Group No 2

Ethereum- A next generation Blockchain

Where It all started

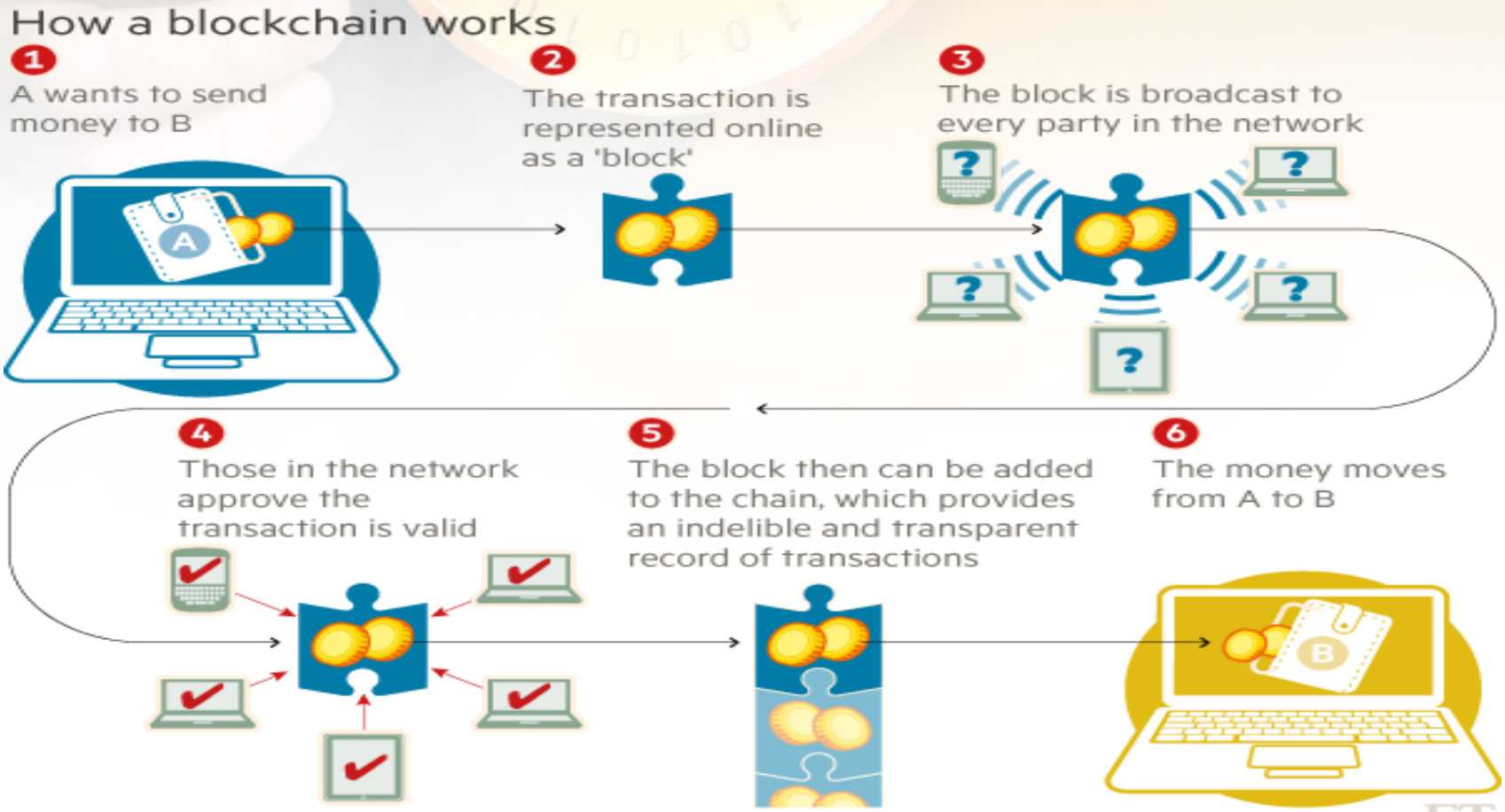
What is Block chain?

Digital messages (transactions) bundled into: ...

Blocks.

Blocks linked in a chain to form chronicle.

How it works???


How a blockchain works
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B
FT

What is Ethereum?

- Ethereum is the largest decentralized software platform that allows you to build smart contracts and decentralized applications without any downtime and without any third party interference.
- It forms a decentralized and Peer-to-Peer network where all the applications run on a public ledger.

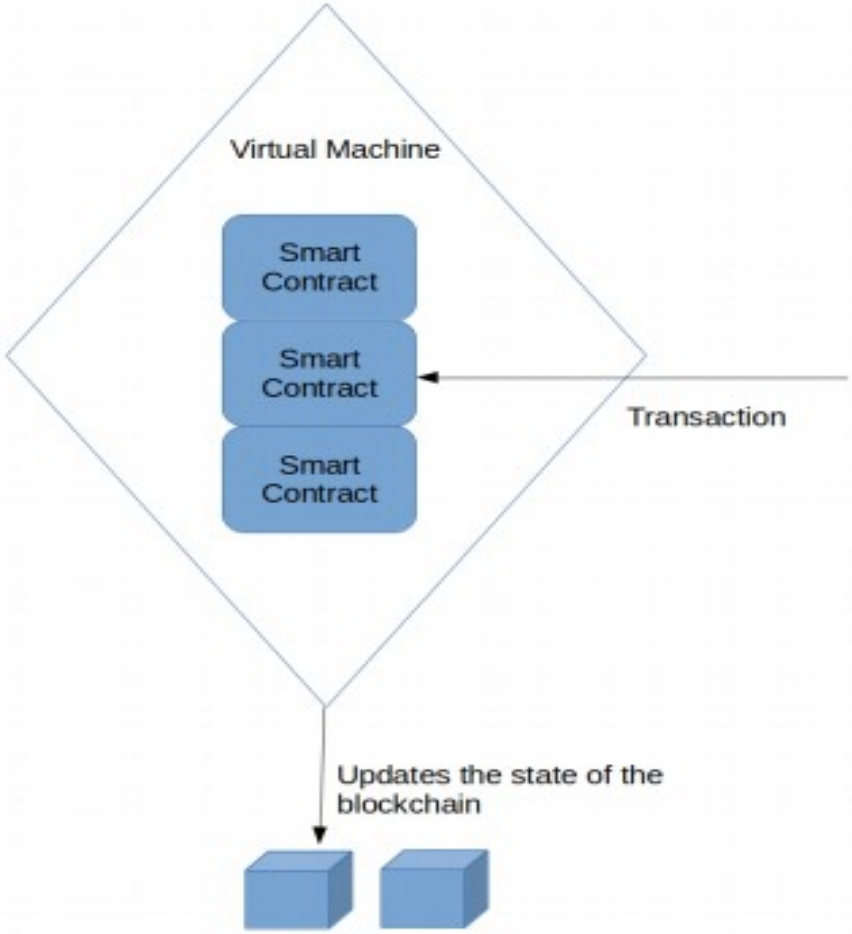
The concep

- It is a Block Chain..... With a few tiny additions

  - A built-in programming language Two types of accounts
  - ○ User accounts (controlled by private keys)
    ○ Contracts (controlled by code)

    Anyone can create an application with any rules by
  - defining it as a contract

Ethereum Node



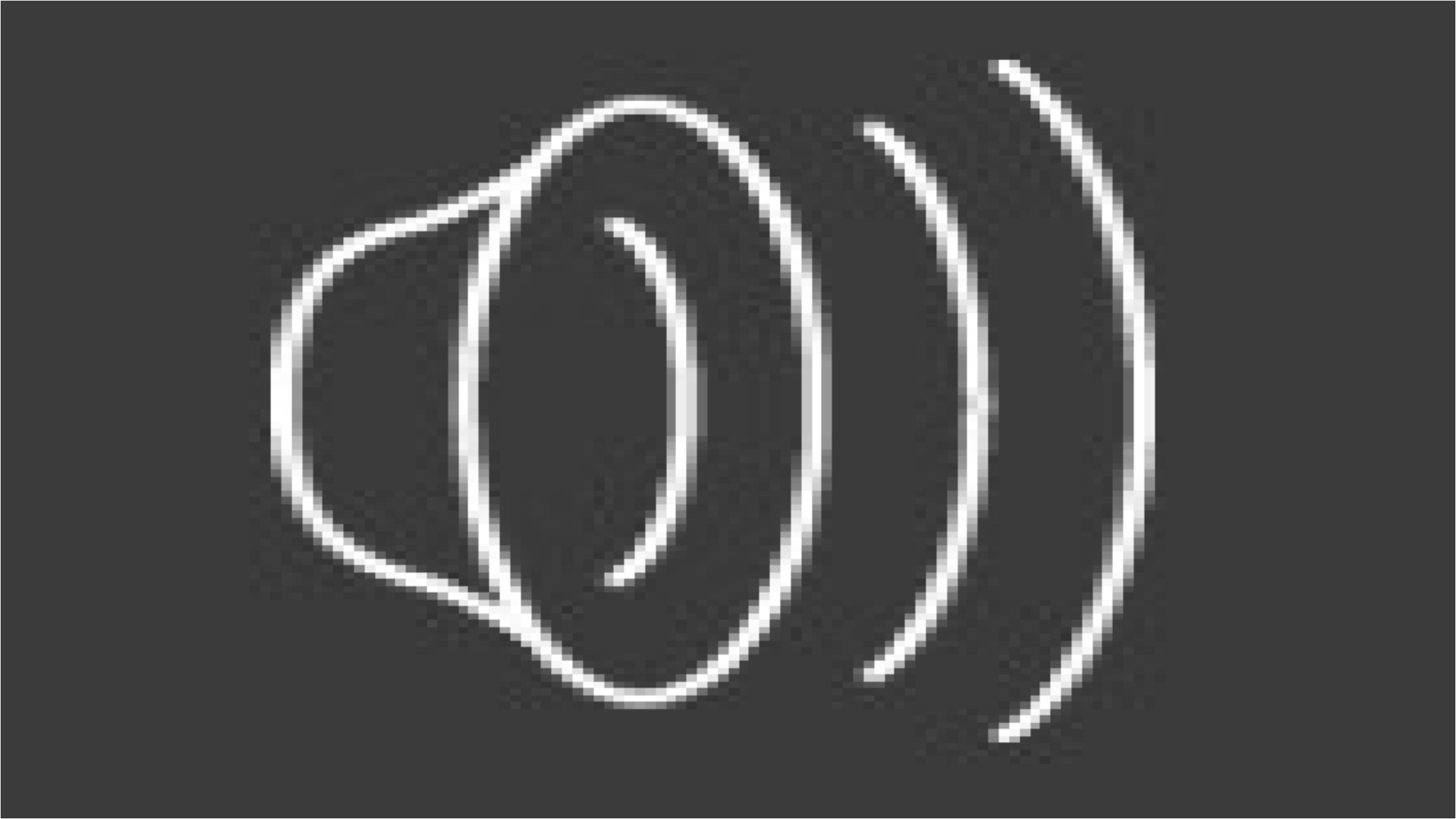
In Simple terms……

Internet is to communication as Ethereum is to agreements

Bitcoin vs Ethereum

- How is Ethereum different from Bitcoin ?

More general, not just a currency each node has a virtual machine forming a planetary scale computer the virtual machines run "smart contracts" users can call functions on the contract = TRANSACTIONS



Block Chain 2.0- Ethereum

- Blockchain with expressive programming language
  - Programming language makes it ideal for smart contracts
- Why?
  - Most public blockchains are cryptocurrencies
    - Can only transfer coins between users
  - Smart contracts enable much more applications

How Ethereum Works?

- Two types of account:
  - **Normal account** like in Bitcoin
    - has balance and address
  - **Smart Contract account**
    - like an object: containing (i) code, and (ii) private storage (key-value storage)
    - Code can
      - Send ETH to other accounts Read/write storage
      - Call (ie. start execution in) other contracts
      -

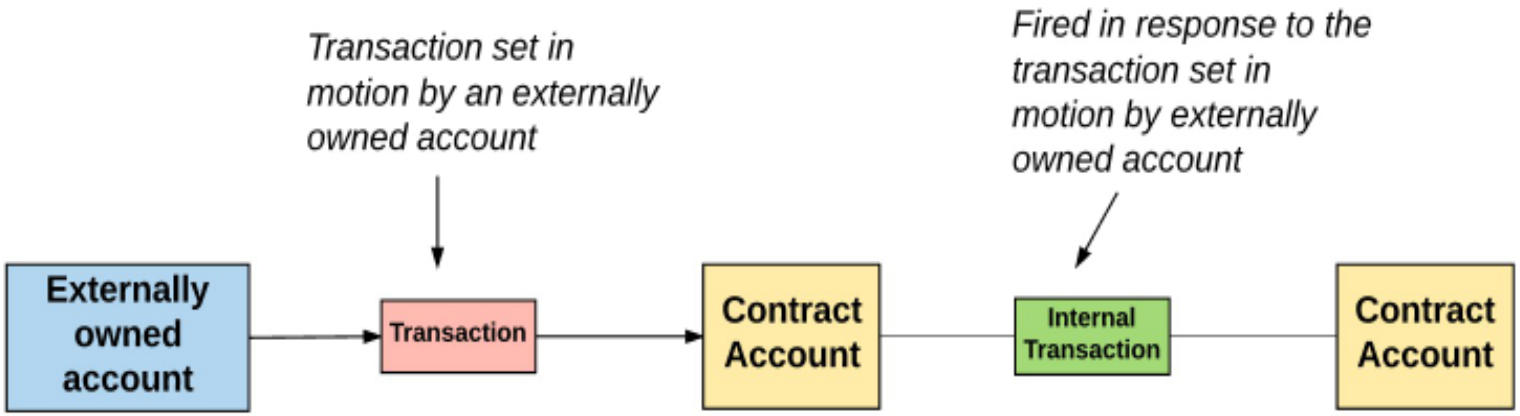
Transaction in Ethereum

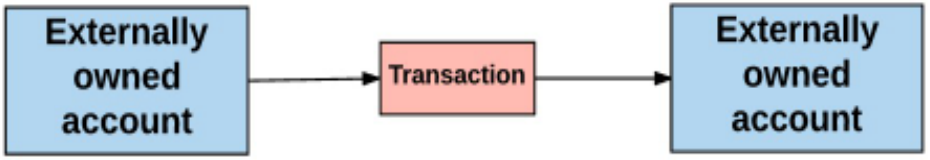
- Normal transactions like Bitcoin transactions
  - Send tokens between accounts
- Transactions to contracts
  - like function calls to objects
  - specify which object you are talking to, which function, and what data (if possible)
- Transactions to create contracts

Transaction in Ethereum

- **nonce** (anti-replay-attack)
- **to** (destination address)
- **value** (amount of ETH to send)
- **data** (readable by contract code) **gasprice**
- (amount of ether per unit gas) **startgas**
- (maximum gas consumable) **v, r, s** (ECDSA
- signature values)

Transaction in Ethereum





Block chain State

- Bitcoin's state consists of key value mapping addresses to account balance

Address	Balance (BTC)
0x123456...	10
0x1a2b3f...	1
0xab123d...	1.1

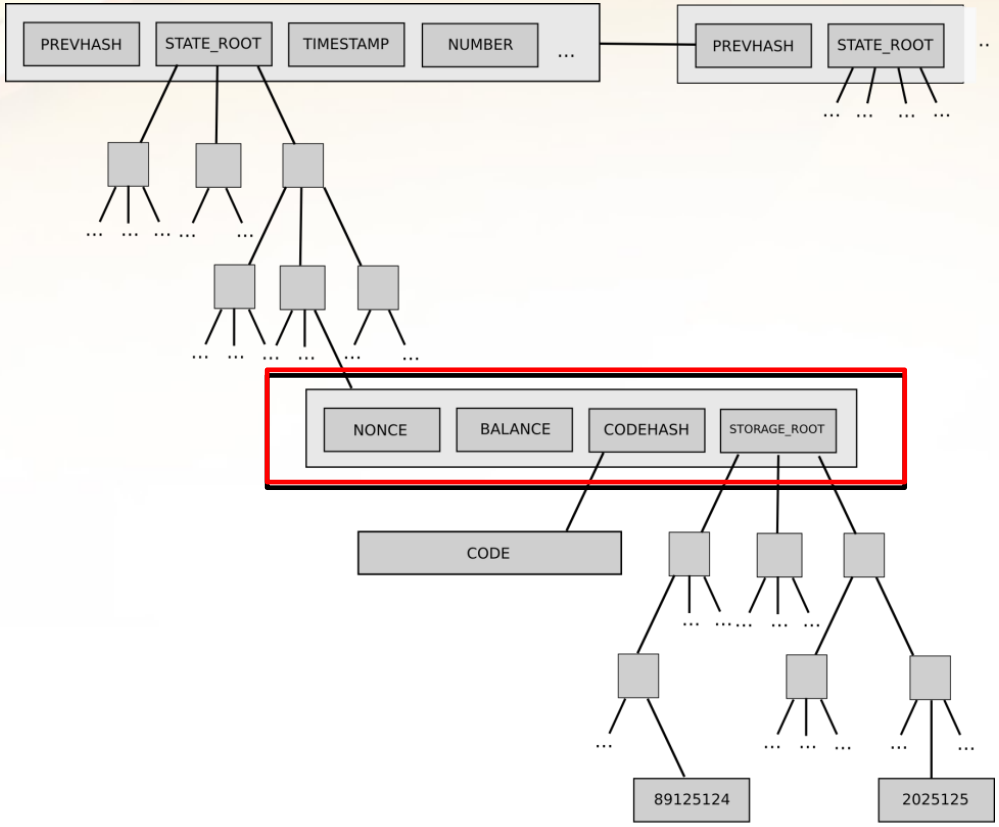
- Ethereum's state consists of key value mapping addresses to account objects

Address	Object
0x123456...	X
0x1a2b3f...	Y
0xab123d...	Z

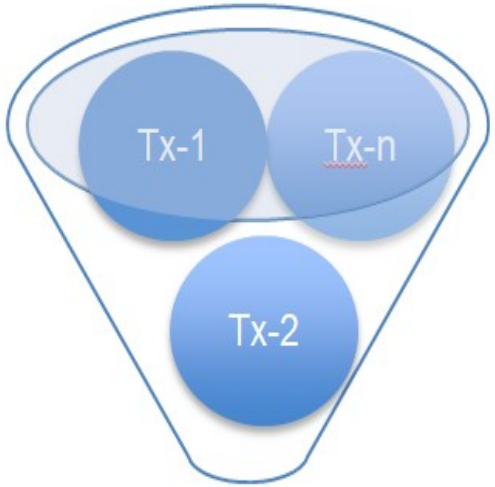
Blockchain != Blockchain state

Account Object

- Every account object contains 4 pieces of data:
  - Nonce Balance
  - Code hash (code =
  - empty string for normal accounts)
    Storage trie root
  -



Block Mining



Miners

Block

- Previous block
- A set of TXs
- New State Root
- Receipt Root
- Nonce

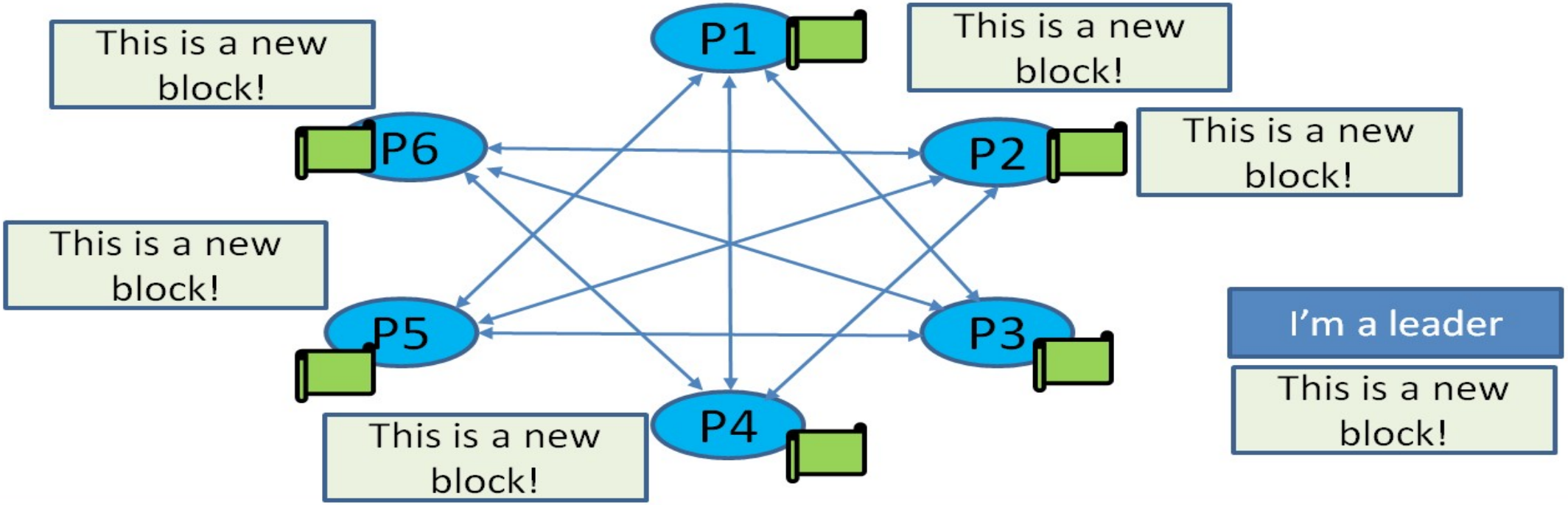
Verify transactions & execute all code to update the state

SHA3(Block) < D

Broadcast Block

Code execution

- Every (full) node on the blockchain processes every transaction and stores the entire state

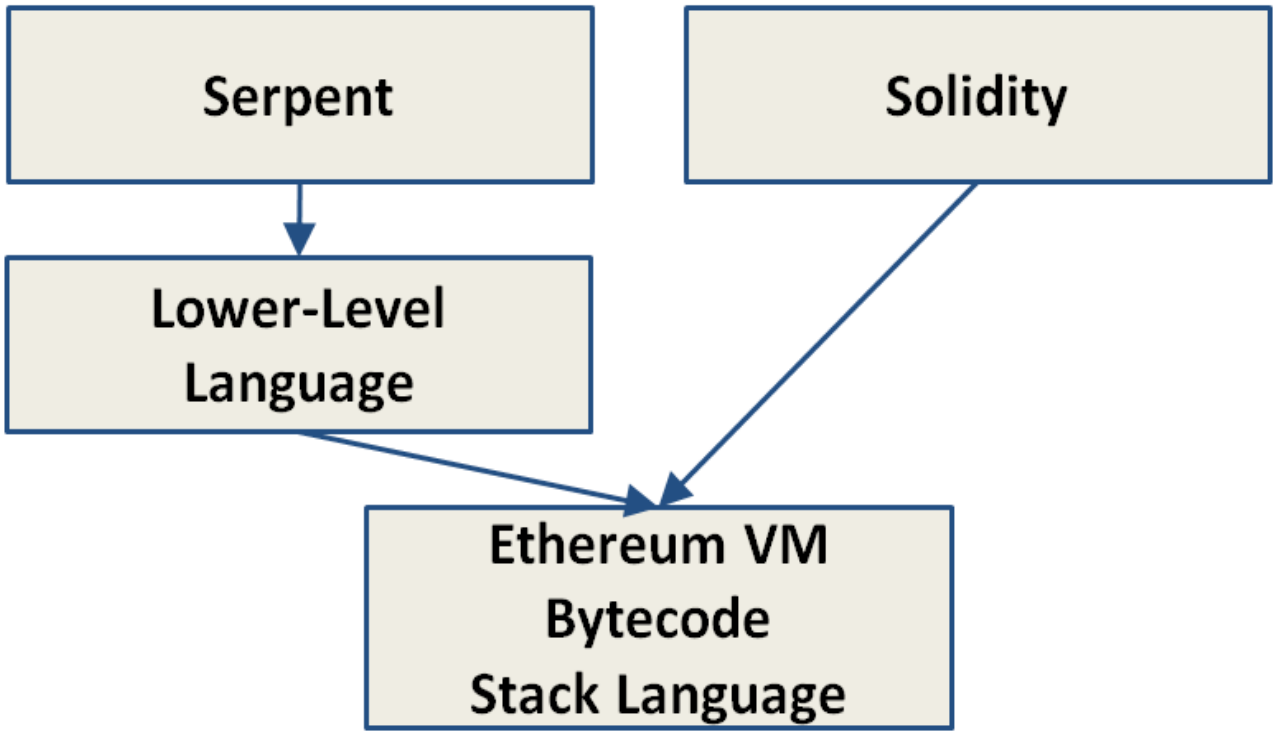


Ethereum Languages

Looks like python

Types, invariants,
looks like Javascript

Functional, macros,
looks like scheme



Example

```
contract Greetings {
    string greeting;
    function Greetings (string _greeting) public {
        greeting = _greeting;
    }

    /* main function */
    function greet() constant returns (string) {
        return greeting;
    }
}
```

What you write

What other see on the blockchain

```
6060604052604051610250380380610250833981016040528.....
```

```
PUSH 60
    PUSH 40
    MSTORE
    PUSH 0
    CALLDATALOAD
.....
```

What people get from the disassembler

DoS Attack Vector

- Halting problem
  - Cannot tell whether or not a program will run infinitely A
  - malicious miner can DoS attack full nodes by including lots of computation in their txs
    - Full nodes attacked when verifying the block

```
int i = 1;
while (i++ > 0) {
        donothing();
}
```

Solution???

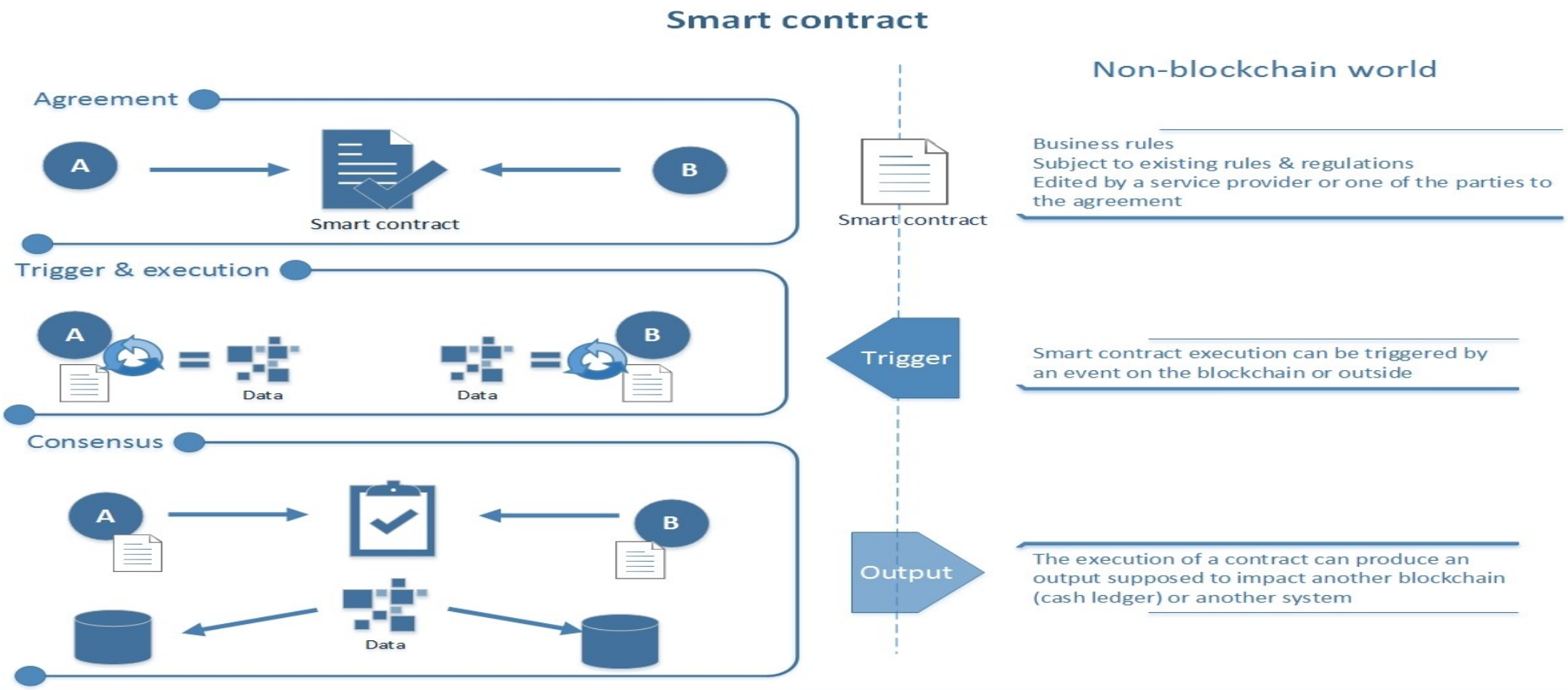
- GAS - Charge fee per computational step (“gas”)
  - Special gas fees for operations that take up storage

Operation	Gas	GasCost
PUSH1	111741	3
PUSH1	111738	3
MSTORE	111726	12
CALLDATASIZE	111724	2
ISZERO	111721	3
PUSH2	111718	3
JUMPI	111708	10

Sender has to pay for the gas

- **gasprice**: amount of ether per unit gas
- **startgas**: maximum gas consumable
  - If **startgas** is less than needed
    - Out of gas exception, revert the state as if the TX has never happened
    - Sender still pays all the gas
- TX fee = gasprice * consumedgas
- Gas limit: similar to block size limit in Bitcoin
  - Total gas spent by all transactions in a block < Gas Limit

Smart Contracts



Why Smart Contracts?

Smart Contracts are Awesome!

1 Autonomy

You're the one making the agreement; there's no need to rely on a broker or lawyer

2 Trust

Your documents are encrypted on a shared ledger

3 Backup

On the blockchain,Your documents are duplicated many times over

4 Savings

Smart contracts save you money since they knock out the presence of an intermediary

5 Accuracy

Smart contracts are not only faster and cheaper but also avoid the errors that come from manually filling out heaps of forms.

Decentralized applications

Benefits of Decentralized networks

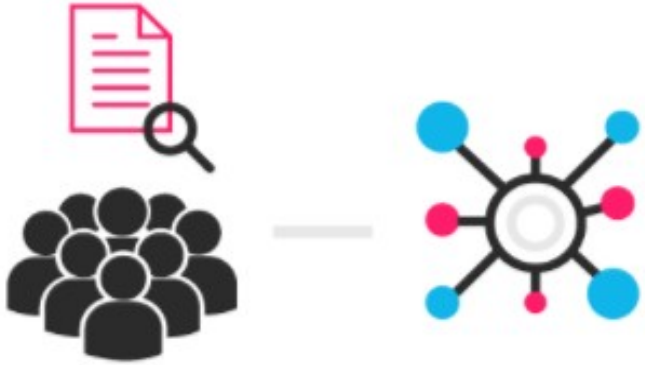
With no central point of failure and secured using cryptography, applications are well protected against hacking attacks and fraudulent activities.

Advantages:

- Immutability
- Corruption & tamper
- Secure

The Blockchain

Blockchain technology is like the internet in that it has a built-in robustness. By storing blocks of information that are identical across its network, the blockchain cannot:



ENTER ETHEREUM

The Ethereum makes the process of creating blockchain applications much easier and efficient than ever before. Instead of having to build an entirely original blockchain for each new application, Ethereum enables the development of potentially thousands of different applications all on one platform.

Ether- The fuel for Ethereum

- Ether is the digital token used by Ethereum. It is also used to pay transaction fees and other computational services on the Ethereum Network.
- Ether is also used as a cryptocurrency and is traded on various exchanges just like bitcoin.
- It is the second most popular cryptocurrency in the world and has a market capitalization of 950 million USD.
- The price of Ether token is also volatile just like other cryptocurrencies and it keeps fluctuating every minute.

Ether wallet

- Ether wallet is a virtual wallet, basically a mobile or web application that lets you store your ether tokens.
  An Ether Wallet also provides several other facilities like
- sending your ethers to another wallet address or receiving ethers from outside sources.
  You can also keep a track of all your transactions. Many
- wallet providers have also released web browser
- extensions of their respective wallets and some are going to release a hardware version as well which will be a USB stick that you can plug into any computer.

Ethereum Virtual Machine

- Ethereum Virtual Machine is a computer software which runs at an abstraction layer straight above the underlying hardware.
- Ethereum uses a Turing Complete Virtual Machine for running and compiling the codes.
- For this reason, Ethereum Virtual Machine is also called

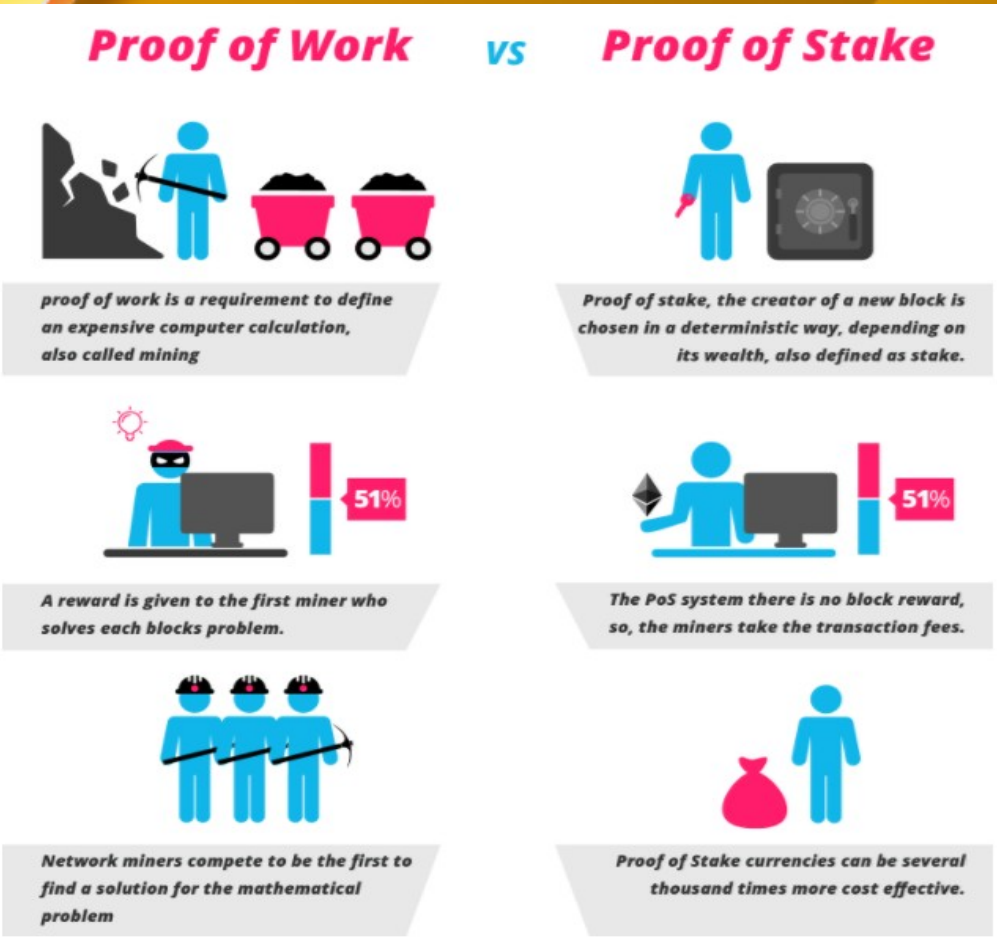
  Turing Complete Virtual Machine
- The term “Turing Complete” flaunts that this s adroit enough to run any code defined by the d

Solidity,The Language Behind Ethereum

- Solidity is one of the two main programming languages that are specifically designed to target the Ethereum Virtual Machine or EVM.
- The other one is Serpent. All the Ethereum based applications and Smart Contracts are written in Solidity. Solidity was initially
- proposed in August 2014 by Dr. Gavin
  Wood and it was later developed by the Ethereum project's Solidity team, lead by Dr. Christian Reitweissner.

Proof of work vs Proof of Stake

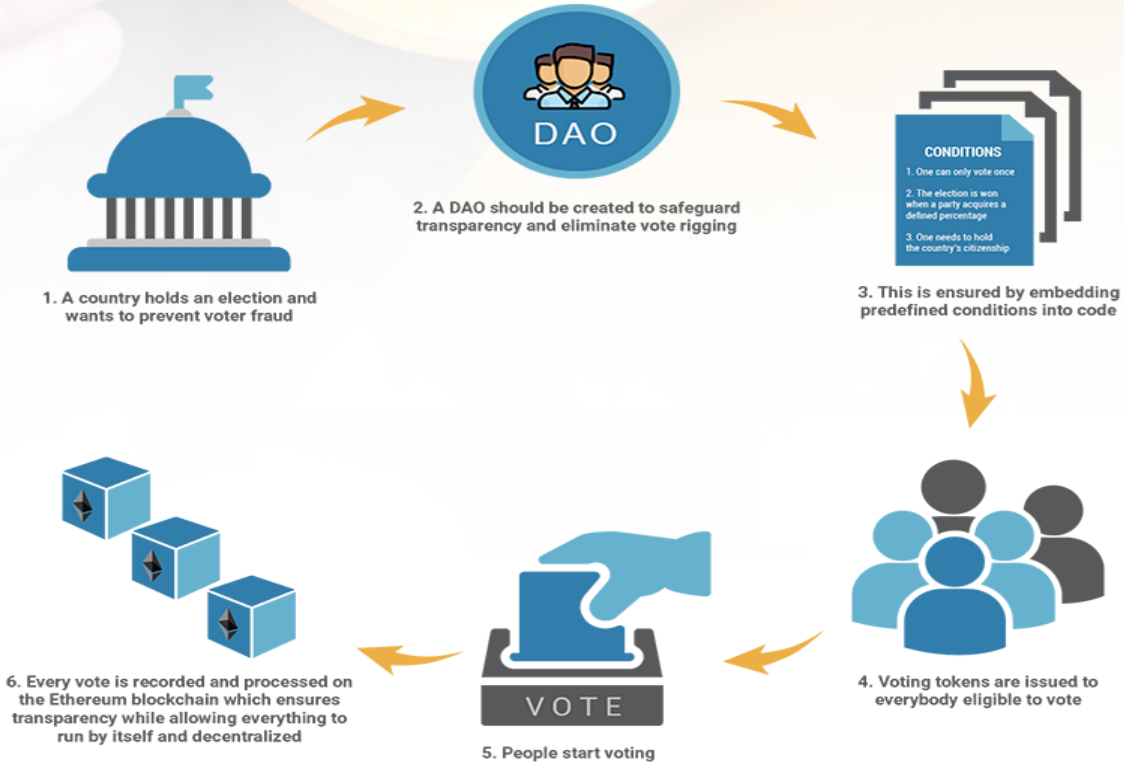
- Proof of work is a protocol that has the main goal of deterring cyber-attacks such as a distributed denial-of-service attack (DDoS) which has the purpose of exhausting the resources of a computer system by sending multiple fake requests.
- It allows trustless and distributed consensus.



What ethereum can be used for?

- Ethereum is VERSATILE. Contracts
- can be used to build currencies, financial derivatives, voting systems, decentralized organizations, data feeds, title registries and thousands of other applications.

Decentralised Autonomous Organisation



Advantages of Ethereum

- Allowing for a turing complete language on the blockchain No
- need for 3rd parties services
- Ethereum acts as a platform for other products and Services, allowing for a robust ecosystem to grow around the system.
- Companies getting involved with improving Ethereum beyond the foundation.

Problems/challenges

1. Privacy

- Ethereum blockchain guarantees correctness and availability, not privacy for smart contracts
  - Everything on the Ethereum blockchain is public
    - Cannot execute on private data (e.g. death will remains secret until the owner dies)
- Transactions are traceable

Privacy solution

- Privacy-Preserving Smart Contracts
- Execute confidential, fair, multiparty protocols
- Zero cash over ethereum, Ring Signature on ethereum
  - Mixing coins with others

Scalability

- Resources on blockchain are expensive
  - Full nodes perform the same on-chain computations Full
  - nodes store the same data
- Gas-limit is relatively small
  - Can't run an OS on blockchain Can't
  - increase gas-limit: DoS vector

The Ethereum network is currently undergoing a DoS attack Ethereum Blog

Posted by Jeffrey Wilcke on September 22nd, 2016.

URGENT ALL MINERS: The network is under attack. The attack is a computational DDoS, ie. miners and nodes need to spend a very long time processing some blocks.

ETHEREUM • FEATURES • TECHNOLOGY CoinDesk

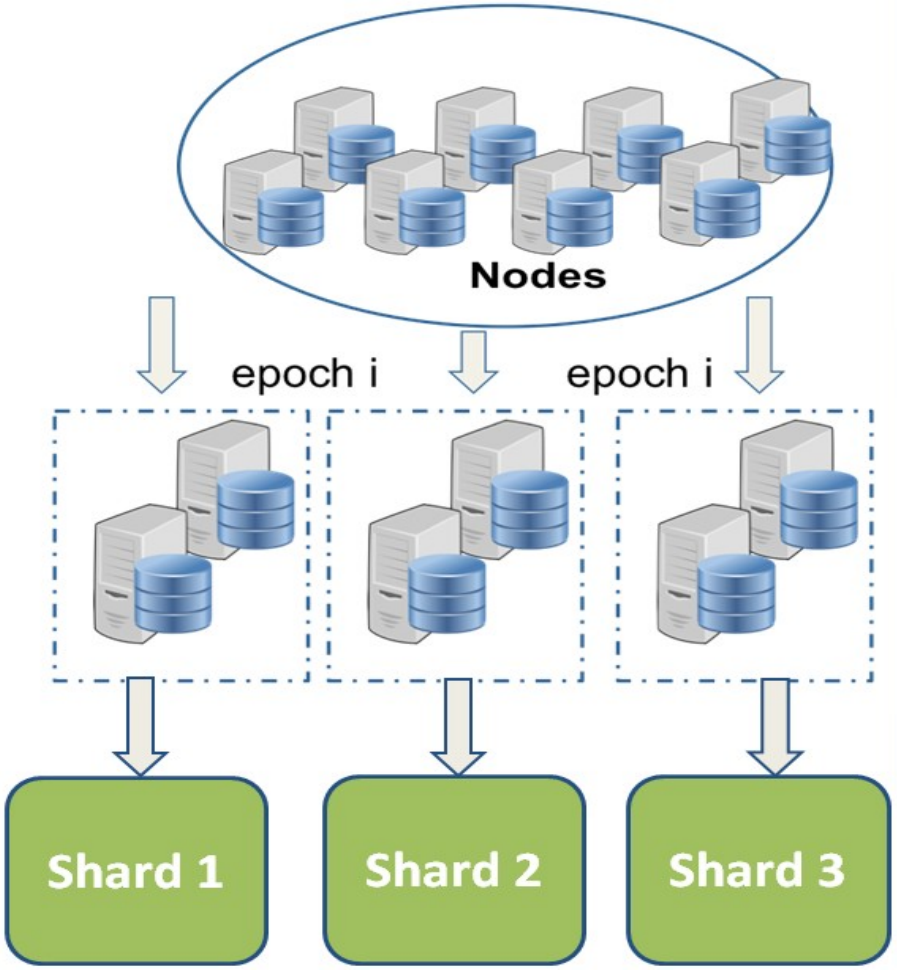
So, Ethereum's Blockchain is Still Under Attack...

Alyssa Hertig (@AlyssaHertig) | Published on October 6, 2016 at 18:05 GMT

FEATURE

Scalability Solution 1: Sharding

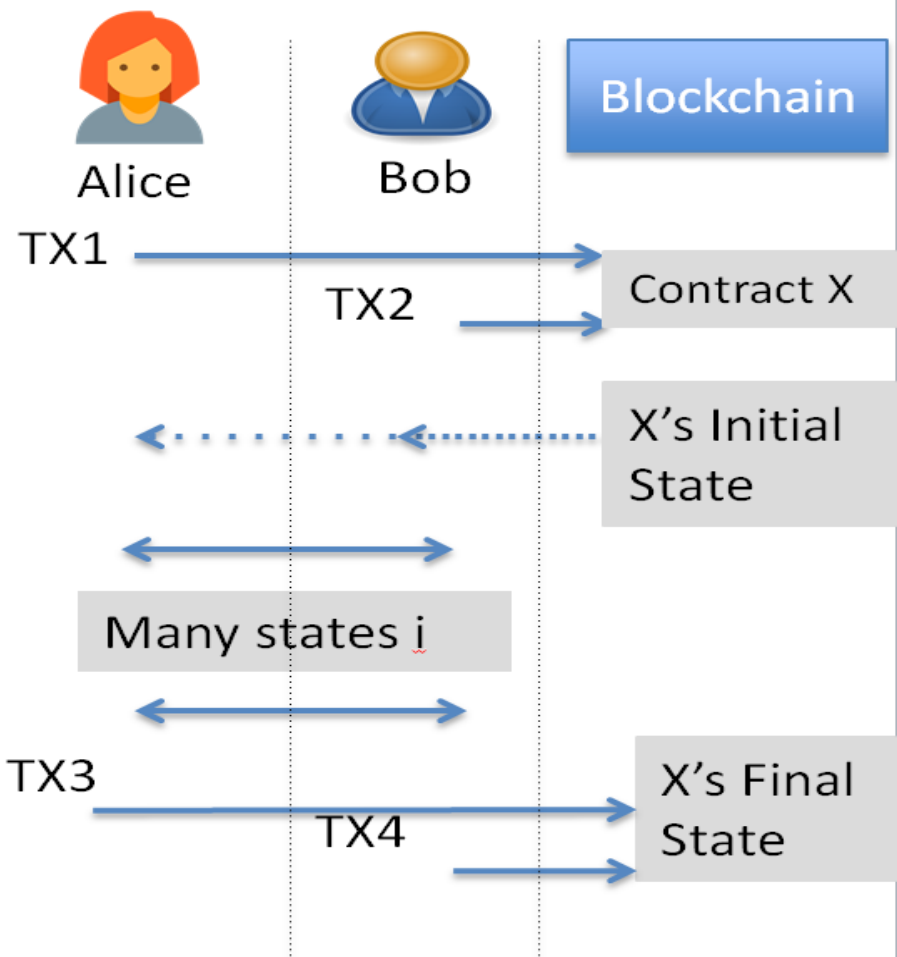
- Divide the network into sub-networks
  - each stores and manages a fraction of the block chain (a shard)
  - Allow scaling up as the network grows
- There is a catch
  - May affect usability or performance
  - May not be compatible with all existing applications



Scalability Solution 2: State Channel

- Similar to payment channel (e.g. lightning network) but for states
  - Scaling by using off-chain transactions
  - Can update the state multiple times
  - Only settlement transactions are on- chain

- Challenges
  - Cannot create state channel for all applications
  - Still early research, more work needed



Security Flaws

- Due to abstraction of semantics
  - Transaction ordering dependence Reentrancy Bug
- Which exploited the
- DAO Obscure VM rules
  - Maximum stack depth is 1024: not many devs know
  - Inconsistent Exception Handling in EVM

The DAO Attacked: Code Issue Leads to $60 Million Ether Theft

Michael del Castillo (@DelRayMan) | Published on June 17, 2016 at 14:00 GMT

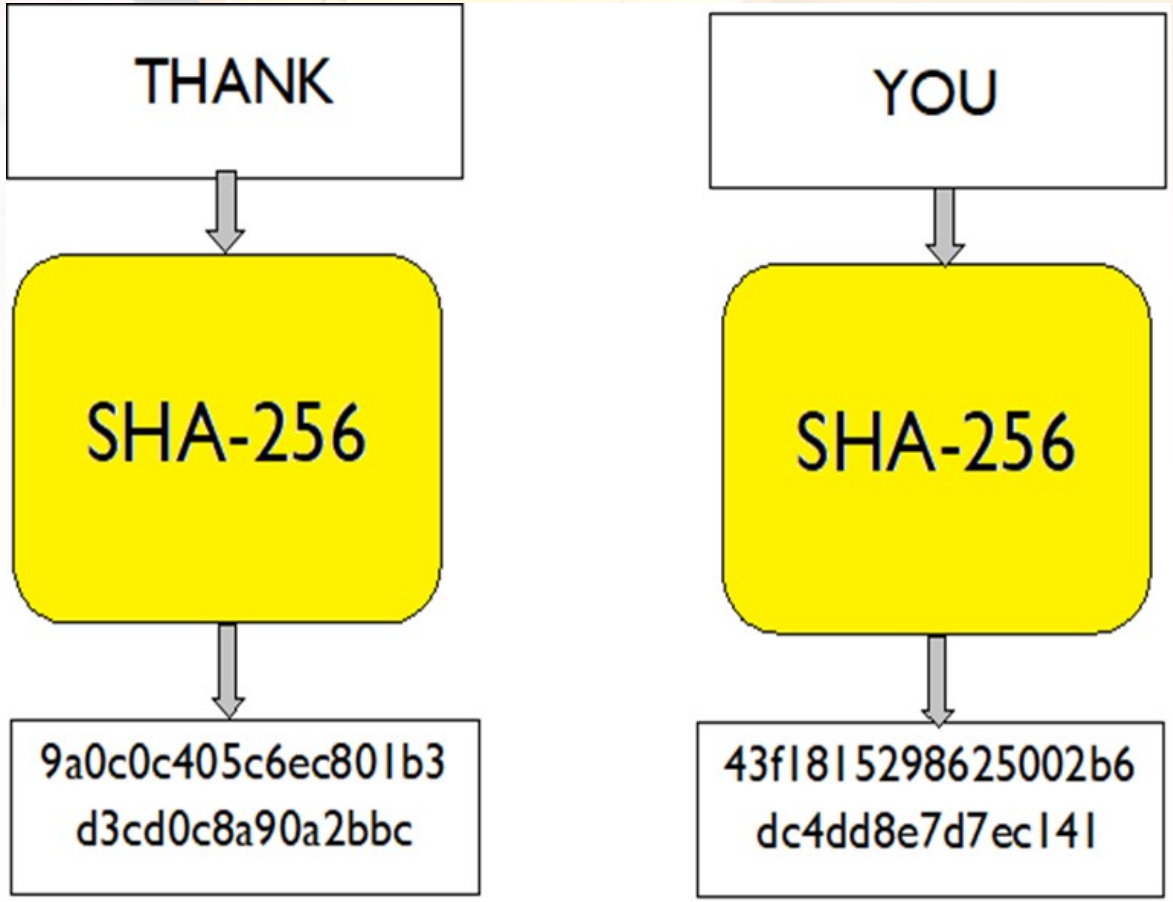
NEWS

Solutions to Resolve Security Flaws

- Create developer tools
  - Smart contract analyzer based on symbolic exec: Oyente Testing
  - and deployment framework: Truffle
  - Formal verification for smart contracts: eth-isabelle , why3
- Design better semantic [CCS'16]
- Educate users
- Idea
  - Create security certificates for smart contracts?

Conclusion

- Ethereum is a fascinating research area at the intersection of multiple fields: cryptography and distributed systems, programming languages and formal verification, economics and game theory, human-computer interaction, finance and law.
- The promise of smart contracts is not limited to making existing processes more efficient by putting parts of their logic onto a very inefficient, yet very secure decentralized network.
- This new way of handling value without a trusted third party opens up whole new classes of previously impossible use cases.


THANK
SHA-256
9a0c0c405c6ec801b3
d3cd0c8a90a2bbc
YOU
SHA-256
43f18152986250 02b6
dc4dd8e7d7ec141