Blockchain Etextbook

Arib Ali, Liam Gillies, Elizabeth Mulvaney

CS 4624 Multimedia, Hypertext, and Information Access
Professor: Dr. Edward Fox

Virginia Tech
Blacksburg, VA 24061
12/02/2021

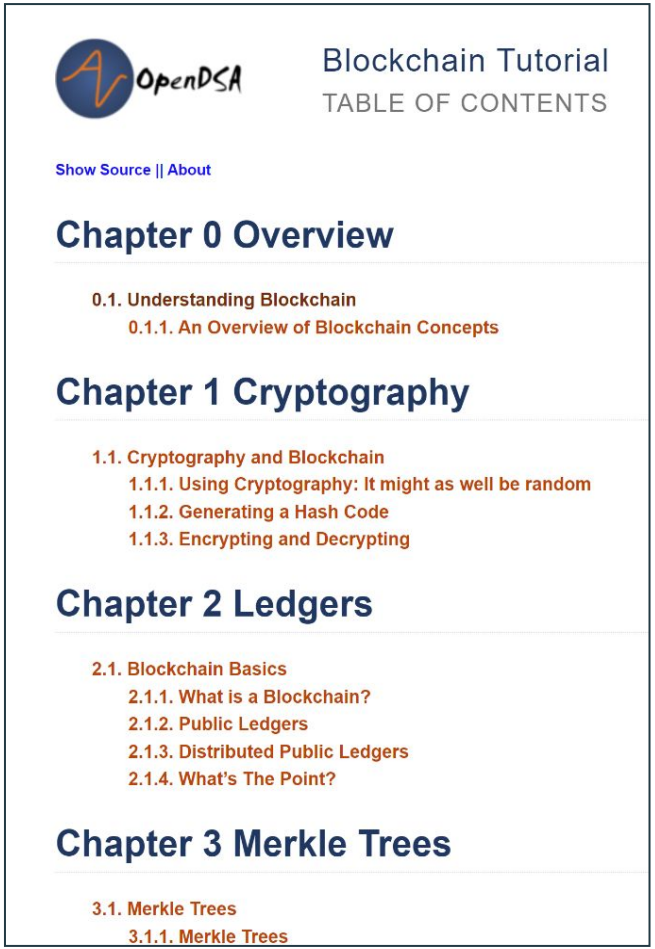
Outline

- Overview of Topic
- Timeline
- Deliverables
  - Hard Forks
  - Proof of Stake
  - Crypto Hacking
  - Ethereum Virtual Machine
  - Ethereum Summary
- Testing
- Challenges & Lessons Learned
- Future Work
- Acknowledgments
- References

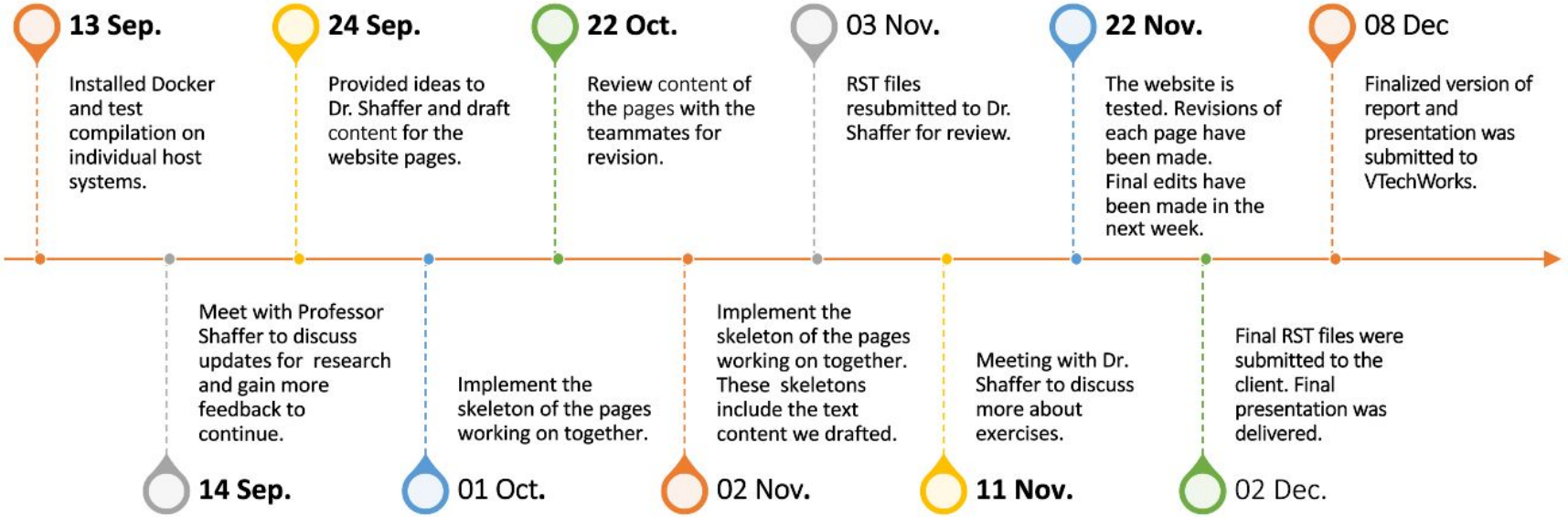
[1]

Overview of Topic

- OpenDSA Blockchain Textbook - Ethereum
- Our task:
  - Ethereum Content and Exercises
- Format
  - RST File for Content,
    HTML/JavaScript for Exercises



Timeline


13 Sep.
Installed Docker and test compilation on individual host systems.
14 Sep.
Meet with Professor Shaffer to discuss updates for research and gain more feedback to continue.
24 Sep.
Provided ideas to Dr. Shaffer and draft content for the website pages.
01 Oct.
Implement the skeleton of the pages working on together.
22 Oct.
Review content of the pages with the teammates for revision.
02 Nov.
Implement the skeleton of the pages working on together. These skeletons include the text content we drafted.
03 Nov.
RST files resubmitted to Dr. Shaffer for review.
11 Nov.
Meeting with Dr. Shaffer to discuss more about exercises.
22 Nov.
The website is tested. Revisions of each page have been made. Final edits have been made in the next week.
02 Dec.
Final RST files were submitted to the client. Final presentation was delivered.
08 Dec
Finalized version of report and presentation was submitted to VTechWorks.

Proof Of Stake

- 2 Quiz Groups
- Details
  - How It Works
  - Proof of Stake vs. Proof of Work
  - Reviewing Previous Sections

4.4.1. What is a consensus algorithm?

A consensus algorithm is a method by which a distributed ledger is updated (that is, a new block is added to the block chain), and all parties come to agreement that this did happen. For more information, see **consensus**.

4.4.2. Block Structure Review

A blockchain is a series of blocks linked by hash pointers (pointers that each have an associated hashcode). A block has a header and a footer where the header contains information related to the identity of the block such as the creation time stamp and reference to the block before it. The footer contains data such as a collection of transactions. For more information, see **blocks**.

4.4.3. What is Proof of Stake?

Proof of stake is a way for an individual to validate (that is, claim the right to add) a new block to a distributed ledger. Proof of Stake is in contrast to the Proof of Work approach used in BitCoin. Proof of Stake is used by the Ethereum cryptocurrency since December 2020, and its most important distinction is that this validation process does not require “mining” in the sense of expending a significant amount of computing resources to claim the right to validate (and add) the next block. To indicate the distinction, the process of making the claim to validate the next block (and thereby gain the associated coin as a reward for this contribution to the community) is referred to as “forging” instead of “mining”.

Other cryptocurrencies that uses proof of stake as their consensus algorithm include Peercoin, Tezos (XZT), Binance coin (BNB), NEO, PIVX, Neblio (NEBL), Cardano (ADA), and Stratis (STRAX).

4.4.3.1. How does it work?

A new block is proposed for addition to the blockchain by a committee of community members selected for the purpose. A committee is a group of at least 128 validators. The number of committee members is decided by how many transactions that need to be approved at a time. For each transaction, there needs to be 32 validators. In addtion, there must also be one more validator to propose a new block to the blockchain. The committee is formed, and then must propose the next block within a set period of time.

To form a new committee, members are chosen at random from a pool of users. Individuals who have more coin invested in the cryptocurrency, and for a longer period of time, have a higher chance of being chosen for the validation committee. In Ethereum 2.0, users are required to stake 32 ETH to be entered for a chance to be a validator in the next committee. Those who have put up this stake form the population that competes to be selected. Individuals with less coin might choose to join a staking pool. Staking pools are groups of individuals who combine their coin together to increase the chances of the pool being chosen as a member in the next committee.

The reason that an individual might stake some coin to compete for a place in the next committee (or might join a staking pool) is that when the committee successfully has a block added to the blockchain, they receive a reward (as explained in the discussion on Ethereum **gas**).

Practicing Proof of Stake Validator

What increases an investor's chance of getting chosen to be a validator?

- Agreeing with previously known validators.
- Trying more complex algorithms for mining.
- Investing more coin into the pool.
- Hacking the cryptocurrency to gain more rewards.

Answer

Correct! Next question...

Show hints (1 available)

Hard Forks

- Details
  - Review: Consensus Algorithms
  - What Is a Hard Fork
  - What are the Effects of a Hard Fork?
  - How a Consensus Algorithm Influences a Hard Fork's Effect
- Quiz: Details of what a hard fork does

4.6.1. Review: What are Consensus Algorithms? ¶

A consensus algorithm is a method by which a distributed ledger is updated (that is, a new block is added to the block chain), and all parties come to agreement that this did happen. There are several implementations of a consensus algorithm including proof of work and proof of stake. Proof of work is where blocks are added by mining: computers guessing at algorithms to find the correct one and add a block to the chain. Proof of stake is similar to gambling where you invest a percentage of your coin to be randomly chosen for a validation committe and in that committee, members add new blocks to chain and approve transactions. For more information, see **consensus**.

4.6.2. What is a Hard Fork?

Another risk to consensus algorithms like proof of stake and proof of work is hard forks. Hard forks might be caused by a change in the blockchain's technology. Hard forks might result in blocks that had previously been validated becoming invalid, while other blocks might become valid by adding them to the chain. These forks can be started by developers or miners who are not satisfied with the current progress of the blockchain. They also are a way to fund projects.

Specifically, hard forks are caused by additions to block code that causes a new path with an upgraded blockchain. This fork causes two paths in the blockchain to appear for miners or validators. A fork like this can occur in any form of cryptocurrency that is based on blockchain. When a fork occurs, the miners, validators, and forgers of a particular coin must follow the changes since when a fork occurs, developers update the base code of blockchain to match the new networking rules. Hard forks can be implemented to undo damage caused by a hack (i.e. reversing transactions), adding new functionality (such as changing the consensus algorithm), and patching security risks.

4.6.3. What are the Effects of a Hard Fork?

Hard forks are in contrast to soft forks, which allows one side of the fork to continue to exist, removing the choice of path a miner can take in a hard fork. Hard forks effectively create a new cryptocurrency, while soft forks do not. Although these changes can be beneficial to blockchain users, they can cause a blockchain to become unstable. This is because hard forks can result from disagreements from within the cryptocurrency's community. Forks can result in price inflations as well, raising the cost of the coin. In addtion, in some cases, adding a hard fork can introduce vulnerabilities into the cryptocurrency. An example of this happened to Ethereum in 2019. A fork was introduced for Ethereum, which caused issues with smart contracts. The Constantinople fork was proposed in increased vulnerabilities within the smart contracts. The hashing algorithm within these contracts became repeatable and thus, increased the chances of a hacker accessing the information within the contracts.

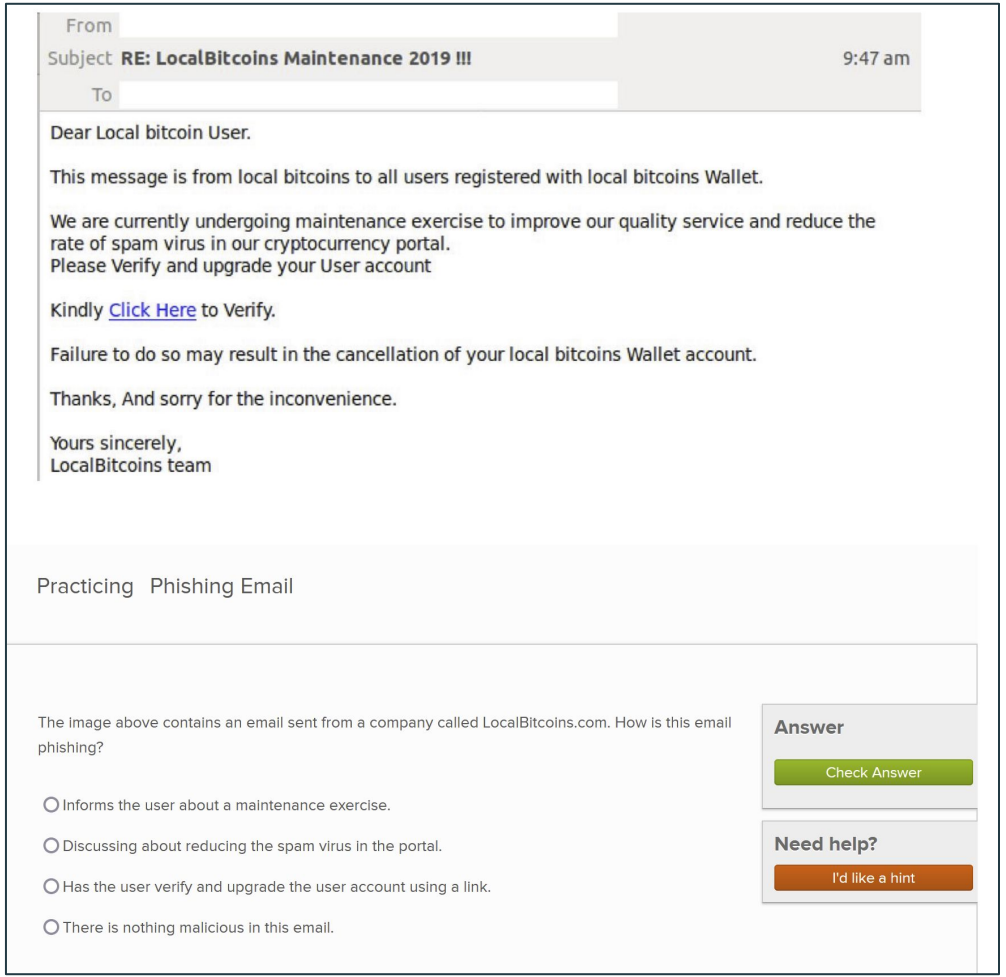
4.6.4. How a Consensus Algorithm Influences a Hard Fork's Effect

In the case of a hard fork for the proof of work algorithm, the miners must decide whethere to continue in the current path, or join the new blockchain. If the miner decides to choose to continue to support both chains in the fork, they must divide their resources between the two chains. Since the computing power is divided between the two chains, there is reduced resources dedicated to a chain or more strain on the computers they use to mine coin. In general, a fork is discouraged for proof of work systems because this causes more of an impact on the value of the currency by decreasing it and the developers of the cryptocurrency would need to choose the fork that does not cause vulnerabilities in the code base.

In proof of stake algorithms, forking is part of the validator's job. A validator must choose which block is beneficial to the

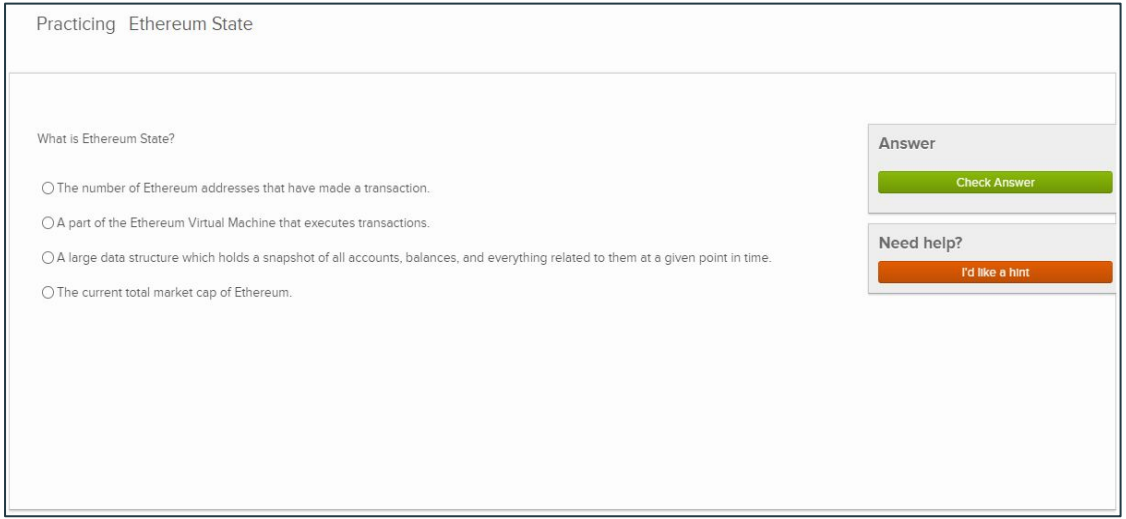
Crypto Hacking

- Quiz for Identifying Phishing
- Sections on:
  - What is Crypto hacking
  - Hacking Strategies
    - Phishing Attacks
    - 51% Attacks
    - Cryptojacking
  - How to Mitigate Risk

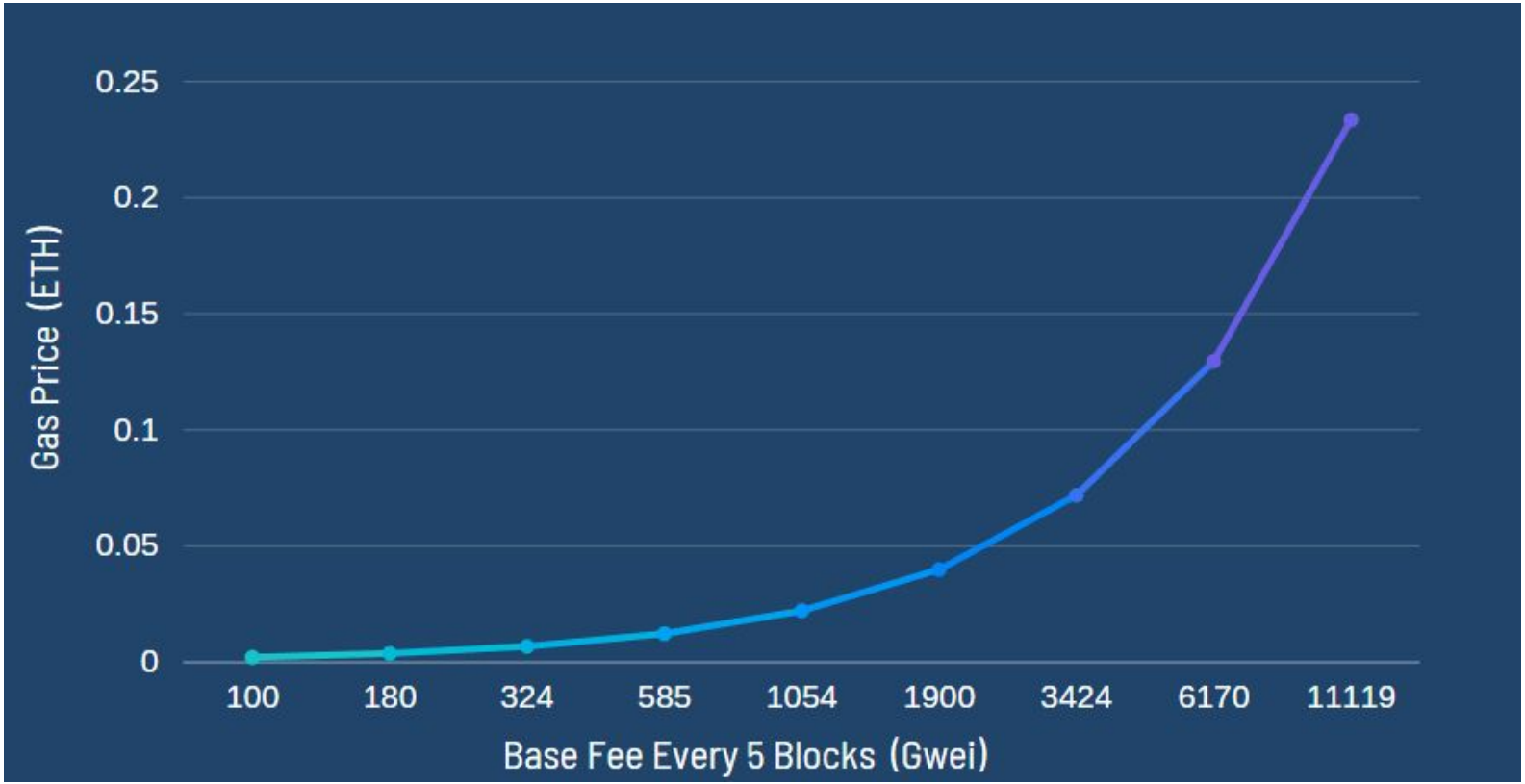


Ethereum Virtual Machine (EVM) and Gas

- Researched online and read Ethereum.org's official documentation
- Wrote prose about both subjects
- Designed exercises and visualizations

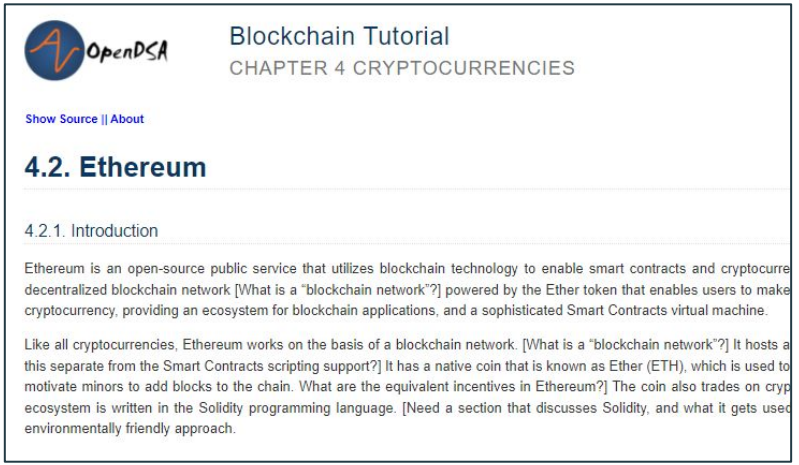


Visualization



Ethereum's Fundamentals

- **History of Ethereum**
  - Early days
  - The rise of the Ethereum blockchain
  - Future
- **Key differences between BTC and ETH**
  - Currency vs. Platform
    - Bitcoin: a credible alternative to traditional fiat currencies
    - Ethereum: A platform to run programmatic contracts and applications via Ether.
  - Average Block time
    - Bitcoin: 10 minutes
    - Ethereum: 10-15 sec



OpenDSA

Blockchain Tutorial

CHAPTER 4 CRYPTOCURRENCIES

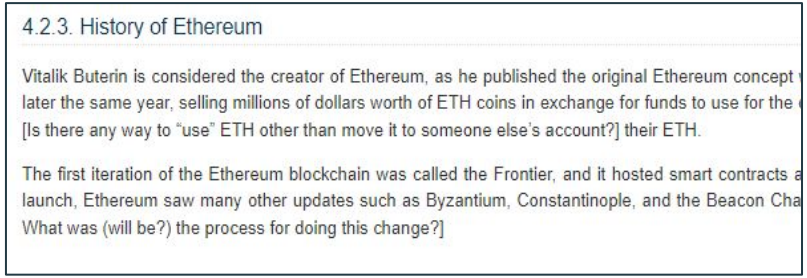
Show Source || About

4.2. Ethereum

4.2.1. Introduction

Ethereum is an open-source public service that utilizes blockchain technology to enable smart contracts and cryptocurre decentralized blockchain network [What is a "blockchain network"?] powered by the Ether token that enables users to make cryptocurrency, providing an ecosystem for blockchain applications, and a sophisticated Smart Contracts virtual machine.

Like all cryptocurrencies, Ethereum works on the basis of a blockchain network. [What is a "blockchain network"?] It hosts a this separate from the Smart Contracts scripting support?] It has a native coin that is known as Ether (ETH), which is used to motivate minors to add blocks to the chain. What are the equivalent incentives in Ethereum?] The coin also trades on cryp ecosystem is written in the Solidity programming language. [Need a section that discusses Solidity, and what it gets used environmentally friendly approach.



4.2.3. History of Ethereum

Vitalik Buterin is considered the creator of Ethereum, as he published the original Ethereum concept later the same year, selling millions of dollars worth of ETH coins in exchange for funds to use for the [Is there any way to "use" ETH other than move it to someone else's account?] their ETH.

The first iteration of the Ethereum blockchain was called the Frontier, and it hosted smart contracts a launch, Ethereum saw many other updates such as Byzantium, Constantinople, and the Beacon Cha What was (will be?) the process for doing this change?]

Testing

- Docker
  - Make Book
  - Exercises: Ensure working properly
  - RST files
- Editing
  - Dr. Shaffer reviewed RST files
  - Edited ourselves
  - Referenced people with no knowledge of Blockchain

```
History of Ethereum
-------------------

Vitalik Buterin is considered the creator of Ethereum,
as he published the original Ethereum concept whitepaper.
Buterin presented his concepts at a Bitcoin conference in Florida in
early 2014.
Following his initial work, others joined to help bring the project to
fruition.
His project raised capital through initial coin offering later the
same year, selling millions of dollars worth of ETH coins in exchange
for funds to use for the development of the project.
Ethereum went live officially in July 2015 even though ETH coins were
purchasable the year before.
Buyers had to wait for its launch before they were able
to move [between accounts?] or use [Is there any way to "use" ETH
other than move it to someone else's account?] their ETH.

The first iteration of the Ethereum blockchain was called the
Frontier, and it hosted smart contracts and used a proof of work
consensus algorithm.
This provided opportunities for people to set up
their mining apparatuses [since Ethereum was originally Proof of
Work?] and start building on the network.
After the initial launch, Ethereum saw many other updates such as
Byzantium, Constantinople, and the Beacon Chain, where each of the updates
changed certain aspects of the blockchain. [This needs a lot of explanation!]
Beacon Chain provided a shift from a proof-of-work to a proof-of-stake
consensus mechanism.  {When? How? What was (will be?) the process for
doing this change?]
```

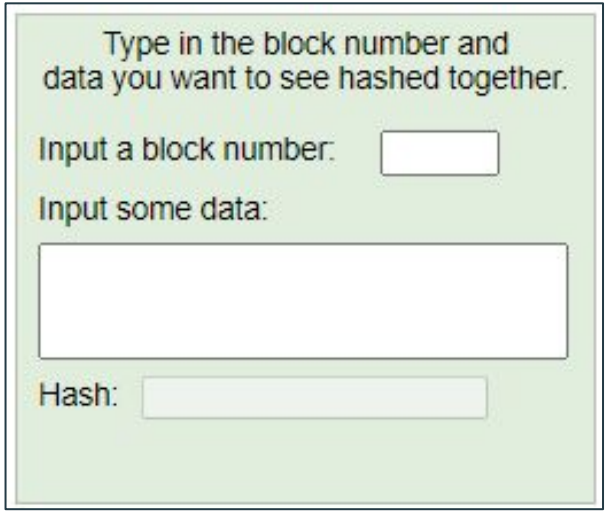
Challenges & Lessons Learned

- Group leader dropped class
- Writing textbook prose is more difficult than it appears
- Researching Blockchain content consumes plenty of time due to limited information available

Future Work

- Update information as it becomes available
- Other consensus algorithms
- Other cryptocurrencies
- Legislation
- Newer visualizations

[4]



[5]

Acknowledgements

[6]

Dr. Fox - Professor of CS 4624

[7]

Dr. Clifford Shaffer - Professor and Associate Department Head for Graduate Studies

Benjamin Parr - M.S. Machine Learning and B.S. Computer Science from Carnegie Mellon Blockchain and Machine Learning Researcher

References

[1] MIT, “Algorand uses a unique blockchain architecture developed by MIT Professor Silvio Micali to offer a decentralized, secure, and scalable platform,” *MIT News*. Cambridge, MA, United States: Massachusetts Institute of Technology. [Image]. Available: https://news.mit.edu/2021/unlocking-potential-blockchain-0616 Accessed on: Nov. 1, 2021.

[2] Ethereum, "Proof-of-stake (PoS)", *ethereum.org*, 2021. Accessed on: Oct. 15, 2021. [Online]. Available: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/. .

[3] J. Frankenfield, "What Is a 51% Attack?", *Investopedia*, 2021. Accessed on: Oct. 28, 2021. [Online]. Available: https://www.investopedia.com/terms/1/51-attack.asp.

[4] OpenDSA, “Blockchain tutorial,” *0.1. Understanding Blockchain - Blockchain Tutorial*. Accessed on: Dec. 02, 2021. [Online]. Available: http://lti.cs.vt.edu/LTI_ruby/Books/Blockchain/html/Introduction.html.

[5] OpenDSA, “Blockchain tutorial,” *0.2. Cryptography and Blockchain - Blockchain Tutorial*. Accessed: Dec. 08, 2021. [Online]. Available: http://lti.cs.vt.edu/LTI_ruby/Books/Blockchain/html/Cryptography.html.

[6] E. Fox, “Dr. Fox,” *Edward A. Fox Information Page.* Blacksburg, VA, United States: Virginia Tech. [Photograph]. Available: https://fox.cs.vt.edu/foxinfo.html. Accessed on: Nov. 2, 2021.

[7] C. Shaffer, “Dr. Clifford Shaffer,” *Virginia Tech Computer Science*. Blacksburg, VA, United States: Virginia Tech. [Photograph]. Available: https://cs.vt.edu/people/faculty/cliff-shaffer.html. Accessed on: Nov. 2, 2021.