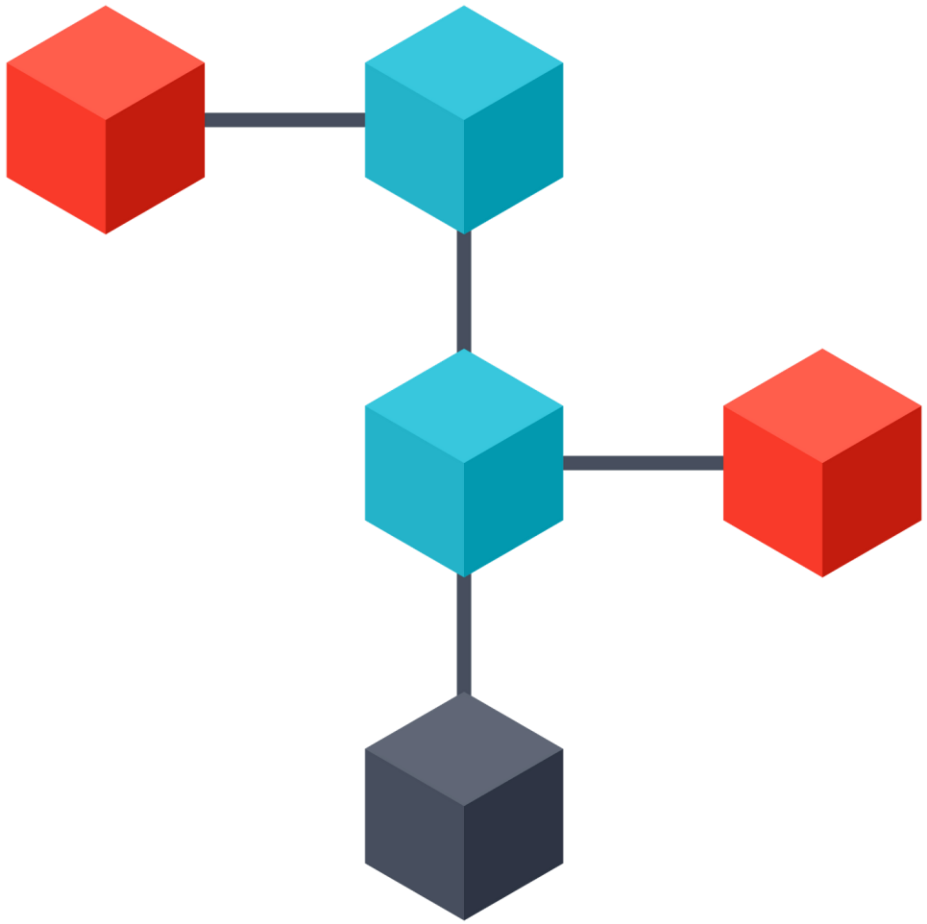
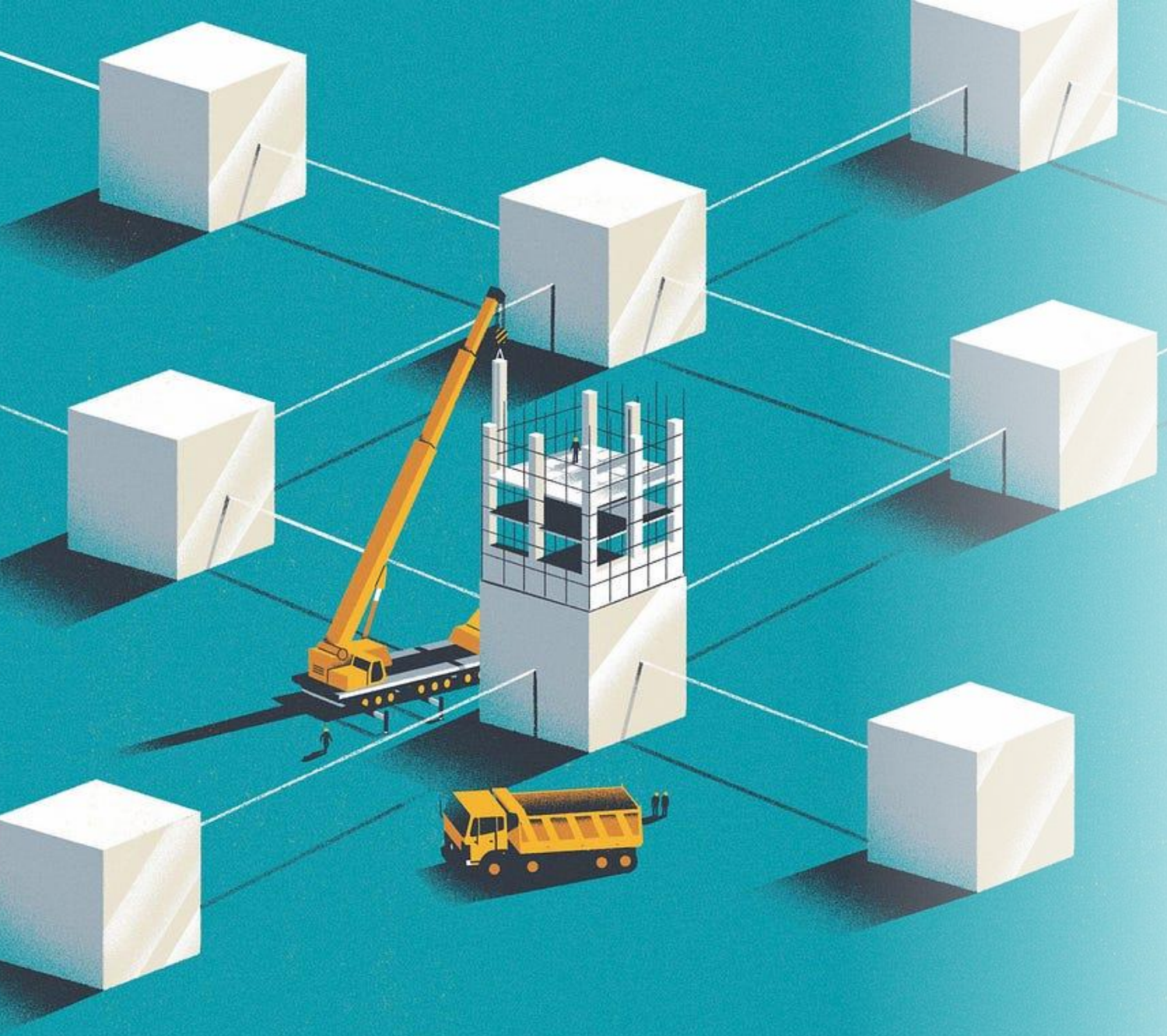


Redefining Trust: An Introduction to Blockchain Technology

Tristan Rocke



The purpose of this presentation is to provide an informative overview of blockchain technology based on personal research. My name is Tristan Rocke, and I am a current Computer Science major who has newly grown fond of this developing mechanism.

I believe that by educating one another on different aspects in tech, we can build a community of creative innovators that can provide fresh ideas and grand opportunities for the world.

In this seminar, I will highlight the key components that work together to provide a secure and immutable network that can provide many uses to our everyday life.

I will be providing my open souce code and documentation for the viewer to obtain more depth examples of smart contracts that are stored on a blockchain and execute when predetermined conditions are met.

These are my findings after a two month inquiry. Thank you, and I hope I can provide useful insight.

Understanding Blockchain Technology

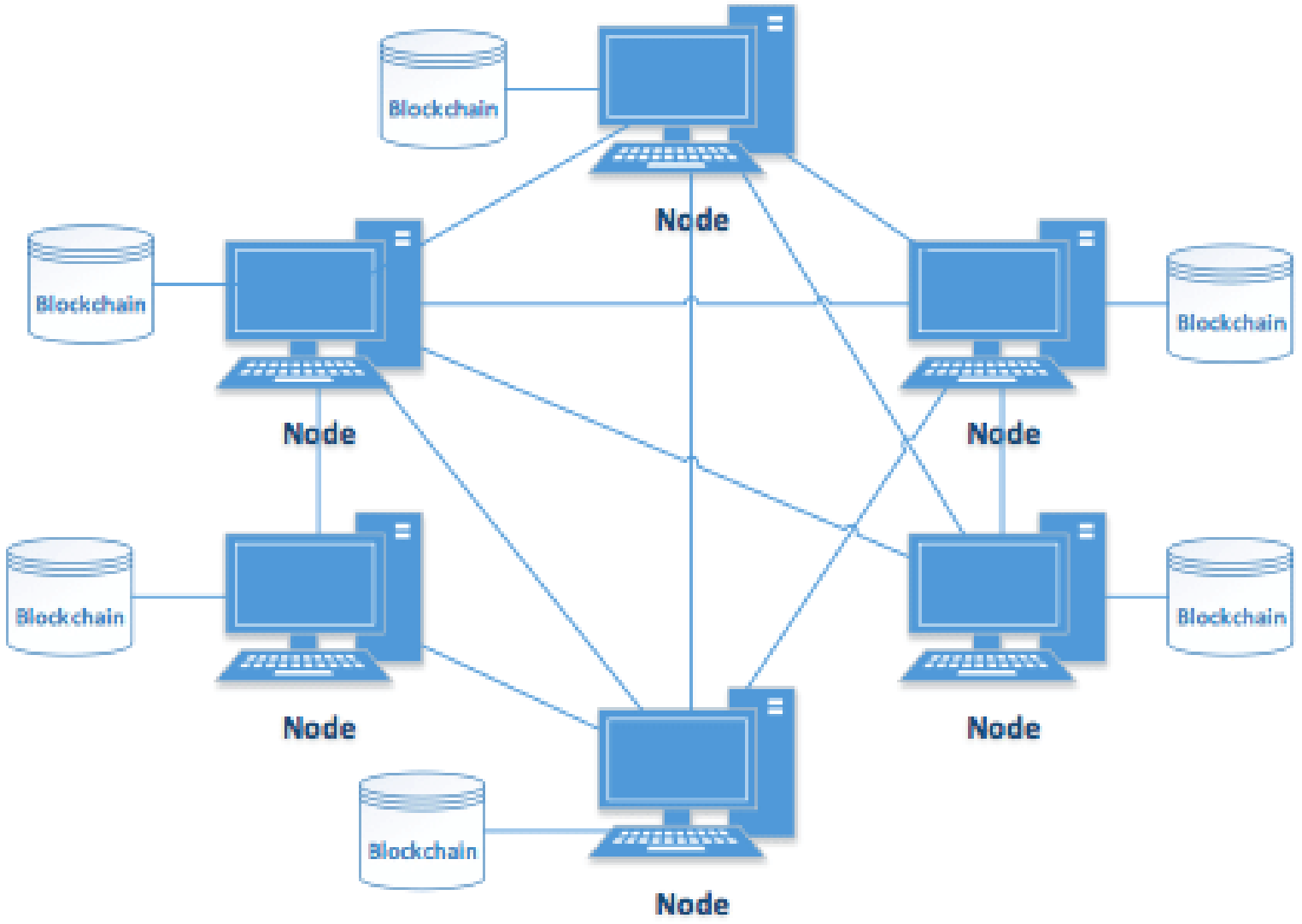
- We can think of blockchain technology as a digital system that allows users to securely and transparently store and exchange information or assets over the internet without needing to rely on a central authority, like a bank or a government.
- Instead of there being a physical ledger, we now have a digital ledger

This digital ledger is distributed across many computers worldwide, thus forming a network. Each computer in this network, is called a "node," and holds a copy of the same ledger. The term "block" is referred to as a container that holds a bunch of transactions or information.

For example, if people are using blockchain for financial transactions, a block could include information about who sent money to whom and how much.

This is where things get interesting. Once a block is filled with transactions or information, it is added to the existing blocks in a specific order, forming a chain.

This chain is what is called the "blockchain." Each block in the chain contains a unique identifier, called a "hash," which helps to identify and link it to the previous block.


Blockchain
Node
Blockchain
Node
Blockchain
Node
Blockchain
Node
Blockchain
Node
Blockchain
Node

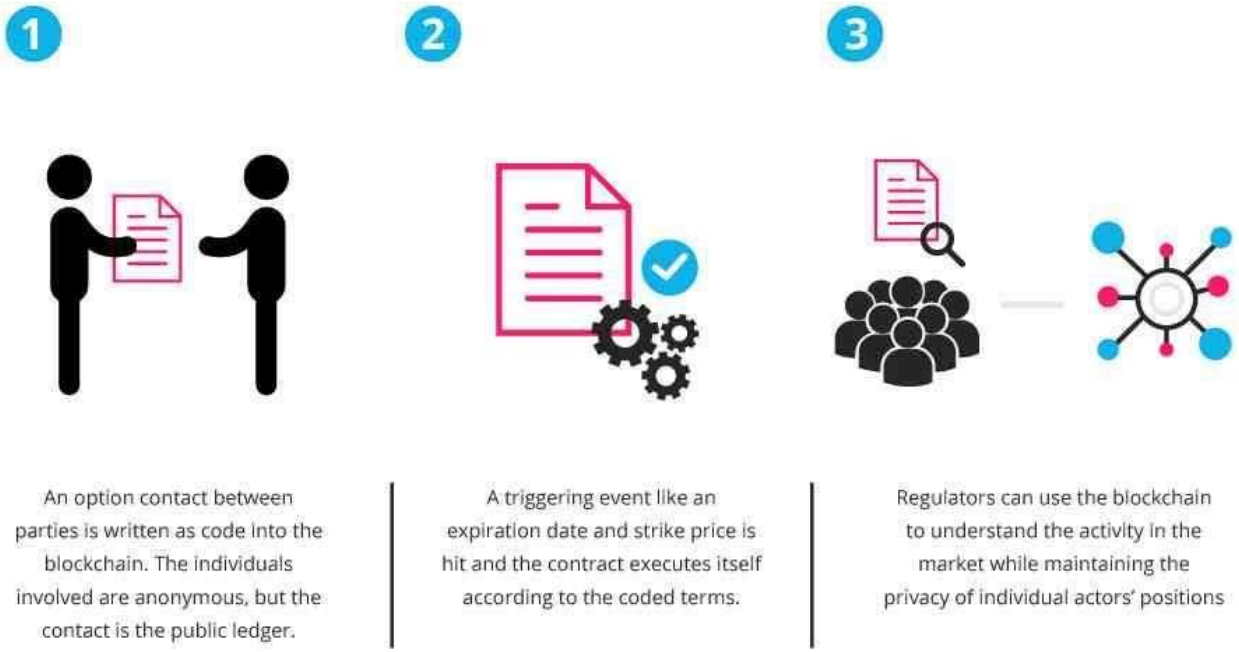
Key components of blockchain

decentralization: What makes blockchain special is its decentralized nature. Instead of relying on a single authority, like a bank, to verify transactions and maintain the ledger, blockchain relies on a network of computers working together.

Transparency and Auditability: Blockchain provides a public record of all transactions. Every transaction recorded on the blockchain is visible to all participants, providing transparency and accountability. This characteristic helps prevent fraud and enhances the trustworthiness of the system.

Immutability: blockchain securely records transactions without the possibility of alteration. Once a block is added to the blockchain, changing the information in it becomes extremely difficult, ensuring the integrity of the transaction history.

Potential for Innovation and Disruption: Blockchain technology has the potential to disrupt traditional business models and enable new forms of decentralized applications and services. It can enable novel solutions in areas such as decentralized finance (DeFi), decentralized identity, decentralized marketplaces, and more. Its relevance lies in fostering innovation, promoting entrepreneurship, and challenging existing centralized systems.



Smart Contracts

Smart contracts are self-executing contracts with the terms and conditions directly written into lines of code. These contracts automatically execute and enforce the agreed-upon rules and actions without the need for intermediaries or manual intervention. Smart contracts are stored and executed on a blockchain, ensuring transparency, security, and reliability. Once the predefined conditions are met, the contract is executed, and the associated actions are carried out. The key advantage of smart contracts is their ability to facilitate trust and automate processes, eliminating the need for third parties and reducing the potential for errors or manipulation. They have a wide range of applications, including financial transactions, supply chain management, decentralized applications, and more.

A new era: Ethereum

Ethereum is a blockchain platform that enables the creation and execution of decentralized applications (DApps) and smart contracts. It is one of the most prominent and widely used blockchain networks.

What sets Ethereum apart from other blockchains, like Bitcoin, is its ability to support programmable smart contracts.

Ethereum introduces its native cryptocurrency called Ether (ETH), which serves multiple purposes within the Ethereum ecosystem. Ether acts as a digital currency that can be used to facilitate transactions and pay for computational resources on the network.

Additionally, Ether is often used as a utility token within DApps, allowing users to interact with and access the functionalities offered by these decentralized applications.

Ethereum has become a thriving ecosystem for developers, entrepreneurs, and users, with a wide range of applications built on top of its blockchain. It has sparked the rise of decentralized finance (DeFi) platforms, non-fungible token (NFT) marketplaces, decentralized exchanges, gaming applications, and more.

Solidity

- Solidity is a programming language specifically designed for developing smart contracts on the Ethereum blockchain. It is a statically-typed, contract-oriented language that allows developers to write code to define the logic and behavior of smart contracts.

- Solidity enables developers to create complex and self-executing contracts that can be deployed on the Ethereum network. It is the most widely used language for writing smart contracts on Ethereum and has become the standard for Ethereum-based decentralized applications (DApps).

ERC-721

In this next section, I will link my GitHub, as well as the tools I will be using to demonstrate the one of most common types of Ethereum based smart contracts, The ERC-721 contract. I have used the knowledge I have gained to form deployable code that will guide the user on how to properly work and navigate a blockchain, especially for a new user. This will be done by using the REMIX IDE which is a cloud-based IDE provided by Ethereum for developers open use. I will also be using ganache which is a test blockchain ledger that simulates live transactions.

1. ERC-721: ERC-721 is a standard for creating non-fungible tokens (NFTs) on Ethereum. Unlike ERC-20 tokens, ERC-721 tokens are unique and indivisible, representing ownership or proof of authenticity for a specific asset. NFTs have gained significant popularity for representing digital art, collectibles, and virtual assets.

Links & Sources of research.

Online documentation and research

- https://remix.ethereum.org/'
- https://ethereum.org/en/what-is-ethereum/
- https://trufflesuite.com/docs/ganache/
- https://docs.soliditylang.org/en/v0.8.20/
- https://docs.openzeppelin.com/contracts/4.x/erc721

GITHUB link: https://github.com/Goodbyefrog/Introduction-to-smart-contracts

Books

Proof of Stake: The Making of Ethereum and the Philosophy of Blockchains (2022) - Vitalik Buterin