Ethereum For Beginners
Introduction to Ethereum

The components of blockchain technology
The Ethereum platform and writing distributed applications
Let’s create a Crypto Currency
Implications for the web, business and society
What is Ethereum?

Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.
Blockchain 2.0 - 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

The core idea was simple: a blockchain with a built-in Turing-complete programming language, allowing users to build any kind of applications on top. - Vitalik Buterin
"There is nothing that bitcoin can do which Ethereum can’t. While Ethereum is less battle tested, it is moving faster, has better leadership and has more developer mindshare." - Fred Ehrsam Coinbase co-founder
tl;dr

There is no Central Authority
It’s all about trust
The Issue of trust

All human societies have a trust problem. Many societies have invented elaborate rituals, laws and governance systems to address this trust problem. At its most fundamental level, blockchain technology tries to do the same. While the Internet provides us with a great way to communicate with individuals the world over, it is difficult to enter into an agreement with them; typically, we must trust either them directly (in the case of an e-commerce site, for example) or a third-party that vouches for them. Both are susceptible to the sorts of abuse that blockchain-based technology can mitigate or remove entirely. - Gavin Wood
Convergence of technologies

● Peer to peer networking
● The Blockchain Mechanism
● Cryptography
Peer to Peer Networks

A Decentralised Network

- No single point of failure
- Censorship proof
- Highly Reliable

Examples:
Napster
Bit Torrent
Spotify
The Blockchain Mechanism

A public ledger - all transactions can be seen by all users of the system

The state of the system is arrived at by a consensus protocol
Cryptography

Public / Private Key Cryptography

Transactions are tamper proof

The origin of a transaction can be verified

(The Public Key is hashed with SHA-3 to produce a 256-bit output. The upper 96 bits are discarded, and the lower 160 bits become the Account Address.)
The peer to peer network gives us a distributed, censorship resistant platform.

The blockchain gives us transparency, verifiable consistency and consensus.

Cryptography gives us secure, tamper proof transactions.

The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority.

Simply put, the blockchain is a machine for creating trust.
Smart Contracts

- Contracts live on the Ethereum blockchain.
- They have their own Ethereum address and balance.
- They can send and receive transactions.
- They are activated when they receive a transaction, and can be deactivated.
- The Ethereum Virtual Machine runs a Turing complete language.
- They have a fee per CPU step, with extra for storage.
- The user can run the application on their local blockchain.
Ethereum Programming Languages

Smart contracts can be written in

Solidity (a JavaScript-like language)
Serpent (a Python-like language),
Mutan (C-like)
LLL (Lisp-like).

They are compiled into bytecode before being deployed to the blockchain.
An Example Smart Contract - A voting application

The state of the contract (voteCount) is maintained on the blockchain along with the smart contract.

After a certain time the smart contract will end the election and publish the results.
contract Ballot {

    struct Voter {
        uint weight;
        bool voted;
        uint8 vote;
        address delegate;
    }
    struct Proposal {
        uint voteCount;
    }

    address chairperson;
    mapping(address => Voter) voters;
    Proposal[] proposals;

    // Create a new ballot
    function Ballot(uint8 _numProposals) {
        chairperson = msg.sender;
        voters[chairperson].weight = 1;
        proposals.length = _numProposals;
    }

    // Give a single vote
    function vote(uint8 proposal) {
        Voter sender = voters[msg.sender];
        if (sender.voted || proposal >= proposals.length) return;
        sender.voted = true;
        sender.vote = proposal;
        proposals[proposal].voteCount += sender.weight;
    }

    function winningProposal() constant returns (uint8 winningProposal) {
        uint256 winningVoteCount = 0;
        for (uint8 proposal = 0; proposal < proposals.length; proposal++) {
            if (proposals[proposal].voteCount > winningVoteCount) {
                winningVoteCount = proposals[proposal].voteCount;
                winningProposal = proposal;
            }
        }
    }

}
Ether buys GAS to fuel the EVM

Every opcode instruction executed by the EVM uses up Gas.
Creating a Crypto Currency Demo
Ethereum IDEs
```solidity
@pragma solidity ^0.8.0

contract example-project {
    // Function to change owner of the contract
    function changeOwner(address newOwner) onlyOwner {
        owner = newOwner;
    }

    // Modifier to check if the msg.sender is the owner
    modifier onlyOwner() {
        if (msg.sender == owner) {
            _;
        } else {
            revert;
        }
    }

    contract example-project is abstract, owned {
        function kill() onlyOwner {
            if (msg.sender == owner) suicide(owner);
        }
    }

    // Abstract contract
    contract NameReg is abstract {
        function register(bytes32 name) returns (string);
        function unregister() returns (string);
        function a(address) constant returns (address);
        function b(address) constant returns (string);
        function c(address) constant returns (string);
    }

    // NameRegWith is an abstract contract that can have multiple NameReg contracts
    contract NameRegWith is abstract {
        function a(address) constant returns (string);
        function b(address) constant returns (string);
    }

    // Example contract
    contract example-project is owned {
        function nameRegIsAbstract() {
            // Code implementation...
        }
    }
}
```
Truffle is a development environment, testing framework and asset pipeline for Ethereum,
Automated contract testing with Mocha and Chai.
MIX IDE
Not just Smart Contracts

Messaging and File Sharing...

- In addition to the use of the ethereum virtual machine to execute contract logic. The ethereum project also introduced two additional protocols to provide peer to peer support for exchanging message as well exchanging static files

- The peer to peer protocol used for exchanging message is named whisper and it provides a powerful distributed and private messaging capabilities with support for single cast, multicast and broadcast messages

- The peer to peer protocol used for exchanging static files is named swarm and it provides a new incentivized approach to distribute static content among peers and exchange them efficiently
Why Use Ethereum?

- Uptime
- Security
- Almost Free
- Transparency
- Micro payments
- DAOs, Consensus applications, governance
- Identity / Reputation Services
Limitations

The Ethereum Virtual Machine is slow, don’t use it for large computations
Storage on the block chain is expensive, use IPFS / Swarm
Scalability is an issue, there is a trade off with decentralisation
Private block chains are likely to proliferate
Implications

- Third-party intermediaries are not needed in order to conduct transactions between two (or several) parties.
- End-to-end resolution to be self-managed between computers that represent the interests of the users.
- Disintermediation
Who should be worried about Ethereum

Middle Men
  Kickstarter take a 5% fee
  OpaVote charges $500 for an election
  Uber / Amazon / * Agencies
  Meetup
  Anyone involved in corruption
  Centralised Businesses and Organisations
The DAO contains some kind of internal property that is valuable in some way, and it has the ability to use that property as a mechanism for rewarding certain activities.

- Outsiders can see the governance algorithm
- It may use voting or prediction markets to choose policy
The DAO has been created

- 1172.78 M DAO tokens created
- 12.07 M total ETH
- 132.32 M USD equivalent
- 1.50 last exchange rate ETH / 100 DAO tokens
- 0 - next price phase

Thank you all for your contribution
Governance

- Liquid Democracy
- Holacracy
- Futarchy
Is this all a lot of hype?
Who is using Ethereum Now?
Decentralised Prediction Market

Provenance powers supply chain transparency and secure traceability for materials, ingredients and products.

Colony harnesses the wisdom of the crowd using AI to make sure that the right things get done by the right people, at the right time.

Autonomous bank & market maker

Rebuilding the music industry on the block chain
Storj - Encrypted distributed storage
Rent out space on your hard drive

Blockchain based microgrid
Brooklyn consumers can transform their homes into connected power stations.

Safemarket - Ethereum version of Open Bazaar
TAKE YOUR COMPANY FROM ANALOG TO DIGITAL
Rent, sell or share anything - without middlemen
With Slock.it, Airbnb apartments become fully automated, wifi routers can be rented on demand and unused office spaces get a new lease on life. It's the future infrastructure of the Sharing Economy.
HYPE ‘R’ LEDGER
Next Steps

Proof of Stake
Sharding
Ring Signature Mixer
Micro payments
DAOs, Consensus applications, governance
Identity / Reputation Services
Proof of Stake

50000-foot view summary: the blockchain is a prediction market on itself. - Vitalik Buterin
Links

Ethereum Oxford
LJC Hack The Tower - June 11