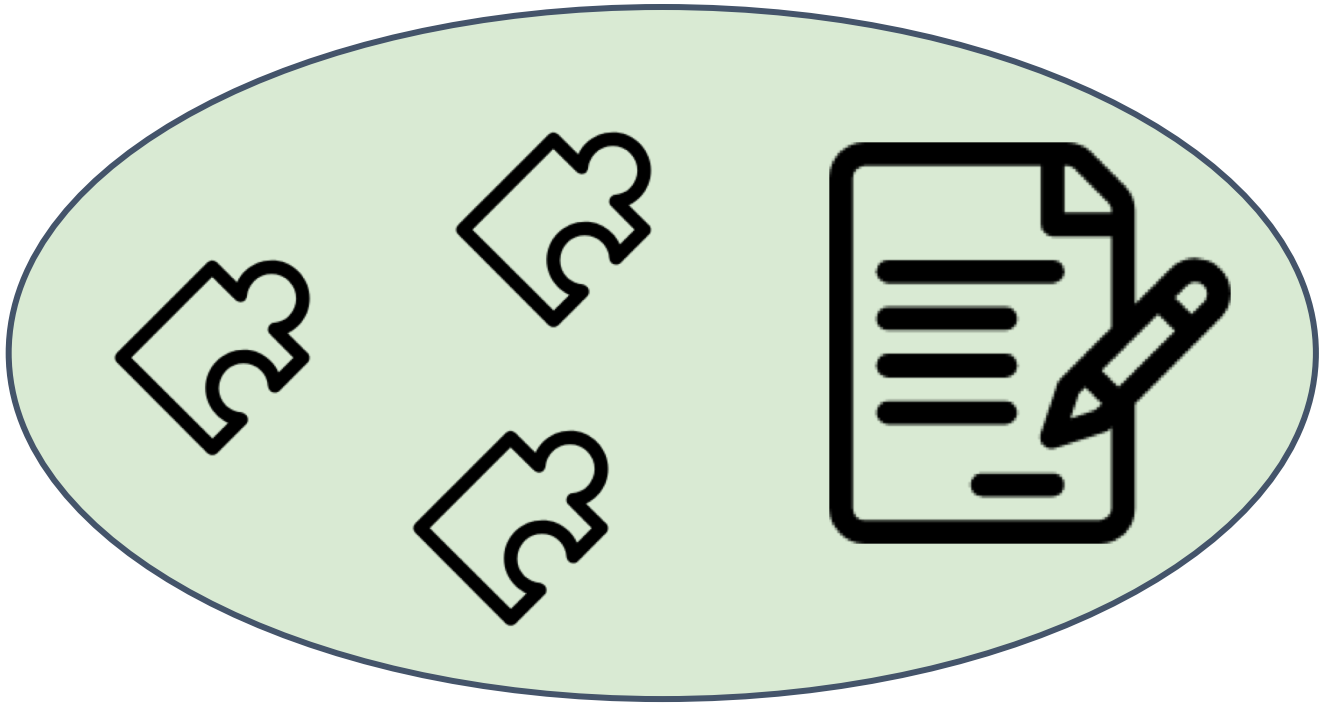


3. Recover the key and sign Tx



- 關鍵在將 key 切成 n 份，但需要搜集足夠的 m 個線索才能重新將 key 組回來
- 優點
  - 不論對 BTC 或 ETH 的交易，因為都是在 key 切份，所以不用管簽名演算法是什麼都能相容
  - 私鑰沒有存放在任何人或裝置上，存的只有 Secret share
  - 容易實現一個簽名的原生交易
  - 隱私性較佳
- 缺點
  - 當要重建 key 的時候，需要搜集 share，任何人只要搜集足夠數量，就能還原回 key
  - 實現在軟體上可能被 side channel attack (從記憶體讀出 key)
  - 當存放 share 的人不同，問題會很嚴重，除非這些人足夠被信任，不然很難判別誰洩露
  - 有 Single Point of Failure 的風險性 (機器的安全很重要)
  - 需要溝通的回合數多
  - audit 相對較麻煩，紀錄誰拿到 share 以及順序很重要
  - 資產保管在他人手上

Threshold **signature**



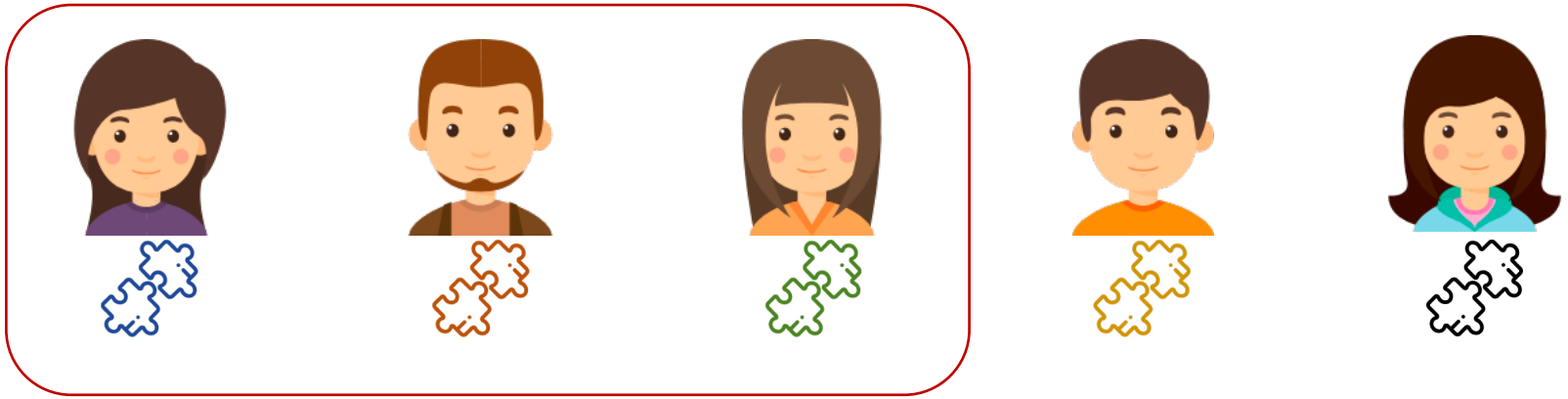
Private key will not be reconstructed.

Ephemeral puzzle

Threshold Signature Scheme

1. Raw Tx generation

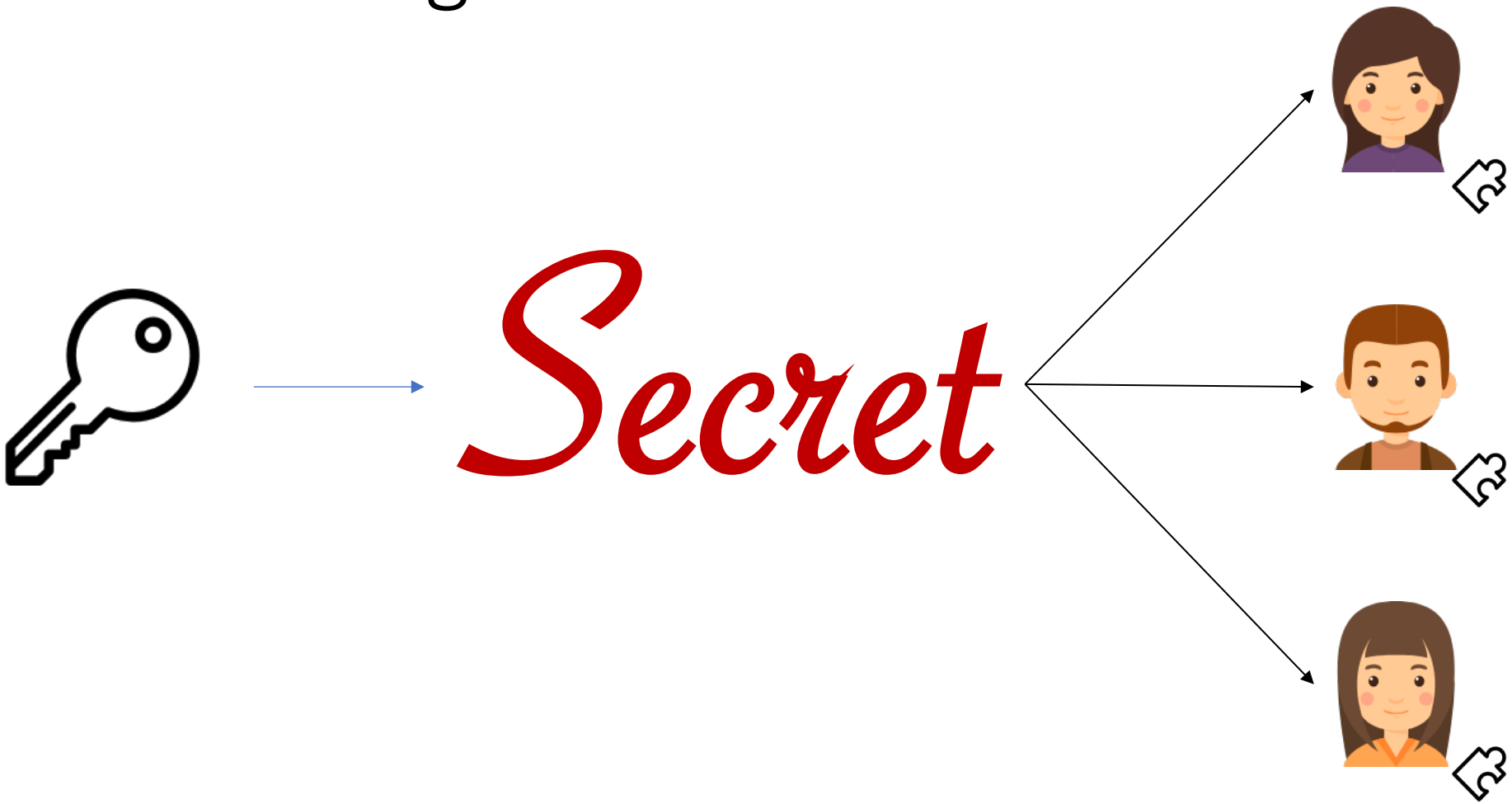
2. Get enough shares to cerate the **signature**



3. Tx + signature

- 每個人一樣會有一份 secret share，但是這個 share 最後只會拼湊出一個簽名
- 優點:
  - 過程中沒有私鑰露出的空間
  - 不會因為有人離職或加入，要重新計算地址或私鑰，前兩種方法需要
  - 隱私性較佳
- 缺點
  - 需要溝通的回合數多
  - audit 相對較麻煩，要記錄誰拿過 share 及順序
  - 對於不同的簽名演算法，會需要重新設計秘密拆分，在不影響既有的 trap-door function 的難度下

Secret sharing



Shamir's Secret Sharing

Example

- ✓(3,5) secret sharing
- ✓K=11, p=17
- ✓Construct a degree 2 random polynomial

  $F(x) = K + a_1x + a_2x^2 \bmod p$

- ✓For a random choice $a_1=8$, $a_2=7$

  $F(x) = 11 + 8x + 7x^2 \bmod 17$

- ✓Share distribution

  $K_1 = F(1) = 7\times1^2 + 8\times1 + 11 \equiv 9 \pmod{17}$
  $K_2 = F(2) = 7\times2^2 + 8\times2 + 11 \equiv 4 \pmod{17}$
  $K_3 = F(3) = 7\times3^2 + 8\times3 + 11 \equiv 13 \pmod{17}$
  $K_4 = F(4) = 7\times4^2 + 8\times4 + 11 \equiv 2 \pmod{17}$
  $K_5 = F(5) = 7\times5^2 + 8\times5 + 11 \equiv 5 \pmod{17}$
  K_1, K_2, K_3, K_4, K_5 : shares given to $(P_1,\ldots,P_5)$

Shamir's Secret Sharing

Example

- ✓(3,5) secret sharing
- ✓K=11, p=17
- ✓Construct a degree 2 random polynomial

  $F(x) = K + a_1x + a_2x^2 \bmod p$
- ✓For a random choice $a_1=8$, $a_2=7$

  $F(x) = 11 + 8x + 7x^2 \bmod 17$
- ✓Share distribution

  $K_1 = F(1) = 7\times1^2 + 8\times1 + 11 \equiv 9 \quad \bmod 17$

  $K_2 = F(2) = 7\times2^2 + 8\times2 + 11 \equiv 4 \quad \bmod 17$

  $K_3 = F(3) = 7\times3^2 + 8\times3 + 11 \equiv 13 \quad \bmod 17$

  $K_4 = F(4) = 7\times4^2 + 8\times4 + 11 \equiv 2 \quad \bmod 17$

  $K_5 = F(5) = 7\times5^2 + 8\times5 + 11 \equiv 5 \quad \bmod 17$

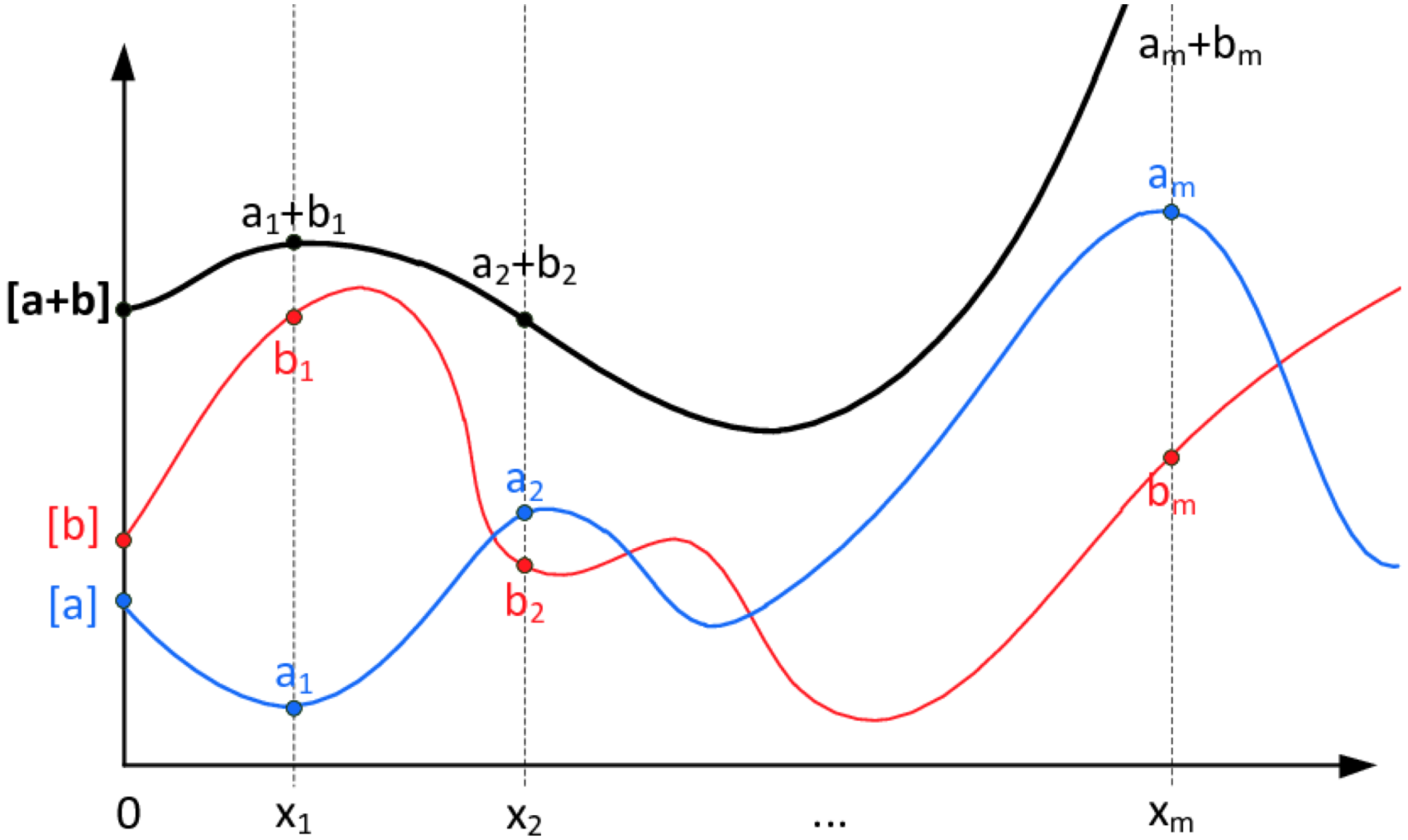
  K_1, K_2, K_3, K_4, K_5 : shares given to $(P_1,\ldots,P_5)$

Using the Lagrange interpolation

For $\Lambda=(K_1, K_2, K_3)$

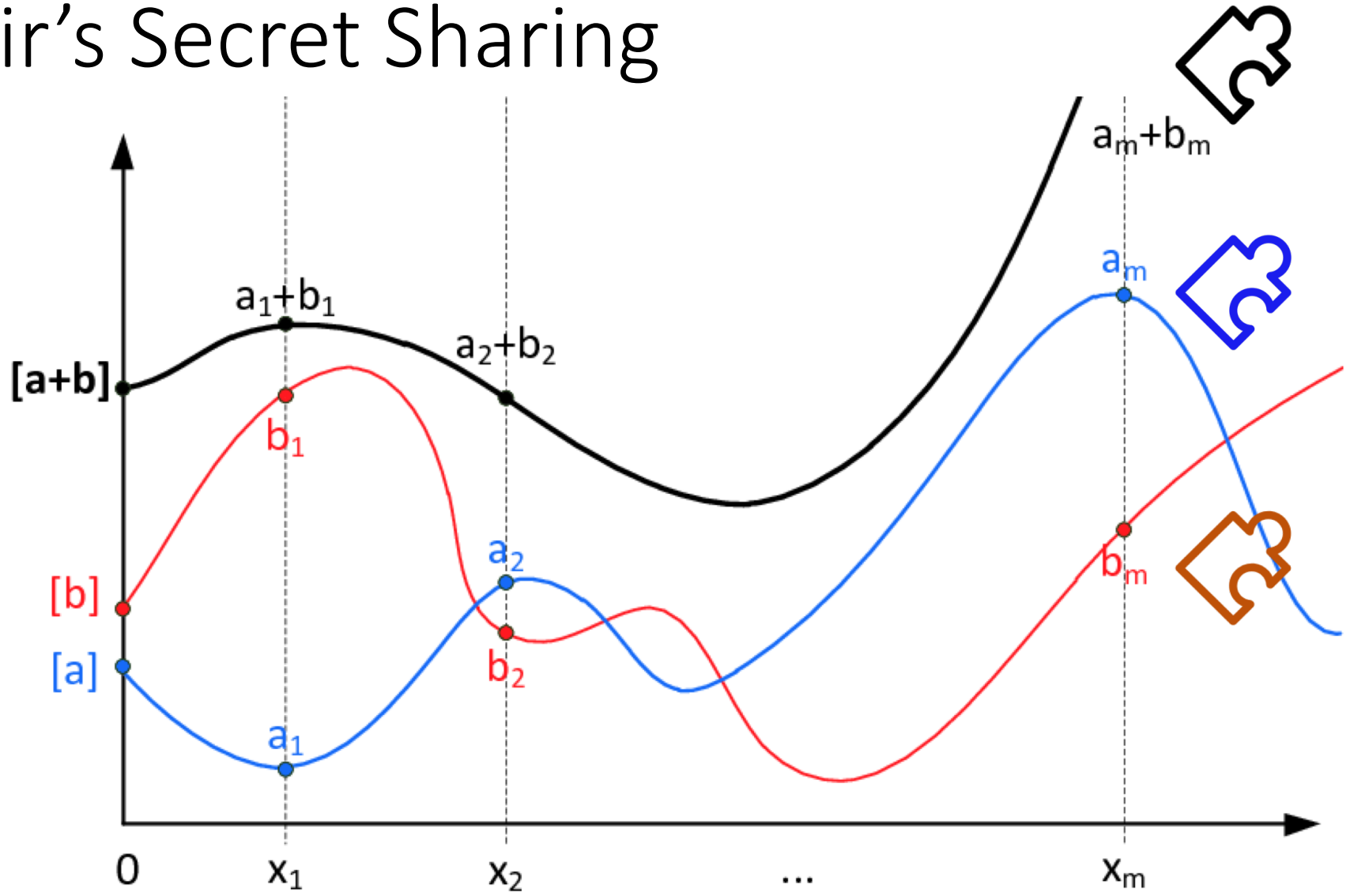
$$K = K_1\left(\frac{2}{2-1}\frac{3}{3-1}\right) + K_2\left(\frac{1}{1-2}\frac{3}{3-2}\right) + K_3\left(\frac{1}{1-3}\frac{2}{2-3}\right)$$
$$= 9\cdot3 + 4\cdot(-3) + 13\cdot1 \bmod 17 = 11$$

Shamir’s Secret Sharing



https://www.researchgate.net/figure/Illustration-of-Shamirs-secret-sharing-scheme-The-secret-values-a-and-b-are-encoded_fig14_267171685

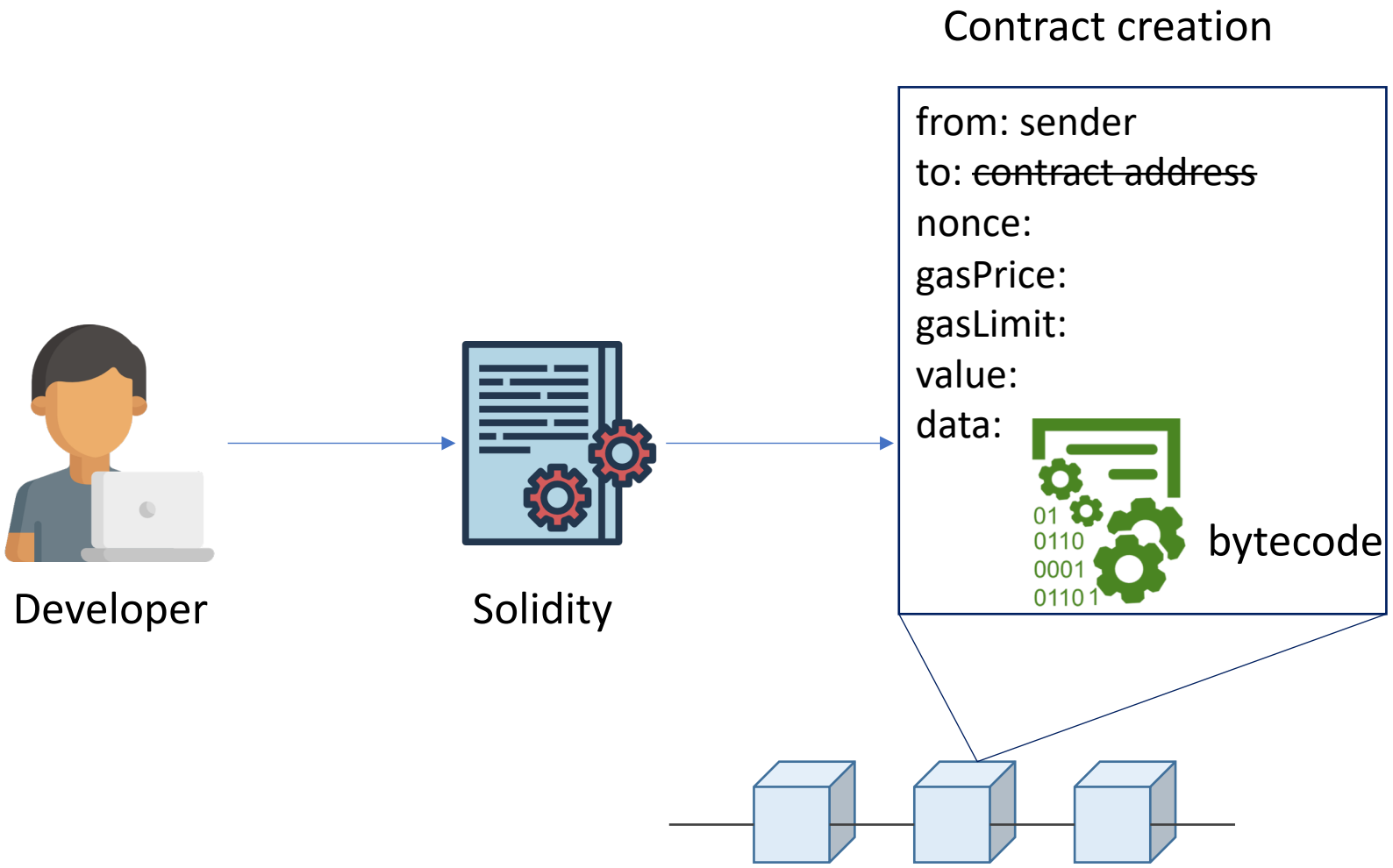
Shamir’s Secret Sharing



https://www.researchgate.net/figure/Illustration-of-Shamirs-secret-sharing-scheme-The-secret-values-a-and-b-are-encoded_fig14_267171685

Contract dev review

Contract development



1. Solidity version
2. Contract vulnerability
3. Enough funds
4. Reasonable gas price
5. Node management
6. Contract maintenance
7. Data migration
8. Data confidentiality
9. Data privacy
10. External event
11. Optimized gas usage
12. Test

Integer Overflow and Underflow

```
mapping (address => uint256) public balanceOf;

// INSECURE
function transfer(address _to, uint256 _value) {
    /* Check if sender has balance */
    require(balanceOf[msg.sender] >= _value);
    /* Add and subtract new balances */
    balanceOf[msg.sender] -= _value;
    balanceOf[_to] += _value;
}

// SECURE
function transfer(address _to, uint256 _value) {
    /* Check if sender has balance and for overflows */
    require(balanceOf[msg.sender] >= _value && balanceOf[_to] + _value >= balanceOf[_to]);

    /* Add and subtract new balances */
    balanceOf[msg.sender] -= _value;
    balanceOf[_to] += _value;
}
```


https://consensys.github.io/smart-contract-best-practices/known_attacks/

Or insufficient funds for gas * price + value

Out of gas

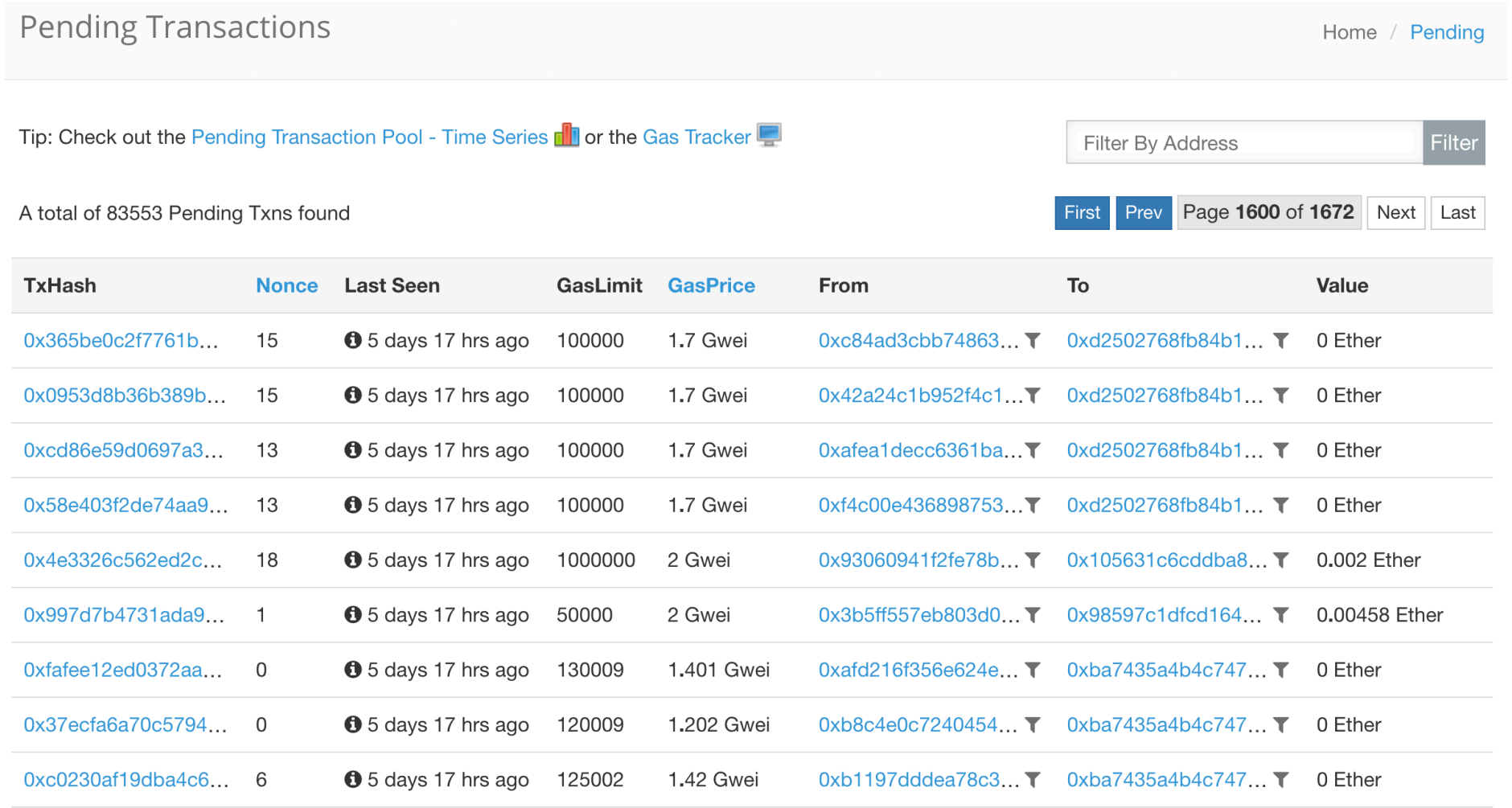
Transaction Information

Tools & Utilities

TxHash:	0x242771b2ed0f643b8d7b018b62affa75e4f93e2516bad0e1109c6e3c41647f08
TxReceipt Status:	Fail
Block Height:	5514060 (1356399 Block Confirmations)
TimeStamp:	228 days 17 hrs ago (Apr-27-2018 09:22:31 AM +UTC)
From:	0x04b01d535e69d5631d68029447eab709eea589a8
To:	Contract 0xc4c376bd3bac6e9e0aaea83b32dcab831258dbb3
	Warning! Error encountered during contract execution [**Out of gas**]
Value:	0.0755 Ether ($6.68) - [CANCELLED]
Gas Limit:	21000
Gas Used By Transaction:	21000 (100%)
Gas Price:	0.000000005 Ether (5 Gwei)
Actual Tx Cost/Fee:	0.000105 Ether ($0.009284)
Nonce & {Position}:	8 | {52}
Input Data:	0x

https://etherscan.io/tx/0x242771b2ed0f643b8d7b018b62affa75e4f93e2516bad0e1109c6e3c41647f08

Pending Transactions



Pending Transactions

Home / Pending

Tip: Check out the Pending Transaction Pool - Time Series or the Gas Tracker

Filter By Address | Filter

A total of 83553 Pending Txns found

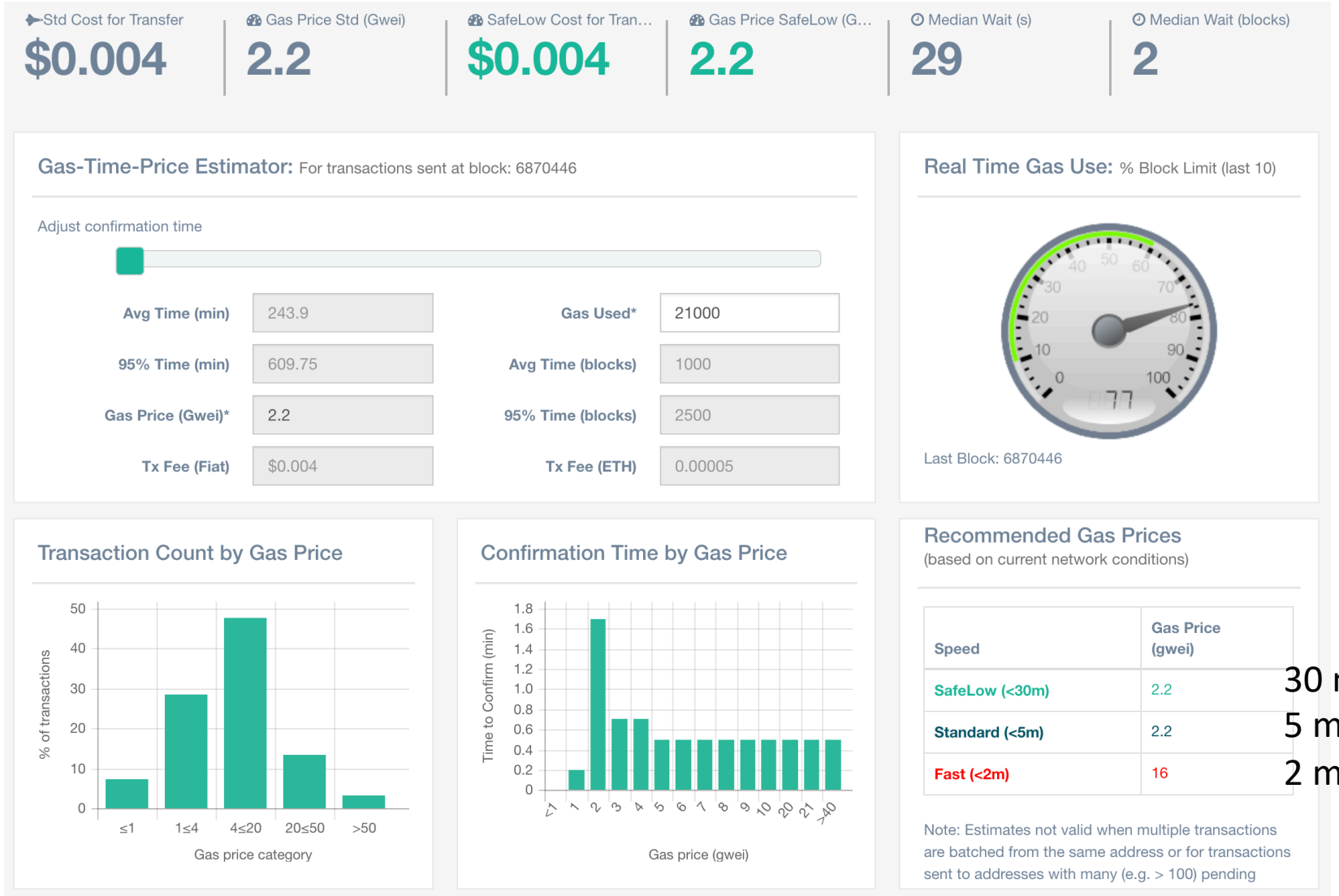
First | Prev | Page 1600 of 1672 | Next | Last

TxHash	Nonce	Last Seen	GasLimit	GasPrice	From	To	Value
0x365be0c2f7761b...	15	5 days 17 hrs ago	100000	1.7 Gwei	0xc84ad3cbb74863...	0xd2502768fb84b1...	0 Ether
0x0953d8b36b389b...	15	5 days 17 hrs ago	100000	1.7 Gwei	0x42a24c1b952f4c1...	0xd2502768fb84b1...	0 Ether
0xcd86e59d0697a3...	13	5 days 17 hrs ago	100000	1.7 Gwei	0xafea1decc6361ba...	0xd2502768fb84b1...	0 Ether
0x58e403f2de74aa9...	13	5 days 17 hrs ago	100000	1.7 Gwei	0xf4c00e436898753...	0xd2502768fb84b1...	0 Ether
0x4e3326c562ed2c...	18	5 days 17 hrs ago	1000000	2 Gwei	0x93060941f2fe78b...	0x105631c6cddba8...	0.002 Ether
0x997d7b4731ada9...	1	5 days 17 hrs ago	50000	2 Gwei	0x3b5ff557eb803d0...	0x98597c1dfcd164...	0.00458 Ether
0xfafee12ed0372aa...	0	5 days 17 hrs ago	130009	1.401 Gwei	0xafd216f356e624e...	0xba7435a4b4c747...	0 Ether
0x37ecfa6a70c5794...	0	5 days 17 hrs ago	120009	1.202 Gwei	0xb8c4e0c7240454...	0xba7435a4b4c747...	0 Ether
0xc0230af19dba4c6...	6	5 days 17 hrs ago	125002	1.42 Gwei	0xb1197dddea78c3...	0xba7435a4b4c747...	0 Ether

https://etherscan.io/txsPending?&m=&p=1600

https://www.etherchain.org/api/gasPriceOracle

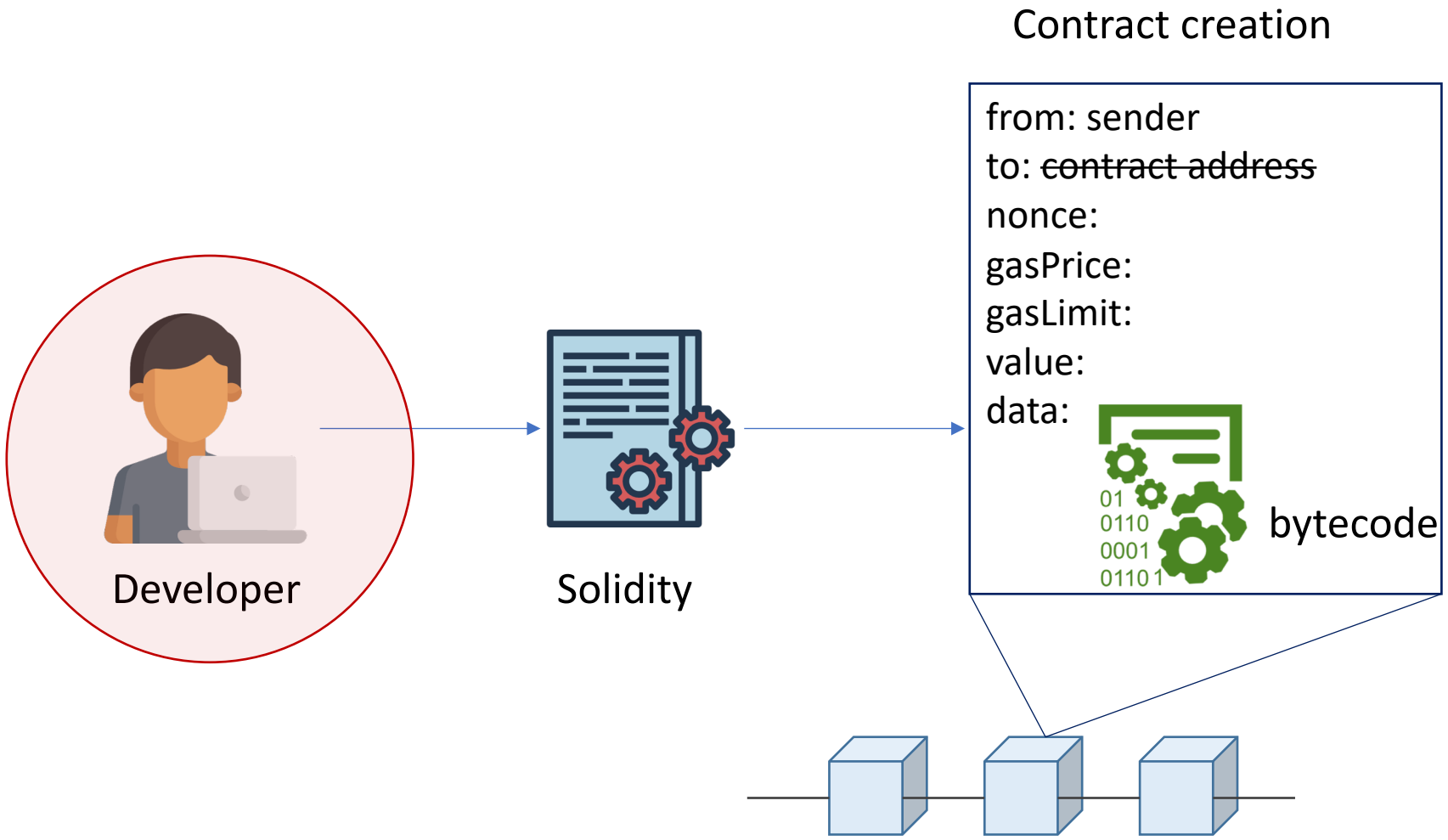
gasPrice prediction



30 mins
5 mins
2 mins

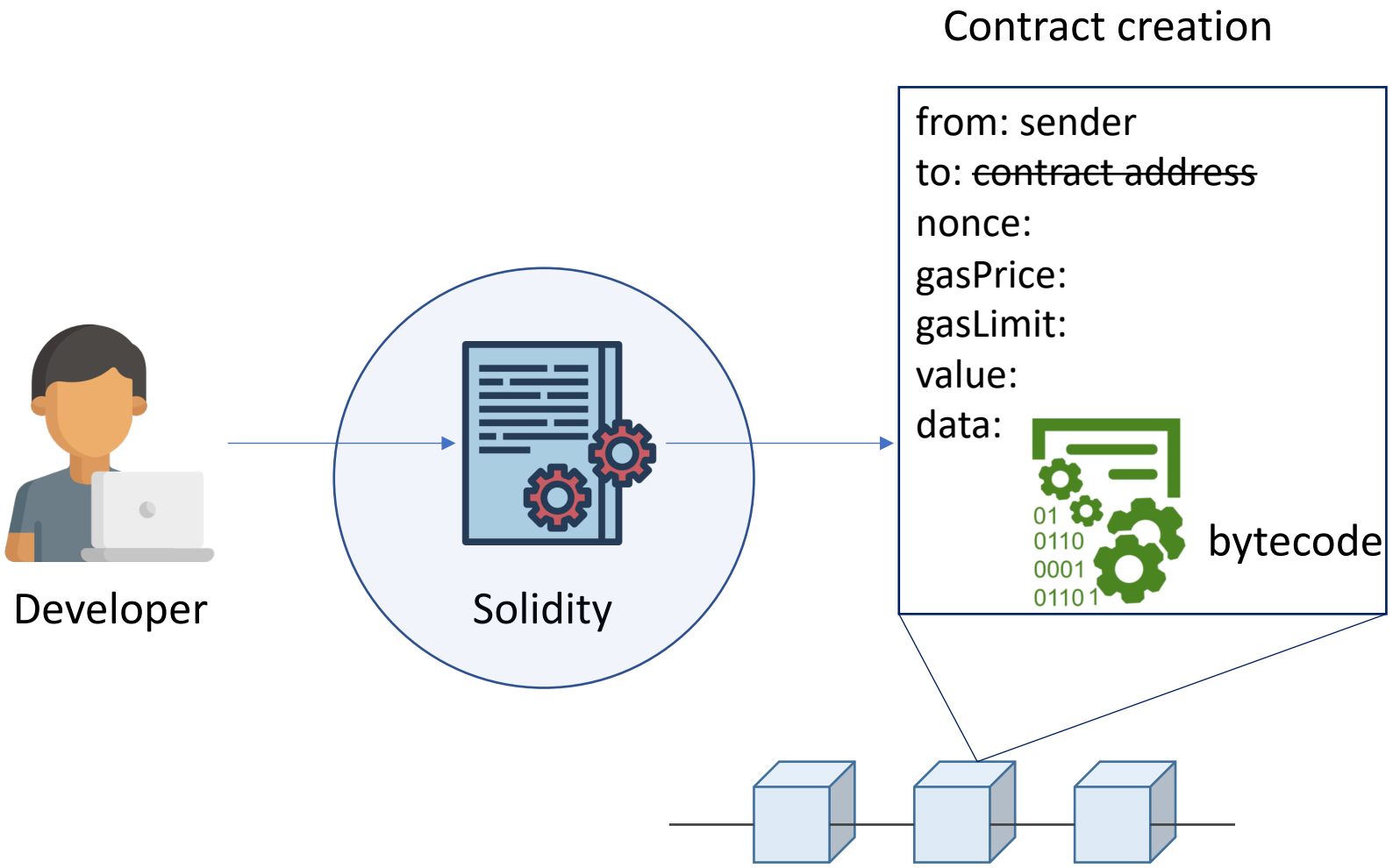
https://ethgasstation.info/

Contract development



1. Solidity version
2. Contract vulnerability
3. Enough funds
4. Reasonable gas price
5. Node management
6. Contract maintenance
7. Data migration
8. Data confidentiality
9. Data privacy
10. External event
11. Optimized gas usage
12. Test

Contract development



1. Solidity version
2. Contract vulnerability
3. Enough funds
4. Reasonable gas price
5. Node management
6. Contract maintenance
7. Data migration
8. Data confidentiality
9. Data privacy
10. External event
11. Optimized gas usage
12. Test

Contract execution

Contract creation

from: sender
to: ~~contract address~~
nonce:
gasPrice:
gasLimit:
value:
data:

bytecode

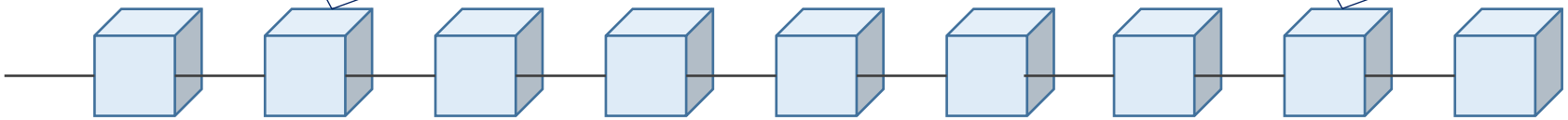
Contract execution

from: sender
to: contract address
nonce:
gasPrice:
gasLimit:
value:
data:

bytecode

Feed data

```
if condition {
    exec something
}
```



Upgrade smart contract

1. Data migration
2. User experience

Contract creation

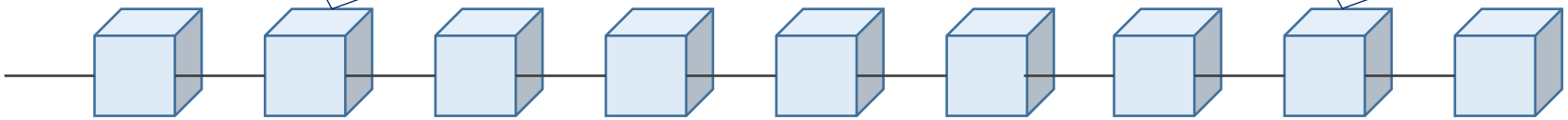
from: sender
to: ~~contract address~~
nonce:
gasPrice:
gasLimit:
value:
data:

bytecode

Change to new contract

from: sender
to: ~~contract address~~
nonce:
gasPrice:
gasLimit:
value:
data:

bytecode



Contract gets hacked

- The DAO
- Parity Wallet

https://www.youtube.com/watch?v=VUH4gRDQYsA