iBlock: A private Blockchain

Abstract
Blockchain technology is a highly promising and futuristic disruptive technology that is still in its early stages of adoption. To better understand this technology by engaging the university members, Gies School of Business at the University of Illinois has deployed a private Ethereum blockchain network. This involves the development of a native ERC-20 token named Gies Coin and a Marketplace Decentralized Application (Dapp). This private network runs currently on a Proof-of-Work mechanism but in the future, we aim to switch to a 'clique' Proof-of-Authority consensus mechanism where an identified group of authorities ensure the integrity of all transactions on the blockchain.

Introduction

Disruptive innovations like the Internet, and Machine learning and Artificial Intelligence has already changed the way our world operates today. Our day-to-day life is highly automated and involves a high volume of value transfer in the form of data, money etc. With such fluxes of value around the world, privacy and transparency issues are on the rise, which most of the time includes a trust factor on the intermediary handling the store of value.

In 2009, Satoshi Nakamoto, as pseudonym, came up the idea of a peer-to-peer version of electronic cash, called Bitcoin, that didn't require an intermediary to exchange it and was completely transparent which also solved the double spending problem. Double spending is the problem where a digital form of cash can be spent more than once. Satoshi Nakamoto solved this problem by coming up with a decentralized public ledger system where a copy of the whole history of transactions is shared throughout the network participants. These participants were called nodes. The system operates by tallying the records available to all nodes and forming consensus over the valid list of transactions by creating a block and adding it to the chain of other blocks in an order, called the "blockchain". Since the system is trustless and consensus-based, it is prone to manipulation by the nodes if majority node operators come together to cheat the system for mutual gains. To prevent this, an incentive program was developed where each node competes with one another to create a block and provide a proof of their work through computation input. This is also called a Proof-of-Work (PoW) mechanism where the node provides a sufficient computational input by finding a unique number developed through encryption (also known as a nonce) to bring a group of transactions together to create a block. The node receives a certain amount of digital cash for providing the work and creating the block. Since Bitcoin is considered a form of digital gold, the process of creating a block was made analogous to mining the gold, and therefore, those nodes who create blocks are called "miners".

Building on the revolutionizing developments in the decentralization of exchange of value, Ethereum protocol introduced smart contracts in 2017, which allowed programmable transactions in exchange of services, paving the way for decentralized apps or Dapps. Its main network (also called Ethereum mainnet) also works on Proof-of-Work, although Ethereum protocol does allow for other consensus mechanism, of one which is Proof-of-Authority (PoA).

In our work, we have implemented PoW for now to test the functionality of the system, but we aim to eventually move to a Proof-of-Authority consensus framework to save on high computational costs and to create a more secure blockchain network. We strive to implement 'clique' proof of authority consensus algorithm which requires a set of recognized authorities to verify transactions and create blocks.

In the coming sections, we discuss the milestones achieved during this summer and future scope of work.

Methodology

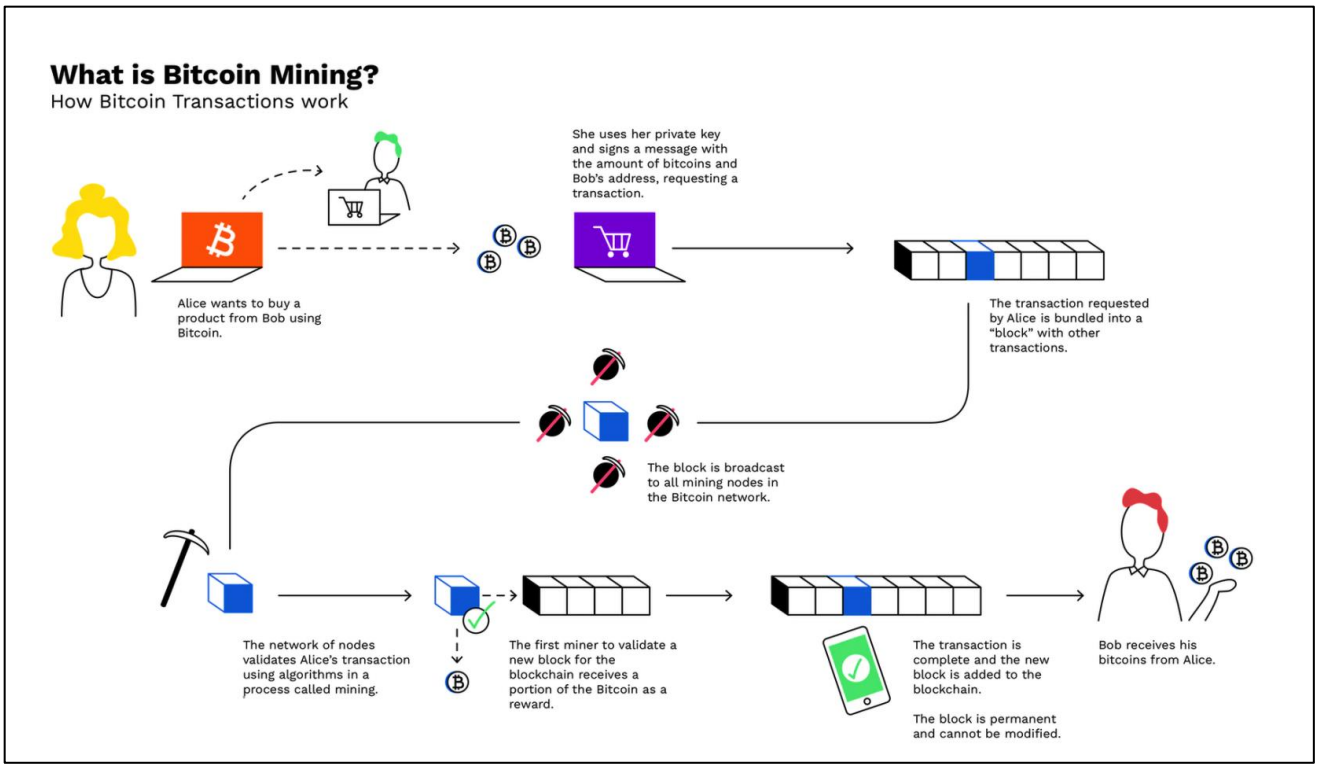
The iBlock private blockchain is an Ethereum private network which means that it follows Ethereum protocol, but it is not connected to the main Ethereum network because the nodes of this network are not connected with the mainnet. The nodes on this network are deployed using Geth. Geth runs a virtual machine, called the Ethereum Virtual Machine (EVM), which compiles the byte code to store the state of the blockchain. The iBlock currently runs a Marketplace dapp that sells Illini merchandize and other Illini products. This Dapp uses a cryptocurrency called "Gies coin" which is an ERC-20 token (explained in glossary). The process of blockchain and marketplace development is explained in detailed below.

Public vs Private blockchain

A Public Blockchain is a permissionless blockchain. Anyone can join the blockchain network, meaning that they can read, write, or participate with a public blockchain. Public blockchains are decentralized, no one has control over the network, and they are secure in that the data can't be changed once validated on the blockchain. On the other hand, a Private Blockchain is a permissioned blockchain. Permissioned networks place restrictions on who is allowed to participate in the network and in what transactions. Since iBlock is a private blockchain, only University of Illinois, Urbana-Champaign students has the access to this network.

Blockchain as a decentralized ledger

The iBlock network uses a PoW consensus mechanism (till now) which means that it works exactly as the Ethereum main network. When we compare Ethereum mainnet with Bitcoin as a decentralized ledger, they work quite the same. Given below (Figure 1) is a schematic representation of Bitcoin (as a PoW network) works. First a list of transactions is created. Then, this list is sent out to all the other nodes in the network. After that, Miners in the network try to find a unique number so that when a block is created, it satisfies a number of trailing zeros in the valid hash. Block is completed once a valid hash is found. Finally, A new block is added to the blockchain network.



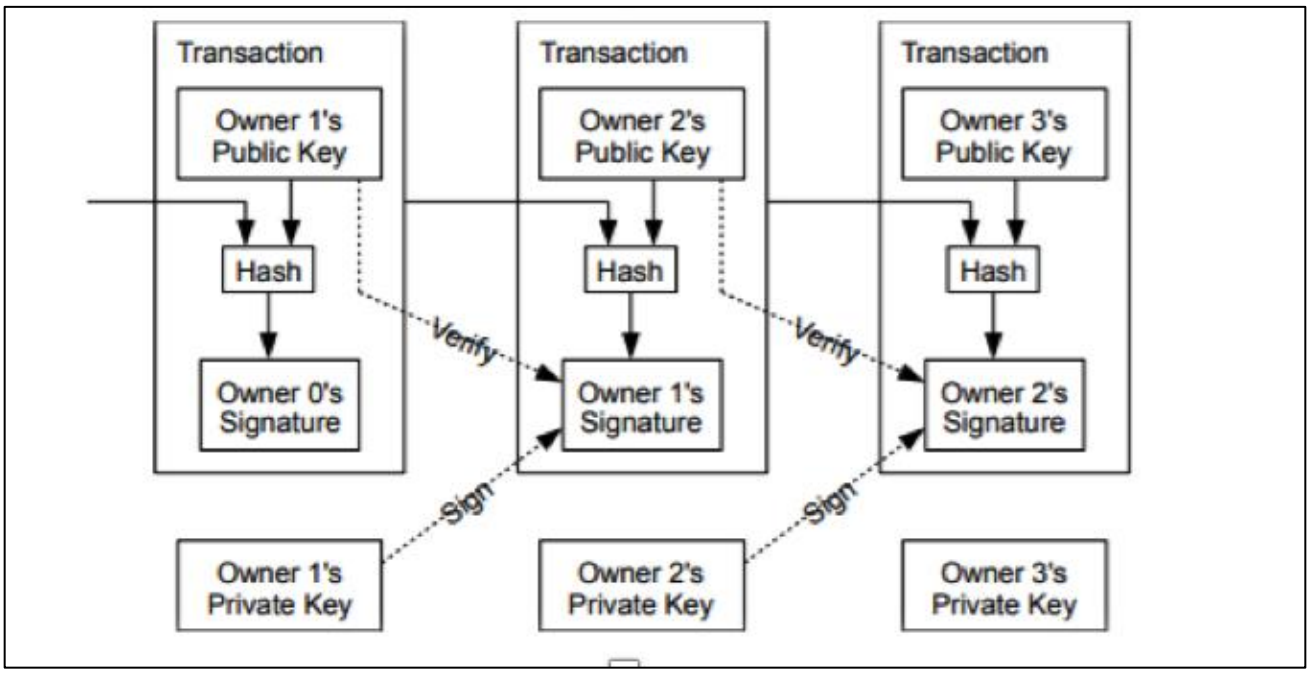


Figure 1: Depicts the functioning of Bitcoin network.

Smart Contracts

A Smart contract is simply a program that runs on the blockchain. It is a collection of code (its functions) and data (its state) that resides at a specific address on the blockchain. A schematic representation of the functioning of a Smart contract is given below (Figure 2). In the Ethereum network, a smart contract is executed as a transaction, since the buyer changes the data stored in the ledger (changes the state of the ledger).

Since each Ethereum transaction requires computational resources to execute, each transaction requires a fee. Gas refers to the fee required to successfully conduct a transaction on Ethereum. Gas fees are paid in Ethereum's native currency, ether (ETH). Gas prices are denoted in gwei, which itself is a denomination of ETH - each gwei is equal to 0.000000001 ETH (10^{-9} ETH).

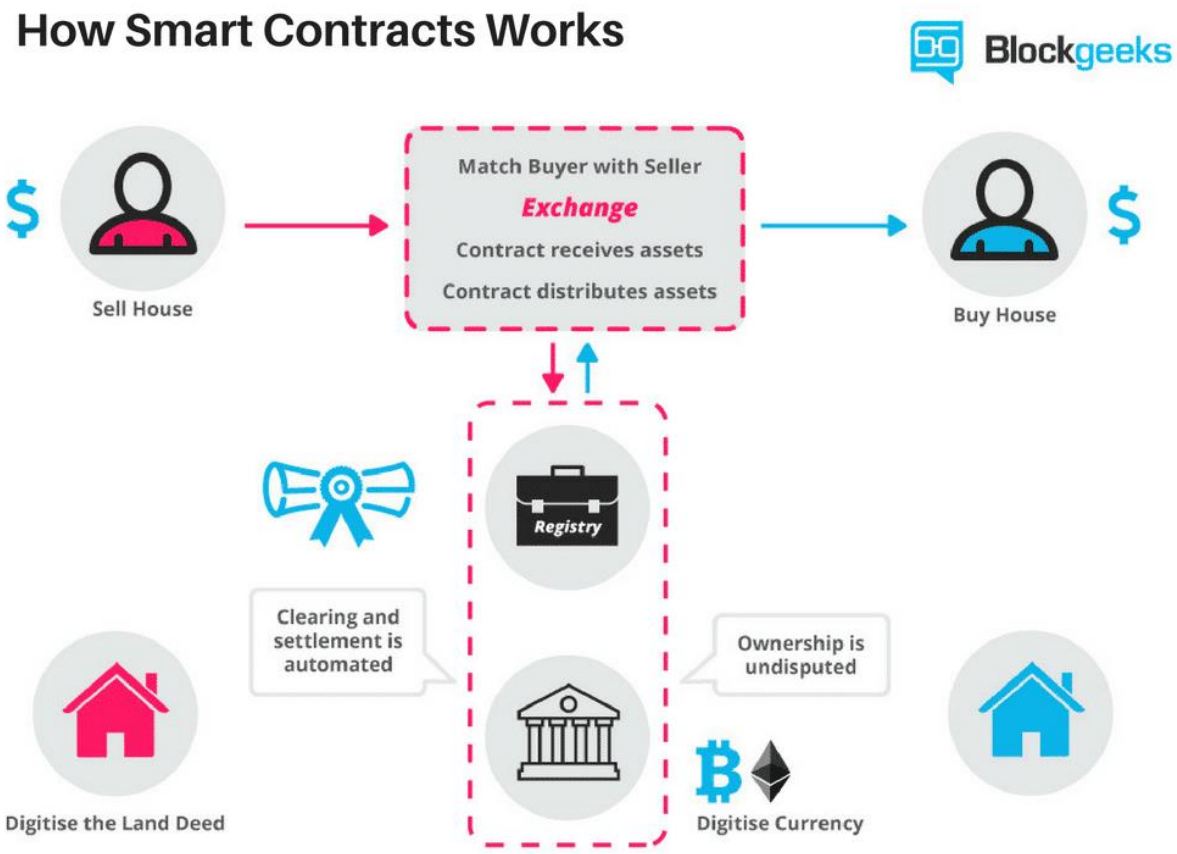


Figure 2: Functioning of a Smart contract.

The Marketplace Dapp

Marketplace will function with the circulation of the Gies coin that is created for exchange within iBlock. Currently, we are working on the tokenomics which includes assigning value to the coin,

deciding the circulation supply, token's nature (inflationary or deflationary), incentives for block creation and deciding the gas fee.

Glossary

1. *ERC-20*: It is a token standard and provides a list of rules that all Ethereum-based tokens must follow.
2. *Node*: A user on the network that holds the whole copy of the blockchain.
3. *Miner*: It is a node that provides the computational work required to create a block and in turn mints the cryptocurrency as an incentive.
4. *EVM*: It is a software platform which helps developers communicate with the machine.
5. *GWEI*: Gwei, short for Giga-wei, is a denomination of the cryptocurrency ether (ETH), which is used on the Ethereum network.