Introduction

This introduction only aims to communicate a basic understanding of HOM Coin, and not any fine details. Any questions not answered in the introduction will be explained in other parts of this document.

HOM Coin is a cryptocurrency and decentralized database focused on real estate, which allows quick and seamless buying of homes. It is implemented as an ERC20 token on the Ethereum blockchain.

As a cryptocurrency, it can be bought, sold, and transferred without a third party. Most transfers complete within 8 to 30 seconds, and are thus far faster than any large bank transfer. The time taken to complete a transfer does not increase with larger transactions either, so expensive homes can be paid for just as fast as a cup of coffee.

As a decentralized database, it functions as a way to store information about houses online. Unlike centralized databases, it cannot be taken offline, and it can be accessed from anywhere. The information on the database is still trustworthy however, because only the HOM Coin contract owner can add or modify entries in this database.

Unlike most other cryptocurrencies, the HOM coin has a fixed price. Nobody wants to sell a home with other cryptocurrencies because they don't know what the currency will be worth when the buy completes. HOM solves this problem. Each HOM coin is worth $1000.

The HOM Coin

HOM coin exists through an Ethereum smart contract, so it inherits the security of an enormous blockchain but can still be engineered to meet requirements. The HOM coin is an ERC20 token, so it can be transferred using any Ethereum wallet. It can also be transferred and managed from computer programs that interface directly with the blockchain.

HOM Coin can be traded without a third party. The HOM Coin smart contract contains functions which allow it to be bought and sold with Ethereum.

The HOM Coin Database

The HOM coin database exists as a collection of Ethereum transactions. When data about a house is created or modified, an Ethereum transaction is sent to the HOM coin smart contract. Cumulatively these transactions form the data in the database, and they can be scanned to get the data about a house. It also records every change ever made to the data in the database, so a history can be kept.

Only the HOM coin contract owner is allowed to update the database, but the information on the database is publicly accessible. This database can be accessed by both centralized programs and decentralized Ethereum smart contracts.

Disclaimer

The HOM Coin Project does not intend to provide any sort of investment opportunity or profit. The value of HOM Coin may depreciate if there is not enough transactions to keep the price stable, or if the HOM Coin smart contract runs out of Ethereum. The HOM Coin contract may be destroyed.

HOM Coin Uses

HOM Coin is intended to be used as a trustless, decentralized payment method for real estate. Additionally, it can be used as a database of homes. Although not all homes on the earth or in any country may be listed, it can be used to search for homes meeting certain criteria. Houses may be listed for sale or lease. Computer programs may listen for homes that just opened for sale. The HOM Coin contract can be freely interacted with from computer programs and smart contracts alike, automation is also possible.

Similar Technologies

There are some similar technologies to HOM Coin, however strengths and weaknesses differ between solutions.

Tether (USDT)

Tether is a stable cryptocurrency built on the Bitcoin blockchain. It's price is kept at one United States dollar, and it is backed in real dollars. The money that it is backed with exists off of any blockchain. It does not, however, have a built in system for buying and selling homes.

Similarities to HOM Coin

- The price is kept stable
- They are cryptocurrencies
- Both operate on the blockchain of a larger cryptocurrency
- Both have some centralized part

Differences from HOM Coin

- Tether is backed in fiat currency, not entirely on the blockchain
- Tether must be traded through some sort of exchange or third party

- Tether requires a company to exist to keep its price stable
- HOM Coin has a centralized program to keep the price stable
- HOM Coin has a built-in database for homes
- Tether is more general-purpose, HOM Coin is more specialized
- HOM Coin can be interacted with via smart contracts, Tether cannot
- Tether does not have a built in system for buying and selling homes

One is not necessarily better than the other in general, but they are better suited for different things. HOM Coin is best for larger transactions and storing data about homes. Tether is better suited for trading and smaller transactions. Both should be used in situations where the value of funds cannot be allowed to change quickly.

It is important to note as well that decentralized applications will find it easier to interact with HOM coin because it exists as a smart contract. Tether cannot be used by smart contracts without some program to transfer data and send transactions between two separate blockchains.

Implementation

The HOM Coin is implemented as an ERC20 smart contract on the Ethereum blockchain. A special program, referred to as the "oracle program", keeps the price of HOM Coin stable.

The Smart Contract

The smart contract doubles as an ERC20 token and a database. Each is entirely separate from the other, with their own owner accounts, variables, functions, and events.

The ERC20 token component is normal and follows the ERC20 token specification, however is has more features. The HOM Coin contract provides functions that allow anyone on the Ethereum network to buy HOM Coin with their Ethereum, or sell their HOM Coin back. Unlike real markets or exchanges, when a purchase or sale is made, no order is created. Instead, the contract itself buys or sells the tokens at a set price. This price is a conversion between HOM Coin and Ethereum, and it is set by the Oracle program. Since the price of Ethereum can fluctuate, the price of HOM Coin relative to Ethereum must change to keep HOM Coin steady against the dollar. When a buy or sell is executed, the smart contract checks to ensure that the transaction is paid for before executing it. If the contract detects any errors or mistakes then the transaction is reverted.

HOM Coin's database is publicly accessible. It can be read by anyone, and it is located on Ethereum's decentralized blockchain. To read from the database one can simply listen for events or read the contract's variables.

Only the database owner may alter the database, create entries, or post house offers.

The Oracle Program

Since Ethereum is volatile, the price of HOM Coin relative to Ethereum needs to change to stay constant against the dollar. The oracle program changes this relative price constantly to keep the HOM Coin price stable.

The oracle program has its own Ethereum address, separate from the database owner or the contract owner. This way, malicious access to one component does not compromise the others.

The oracle program must execute transactions to keep the HOM Coin price stable, which have transaction fees. This is why every trade executed on the HOM Coin contract has a tiny fee, which goes to this program. The fees lower as the oracle program collects more Ethereum, and increase as the Ethereum is spent. If the oracle program has enough Ethereum, then half of the fees go to the owner account instead, and the other half is kept by the HOM Coin smart contract.

Team

Dylan Brophy

Blockchain engineer and HOM Coin CEO. Ensuring security, reliability, transparency, and good business. Dylan is in charge of writing the smart contract and overseeing every aspect of the HOM Coin project.

Patrick Hustad

Pat Hustad is a licensed realtor and software engineer developing a new real estate protocol to allow users to find a home, transfer funds and sign paperwork turning home buying into a seamless process that can take as little time as making a purchase on Amazon.

Brian Helm

Brian Helm is a software engineer developing the HOM coin purchasing system along with the platform that will power the HOME buying transaction from start to end.

Roadmap

Pre-Donation and Setup Stage

The whitepaper, website, and social media all must be complete and/or set up at this point. The HOM Coin smart contract should be mature at this point, but may not be finalized. A contact email needs to be made available in this stage. The website should have an about page, documentation on the smart contract, and a donation system receiving Ethereum, Bitcoin, and US Dollars.

Marketing and Press

The object of this stage is to make HOM Coin known and to start raising capital. Press releases and articles are to be made for this purpose.

Once HOM Coin is known, there should be some people willing to donate. This money will be used to keep the project website up, pay any unexpected expenses, and in the future to do professional smart contract audits. Ethereum will be purchased and donated to the smart contract to allow the buying and selling of HOM Coin. Any money left over will be kept in a bank account to earn interest. 20% of this interest will stay with the HOM Coin project, the remaining 80% will be given to the team members, divided equally. This way, the team can still be paid, and the HOM Coin project can earn money still when idle.

Additionally we may be able to receive feature requests or ideas for HOM Coin.

Working Trading Platform

This stage serves to put HOM Coin in the hands of consumers and to earn more money to create HOM Coin. By this time the final HOM Coin smart contract will need to be deployed.

HOM Coin will need to be available for trade in fiat currency. Although it can always be traded through the smart contract, an easy-to-use trading platform will allow users to buy and sell HOM Coin, and provide another source of funds and income.

This is not easy to set up in earlier stages because regulations require that trades only be executed by those older than 18, thus an identity verification process must be implemented. In this stage funds may also be used to create and maintain this system.

Legal System to Buy Houses

The final stage listed here will create a way to allow consumers to use HOM Coin to legally purchase houses on the blockchain. This system can be given to outside companies such as Propy and Homebay to create a standardized system for efficiently and easily buying houses using blockchain technology.

At the end of this stage HOM Coin will be completely usable and operational, both within the blockchain and outside of it.

HOM Coin Adoption

With HOM Coin fully functional, it can now be adopted by consumers, builders, and companies to completely upgrade and streamline the real estate industry. HOM Coin will need to be used by a few companies at first to move towards being an industry standard. Gradually all participants in the real estate industry will need to accept HOM Coin as a system of buying and selling houses to compete in their markets.

Security

This section is intended as a discussion to confirm that the HOM Coin smart contract is indeed safe to use. It is also intended as a way to know what attacks may be possible in the future, and to find ways to prevent these attacks.

Potential Security Weaknesses (and solutions)

Smart Contract Vulnerabilities

Hypothetically, there could be a bug in the smart contract that would make it vulnerable to attack, but this is extremely unlikely. The prototype HOM Coin contract has already been through many test versions, and the most sensitive logic is very simple, so has less room for security holes. The smart contract has not yet been audited by professionals, however it has been checked for many smart contract vulnerabilities (More details on audits will be available in the "Smart Contract Audits" subsection).

Note that all of the vulnerabilities listed here can be found in other smart contracts, and the HOM Coin contract was checked and secured against them.

Reentrancy

The HOM Coin smart contract strictly follows the "Checks Effects Interactions" pattern, which prevents reentrancy. The smart contract state is fully updated before any transfers of funds occur.

Reentrancy can allow another smart contract to withdraw all of the Ether in vulnerable smart contracts.

Overflows

The HOM Coin smart contract checks for overflows before executing any transaction involving transfers of currency. If an overflow condition is detected then the transaction is reverted. It is possible (however extremely improbable) that an overflow case still exists in the smart contract.

Overflows can allow an attacker to "trick" a smart contract by making it add two numbers, the result of which the contract cannot process. Instead of reverting the transaction, a vulnerable contract would make this number significantly smaller to allow processing, thus making calculations incorrect, often involving transfers of currency.

Unexpected Ethereum

The balance of the smart contract does not change the functionality of the contract, or how the contract behaves, besides the ability to send Ethereum to sellers. Thus, if the HOM Coin smart contract receives unexpected Ethereum, it only helps the contract to be able to buy more HOM Coin back.

Unexpected Ethereum can be an issue when a smart contract checks for exact balances or requires the balance to fit specific parameters. If Ethereum is received unexpectedly, then the contract can be broken.

Libraries

This does not apply because the HOM Coin smart contract uses no external contracts. It does transfer fees to the Oracle program and the owner account, however there is no vulnerability to be exploited there.

Some contracts that use libraries can end up using a maliciously deployed smart contract instead of the intended library, thus causing miscalculation.

Short Address Attack

The HOM Coin smart contract checks transactions for maliciously encoded data, preventing incorrect transfer of funds or improper interpretation of function arguments.

Vulnerable ERC20 tokens can be sent a transaction with a "short address," making unexpected third-party applications like exchanges and Dapps accidentally send an attacker 256 times the amount of tokens expected to be sent.

Unchecked Call Return Values

Neither the call() function nor the send() function are used in the HOM Coin smart contract, so there is no need to check these return values.

Some contracts may fail to send Ethereum using these functions, but without checking for this failure. Thus, the transaction is not reverted or otherwise handled properly.

Ecosystem Vulnerabilities

The biggest security risk is the HOM Coin owner account. If an attacker gains access to this account, they would be able to:

- Change the Oracle account (with the Oracle account's permission)
- Destroy the HOM Coin smart contract, transferring all funds to the Oracle account
- Mint tokens to the HOM Coin smart contract
- Destroy their own tokens
- Change the smart contract's fees and receive some of those fees

There is little incentive for an attacker to do any of these things, unless their purpose was to simply break HOM Coin. The most this attacker would be able to get is some fees. It would be extremely difficult to gain access to the owner account as well, because doing so would likely involve physically finding a device with the private key. The effort required to execute any of these attacks is simply not worth the reward. The owner account private key could be stored on a hardware wallet with a password to make things even more difficult. At that point the attacker would need to physically locate and steal the hardware wallet, then obtain the password. This effort is nearly impossible.

The next biggest hole is the oracle program, which controls the token price. This program has an Ethereum account as well, but it cannot be put on a hardware wallet. The oracle program needs untethered access to the Ethereum account. The easiest way of attacking this program is by attempting to disconnect it from the Ethereum network, making price updates impossible. This can be mitigated easily my moving the oracle program to another machine that can communicate with the Ethereum network. The oracle program should be running on a computer that cannot be accessed from the internet at all. The computer cannot have any remote desktop software, SSH, HTTP server, and preferably no servers at all. Attackers will not be able to access the computer any way other than physically. The oracle account has a password too. The Oracle program must unlock the wallet using the password for a few seconds to update the price, but it locks the account afterwards. The Oracle program has the password so it can do that, so the password could more easily be found once the computer was accessed.

The Ethereum blockchain is completely secured. A transaction cannot be made without signing from a private key, so an account cannot be accessed without a private key. The blockchain itself has, to anyone's knowledge, never been hacked. Smart contracts on the blockchain have been hacked, but this is rare and requires the contract to have a security hole.

Smart Contract Audits

Thus far the HOM Coin smart contract has not been audited by any company, but has been analyzed by Dylan Brophy. Smart contract audits are planned for the future.