	Hope Foundation's **Finolex Academy of Management and Technology, Ratnagiri** **Information Technology Department**		
Subject name: Cloud Service Design Lab			Subject Code: ITL603
Class	TE IT	Semester – VI (CBCGS)	Academic year: 2018-19
Name of Student	**Kazi Jawwad A Rahim**	**QUIZ Score : 08/10**	
Roll No	**27**	Assignment/Experiment No.	06
Title: Case study on Block chain and Ethereum			

1.Course objectives applicable

COB1. To understand use of block chain technology.

COB2.To understand the importance block chain and ethereum for security purpose.

2. Course outcomes applicable:

CO1 -To understand fundamental concept of block chain and ethereum

CO2-To identify use of block chain and ethereum in real time applications

3. Learning Objectives:

1. To understand concept of block chain
2. To understand the concept of block chain for application purpose

4. Practical applications of the assignment/experiment: In cloud environment

To create a permanent, public, transparent ledger system for compiling data on sales.

5. Prerequisites:

1. Prior knowledge of data security.

6. Hardware Requirements:

1. Internet Access with Browser

7. Software Requirements:

Browser like Chrome, Internet Explorer Edge

8. Quiz Questions (if any): (Online Exam will be taken separately batchwise, attach the certificate/ Marks obtained)

1. What is block chain?
2. What are practical applications of block chain?

9. Experiment/Assignment Evaluation:

Sr. No.	Parameters	Marks obtained	Out of
1	Technical Understanding (Assessment may be done based on Q & A **or** any other relevant method.) Teacher should mention the other method used -		6
2	Neatness/presentation		2
3	Punctuality		2
Date of performance (DOP)		**Total marks obtained**	**10**
Date of checking (DOC)		**Signature of teacher**	

Blockchain

A blockchain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree). Blockchain was invented by a person using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. The identity of Satoshi Nakamoto is unknown. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications, and blockchains which are readable by the public are widely used by cryptocurrencies. Blockchain is considered a type of payment rail. Private blockchains have been proposed for business use. Sources such as Computerworld called the marketing of such blockchains without a proper security model "snake oil".

Structure

A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently and relatively inexpensively. A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests. Such a design facilitates robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending. A blockchain has been described as a value-exchange protocol. A blockchain can maintain title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

Blocks

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block. Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any blockchain has a specified algorithm for scoring different versions of the history so that one with a higher value can be selected over others. Blocks not selected for inclusion in the chain are called orphan blocks. Peers supporting the database have different versions of the history from time to time. They keep only the highest-scoring version of the database known to them. Whenever a peer receives a higher-scoring version (usually the old version with a single new block added) they extend or overwrite their own database and retransmit the improvement to their peers. There is never an absolute guarantee that any particular entry will remain in the best version of the history forever. Blockchains are typically built to add the score of new blocks onto old blocks and are given incentives to extend with new blocks rather than overwrite old blocks. Therefore, the probability of an entry becoming superseded decreases exponentially as more blocks are built on top of it, eventually becoming very low. For example, bitcoin uses a proof-of-work system, where the chain with the most cumulative proof-of-work is considered the valid one by the network. There are a number of methods that can be used to demonstrate a sufficient level of computation. Within a blockchain the computation is carried out redundantly rather than in the traditional segregated and parallel manner.

Block time

The block time is the average time it takes for the network to generate one extra block in the blockchain. Some blockchains create a new block as frequently as every five seconds. By the time of block completion, the included data becomes verifiable. In cryptocurrency, this is practically when the transaction takes place, so a shorter block time means faster transactions. The block time for Ethereum is set to between 14 and 15 seconds, while for bitcoin it is 10 minutes.

Hard forks

A hard fork is a rule change such that the software validating according to the old rules will see the blocks produced according to the new rules as invalid. In case of a hard fork, all nodes meant to work in accordance with the new rules need to upgrade their software. If one group of nodes continues to use the old software while the other nodes use the new software, a split can occur. For example, Ethereum has hard-forked to "make whole" the investors in The DAO, which had been hacked by exploiting a vulnerability in its code. In this case, the fork resulted in a split creating Ethereum and Ethereum Classic chains. In 2014 the Nxt community was asked to consider a hard fork that would have led to a rollback of the blockchain records to mitigate the effects of a theft of 50 million NXT from a major cryptocurrency exchange. The hard fork proposal was rejected, and some of the funds were recovered after negotiations and ransom payment. Alternatively, to prevent a permanent split, a majority of nodes using the new software may return to the old rules, as was the case of bitcoin split on 12 March 2013.

Decentralization

By storing data across its peer-to-peer network, the blockchain eliminates a number of risks that come with data being held centrally. The decentralized blockchain may use ad-hoc message passing and distributed networking. Peer-to-peer blockchain networks lack centralized points of vulnerability that computer crackers can exploit; likewise, it has no central point of failure. Blockchain security methods include the use of public-key cryptography. A public key (a long, random-looking string of numbers) is an address on the blockchain. Value tokens sent across the network are recorded as belonging to that address. A private key is like a password that gives its owner access to their digital assets or the means to otherwise interact with the various capabilities that blockchains now support. Data stored on the blockchain is generally considered incorruptible. Every node in a decentralized system has a copy of the blockchain. Data quality is maintained by massive database replication and computational trust. No centralized "official" copy exists and no user is "trusted" more than any other. Transactions are broadcast to the network using software. Messages are delivered on a best-effort basis. Mining nodes validate transactions, add them to the block they are building, and then broadcast the completed block to other nodes. Blockchains use various time-stamping schemes, such as proof-of-work, to serialize changes. Alternative consensus methods include proof-of-stake. Growth of a decentralized blockchain is accompanied by the risk of centralization because the computer resources required to process larger amounts of data become more expensive.

Openness

Open blockchains are more user-friendly than some traditional ownership records, which, while open to the public, still require physical access to view. Because all early blockchains were permissionless, controversy has arisen over the blockchain definition. An issue in this ongoing debate is whether a private system with verifiers tasked and authorized (permissioned) by a central authority should be considered a blockchain. Proponents of permissioned or private chains argue that the term "blockchain" may be applied to any data structure that batches data into time-stamped blocks. These blockchains serve as a distributed version of multiversion concurrency control (MVCC) in databases. Just as MVCC prevents two transactions from concurrently modifying a single object in a database, blockchains prevent two transactions from spending the same single output in a blockchain. Opponents say that permissioned systems resemble traditional corporate databases, not supporting

decentralized data verification, and that such systems are not hardened against operator tampering and revision. Nikolai Hampton of Computerworld said that "many in-house blockchain solutions will be nothing more than cumbersome databases," and "without a clear security model, proprietary blockchains should be eyed with suspicion."

Permissionless

The great advantage to an open, permissionless, or public, blockchain network is that guarding against bad actors is not required and no access control is needed. This means that applications can be added to the network without the approval or trust of others, using the blockchain as a transport layer. Bitcoin and other cryptocurrencies currently secure their blockchain by requiring new entries to include a proof of work. To prolong the blockchain, bitcoin uses Hashcash puzzles. While Hashcash was designed in 1997 by Adam Back, the original idea was first proposed by Cynthia Dwork and Moni Naor and Eli Ponyatovski in their 1992 paper "Pricing via Processing or Combatting Junk Mail". Financial companies have not prioritised decentralized blockchains. In 2016, venture capital investment for blockchain-related projects was weakening in the USA but increasing in China. Bitcoin and many other cryptocurrencies use open (public) blockchains. As of April 2018, bitcoin has the highest market capitalization.

Permissioned (private) blockchain

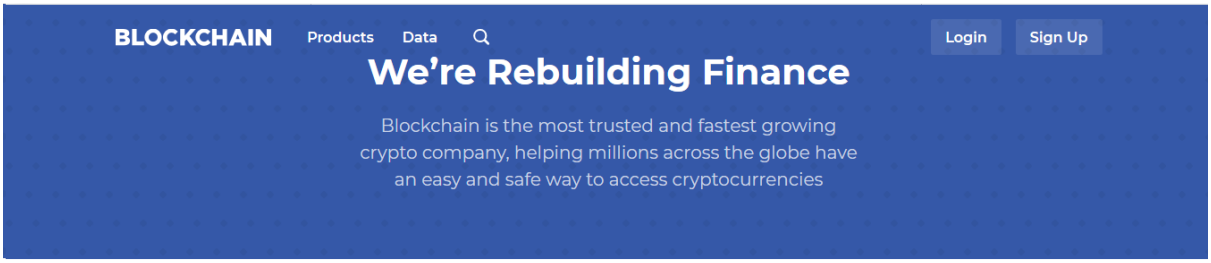
Permissioned blockchains use an access control layer to govern who has access to the network. In contrast to public blockchain networks, validators on private blockchain networks are vetted by the network owner. They do not rely on anonymous nodes to validate transactions nor do they benefit from the network effect. Permissioned blockchains can also go by the name of 'consortium' or 'hybrid' blockchains. The New York Times noted in both 2016 and 2017 that many corporations are using blockchain networks "with private blockchains, independent of the public system."

Disadvantages of private blockchain

Nikolai Hampton pointed out in Computerworld that "There is also no need for a '51 percent' attack on a private blockchain, as the private blockchain (most likely) already controls 100 percent of all block creation resources. If you could attack or damage the blockchain creation tools on a private corporate server, you could effectively control 100 percent of their network and alter transactions however you wished." This has a set of particularly profound adverse implications during a financial crisis or debt crisis like the financial crisis of 2007–08, where politically powerful actors may make decisions that favor some groups at the expense of others, and "the bitcoin blockchain is protected by the massive group mining effort. It's unlikely that any private blockchain will try to protect records using gigawatts of computing power — it's time consuming and expensive." He also said, "Within a private blockchain there is also no 'race'; there's no incentive to use more power or discover blocks faster than competitors. This means that many in-house blockchain solutions will be nothing more than cumbersome databases."

Uses

Blockchain technology can be integrated into multiple areas. The primary use of blockchains today is as a distributed ledger for cryptocurrencies, most notably bitcoin. There are a few operational products maturing from proof of concept by late 2016. As of 2016, some observers remain skeptical. Steve Wilson, of Constellation Research, believes the technology has been hyped with unrealistic claims. To mitigate risk, businesses are reluctant to place blockchain at the core of the business structure.



BLOCKCHAIN BY THE NUMBERS

34,000,000+ Wallets

25K+ API Developers

140 Countries

10,000+ Club Mates Consumed

100,000,000+ Transactions

#1 Leading Research

Backed by the Best

We've raised $70M from the leading investors in Silicon Valley, Wall Street, and London

What Motivates Us

Our collective desire to offer financial empowerment is driven by our values

CHALLENGE CONVENTION

We challenge the status quo and transcend the boundaries of today to create an open financial future that supports the broadest global community possible.

THE POWER OF THE END-USER

Our customers should own their financial future so we empower them to "Be Your Own Bank". Our users come first.

SANCTIFY SECURITY

Our users' security and privacy are critical to our success and we will not forsake them in service of our ambition.

BE HONEST. HUMBLE. HUMAN.

We build connections with each other and our users by communicating frequently, authentically and openly and we build trust by doing what we say we'll do.

DELIGHT IN THE DETAILS

We believe we cannot get the big things right if we don't get the little things right first. Sometimes that makes things harder. Luckily, we're ok with hard.

Ethereum

Ethereum is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract (scripting) functionality. It supports a modified version of Nakamoto consensus via transaction-based state transitions.

Ether is a token whose blockchain is generated by the Ethereum platform. Ether can be transferred between accounts and used to compensate participant mining nodes for computations performed. Ethereum provides a decentralized virtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public node. The virtual machine's instruction set, in contrast to others like Bitcoin Script, is thought to be Turing-complete. "Gas", an internal transaction pricing mechanism, is used to mitigate spam and allocate resources on the network. Ethereum was proposed in late 2013 by Vitalik Buterin, a cryptocurrency researcher and programmer. Development was funded by an online crowdsale that took place between July and August 2014. In 2016, as a result of the exploitation of a flaw in The DAO project's smart contract software, and subsequent theft of $50 million worth of Ether, Ethereum was split into two separate blockchains – the new separate version became Ethereum (ETH) with the theft reversed and the original continued as Ethereum Classic (ETC).

Characteristics

As with other cryptocurrencies, the validity of each ether is provided by a blockchain, which is a continuously growing list of records, called blocks, which are linked and secured using cryptography. By design, the blockchain is inherently resistant to modification of the data. It is an open, distributed ledger that records transactions between two parties efficiently and in a verifiable and permanent way. Unlike Bitcoin, Ethereum operates using accounts and balances in a manner called state transitions. This does not rely upon unspent transaction outputs (UTXOs). State denotes the current balances of all accounts and extra data. State is not stored on the blockchain, it is stored in a separate Merkle Patricia tree. A cryptocurrency wallet stores the public and private "keys" or "addresses" which can be used to receive or spend Ether. These can be generated through BIP 39 style mnemonics for a BIP 32 "HD Wallet". In Ethereum, this is unnecessary as it does not operate in a UTXO scheme. With the private key, it is possible to write in the blockchain, effectively making an ether transaction. To send ether to an account, you need the public key of that account. Ether accounts are pseudonymous in that they are not linked to individual persons, but rather to one or more specific addresses. Owners can store these addresses in software, on paper and possibly in memory ("brain wallet").

Applications

Ethereum is written in Turing complete language, which includes seven different programming languages. Developers use the language to create and publish applications which they know will run inside Ethereum. It's a cumbersome system, but that's not deterring developers from writing Ethereum programs. Ethereum blockchain applications are usually referred to as DApps (decentralized application), since they are based on the decentralized Ethereum Virtual Machine, and its smart contracts. Many uses have been proposed for Ethereum platform, including ones that are impossible or unfeasible. Use case proposals have included finance, the internet-of-things, farm-to-table produce, electricity sourcing and pricing, and sports betting. Ethereum is (as of 2017) the leading blockchain platform for initial coin offering projects, with over 50% market share. As of January 2018, there are more than 250 live DApps, with hundreds more under development. Some application examples include: digital signature algorithms, securitized tokens, digital rights management, crowdfunding, prediction markets, remittance, online gambling, social media platforms, financial exchanges and identity systems.

Performance

In Ethereum all smart contracts are stored publicly on every node of the blockchain, which has costs. Being a blockchain means it is secure by design and is an example of a distributed computing system with high Byzantine fault tolerance. The downside is that performance issues arise in that every node is calculating all the smart contracts in real time, resulting in lower speeds. As of January 2016, the Ethereum protocol could process 25 transactions per second. In comparison, the Visa payment platform processes 45,000 payments per second leading some to question the scalability of Ethereum. On 19 December 2016, Ethereum exceeded one million transactions in a single day for the first time.

- Micro Raiden was launched November 2017.
- Buterin and Joseph Poon (a co-author of Bitcoin's Lightning Network whitepaper) announced in 2017 their plan to launch a scaling solution called Plasma which creates "child" blockchains to the "main" parent blockchain. The plasma project has skeptics; specifically, Vlad Zamfir (Ethereum's lead researcher on proof of stake) has publicly questioned the plasma project's viability.
- Ethereum engineers have been working on sharding the calculations, and the next step (called Ethereum 2) was presented at Ethereum's Devcon 3 in November 2017.

Ethereum's blockchain uses Merkle trees, for security reasons, to improve scalability, and to optimize transaction hashing. As with any Merkle tree implementation, it allows for storage savings, set membership proofs (called "Merkle proofs"), and light client synchronization. The Ethereum network has at times faced congestion problems, for example, congestion occurred during late 2017 in relation to Cryptokitties.

How much is it worth?

Like all assets, the market value for a single ether is determined by supply and demand. The current price is $162.25.

Why should I use it?

As the Ethereum platform grows, it will change the way we do business and transact on a daily basis. We want to give you the opportunity to start using ether now, so you'll be ready for what the future brings.

How do transactions fees work?

When you send ether or do anything else on the Ethereum block chain, you must pay miners for the computation of that transaction. In your Blockchain wallet, we'll set this as fixed fee for you.

How is it different from Bitcoin?

Ethereum expands on Bitcoin by harnessing blockchain capability for computer code. Ethereum has a wide range of potential applications such as voting, global supply chains, medical records and the financial system.

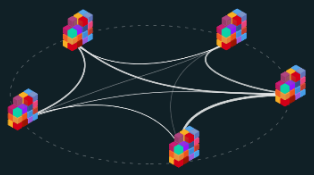
Build unstoppable applications

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.

These apps run on a custom built **blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property.**

This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middleman or counterparty risk.

The project was bootstrapped via an ether presale in August 2014 by fans all around the world. It is developed by the Ethereum Foundation, a Swiss non-profit, with contributions from great minds across the globe.



On traditional server architectures, every application has to set up its own servers that run their own code in isolated silos, making sharing of data hard. If a single app is compromised or goes offline, many users and other apps are affected.

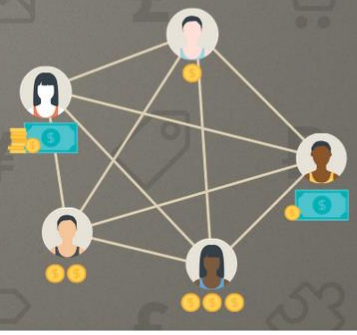
On a blockchain, anyone can set up a node that replicates the necessary data for all nodes to reach an agreement and be compensated by users and app developers. This allows user data to remain private and apps to be decentralized like the Internet was supposed to work.

Learn **Solidity**, a new language for smart contracts

Design and issue your own cryptocurrency

Create a tradeable digital token that can be used as a currency, a representation of an asset, a virtual share, a proof of membership or anything at all. These tokens use a standard coin API so your contract will be automatically compatible with any wallet, other contract or exchange also using this standard.

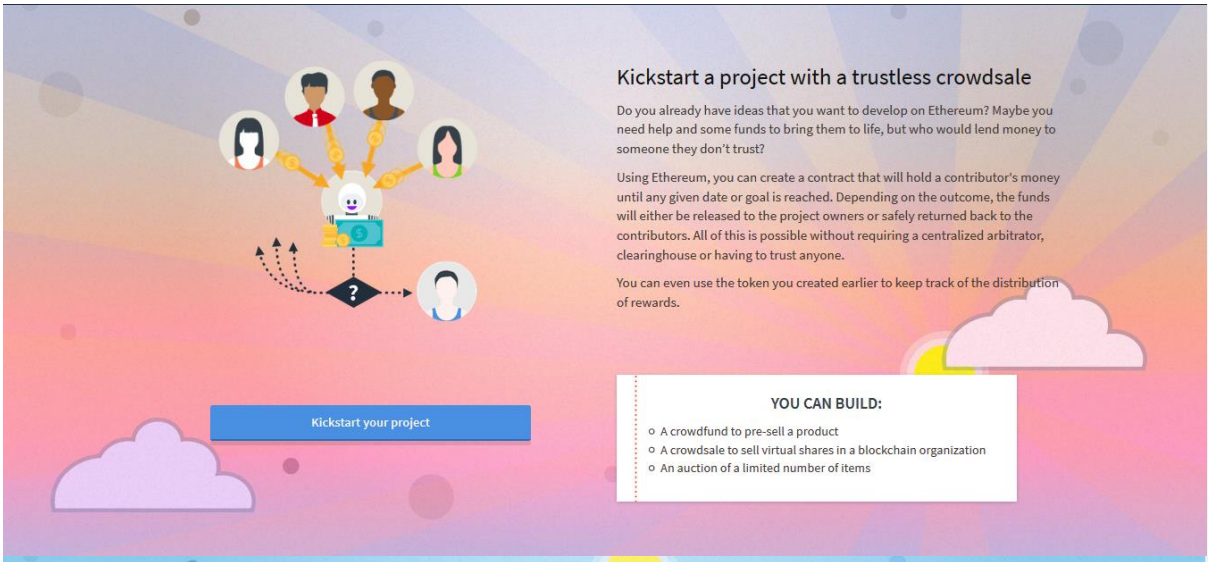
The total amount of tokens in circulation can be set to a simple fixed amount or fluctuate based on any programmed ruleset.

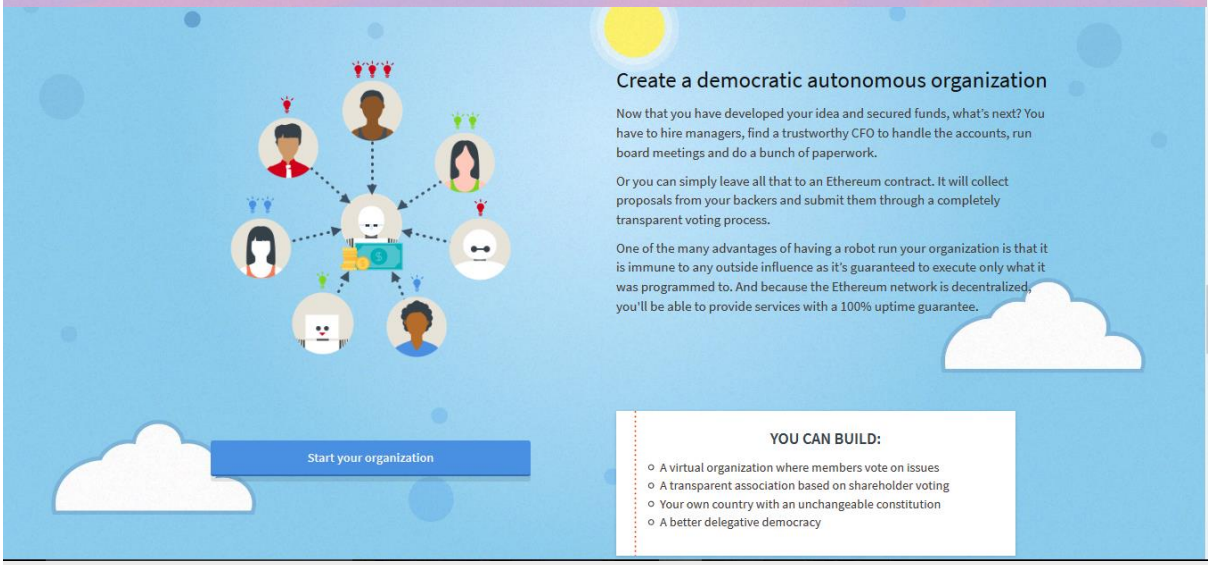


Issue your token

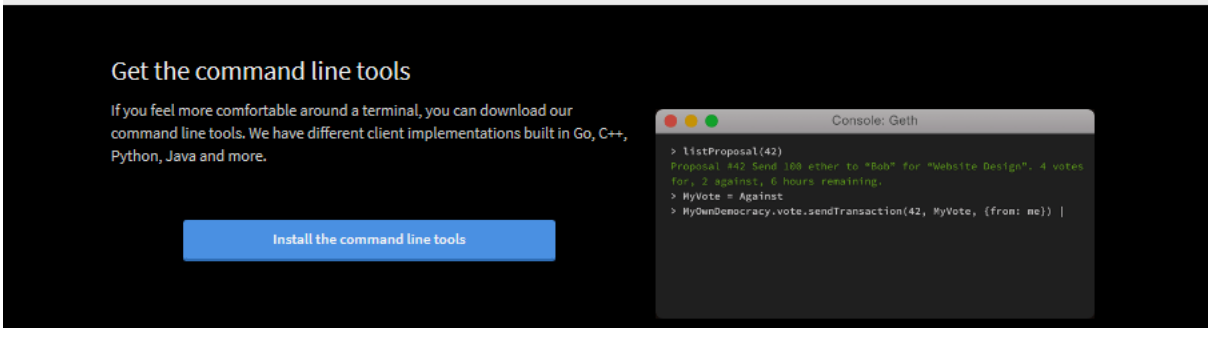
YOU CAN BUILD:

- A tradeable token with a fixed supply
- A central bank that can issue money
- A puzzle-based cryptocurrency


Kickstart a project with a trustless crowdsale
Do you already have ideas that you want to develop on Ethereum? Maybe you need help and some funds to bring them to life, but who would lend money to someone they don't trust?
Using Ethereum, you can create a contract that will hold a contributor's money until any given date or goal is reached. Depending on the outcome, the funds will either be released to the project owners or safely returned back to the contributors. All of this is possible without requiring a centralized arbitrator, clearinghouse or having to trust anyone.
You can even use the token you created earlier to keep track of the distribution of rewards.
Kickstart your project
YOU CAN BUILD:
A crowdfund to pre-sell a product
A crowdsale to sell virtual shares in a blockchain organization
An auction of a limited number of items


Create a democratic autonomous organization
Now that you have developed your idea and secured funds, what's next? You have to hire managers, find a trustworthy CFO to handle the accounts, run board meetings and do a bunch of paperwork.
Or you can simply leave all that to an Ethereum contract. It will collect proposals from your backers and submit them through a completely transparent voting process.
One of the many advantages of having a robot run your organization is that it is immune to any outside influence as it's guaranteed to execute only what it was programmed to. And because the Ethereum network is decentralized, you'll be able to provide services with a 100% uptime guarantee.
Start your organization
YOU CAN BUILD:
A virtual organization where members vote on issues
A transparent association based on shareholder voting
Your own country with an unchangeable constitution
A better delegative democracy


Build a new kind of decentralized application
Now it's your turn: start building what you dream of creating in Ethereum! Could your business be enhanced by operating on a cryptographically secure, decentralized, tamper-proof network?
Check out the many great projects* already being built on Ethereum. And since you'll be among the first developers in the world that are able to program decentralized applications, some of them might need your help.
*The above list is maintained by an independent party and the Foundation does not endorse its content or any particular project


Get the command line tools
If you feel more comfortable around a terminal, you can download our command line tools. We have different client implementations built in Go, C++, Python, Java and more.
Install the command line tools
Console: Geth
> listProposal(42)
Proposal #42 Send 100 ether to "Bob" for "Website Design". 4 votes for, 2 against, 6 hours remaining.
> MyVote = Against
> MyOwnDemocracy.vote.sendTransaction(42, MyVote, {from: me})

11. Learning Outcomes Achieved

Understood the concept of block chain and its use from application point of view.

12. Conclusion:

1. **Applications of the studied technique in industry**
   To create a permanent, public, transparent ledger system for compiling data on sales.

2. **Engineering Relevance**
   a. Used in banks and data analysis
3. **Skills Developed**
   a. Understanding fundamentals of block chain and ethereum.

References:

[1] https://en.wikipedia.org/wiki/Blockchain

[2] https://www.blockchain.com/

[3] https://en.wikipedia.org/wiki/Ethereum

[4] https://www.ethereum.org/