Blockchain 101 – Introduction for Developers

Razi Rais | Microsoft

@razibinrais

www.razibinrais.com

About Me

Microsoft

www.razibinrais.com

@razibinrais

Join THIS group!

www.meetup.com/msftcloud

Meeting every month

Open to everyone!

What we going to cover today?

What is a Blockchain | How it works? | Accounts |Transactions | Smart Contracts | ETH

{Developer Focus}

What we NOT going to cover today?

Wallets | ICO's | Business Cases | Everything else

Level Set

Crypto 101

- Hashing
- Public Key Encryption

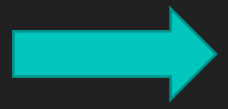
What is Hashing?

What is Hashing?

Example:

I want to have a cup of coffee

Input



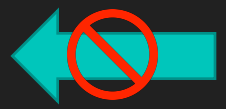
3f7f81df1a1d31cc1af434b711bd8e33b1ce

Hash

Similar input results in very different hash values

Also..

Hashing Function
f(x)



Hash

Strictly One Way

Common Hashing Algorithms

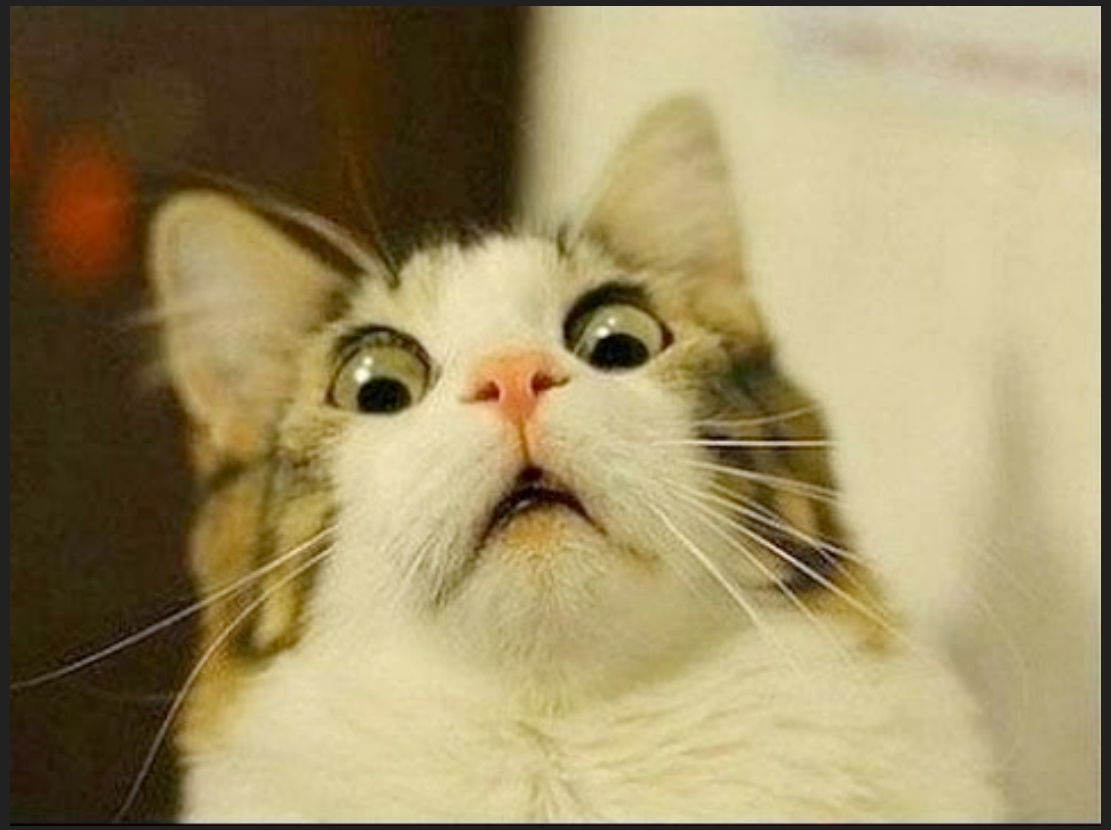
Secure Hashing Algorithm (SHA)

SHA3 | SHA3-224, **SHA3-256**, SHA3-384, SHA3-512, SHAKE128 and SHAKE256

SHA-2 |SHA-224, **SHA-256**, SHA-384, SHA-512, SHA-512/224 and SHA-512/256

Keccak256 ← Ethereum uses it. Similar to SHA3 but.. http://keccak.noekeon.org

MD2/4/5, SHAKE128/256/512. Many more explore http://emn178.github.io/online-tools/index.html

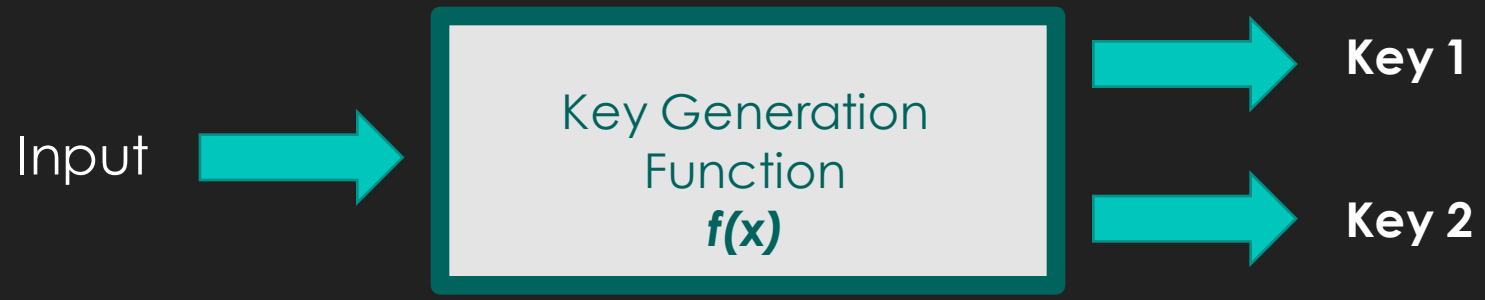


Public Key Encryption

How to send messages secretly?

How to verify message source?

Public Key Encryption



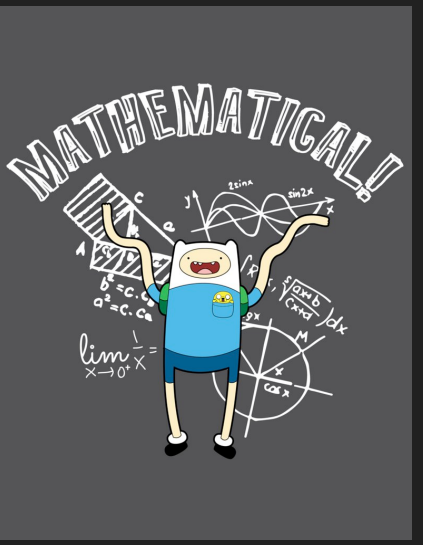
Public Key Encryption

Input

Key Generation Function
f(x)

Key 1

Key 2



Public Key Encryption

Rivest Shamir Adleman (RSA) | PKCS#1

Elliptic Curve Cryptography | ECDSA (**secp256k1**) | Others

Early Days | Homomorphic Encryption

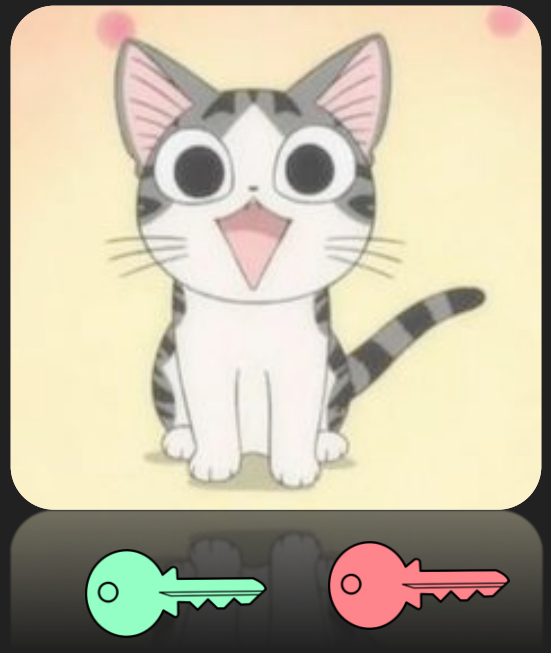
Public Key Encryption In Action!

Bob And Alice
World Domination Plan

Bob and Alice generates key pair

Bob generates a key pair

Alice generates a key pair



Bob's Public Key

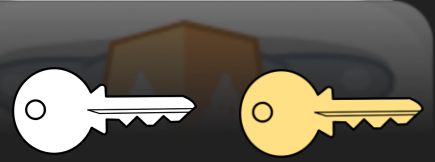
Bob's Private Key

Alice's Public Key

Alice's Private Key

Bob and Alice generates key pair

Bob generates a key pair



Bob's Public Key

Bob's Private Key

Alice generates a key pair

Alice's Public Key

Alice's Private Key

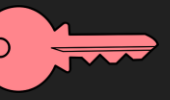
Bob and Alice share their Public Keys

Bob's Private Key

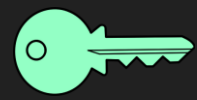
Bob's Public Key

Bob share his public key with Alice.

Alice's Public Key



Alice's Private Key



Alice's Public Key

Alice share her public key with Bob.

Bob's Public Key

Great!

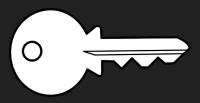
Bob And Alice
Lets send messages secretly!

Alice and Bob encrypted message exchange

Alice

Anarchy

Encryption Function



Bob's Public Key

Q198$2#(*N

Evil (Eve)

Decryption Function

Bob's Private Key

Anarchy

Bob

Bob has a concern?

How do I know that message was send by Alice and not Eve?

How about we do this….

Alice

(1) Hash the Message
(2) Sign the Message | Alice's Private Key
(3) Encrypt Message | Bob's Public Key
(4) Send All of Above to Bob

Bob

(1) Decrypt Message | Bob's Private Key
(2) Verify Signature | Alice's Public Key
(3) Alice's Message Hash == Bob's Message Hash
(4) All of above works? we are good!

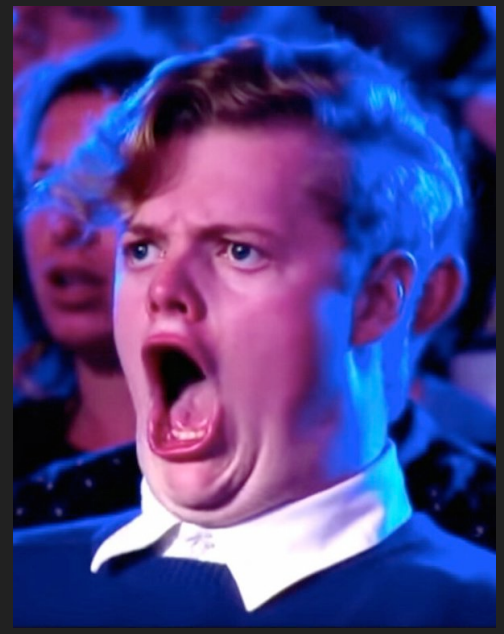
How about we do this….

Alice

(1) Hash the Message
(2) Sign the Message | Alice's Private Key
(3) Encrypt Message | Bob's Public Key
(4) Send All of Above to Bob

Bob

(1) Decrypt Message | Bob's Private Key
(2) Verify Signature | Alice's Public Key
(3) Alice's Message Hash == Bob's Message Hash
(4) All of above works? we are good!



Signing + Hashing + Encryption

Alice

Anarchy

Hashing

Signing

Encryption

BC1EFC

Alice's Private Key

Bob's Public Key

HASH: BC1EFC
SIG: 0E#N8OO
MSG: 0E#N8OO

Evil (Eve)

HASH: BC1EFC
SIG: 0E#N8OO
MSG: 0E#N8OO

Decryption

Verify Signature

Verify Hash

Bob's Private Key

Alice's Public Key

BC1EFC == BC1EFC

Anarchy

Bob

Eve …

Evil (Eve)

I will find new ways.. *Gradatim Ferociter*

Blockchain - Core Concepts

Others ..

Blockchain - Core Concepts

Visual Approach

Ethereum

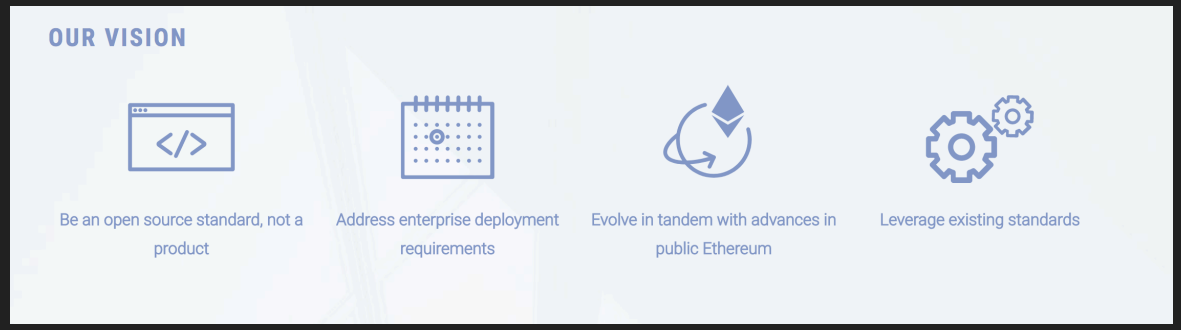
Project was bootstrapped in august 2014

Decentralized platform for Smart Contracts

Public/Private

www.ethereum.org/foundation

Enterprise Ethereum Alliance



https://entethalliance.org/members

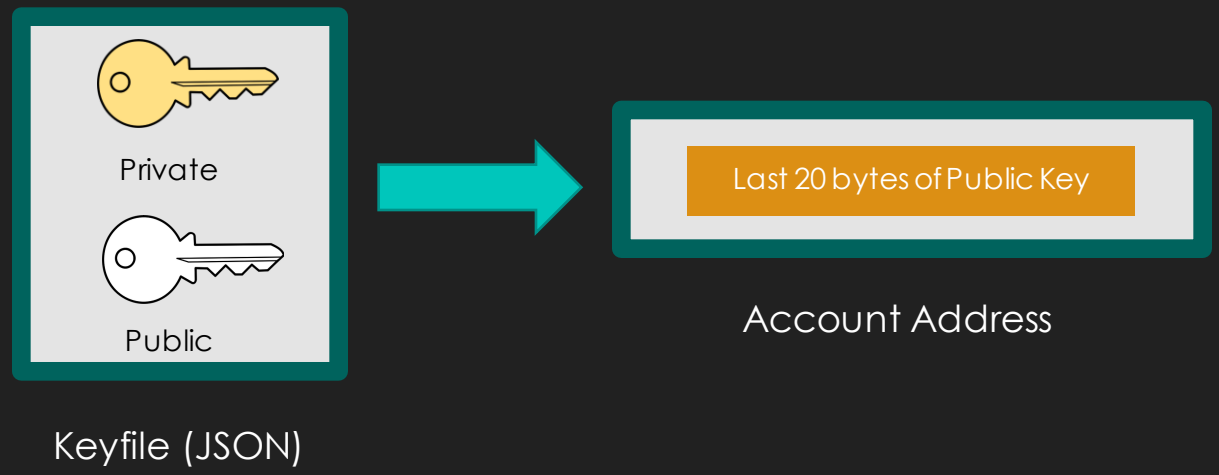
https://entethalliance.org/about

ENTERPRISE
ETHEREUM
ALLIANCE

Ethereum Accounts

Externally Owned Accounts | Contract Accounts

Externally Owned Accounts (EOA)



Never lose your private key!

How to get started with Ethereum?

Tools | **Truffle** | **Remix** | Others

Software | Eth | **Geth** | Parity | Others

Test/Deployment | TestNet | **Private** | Public

Transaction

Signed data package sent from an **externally owned account** to another account on the blockchain.

tx(recipient, sender-signature, value-in-ether, start-gas, gas-price)

Transaction

DEMO

Truffle

DEMO

Smart Contract

{ code } + state
<<Specific Address>>

EVM byte code
Solidity | High Level Language
LLL | Low level Language

Smart Contract

DEMO