AURA

youstock

White Paper

2018

INTRODUCTION

What is Aura

Aura is a new blockchain and smart contract ledger based on the ethereum protocol. Being derived from Ethereum[1], It shares nearly all the same properties, including a built in turing complete scripting language that allows users and developers to create decentralized applications easily without having to worry about all the headache involved with creating and launching an entirely new blockchain.

Aura is a mineable cryptocurrency, not an ERC20 token[2]. It was created to be the foundation for the YouStock platform. It is a standalone decentralized blockchain and as such, can be used for any purpose that users or developers see fit. Nobody owns the Aura blockchain and anybody can use it create dApps or smart contracts or send aura[3] or anything else.

What is YouStock

YouStock is a new platform that will allow people to easily and effortlessly create a new "stock" or digital token that represents themself. We refer to this concept as "tokenized selfhood" or "people stocks". Stock creators can choose the total supply, and how many decimal places they can be divisible by (up to 18 decimal places). Users will be able to trade their stock/token with others without needing permission from anyone. This is possible due to the decentralized nature of blockchain technology.

YouStock is being built on top of Aura in order to provide this service, and aims to hide the complexities of cryptocurrency and blockchains from the end user. People will be able to easily and securely create, send, receive, and trade tokens and aura without necessarily knowing they're using a blockchain. By providing this platform, we hope users will find new and interesting ways to utilize their own stocks.

Use Cases

Athletes

Prominent and upcoming athletes can create a stock for their fans to trade. The value of the stock may fluctuate based on the athlete's performance or their stardom, market forces will ultimately determine that. Buying stock in a young promising rookie could be very lucrative for fans and traders alike. On top

[1] "White Paper · ethereum/wiki Wiki · GitHub." https://github.com/ethereum/wiki/wiki/White-Paper. Accessed 10 Feb. 2018.
[2] "ERC20 - Wikipedia." https://en.wikipedia.org/wiki/ERC20. Accessed 10 Feb. 2018.
[3] In this paper we refer to lowercase 'aura' as the unit of cryptocurrency or the fuel needed for the blockchain to operate. The uppercase 'Aura' refers to the blockchain as a whole.

of that, funds raised from an initial self offering (ISO)[4] would help offset the notoriously low pay college athletes receive, while simultaneously giving fans a new way to interact with their favorite players. Every athlete in every sport--organized, extreme, eSports, you name it--could benefit from this technology. It could also be integrated into fantasy sports and add another layer of engagement to that activity.

> "By holding an ISO, it is possible for users to attain some cryptocurrency without ever having to have owned any, and without having to do a bank transfer. This could act as a gateway for users into the cryptocurrency space."

Celebrities

Like Athletes, famous and upcoming celebrities could create a stock for their fans to trade. Fans that want to support their favorite actor or musician could buy stock in them. If you discover a young upcoming artist that you know will go on to be big, buy their stock, which simultaneously supports them and also gives you a chance to share in their future success. Artists could also incentivise their largest shareholders by giving them early access to brand new content and exclusive access to their projects.

Students and Academia

Students could potentially offset some of the expenses of school by selling some of their stock, or trading it in return for lessons. Teachers who accepted the student's stock in exchange for lessons would now have a financial incentive to help the student become as successful as they can be, and to be reach their full potential. While most teachers altruistically want their students to go on and be successful, this unique situation would give teachers even more motivation to help all their students succeed.

[4] Initial Self Offering (ISO) is like an Initial Public Offering (IPO), Initial Coin Offering (ICO), Initial Token Offering (ITO), or Token Generation Event (TGE). Essentially the first offering of a person's stock to trade with the general public.

It is often pointed out that teachers wages are too low to attract the best people for the job. This kind of incentive structure could potentially make teaching a more lucrative and sought after profession. And it doesn't have to be just between students and teachers. This type of agreement could be made with mentors or even other students that want to help each other.

Employees

After graduating--or instead of--employees could tokenize themself and offer to work for their largest shareholder in addition to a fixed salary. This would encourage companies to bid on the best employees, and has the added effect of aligning the employer's interests with that of the employee's. They both now have a financial interest in the employee to grow and be more successful. If an employee outgrows their position and another company wants to acquire them, they may agree to buy out the former employer's position.

Fundraising

YouStock can also be used as a personal fundraising platform similar to go-fund-me, patreon, kickstarter, and others. This method comes with the additional benefit of giving the donors a digital uniquely identified token that could retain value on it's own. Donors could keep it as a badge of honor that they donated such and such amount to a person or cause, and prove it on the blockchain.

These are just a few ideas on ways people might want to use the platform. We'll leave it up to the users to decide how they want to use it, and we'll do our best to make sure it's 100% permissionless, trustless, and free to use for all time. The anti-fragile nature of cryptocurrency makes this kind of thing possible long term.

Aura Technical Details

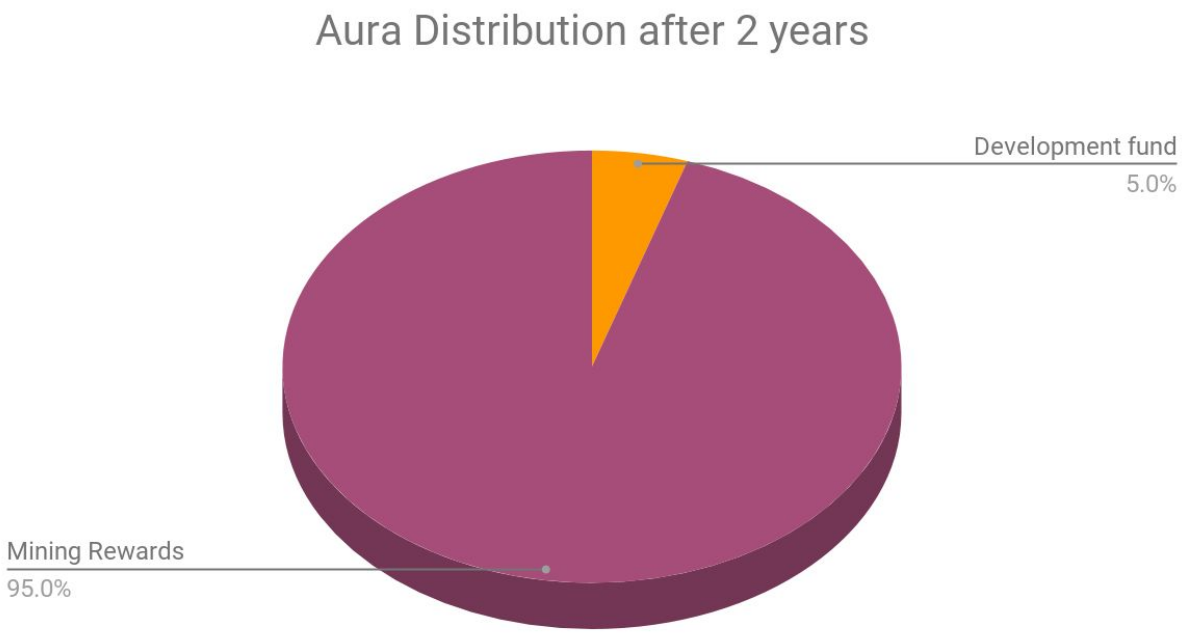
Specifications

Aura Specifications	
Market Ticker	ARA
Hashing Algorithm	Dagger-Hashimoto
Target Block Time	15 seconds
Standard Block Reward	3 aura
Total Aura to be Mined	12,000,000
Development Fund	600,000 (5%)

Distribution and Consensus

Initially the chain will use proof of work (POW) mining via the Dagger-Hashimoto[5] (Ethash) algorithm. This will go on for roughly 2 years, or 3.8M blocks. This works out to roughly 12,000,000 aura minted through mining[6]. After this time, Aura will switch to a proof of stake (POS) system modeled after ethereum's Casper[7]. Once Casper is released on the main ethereum blockchain, which is expected to occur sometime in 2018, we will finalize the POS details for Aura and start preparing our switch around the 2 year mark. Switching to a POS consensus algorithm will dramatically reduce the amount of energy needed in order to create blocks and keep the network secure, and will potentially increase performance of the network in terms of transactions per second.

The POS system will incorporate the use of Masternodes to verify and add new blocks to the blockchain. The amount of aura needed to create a Masternode will likely be around 1000, but this number is subject to change as the POS switch nears, and will be dependent on the community of miners and users. The inflation rate after switching to POS will likely be less than 1% a year, but this will ultimately be determined by community sentiment.



[5] "wiki/Dagger-Hashimoto.md at master · ethereum/wiki · GitHub." https://github.com/ethereum/wiki/blob/master/Dagger-Hashimoto.md. Accessed 10 Feb. 2018.
[6] The exact amount may be slightly different due to uncle block rewards. We will try to time the switch to POS so that we are as close to 12,000,000 mined aura as possible.
[7] "Introducing Casper "the Friendly Ghost" - Ethereum Blog." 1 Aug. 2015, https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/. Accessed 10 Feb. 2018.

Smart Contracts

Aura inherits the smart contract language Solidity and EVM from ethereum. "Solidity is a contract-oriented, high-level language for implementing smart contracts. It was influenced by C++, Python and JavaScript and is designed to target the Ethereum Virtual Machine (EVM)."[8] Being influenced by the most common high level languages, solidity is approachable to a wide range of programmers and developers. Unlike Bitcoin's custom stack based scripting language, solidity enables rapid decentralized application development.

Smart contracts are programmable pieces of code that are embedded into a blockchain transaction. The smart contract code gets executed when the transaction is included in the blockchain. The execution happens the same way for all network participants, and is required to gain consensus. This ensures that the code execution is legitimate and performs the changes to the blockchain state that everyone expected based on the code that was written. Bitcoin also had smart contracts from day one, but they are very hard to write and are much more limited in capability out of concern for developer errors.

ERC20

The ERC20 standard defines a common set of methods or functions that are needed to create a new transferable token on top of an ethereum based blockchain. Using this standard, anyone can issue a new digital token in any amount that they choose by deploying a smart contract to the blockchain that adheres to the ERC20 token standard. They can then send any amount of the token to any wallet on the blockchain.

Decentralized applications (dApps) can be created as separate smart contracts and are able to interact with the newly created tokens. One such dApp is a decentralized exchange. This is the underlying technology that YouStock will utilize to support people stocks.

Blockchain

At its core, Aura is not much different from existing cryptocurrencies and blockchains. It is a clone of ethereum, the first cryptocurrency and blockchain platform with a turing complete scripting language built in. This allows developers to add any kind of condition that can be programmed into a transaction.

Colored coins on bitcoin and similar blockchains were also considered for this project, but they are more of an afterthought and depend on a hokey implementation using OP_RETURN. Ethereum is more suited for building additional functionality on top of blockchain transactions. Using smart contracts written in Solidity, we can support all of the functions needed to create and trade any number of people stocks on the platform. Other platforms that support tokens like Waves, Dash, and others were also considered, but Ethereum has a much more developed ecosystem of services built around it that Aura and YouStock are able to utilize.

[8] "Solidity — Solidity 0.4.20 documentation." https://solidity.readthedocs.io/. Accessed 10 Feb. 2018.

Reference Client

The Aura blockchain reference client is a modified version of geth (go-ethereum) that connects to the Aura chain instead of the main ethereum chain. This is the standard way to integrate the Aura blockchain into other services. It's also possible to access the Aura network directly from the canonical version of geth provided by the Ethereum Foundation by providing the aura genesis json file, an alternate data path, and aura bootnodes when launching geth. This may not always be possible going forward if the code bases diverge too much over time. In general we will attempt to keep Aura's version of geth up to date with the canonical version, but there may be design decisions in the future that necessitate a divergence.

Scaling

One of the main reasons for a separate blockchain is high transaction fees on the Ethereum mainnet that will continue to rise as the platform continues to gain traction around the world. Because the blockchain is a shared resource, the cost to use it goes up as more and more people are competing for block space. This is known as the scaling problem and has been one of the biggest debates in the bitcoin community for the past several years. It is not an easy problem to solve, and we've already seen several forks of bitcoin due to disagreements about how to scale.

The most promising solution appears to be the use of payment channels, which allow large number of transaction to take place off chain, thus reducing the amount of transactions that occur on the main chain. In bitcoin, this is referred to as the Lightning Network. In Ethereum, it's known as the Raiden Network. Both use the same concept of payment channels, but require a slightly different implementation since ethereum and bitcoin are different protocols. We will keep our eye on this technology as it advances and incorporate it into Aura when it makes sense to do so.

YouStock Platform

Web Portal

The main interface for end users will be a hosted blockchain-aware web platform that makes all of the underlying blockchain actions much more user friendly and easy to follow. From here, users can create new accounts, create new wallets, create new stocks, find other people's stocks, and access the decentralized exchange to trade stocks. Note that all of these actions can already be performed on the Aura blockchain, but it requires some familiarity with ethereum and can be somewhat difficult for regular users. The aim of YouStock is to remove this difficulty.

The portal will support multiple ways to access your wallet. The most common way will be a simple username and password that everyone is already familiar with. This is the hosted option in which the private keys reside on YouStock's servers. This provides the highest amount of convenience and will be necessary to onboard new users who've never had to deal with cryptocurrency before. In addition, the

portal will support client side wallet integrations so that the more crypto-educated crowd can use the same platform without having to entrust their private keys with YouStock. It will support keystore based wallets, chrome extension based wallets, and local node command line wallets. Users will also have the option to browse and demo the portal without logging in or loading a wallet.

After logging in, users will be greeted with the main page. Popular and staff picked people stocks will show up on the front page for users to browse. This page will also show general announcements and news about the platform, along with high level information about their own stock holdings and aura balance at a glance. The navigation side bar will contain links to a wallet page, a self stock page, a stock browsing page, an exchange page, a block explorer page, and a network stats page.

The wallet page will have provide all of the common features you'd expect to see in a modern cryptocurrency wallet. You'll be able to easily send funds and stocks to other users. Keep an address book for common addresses to send to. See a list of transaction history for past transactions. View your balance of aura and individual stocks in your wallet. Sign messages using your private key to prove authenticity, among other actions.

The self stock page will be the home of your individual stock. This is where you can decide to create a stock, define its parameters, and choose how you want to launch it. From this page you'll also be able to link your other social media accounts to let investors know who your are, post a bio and photo, and tell your story about why you are creating a stock and how you intend to use it. You'll also be able to see it's current value and quickly buy or sell your stock from this page.

The stock browsing page is where you go to find other people to invest in. There will be multiple ways to search for specific individuals based on categories, as well as featured and highlighted stocks. When you find a stock that looks interesting, you can click it to view more info and decide if you want to buy. You'll be able to buy from this page easily with the click of a button (and entered password), provided you have enough aura in your chosen wallet to cover the purchase.

The exchange page will be a standard exchange interface that traders have come to know and love, replete with a full order book, candle and depth charts, recent global and personal trades, volume information and all the rest. Users will have the option to switch between the decentralized and centralized versions of the exchange. The interface will be the exact same for both, but the fees and speed of trades will be slightly different for each version. If you place a decentralized order, it requires an on chain transaction, which requires a transaction fee. YouStock will act as an intermediary if the books between the centralized and decentralized versions overlap.

The block explorer page will allow users to view the entire blockchain, and have a matching style of the YouStock website. Similarly, the network stats page will display many of the nodes in the network and give an overview of the distribution of nodes.

After the main web portal is complete, we will begin work on native mobile applications for android and iOS to provide the same services on the go.

Initial Self Offering (ISO)

New stocks are generated by deploying a custom ERC20 compliant smart contract on the Aura blockchain. This smart contract defines the total amount of shares in the stock, how many decimals, and a few functions that allow the stock to be traded. A ticker is optional but most stocks will be referred to by the name of the stock creator on the YouStock apps. Once the smart contract is confirmed in the blockchain, a new token has been created, 100% owned by the creator, and can be sent to any other address.

When creating a self stock, users may want to hold a public auction type event in order to establish a base price and attract investors. The terms of such an event can be structured in a few different ways, and we are seeing more and more innovation in this particular area. The standard way is to create a smart contract that has a fixed price and a fixed time window from which investors can purchase the stock. After the initial sale ends, investors are free to trade on the exchanges if they wish. Additional rules and incentive structures can be programmed into the ISO smart contract to attract early or big investors. Discounts for the first x amount of stock sold, or during the first few hours or days, or for investing over a certain amount. Brackets can be formed based on quantity or time frames to reward big and early investors on a sliding scale.

Even more advanced constructs can be used as well, such as what's known as a reverse dutch auction. In this type of ISO, the sale price starts out very high and slowly lowers overtime. Investors have to decide when it's worth it to jump in, and try to time it just right. Go in to early, and you may overpay compared to later entrants. Go in too late and you may miss out if all the stock sells out too quickly. These and many other options will be available to users creating self stocks and holding ISOs.

By holding an ISO, it is possible for users to attain some cryptocurrency without ever having to have owned any, and without having to do a bank transfer. This could act as a gateway for users into the cryptocurrency space.

Digital Identity

Individual stocks are primarily identified by the wallet address that deploys the ERC20 contract. Additional information about the stock can be stored permanently on the block chain inside of transactions, using simple key value pair notation. Standardized field names will be picked up by the YouStock client for the most common types information. Values can be updated or deleted by creating a new transaction with the same key. Things like first and last name, twitter handles, youtube channels, and other social media accounts can be linked this way and give investors information about the person behind a particular stock. The other way is to store this information off chain on our website, in a decentralized file-sharing swarm cloud, or any other website. Messages can be signed by the stock issuer for additional security and proof of who is behind the stock. Both options will be made very easy for users to do on our desktop, web, and mobile clients. A user's YouStock profile page will enable stock creators to showcase their stock and link their other online accounts.

Sending Stocks

Instead of trading on an exchange, stocks can be sent directly to other people. The ERC20 protocol defines standards for sending custom assets between accounts. The transfer function implemented in the ERC20 smart contract simply takes the destination address and amount to send as input parameters. There are also approve and transferFrom methods that can be used to transfer stocks, and help with creating decentralized exchanges. Unlike traditional company stocks, peoples stocks on the YouStock platform will be extremely flexible and accessible 24/7.

Decentralized Exchange

In order to trade stocks in a decentralized fashion, a separate smart contract is used that has similar methods as existing centralized exchanges. Namely, the ability to deposit and withdraw funds, place bid and ask orders, or fulfill existing bid/ask orders. When users deposit funds to the exchange smart contract, it now has control of the funds and they will be governed by the rules of contract. Only the user who deposited the funds can place bid/ask orders with them, fulfill existing bid/ask orders, and withdraw the funds. There is no way for a hacker to gain access to the exchange contract and steal the funds like they can on a centralized exchange. However, other attack vectors, such as phishing attacks, can still be used so caution needs to be taken anytime you're dealing with a digital crypto asset.

There are a number of existing smart contracts on ethereum that implement a decentralized exchange. We plan on building on top of the success that other teams have found in this area. Some existing ones include EtherDelta, Tidex, (get a big list of decentralized exchanges)

Centralized Exchange

While decentralized exchanges eliminate counterparty risk, there still are some advantages to having centralized exchanges. Centralized exchanges keep the bulk of trades off chain, reducing congestion and not contributing to higher on chain fees. They allow for quick sub second trading and are typically more suitable for low value trades. They are also necessary to trade between fiat and digital currency. For this reason, YouStock will also run a centralized exchange for those who would rather use it. This will likely be the most convenient option, especially for users who host their wallet on the YouStock servers already.

A portion of the development fund will be set aside specifically to provide liquidity for the Aura and YouStock networks. This will allow new entrants to come into the system using other forms of currency and also exit the system without causing drastic changes in the exchange price.

User Incentivization

In order to make the platform as user friendly as possible to new users, we are reserving a large amount of the development fund to award users for signing up with the platform. This will give all users a small amount of aura that can cover 100s or 1000s of transactions. We intend to keep transaction fees low so it won't need to be very much. This way users can start using the platform right away without having to

spend a dime. If they stick around and use up all their initial allotment of aura, then they can consider buying more to cover transaction fees. Another way they could get more aura is by creating a self stock and either run an ISO or just trade a small amount with others. A portion of the development fund will also be reserved strictly to buy up people's stocks they create, which will give users an additional incentive to create one. Other actions can be incentivized as well and we will explore more incentivization programs when the platform is live.

Underwriting Services

Before you trade aura for somebody else's stock, you want to make sure they really are who they say they are. The easiest way for celebrities and public figures to do this is post their stock address on their other social media accounts. Additionally, it would be useful to have some sort of agency or service provider that is specifically designed to verify stock identities, and give a stamp of approval. YouStock intends to provide this service for highly sought after stocks, similar to twitter's verified status program. Additionally, up and coming individuals can request to have their identity verified by us.

In addition, users may want to enlist the help of us in order to launch their own stock. We will provide this service, and underwrite stock ISO to provide legitimacy and convenience for those listing their own stock. We will help to plan the ISO, market it, defining the terms, and providing liquidity. These are just a couple of ways YouStock might monetize the platform.

Encrypted messages

If you create a self stock, you need a plan to keep investors up to date with your progress. For famous celebrities, athletes, and other well known people, it's not as important since their lives are very public already. But for more private individuals, you should keep your investors who have backed you up to date with your progress. One way to do this privately is to encrypt updates using the public key of your top investors who hold a certain amount of your stock. Then only they can decrypt the message to read it. Or, if you prefer, you can just have public updates. However, this can be used as an incentive for investors to acquire a larger amount of your stock, if it means they'll get access to real-time updates.

Platform Architecture

YouStock will be built using the MEAN stack. MEAN stands for MongoDB, Express, AngularJS, and NodeJS. "MongoDB is the leading NoSQL database, empowering businesses to be more agile and scalable. Express is a minimal and flexible node.js web application framework, providing a robust set of features for building single and multi-page, and hybrid web applications. AngularJS lets you extend HTML vocabulary for your application. The resulting environment is extraordinarily expressive, readable, and quick to develop. NodeJS is a platform built on Chrome's JavaScript runtime for easily building fast, scalable network applications."[9]

These technologies will be deployed on elastic cloud computers and will allow us to easily scale up to meet user demands and provide a snappy smooth experience for users even during high traffic times.

[9] "MEAN stack." http://mean.io/. Accessed 11 Feb. 2018.

Security will be the top most priority, with regularly scheduled bi-daily audits and funds primarily stored in cold storage.

Roadmap

- *September 2017*
  Initial project concept and blockchain experimentation

- *January 2018*
  Create ethereum fork and block explorer, Aura mainnet launch

- *February 2018*
  Aura services (mining pools, GUI and Web wallets, network stats, Exchanges)

- *March 2018*
  Basic wallet support: view balance, send/receive aura, keystore, private key, mnemonic phrase

- *April 2018*
  Cross chain atomic swaps
  Auradex and the ability to trade aura for ether directly

- *May 2018*
  People Stocks
  Advanced wallet support, create tokens, view/send/receive tokens

- *June 2018*
  YouStock Alpha
  Market: Buy/Sell/Trade people stocks

- *Q3 2018*
  YouStock Beta
  Expanded wallet support, testing, more cross-chain swap options

- *Q4 2018*
  YouStock 1.0

- *Q2 2019*
  YouStock Android and iOS Mobile Apps

Funding

Development Fund

The development fund came from a 5% premine of the initial Aura coin supply. It will primarily be used to incentivize users of the YouStock platform. This includes incentives for creating an account and creating a stock, and other actions that encourage use of the platform. The development fund is also meant to cover operational costs, including bounty costs, management and rewards, marketing, exchange listing and server costs, and freelance work. The development fund may be used to compensate new team members or other unforeseen costs as the project matures.

Summary

YouStock is a new platform and tokenized selfhood community for creating and trading people stocks. Aura is the blockchain and base cryptocurrency that will power the YouStock platform. YouStock enables anyone to create a new digital asset that represents themself and trade shares with anyone else. These digital assets are implemented as ERC20 tokens on Aura, and will be tradeable on centralized and decentralized token exchanges. New user friendly interfaces for the web and mobile will be created to hide the underlying complexities of the blockchain and smart contracts from end users, and allow them to easily create and trade stocks with other users for any purpose they see fit.