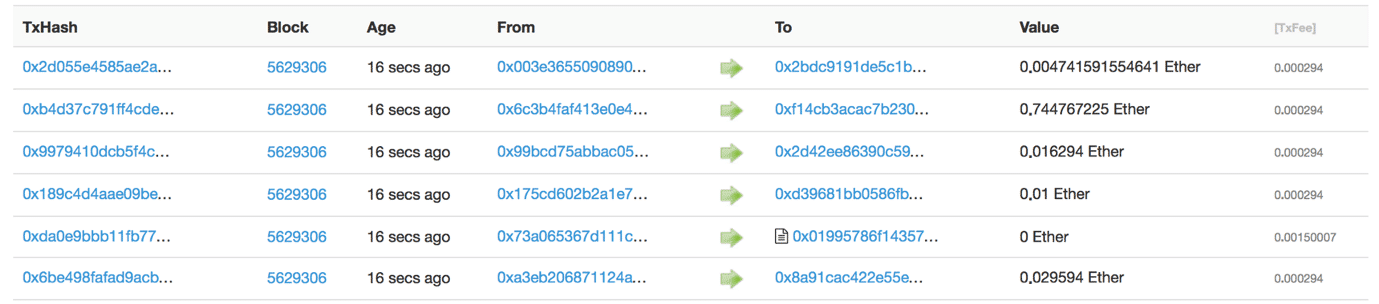
Blockchain is a fairly new technology that emerged with the introduction of the famous CryptoCurrency BitCoin. But there are many uses of blockchain besides just CryptoCurrency, for example, Walmart has a blockchain that allows them to track their produce and the United States Postal Service has placed a patent to use blockchain as an identity verification measure. Blockchain is used for tasks as simple as securing databases to as complicated as monitoring carbon offsets. It can also be used to manage an auction and would be able to safely transfer money, keep identities of bidders secure, and keep an accurate ledger of the bids.

A blockchain is basically a permanent digital ledger of transactions. Blockchains are decentralized meaning that the network has no central authority. That way there is not just one authority deciding what is true and altering the ledger for their own benefit. These ledgers are immutable; it is essentially impossible to change the ledger.[1] This is because of the chained blocks in the blockchain. Each block’s hash, “the output of a mathematical function”[2], requires its previous block’s hash.

Blockchains are also very secure while being transparent at the same time. They are transparent in the sense that the ledger is visible to everyone in the network, but it is secure and private in the sense that a user’s information is not shown. Instead, their public addresses are shown. For example, in figure 1 all of the transactions can be seen but the identities of the users are represented as their public addresses. Blockchains are also very secure in storing information **Figure 1:** This is a sample of an Ethereum (IDE for blockchain smart contracts) ledger. because, as mentioned above, they are impossible to alter. It would take 51% of the servers to alter a block.[3] Creating a fake block can be easily spotted by the network unless 51% majority is in on the fraudulent activities and verifies the block. But the 51% attack is very very rare in large networks.[3]

As mentioned above, blockchains can be used for a lot of functions including auctions. Auctions deal with sensitive information, such as large amounts of money and the identities of the people with large amounts of money. There are many types of auctions; the four basic types of auctions are English auctions, Dutch auctions, first-price/sealed-bid auctions, and second-price/sealed-bid auctions, also known as Vickrey auctions.[4]  The first two auction types are open, meaning that all the people know what each other’s bids are, however, the latter two are sealed-bid, where each person places their bid in an envelope. Also, only the Vickrey auction is a second-price auction, meaning the highest bidder gets to pay the second-highest bid.[4]  In the first-price auctions, the highest bidder pays the price they bid, but in the last auction type, the second-bid auction, the highest bidder gets to pay the second-highest bid. [4]

The goal is to build a smart contract for a blockchain-based English auction with one aspect of the Vickrey, which allows the highest bidder to pay the second-highest bid. The goal is also to learn more about blockchain and how it works.

More research was conducted to understand blockchains, the IDE called Ethereum that is well known for running smart contracts, and the programming language Solidity. After a base auction code was required, changes were made to add the extra features to the auction. Then the code was tested to find any glitches and to make sure that the number of ethers was correctly being subtracted and returned.