Aurora: A Decentralized Financial Institution Utilizing Distributed Computing and the Ethereum Network

Aurora Labs

Version 0.9.5
January 21st 2018

Abstract

Aurora is a suite of dapps and protocols that together comprise a fully decentralized and autonomous banking and finance platform. Complete with its own stablecoin, the boreal, Aurora aims to recreate and improve upon the existing financial ecosystem in a decentralized fashion. Aurora offers a stable, private, and open financial system to anyone in the world regardless of geographic location, class status, or privacy preferences. The primary components of Aurora are a cryptocurrency bank (Decentralized Capital) and a financial asset exchange (IDEX) which work together to offer the same financial services of the modern world. All of Aurora operates on a distributed computing network and utilizes an EVM compatible childchain for transaction processing, decentralizing the whole system and enabling it to run autonomously.

Inspired by F.A. Hayek's and George Selgin's work on Free Banking theory, Decentralized Capital supplies loans in a decentralized stablecoin known as boreals, and provides modern day banking services to those who are underserved by the current system. The boreal is backed by a combination of cryptocurrency reserves, debt from loans, and dapps endorsement, ensuring price stability that is on par with existing fiat options. In addition to providing banking services, Decentralized Capital will market make on IDEX, helping maintain boreal price stability, and hedge the reserves through tools such as predictions markets. Traders on IDEX can utilize the boreal as payment for trading fees or as a stable base currency, ensuring that there is demand for boreals early on within the Ethereum ecosystem. Once boreals are an established stable currency within the cryptosphere, Aurora will begin expansion into other markets while Decentralized Capital will transition to sustainable fractional reserve banking.

Table of Contents

1. The Status Quo

Modern financial systems have enabled rapid economic expansion and improved the lives of billions around the world. However, the fundamental design of the system has led to an unreasonable concentration of wealth and power in the hands of those who manage it. Financial crises are a matter of when, not if, and third world countries have not experienced nearly the same benefits as those in the first world. Many of these issues stem from the fact that currency issuance is by and large monopolized by national governments, entities that are inherently biased towards decisions that support the health of their own economy. These decisions have the side effect of picking winners and losers in the financial markets, and in doing so leave the governing bodies open for corruption and political influence. Most importantly this abuse ultimately undermines the stability of the national currency, enriching those in power at the expense of currency holders.

1.1 The Current Model and the Role of Central Banks

Most of the largest economies have converged to a similar model, that of a state sponsored central bank. The most prominent of these is the US central bank, the Federal Reserve. The Fed and others act as a bank for commercial banks and the government. As the "banker's bank" the Fed provides services to financial institutions in the same way that commercial banks provide services to individuals, e.g. executing transfers from one bank to another. This includes acting as the "lender of last resort," providing troubled commercials banks with short-term loans when the risk of insolvency prevents them from securing loans from other commercial banks.

The Fed also acts as the bank of the US government, handling all tax revenue and outgoing government payments. Included in these services the Fed sells government securities such as treasury bills, notes, and bonds - various forms of government debt with different maturity dates.

The most important task of the Fed is managing the supply of US Dollars through a process known as monetary policy. The goals of this policy are sustainable economic growth, full employment, and stable prices. Through monetary policy the Fed and other central banks attempt to "tweak" the economy to the right levels. For example, if the economy is showing signs of slowing growth, the Fed may determine that it's best to lower interest rates. As interest rates decline more individuals and businesses are willing to borrow to finance investments, purchases, or other forms of financial activity, increasing overall spending in the US economy.

However, as previously mentioned, the Fed only banks the national government and large commercial banks, and does not lend directly to businesses and consumers. The Fed must therefore pursue policy goals through these other entities by using a specific set of tools designed to influence the lending decisions of commercial banks. The Fed achieves this by ensuring banks have more cash than they need, excess reserves above the amount banks are required to hold by law. Banks then lend this excess cash to businesses and consumers for use in investment, wages, or purchase of goods and services.

Central banks like the Fed have three main tools to affect the money supply:

1. Open Market Operations - The Fed is constantly buying and selling US government securities in financial markets. Buying US government securities replaces those assets on the commercial bank's balance sheet with cash. The bank now has excess reserves and is incentivized to loan them out to customers, and in order to attract new customers they must lower interest rates. Open market transactions directly influence the level of reserves in the banking system, which in turn affects the amount and cost of credit as reflected through interest rates. This is the most frequently used tool of monetary policy.

2. Discount Rate - The discount rate is the interest rate that commercial banks pay on short-term loans from the Fed. The discount rate helps influence the lending policies of commercial banks and is an important signal to the market of the Fed's intentions. Reducing the discount rate makes it cheaper for commercial banks to borrow money from the Fed and leads to an increase in available credit and lending activity in the economy.
3. Reserve Requirements - The Fed mandates that commercial banks hold a certain percentage of deposits in reserve, limiting how much can be loaned or invested. Reserve ratios are typically around 10%. Though rarely employed, a reduction in reserve requirements would directly translate into an increase in excess reserves, reserves which could immediately be loaned out to customers.

1.2 The Value of the US Dollar

What gives the US dollar value? Many economists will tell you that a dollar has value because people accept it as a medium of exchange. But people wouldn't accept it as a medium of exchange unless they believed it has value. This sort of circular reasoning is not a sufficient explanation.

An alternative understanding is that the dollar has value because of credit, the expected repayment of debts. This manifests itself in a few different ways:

- The US Government exclusively does business in the US dollar; all purchases by the government are made using dollars, and they accept the dollar, and only the dollar, as payment for taxes. The US economy is the largest in the world, and necessitating that all citizens pay taxes using its currency ensures there is a significant demand for dollars.
- Commercial banks are in the business of using customer deposits as investment capital or to issue loans to other businesses and consumers. U.S. financial institutions are required by law to accept the dollar as repayment of debt, and are forbidden from accepting any other form of currency for the same purpose. These loans are backed by businesses, real estate, goods etc. that they were used to purchase, in essence collateralized by the whole of the US economy.
- The Fed, like any other bank or business, has a balance sheet that consists of assets and liabilities. The liabilities are comprised mostly of reserves, the dollar deposits of various commercial banks, while the assets consist mostly of US government debt, or more recently Mortgage Backed Securities (MBS). The reserves are in effect collateralized by the US government debt. Typically the value of the Fed's assets remain relatively stable, as US treasuries are considered one of the safest investments in the world. The health of the Fed therefore heavily relies on the health and creditworthiness of the US government.

Looking at it from this perspective it's clear how important the US economy is to the success of the dollar as a currency. There's nothing "behind" the dollar except the full faith and credit of the United States Government. That's actually quite a bit, at least until it isn't. But, as long as people believe it to be worth something, it will be. And as long as the U.S. Government requires all taxes and fees due to it to be paid in dollars, and the American people are paying their taxes, it will at least have that much value.

In summary, each country has a central bank which is issuing currency and backing it with the debt of their government, or, in more recent times, financial instruments created by their own commercial banks. The commercial banks loan this currency to businesses and consumers for use in capital investments, payment of wages, consumer purchases, etc. The result is an interrelated web, one full of systematic risk. The value of US treasuries, and therefore the Fed's assets, depends on the perception of the US government's ability to repay, an ability which is a function of tax revenue and correlates with the performance of the US economy. The commercial banks' health is tied to its ability to collect on outstanding liabilities and is also a function of the US economy, as economic downturns lead to higher

default rates. The strength of the currency in international markets is therefore dependent on the strength of the underlying economy, and each central bank will do everything they can to use their power to further the economic interests of their state and government.

1.3 Misaligned Incentives

So why does this matter? The architecture results in a concentration of power and misaligned incentives which lead to market distortions and corruption. As lender of last resort, the Fed will assist commercial banks who get into trouble in terms of their financial solvency. Traditionally this has meant providing emergency loans, however during the latest financial crisis the Fed went so far as to issue new reserves and use them to purchase financial assets - Mortgage Backed Securities (MBS) - from troubled companies. This amounts to backing reserves with low-quality loans created by the private sector. Issuing new reserves to purchase US government debt doesn't increase the existing deficit, it's like taking money from your left pocket and moving it to the right pocket. However, now the Fed is using lower quality financial assets as collateral, increasing the risk associated with central bank insolvency.

These decisions from the Fed makes perfect sense based on their stated goals; bankruptcies in the financial industry can have widespread impact, and the actions did appear to stop the problem for the time being. Unfortunately it's now been made clear to commercial banks that they can lend recklessly and invest in riskier assets, aiming for outsized returns but knowing that if they fail the losses will be socialized and passed on to taxpayers. It's created the infamous "Too big to fail" institutions, ones that are so intertwined with the US economy that bankers and politicians believe they must be protected at all costs. They aren't wrong to be concerned; if these institutions were allowed to collapse it would have a terrible impact on the US economy and world economy. But had they been initially allowed to fail when they made reckless lending decisions, banks would be forced to be more conservative in both the amount of reserves they hold and the quality of their loans, reducing the risk to the system without a tax-payer funded guarantee.

Central bank policy is also subject to political influence. Central bankers are tasked with acting independently, but the fed governors are appointed to their position by the President. Their decisions have a huge impact on the economy, and thereby the popularity of the President's administration, so it's only natural that there will be some pressure to act a certain way. As Richard Nixon famously said in his speech appointing Arthur Burns as Fed chair in 1970: "I respect his independence. However, I hope that independently he will conclude that my views are the ones that should be followed."

There is additional pressure from private enterprise, as central bank policy also distorts the decisions of other investors in the market. Investors carefully watch the Fed and other central banks for signs of what their next move will be regarding interest rate targets. A correct investment decision can become the wrong one if monetary policy isn't properly accounted for. A classic example of this is the "Greenspan Put", a term that arose in 1998 when the Fed lowered interest rates following the collapse of a large financial institution. Unsurprisingly investors reacted by borrowing more heavily and investing in securities, helping prop up the equities market.

An additional side effect is the temptation for governments to use their central banks to fund government debt, a process known as seniorage. The central bank can issue new currency and use it to buy government bonds, after which the government can use the additional cash to finance whatever programs are in place. An additional benefit of seniorage is that the resulting inflation reduces the cost of existing debt, as the US debt is denominated in its own currency. The US government is fortunate that the US dollar is the world reserve currency, and as a result is able to do this without too much consequence. Other countries such as Argentina, Venezuela, or most infamously Zimbabwe have not been so lucky. Their monetary policy decisions in the past led to a rapid expansion of the money supply

and runaway inflation, and ultimately a situation where other countries no longer believe they can repay their debts. The results for the citizens of those countries was many years of recession and economic depression.

2. Free Banking

Free banking is an alternative to the state sponsored and supported financial system that is so prevalent today. Free banking is rooted in the belief that private actors can provide a better, more stable currency than that provided by governments.

2.1 A Market Driven Alternative

In a free market, firms who provide better products and services win out over inferior options, as consumers switch their demand to the superior offering. Similarly, in free banking individual banks create and maintain their own currency, and consumers are free to pick the currency that best suits their needs from a set of competing offerings. Debtors, including most governments, will prefer an inflationary currency as it reduces the cost of loan repayment, while lenders and savers will prefer a deflationary one. Given these competing priorities it's reasonable to conclude that market participants will gravitate towards currencies that best maintain a stable value.

A free banking system allows for private enterprises to match currency supply with demand. Macro and seasonal business cycles influence the amount of currency required to support all economic activity. The supply of currency should expand and contract in order to match these changes in demand. This coordinated movement ensures that the value of the currency remains stable relative to broader market prices. In countries and time periods where supply rapidly outstrips demand, currency holders experience inflating prices and a rapid devaluation of the currency.

Additionally a free banking system can eliminate the moral hazard created by central banks operating as a lender of last resort. In free banking each bank is responsible for its own solvency and required to hold adequate reserves to ensure it is able to meet all of the withdrawal demand. If a bank is unable to meet demand it must secure additional funding through other banks or private investors or else risk insolvency. Sound banks are able to find lenders and increase their reserves without issue, while reckless banks or those with too much risk will collapse. Consumers must be more diligent to understand the risk profile of their financial institutions, and any negligence on the part of the bank or its depositors will lead to a more localized failure.

Free banking is NOT a 100% reserve model. If consumers wanted a business just to hold their funds for safe keeping they would have to pay for the service, and that becomes more like a storage facility. Banks are in the business of allocating unused capital; they pay depositors interest to encourage them to deposit idle funds, and loan or invest those deposits in other parts of the economy. However, when properly managed, banks increase financial opportunity and allow all actors to participate in the economy and share in its growth.

2.2 A History of Free Banking

Free banking has a strong track record in countries and time periods where it was allowed to flourish, a prime example being England during the late 1700s. At one point the system was so successful that the citizens of England preferred private coins over those provided by the Bank Of England. The private coins were more widely circulated, in particular in the industrial areas of Northern England, and

contained more intricate designs that helped combat counterfeiting. It is argued that the beginning of the industrial revolution in England would not have been possible without private issuers of coins. Their success eventually led to the English government outlawing the private minting of coins, killing the industry that was sure to make them obsolete.

The story is similar in the US, where mounting regulations inhibited the operations of banks, generating crises which eventually begot more control and regulation. Early on commercial banks were prohibited from creating branch banks, limiting their operations to a single physical location; this eliminated their ability to diversify, and ensured that any local economic hardship impacted bank solvency. It also made it difficult to move currency supply to areas with greater demand, leading to supply shortages during periods of high demand such as harvest season.

During the civil war, the US government imposed a costly tax on state chartered banks for issuing currency, effectively revoking their ability to do so. Simultaneously the government created national banks, a new type of bank under federal charter, which were exempt from the tax for printing currency, provided that the reserves were held in US government bonds. It was a clever way to fund the war, but has the unintended consequence of tying currency supply to the level of government debt. After the war the currency supply shrank as the government serviced its debt, leading to supply shocks and financial crises that served as justification for further expansion of Federal control and regulation.

During this time period an important counter example was unfolding just north in Canada. Canadian banks were relatively uninhibited in their currency issuance; they were chartered by the government, creating a barrier to entry, but outside of that practiced what we've outlined as free banking. Each bank was able to print their own currency and match supply with demand as they saw fit, in addition to practicing branch banking which allowed them to diversify geographically. Over the same 20 year period that saw half of all USD removed from circulation, Canada's money supply resembled that of a saw tooth pattern. During agricultural harvests the demand for currency increased as it was needed for trading goods that were coming to market. After the harvest season was over the demand fell, and the banks removed currency from circulation to absorb the reduction in demand. The system of decentralized banks using local knowledge and flexibility to meet currency demand was far superior to that of the US's system.
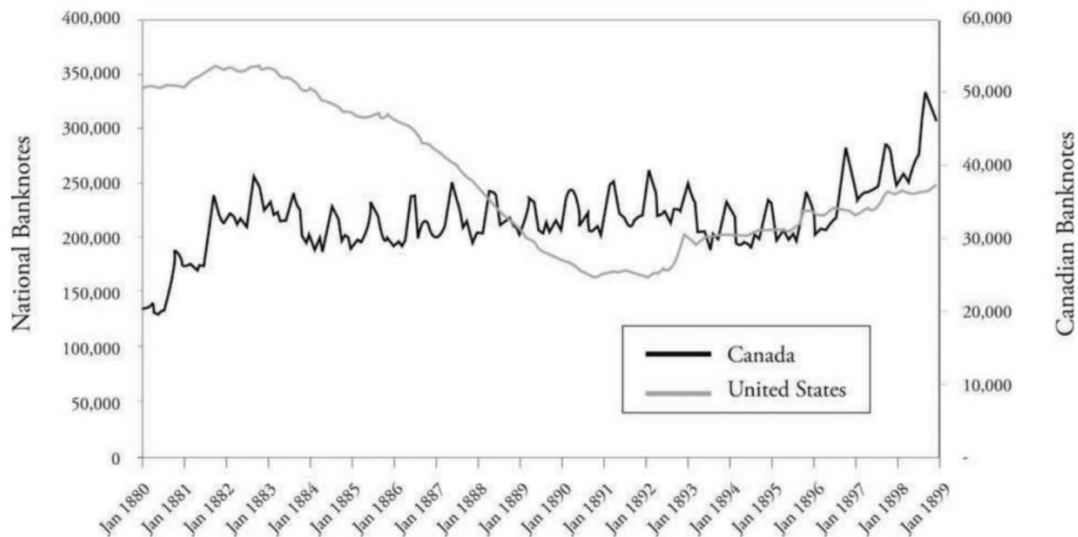

Figure 1: US & Canada Outstanding Bank Notes 1880-1900

2.3 How We Got Here

Banks and currency began as a private endeavor, agreements between different consumers and businesses on how to trade goods and settle debts. Over time this industry came to be controlled and regulated by government entities, originally monarchs and emperors, and eventually through the central banking model that is most prevalent today.

This transition occurred under the guise of protection and stability; in reality the world's second central bank, the Bank of England, came about in 1694 when the crown granted them an exclusive charter in return for a loan to wage war against France. At first the Bank of England was competing against other banks. Over time, through more government intervention and favoritism, control of the currency supply was granted solely to the Bank of England.

The English central bank model has since become the central banking model used around the world, leading to the modern standard where currency production is almost exclusively a right of the state. We believe that the solution to fixing modern banking is to increase transparency and eliminate the favoritism that allows individuals and institutions to act recklessly and without recourse. We want to give consumers visibility into the health of the bank and an opportunity to vote with their wallet.

3. Aurora

Aurora is a collection of Ethereum applications and protocols that together create a decentralized banking and finance platform. Inspired by free banking, Aurora provides customers with an advanced, open, and stable financial network available to anyone in the world regardless of geographic location or class status. Aurora's own stable currency, the boreal, is backed by a combination of cryptocurrency reserves and debt, and is available to customers via loans based on their digital economic reputation. Traders on IDEX, the network's decentralized smart contract exchange, can utilize the boreal as payment for trading fees or as a stable base currency.

3.1 Decentralized Capital

Decentralized Capital is a decentralized bank that provides loans to customers in the form of a new stablecoin, boreals. Demand for boreals is generated due to its stable value and use in loan repayment. Decentralized Capital will engage in a number of other different activities analogous to open market operations with the ultimate goal of boreal price stability, and a secondary goal of profit maximization. Decentralized Capital will expand the supply of boreals slowly over time. In the beginning boreals will be backed 100% by the ether that is used to buy them.

The components required to run the bank are computationally heavy and as such are not suited for operating on a blockchain. The majority of the infrastructure for Decentralized Capital's crypto-banking will therefore reside off chain on a distributed computing network. The end state is dependent on a decentralized infrastructure and Aurora will utilize one of the many options such as Golem, IEX, Maidsafe, or even its own separate network, to meet this demand. Operating Aurora as a decentralized network ensures that it is as robust as possible and free from DDOS attacks.

3.1.1 Boreals

Boreals (BRL) is a price-stable decentralized cryptocurrency built on the Ethereum blockchain. BRL supply is carefully managed by Decentralized Capital in order to match it with demand and maintain price stability, originally assessed by keeping parity with USD, and over time transitioning to a basket of

goods and commodities. Boreals are backed by a combination of debt and reserves in ether. Decentralized Capital will initially aim for full 100% reserves in ether with the eventual goal to move to sustainable fractional reserve banking.

3.1.1.1 Boreal Loans

Boreal loan borrowers must first apply through Decentralized Capital and are subject to a background and credit check. Once approved the borrower is issued their boreals, as well as provided with a repayment schedule. The borrower can then use the boreals directly to purchase products and services on the Ethereum network, or sell them on the open market for another cryptocurrency.

Any user on the Ethereum network is eligible for a loan from the bank. Credit will begin very conservatively, but as borrowers build up a history they'll be able to take out ever larger loans at better interest rates. This is not unlike how it works today, where a new college grad has a lower credit limit than someone who's shown an ability to manage credit card debt or service a mortgage.

The bank will assess credit worthiness through all available data. Identity services such as uPort and RepSys will serve as a proxy of a borrower's trustworthiness. Previous loan history, KYC attestations, etc. will allow the bank to build an accurate profile of the user. Other less typical credit indicators, such as professional skills and work experience, can also be used, provided this information is tied to the individual's on-chain identity. For example, Firstblood players taking a loan for competitive wagers could be assessed based on their League of Legends win history. Many different criteria will inform creditworthiness, and there is no one size fits all.

Borrowers have the option to take a new loan that is uncollateralized, or to collateralize a loan by providing cryptocurrency to the bank. Collateralized loans will have lower interest rates as the existence of collateral lowers the risk to the bank. The collateral can be in the form of high quality ERC20 Ethereum tokens. In the event of default the collateral will be sold and the customer's uPort history will be updated to reflect the default, resulting in a lower credit score and stricter lending standards in the future.

3.1.1.2 Demand for Loan Repayment

The loan system not only serves as a method for distributing boreals, but also as the core driver of demand to ensure that boreals maintain a value floor. Every loan, both principal and interest, must be repaid in boreals. Borrowers will purchase these boreals on the open market or from the bank in order to repay these debts. Whenever the price of boreals falls below its target value, borrowers are incentivized to buy up the cheaper currency, as this represents an opportunity to reduce the overall cost of their loan. Decentralized Capital will provide a software tool to help borrowers manage this process.

Decentralized Capital opens the doors to many possibilities by acting as the central piece of the Aurora ecosystem. The combination of uPort, risk algorithms and a decentralized network allow for an unbiased autonomous credit system that is accessible to customers worldwide. As users build up their uPort profile with attestations Decentralized Capital will be able to operate more accurately, which will result in those with good credit having access to better rates than is possible in the traditional banking system. Decentralized Capital also opens up to a wider customer base including those who need an immediate crypto loan, or a small amount of cryptocurrency to begin using other Ethereum products and services.

3.1.1.3 Buying and Redeeming Boreals

Exchange Markets – The majority of boreal purchases will occur on open market exchanges. Users with new boreal loans may sell those boreals in order to convert into another currency. Existing borrowers will purchase these boreals in order to repay outstanding loans. The fact that all loans, both principal and interest, must be repaid in boreals, will ensure that there is upward pressure on the boreals price.

Direct purchases - If demand ever outstrips supply, consumers/borrowers can purchase new boreals directly from Decentralized Capital at par value plus a 0.5% transaction fee. This guarantees that borrowers can always repurchase the necessary assets for repayment at a reasonable rate, as well as provides an additional source of profit for the bank. Direct purchases also allow anyone to move large amounts of funds into boreals without the slippage that would arise from making a large purchase on an exchange. All Ether that is used to purchase boreals from the bank is added to the pool of reserves.

Redeeming boreals - Each boreal is backed up by a combination of reserves and debt. Users of boreals are able to redeem their boreals for Ether for a 1% fee. This ensures that there is a price floor on the asset that allows for users to easily get their funds out. In the event that the demand to withdraw ether from the boreals is too great to meet supply, Decentralized Capital reserves the right to suspend withdrawals until existing loans have been repaid and the reserves have been replenished enough to buy back the boreals.

3.1.2 Reserves

Decentralized Capital will hold reserves in ether. The primary purpose of the reserve is to back the boreal currency and allow customers to easily convert in and out. Additionally the reserves can be used as liquidity for boreals market making, an activity which serves to maintain the stability of boreals and generates revenue for the bank, as well as an emergency fund in the event that the price of boreals breaks the target value.

Initial reserves will come from people buying boreals to use on IDEX as well as company holdings of the AURA token. This reserve will grow over time due to the various profitable activities supported by the bank.

- Interest on loans through Decentralized Capital and IDEX margin lending
- Revenue from IDEX
- Revenue from direct purchases of boreals
- Market making/purchasing assets below par
- Secondary income services

The reserve funds must be held in decentralized Ethereum assets as this ensures that the funds can only be controlled by Decentralized Capital.

3.1.2.1 Reserve Requirements

Initially Decentralized Capital will aim for 100% reserves. This will be maintained while the core components of the bank are being built. Once the bank is fully decentralized and operations are stable, Decentralized Capital will focus on moving the bank over to a sustainable fractional reserve model. In this model there must always be sufficient reserves on hand to help insulate the bank from fluctuations in demand. Decentralized Capital will utilize measurements such as the velocity of boreals and total outstanding notes to help with determining the ideal reserve level. Decentralized Capital will change the

reserve ratio as needed to maximize profits while ensuring that the system maintains its ultimate goal of price stability. History suggests that when optimized that the reserve requirements should be minimal; during the free banking period in Scotland, the public trust in the banks was so high that they were able to operate safely with reserve ratios as low as 2%.

3.1.2.2 Hedging Reserves

Reserves consist exclusively of Ethereum-based decentralized assets, ensuring that only Decentralized Capital can access and control them. Aurora is designed to operate outside of the existing financial ecosystem, and holding reserves in other assets would increase the risk of government interference. The majority of these assets are also subject to price speculation and may not be stable over longer periods of time. To counteract this Decentralized Capital will hedge the price volatility using other decentralized platforms such as Augur or Stabl, ensuring that the reserves maintain their fiat denominated value. The exact amount of hedged vs unhedged funds will be decided by the Decentralized Capital.

3.1.3 Market Making

Decentralized Capital will utilize market making to help maintain the target value. If boreals are trading below the target price, Decentralized Capital will purchase boreals in order to bring the price back in line. This reduction in supply results in a shortage of boreals for those customers who need them to pay IDEX fees or repay outstanding loans. As the remaining boreals are repurchased the value will increase above the target; once it reaches the 0.5% premium it will make more sense for borrowers to buy boreals directly from Decentralized Capital.

This cycle of purchasing and selling will not only help maintain price stability, but will also serve as a source of revenue for the bank. Assets purchased below par and resold directly to debtors will generate a minimum revenue of 0.5% per transaction. As the market grows and the bank repeats these actions again and again, the revenue potential from these operations becomes enormous.

3.1.4 Setting the Target Value

Boreals are required to cover fees and repay loans to the bank, and as such Decentralized Capital has the privilege of setting the official target value that it will accept for boreals. At launch the boreal target price will be set equal to 1 USD. Decentralized Capital will research different models of stability targets and engage with economic experts to design a system such that boreals neither gain nor lose value. This will create a currency that maintains its purchasing power over time and is completely immune from inflation.

3.1.5 Early Bank Implementation

Included in the Aurora MVP client is an early iteration of Decentralized Capital. Users can deposit ether and in return receive boreals at the rate of 1 USD per boreal, plus applicable fees. These boreals serve multiple purposes early on: to pay fees on IDEX at a 5% discount, as a stable value to trade against volatile Ethereum assets, or as a store of value and hedge against cryptocurrency price decline. Users can also redeem boreals for ether directly from the Decentralized Capital interface.

Operating in a limited fashion will enable us to collect real data about the demand for a privately managed stablecoin and learn how best to match supply with demand. In the early stages it is expected that boreals will fluctuate within a specific price range; during this period we'll optimize maintaining price stability on IDEX. Decentralized Capital will analyze usage data such as the amount of boreals used for fee payments, the amount used as stable value in trades, the amount held as a long term stable value, and the overall velocity to assess and understand demand. This information will inform when

Decentralized Capital enables or disables deposits and withdrawals, with the goal of matching the supply to the demand. Total Boreal supply will be limited and expanded conservatively with respect to the demand. If the supply ever expands too far above the demand, Decentralized Capital will utilize the Ether reserves to purchase boreals on the open market. Data garnered from this early implementation will be used to guide further development of the bank prior to adding lending to the list of provided services.

3.2 IDEX

A decentralized bank is revolutionary in part because it's the first example of a financial system that exists outside of the traditional market and credit system. However, this same power also increases the threat of loan defaults from customers. We expect that at first it will be difficult to accurately gauge who is worthy of loans, but as the system grows and on chain identity tools advance, Decentralized Capital will see a steady decline in the default rate. To keep the bank truly decentralized and open to customers from anywhere in the world, it is crucial that the bank has additional revenue sources to offset and weather any unexpected string of loan defaults. This additional revenue source will be generated by IDEX.

3.2.1 IDEX Overview

International Distributed Ethereum Exchange (IDEX) is a decentralized high throughput exchange network which is built into the Aurora client. IDEX is composed of a combination of Ethereum contracts and a shared database that matches trades and manages the order transaction queue. Revenue from this exchange network is shared equally between the bank and network participants running the Aurora client. Fees on IDEX may be paid on boreals at a slight discount, providing boreals with an immediate use case and helping establish them as a reputable stablecoin.

3.2.2 IDEX Specification

IDEX provides a real-time, high-throughput trading experience in conjunction with blockchain based execution and settlement. Users can trade continuously without waiting for transactions to mine, fill multiple orders at once, and cancel orders immediately and without gas costs.

IDEX is composed of a centralized trading engine and decentralized Ethereum smart contracts. The trading engine hosts the off-chain balances and orderbook, matches trades, and manages the queue of pending transactions, while the Ethereum smart contract stores all assets and manages trade execution and settlement. By separating trade matching from on-blockchain settlement, IDEX combines the speed and user experience of centralized exchanges with the security and auditability of decentralized exchanges.

The first iteration of IDEX is semi-decentralized; the trading interface is run locally by the end user, while Aurora Labs manages the server responsible for matching and settling trades. The current architecture is captured in the following graphic:
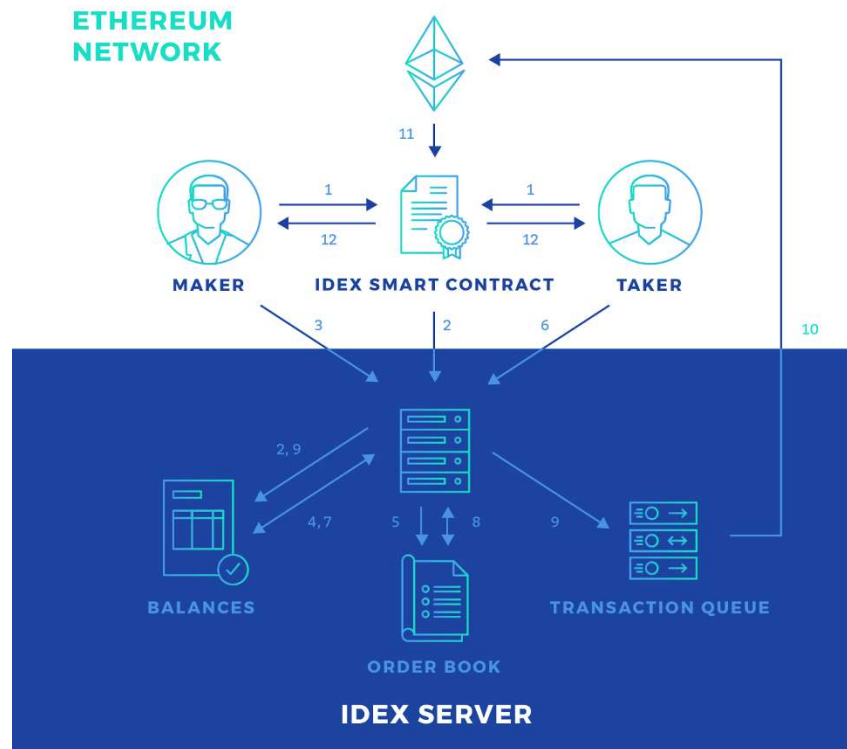
Figure 2: IDEX Transaction Process

1) The maker and taker deposit their tokens into the IDEX contract.
2) The IDEX database is updated to include the customer addresses and token balances.
3) Maker creates and submits a signed order that includes the relevant trade data.
4) IDEX confirms that the maker's account has sufficient funds and that the signed transaction matches what was submitted to IDEX.
5) If all checks in part 4 pass, the order is added to the orderbook.
6) The taker submits a matching order, signing a transaction with the same price as the target order and an amount less than or equal to it.
7) IDEX confirms that the maker's account has sufficient funds and that the signed transaction matches what was submitted to IDEX.
8) If all checks in part 7 pass, the trade is marked as matched and the orderbook is updated.
9) The IDEX database is updated to reflect the new balances, and both traders can continue to make new trades based these updates. Simultaneously, the signed order is added to the queue to be broadcast to the Ethereum network for processing.
10) After all dependent trades have mined, the transaction is dispatched to the blockchain.
11) The transaction is mined and the contract balances update to reflect the trade.
12) Once the transaction has mined, the maker and taker are able to withdraw their funds.

The fully decentralized version of IDEX will be incorporated into the Aurora client. Traders can use the client for transactions without requiring any further effort to support the network.

3.2.3 IDEX Fees in Boreals

To help generate demand for boreals early on IDEX will provide a 5% trade fee discount to those who pay using the stable currency. Users who wish to do so must first deposit their boreals to the trade fee wallet and transfer them into a trade fee credit (deposited boreals cannot be withdrawn). When initiating a trade, IDEX first checks the customer's trade fee wallet for boreals before taking the trade fee from the traded asset.

3.2.4 Boreal Margin Lending

Margin loans are short term loans with fairly high interest rates, a perfect use case for boreals. Decentralized Capital is the only entity allowed to supply boreals for this purpose, creating an additional source of revenue as well as an additional channel for distributing boreals.

3.2.5 IDEX Margin Lending by Peers

Customers can deposit their Ethereum assets with the bank, and in return receive a new Ethereum cryptobond. The new bond will have a set duration and interest rate. During the life of the bond, the deposited funds will be used for IDEX margin lending in order to generate revenue for the bank. At the end of the bond period the depositor can exchange their bond for the original loaned amount plus interest. Tokenizing the deposit brings liquidity to the margin loan market and allows any depositor to exit their position before the expiration of the margin loan period.

3.3 Snowglobe

Snowglobe is a protocol for high-performance, EVM-compatible, decentralized childchain exchanges. Snowglobe allows for all exchanges on the network to share liquidity in one orderbook while maintaining their high-performance characteristics.

The protocol consists of five main components:

1. Snowglobe childchain blockchain
2. Snowglobe Ethereum contract
3. Distributed orderbook
4. Local transaction arbiter(s)
5. Global transaction arbiter

3.3.1 Snowglobe Components

The **Snowglobe childchain blockchain** architecture consists of two levels of sharded POS blockchains. The top level is a single blockchain that acts as the parent chain for each of the individual chains below it. On the parent level blockchain funds are held in different smart contracts representing the balance of each exchange on the protocol. The integrity of the parent chain is enforced by the AURA token.

The second level of Snowglobe consists of the childchains for each exchange that uses the protocol. Each childchain is used to manage the assets and trades of an individual exchange. Trades within a single exchange only impact the balances within a single chain, while trades across exchanges impact the balances on both the individual exchanges and the parent chain of the protocol, reflecting the change in balances at the exchange level.

The **Snowglobe Ethereum contract** holds all of the Ethereum assets traded on the protocol, regardless of which individual exchange the user is trading on, and is the conduit between the Ethereum blockchain and Snowglobe. When a user deposits via a particular exchange, for example IDEX, their funds are sent to the Snowglobe contract with the appropriate flag to indicate the correct exchange. The funds are locked in the contract, while simultaneously new mirror assets are created on the Snowglobe parent chain. These funds are reflected in the IDEX exchange balance on the parent chain, and also propagate down into the IDEX childchain for trading.

Each exchange will host their own **distributed orderbook** on a universal P2P service that allows for real-time communication. Though each exchange has their own orderbook, liquidity is shared across all exchanges on the protocol. Traders on any exchange will just see one unified orderbook, oblivious to where the order is actually hosted. Due to the competitive nature of the space we are not revealing the exact proposed method for decentralizing the orderbook at this time. The orderbook infrastructure will be built into the client of each exchange, and settlement of trades will be enforced by the protocol.

The final piece, and the key to coordinated operation across multiple exchanges, is the transaction dispatcher known as the **local and global arbiters**. Like the current semi-decentralized approach of IDEX, the arbiters are responsible for queuing and broadcasting pending transactions in the correct order. Each exchange will have the local arbiter built into their own POS mining client. Miners will stake the exchange's own currency, using cryptoeconomics to ensure each chain mines their own transactions in the correct order and to maintain the integrity of the individual chain.

Transactions that occur outside of individual exchanges, withdrawal requests or trades across orderbooks, must be overseen by the **global transaction arbiter** of the Snowglobe parent chain. Trades that cross exchange orderbooks result in a transfer of funds from one contract to another on the parent level chain of Snowglobe, and it's critical that these transfers are properly validated. The miners of the IDEX chain oversee both the local arbiter of IDEX and the global arbiter of Snowglobe, staking the AURA token to secure both chains.

The protocol will include fraud prevention measures to ensure that all funds are secure even in the event that AURA staking is compromised. Each withdraw from Snowglobe to the mainnet has a time lock, a delay between the withdrawal request and execution. All exchanges on the network will be monitoring withdrawal requests to the parent chain, ensuring that if a bad actor takes control of the parent chain they will be unable to successfully withdraw any funds. In the event of a fraudulent withdrawal, each exchange on the protocol can ping the on-Ethereum contract directly to stop the request. After more than half of the exchanges have pinged the contract, withdrawals from the parent chain will be frozen. Each exchange can then settle their own state and message the contract with the balance of which assets belong to which addresses on their exchange. After all exchanges have pinged the contract with the current state, the contract will release all assets to their rightful owners on the mainnet.

3.3.2 Snowglobe Incentives
For Snowglobe to appeal to other exchange partners, it is important that two main criteria are met:

1. Exchanges must be able to keep their own utility token for use in securing their childchain
2. The protocol must not charge the exchanges any extra fees to participate

On the flip side, AURA stakers must be incentivized to maintain the integrity of the parent Snowglobe chain in addition to the IDEX childchain. This incentive comes in the form of supporting and accepting the Boreal. IDEX customers have the option of paying their trade fees in boreals, the stablecoin of the Aurora network. Exchanges that join Snowglobe must accept Boreals at the target value whenever IDEX customers use them for fee payment in cross exchange trades. This effectively ensures that every exchange on Snowglobe is backing the Boreal and contributing to its usability.

4. Operating Aurora on a Distributed Computing Network

Blockchain networks are limited in terms of computational power making it extremely expensive to run simple programs directly on chain; many programs are not even possible to run on chain. Given these limitations, the best approach is to create a hybrid system that uses an evm-compatible blockchain for transaction processing and a separate network for Aurora governance. There are many teams working to offer distributed computing such as Golem, IEX or Maidsafe. The specific choice will depend on the development progress and direction of each team. It's also possible that we determine Aurora is best served by building its own distributed computing network on the foundation laid down by Snowglobe.

4.1 Open Access

Every component that makes up Aurora is available to users all over the world, all that is needed to access is an internet connection. This results in a financial ecosystem which is inclusive of the entire human population. Once privacy controls such as zk-snarks become standard, boreals and IDEX will implement them and allow for users to engage in completely private transactions. The open and private protocol makes it impossible for any user to be censored, and by implementing this as a decentralized program combined with an evm-compatible blockchain it is impossible for users to have their funds confiscated.

4.2 Operating on a Distributed Computing Network

In addition to guaranteeing open access, operating the infrastructure in a distributed manner brings many additional benefits. Decentralized operations make it much harder to DDOS the Aurora infrastructure, ensuring that the network is always available. Additionally Aurora will be able to access computing power for the best rates possible. It is conceivable that Aurora will eventually incorporate machine learning algorithms operate an AI banker. Operating on a distributed network would give Aurora access to a lot of cheap computing power.

5. Jumpstarting a Currency

Currencies are their own form of network. Success requires a group of consumers and businesses that value the asset and are willing to use it as a medium of exchange. Like any network it grows more valuable as you add more participants. However it also suffers from the "cold start" problem, the difficulty of building a core user base when the product's usefulness is a function of the size of the network. Aurora is taking a measured approach to launch and nurture the boreal to help overcome these challenges.

5.1 Building the Base

Before businesses are willing to accept boreals as payment, there must be demand from consumers to use them. The historically deflationary nature of cryptocurrencies has killed almost all incentive to spend them. Thousands of businesses were onboarded to platforms that would allow them to accept bitcoin, but no one wants to pay with an asset that may be 10% more valuable a few days later. The stability of boreals is therefore the prime factor in attracting customers interested in using the boreal as a currency.

Single user utility - this is a common solution to the cold start problem. It's impossible to launch a network of this scale overnight, so it's important that early on individual users realize a benefit to possessing and spending boreals. This value comes in the form of discounted transaction fees on IDEX. All traders are incentivized to purchase and hold a limited amount of boreals in order to increase the profitability of their trading activities, even if they are the only one doing so.

Network density - another critical component of the early stage is network density. Beginning with a tight knit group of users creates the many connections necessary for a healthy network. Popular examples include launching Facebook at Harvard before slowly expanding to other universities, or using SXSW for the genesis of Twitter. A narrow but deep user group is self-sustaining and can slowly grow over time.

The cryptocurrency community is the ideal launch pad for the boreal. Crypto users are in need of a stable, blockchain-based asset to trade against or hedge with. The lack of stability in other crypto currencies has been a large deterrent from wider adoption and economic activity. Crypto users are inherently forward thinking, and generally more open minded and willing to experiment with new forms of economic incentives and financial structures. Proving out the use case and viability of a privately managed currency in this space will provide the proof needed before slowly transitioning the boreal to different target demographics.

5.2 Partnering with Dapps to Accept Boreals

So far our discussion has focused on generating demand for boreals from the consumer side, ensuring that customers who possess boreals can sell them at any time for fair value. A good currency should also be accepted by a variety of retailers so that customers have a place to spend directly. To help facilitate this Aurora will partner with other dapps who agree to accept boreals at their target value in lieu of other forms of payment. Profit sharing proportional to use on each platform will incentivize dapp operators to participate, and the more boreal denominated transactions the more profits are earned. Every onboarded dapp will further strengthen the stability of boreals, as the currency becomes in a way backed by the dapp's own profitability and success. As more and more dapps back boreals and the market of potential use cases grows, so will demand for the currency. Combined with a prudent loan program and open market operations, Aurora will balance supply with increases and decreases in demand.

Dapp backing will serve as an additional mechanism to encourage the public to purchase boreals any time they fall below the target value. For a heavy consumer of partner dapps it makes sense to purchase boreals whenever they fall below the target value and lower the cost of usage. The more dapps that partner with Aurora and the more recurring customers they have, the stronger this effect will be.

6. Why Blockchain?

A blockchain based system will provide Aurora with some unique properties that make it ideal for implementing a free banking platform.

- Counterfeit Protection - All previous free banking systems utilized physical currency, and resources had to be spent to prevent counterfeiting. A blockchain eliminates this risk, as only Decentralized Capital can mint authentic boreal assets.
- Low Distribution Costs - Blockchain assets can be sent anywhere in the world for fractions of a penny. This makes it easier for Aurora to distribute the currency and for consumers and businesses to spend it.
- Auditability - A blockchain provides an immutable record of transaction history. This information allows consumers to assess the health of the ecosystem by analyzing the supply of and demand for boreals. The Aurora Foundation can combine this information with other metrics such as velocity to refine the design of Decentralized Capital to help manage the supply and reserve ratios.
- Open - The Ethereum network, and by extension boreals, is open to any consumer who has access to the internet. Once Aurora is fully autonomous, the decentralized network makes it impossible to shut the system down, ensuring that the project is not hampered due to government intervention.

Lastly, the Ethereum blockchain is the ideal platform to build on due to the experimental nature of the community. Most consumers outside of cryptocurrency enthusiasts won't immediately understand or be interested in using a decentralized stablecoin, making it much harder to gain customers and adoption. On the other hand, cryptocurrency users have long sought to create such a product, and boreals represents a novel and viable option. These users are skeptical of the current banking ecosystem that is dominated by central banks, and will immediately see the value in creating a private banking system that is outside of government control.

7. AURA Token

IDEX will be the first exchange to operate on the Snowglobe network, transitioning from a semi-decentralized to a fully decentralized exchange. All fees from IDEX are remitted to the Aurora reserves. As the reserves grow Aurora can increase the value of outstanding loans, generating additional revenue for the Aurora network. Fees from the Aurora banking system will then flow back to those who stake the AURA token and provide the economic foundation that holds Aurora and Snowglobe together.

Similar to other blockchain networks, Snowglobe requires a well-designed incentive structure to ensure that the integrity of the order book and transaction sequence are not compromised. Aurora has its own native network token, AURA, that aligns the interests of Aurora and the Snowglobe operators. All of the revenue from Aurora is used to compensate those who stake their AURA and provide security for the Snowglobe network. AURA staking aligns the economic interests of the operators with the health of the network, and makes it extremely costly for any would be attacker to disrupt operations.

Prior to the launch of Snowglobe, all revenue from IDEX will be deposited into the boreal reserves. This revenue will be collected for future use in aligning economic incentives with AURA holders after the Snowglobe protocol is live. In the event that there is not enough revenue from Aurora to provide sufficient security for the platform, fees from IDEX may be used directly to enforce security in the system, bypassing the remittance to Aurora reserves.

7.1 AURA Token Details
Supply: 1,000,000,000

50% will be used to help accelerate adoption of the Aurora network. Of the total amount of AURA tokens, 40% will be used to help subsidize the growth of Aurora by distributing AURA to users and community members through programs such as market maker rewards, marketing campaigns, and air drops. The remaining 10% will be given out proportionally to individuals who purchase IDEX memberships.

The remaining 50% of AURA will be used as follows:

- 20% founding team
- 10% future employee token pool
- 10% future use
- 5% initial investors
- 5% businesses expenses

7.2 Market Maker Reward Program
Aurora is implementing a crypto rewards program, enabled by the AURA token, to encourage the creation of limit orders on IDEX. This program is designed to jump-start exchange usage and encourage the growth of liquid order books.

Market makers who place and execute limit orders on any IDEX market are eligible to receive AURA token grants. 20% of the total AURA token supply will be distributed to the community via this grant program at a rate of one percent of the total *remaining* reward tokens per month. With each additional month the number of AURA rewards will be slightly reduced, providing an incentive for market makers to join early and ensuring that the rewards program can continue indefinitely. Traders will receive AURA proportional to the fees they spend on their limit orders. For example, if three traders trade during a one month period with trader A paying 5 eth in fees, trader B paying 2 eth in fees and trader C paying 3 eth in fees, they will receive 50%, 20%, and 30% of the total AURA distributed that month respectively.

Funds that are held in the reward program pool will be used as backing for boreals in the event that the reserve value drops significantly. This will ensure that there are at least 200% reserves for boreals at any given moment. With Decentralized Capital holding a large portion of AURA in reserves, Aurora will capitalize on its own growth and allow more boreals to be created off of this wealth, improving the position of everyone holding AURA.

7.3 Membership Sale (IDXM)
IDXM is a crypto membership that entitles the holder to free or discounted trades on IDEX until the year 2021. IDXM also provides members with a 2x accrual rate in IDEX's market making rewards program for life. Each IDXM purchase in the token sale also granted the owner 50,000 AURA per IDXM in the AURA airdrop. A total of 2,000 IDXM exist, and Aurora Labs sold 1,600 at the launch of the IDEX mvp.

Each full IDXM (1 IDXM) entitles the token holder to 100% of the membership rewards. IDXM is divisible to 8 decimal places, and membership rewards are applied on a pro rata basis. Additional IDXM above one grants no further membership benefits including both trade discounts and AURA reward multipliers. The benefits are the same whether a user owns one or five IDXM.

IDXM members are able to choose from the following membership benefits:

1. Free trades and no AURA rewards
2. 2x Market Making rewards and full trade fees
3. A proportional mix of both

Membership benefits are a function of both the amount of IDXM held by the member and the choice of rewards. Membership benefits do not increase for any holdings above one full membership. Members can view and set their benefit choices using the benefits tab of the exchange.
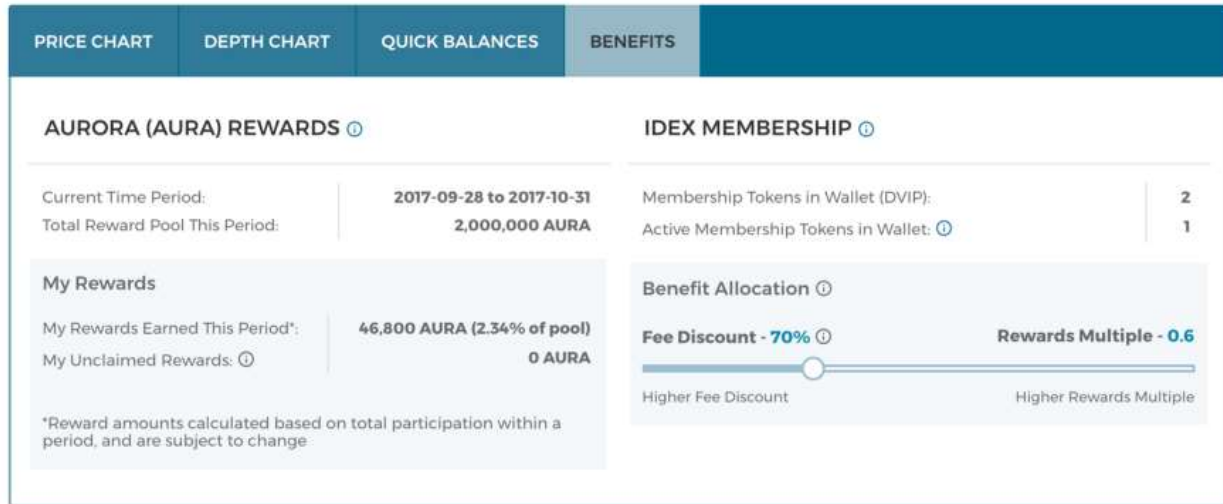

Fig. 3 – IDXM Benefits Allocation

The rewards multiplier and fee discount are represented by the following formulas:

Fee Discount Percentage = (1- x) * (IDXM) * 100
Rewards Multiplier = ((1 – IDXM) + (IDXM * x) * 2)
x = rewards percentage; values range from zero, all fee discount, to one, all rewards multiplier
IDXM = number of active IDXM held; capped at one if holding more than one active IDXM

For example:
1. Joe has 2 IDXM
    a. If Joe sets his reward percentage to 0, he'll pay 0 trade fees and does not participate in AURA rewards
    b. If Joe sets his reward percentage to 1, he'll pay 100% of the trade fees and receive 2x market making rewards
    c. If Joe sets his reward percentage to 0.5, he'll pay 50% of the trade fees and receive 1x market making rewards
2. Jane has 0.6 IDXM
    a. If Jane sets her rewards percentage to 0, she'll pay 40% of the trade fees and does not participate in AURA rewards
    b. If Jane sets her rewards percentage to 1, she'll pay 100% of the trade fees and receive 1.6x market making rewards (1x standard rewards + 0.6x membership rewards)

c. If Jane sets her rewards percentage to 0.75, she'll pay 85% of the trade fees and receive 1.3x market making rewards (0.85x standard rewards + (0.75*0.6=0.45x) membership rewards)

7.4 Use of Funds

The revenue from selling memberships will be used to further expand IDEX capabilities, develop the Snowglobe protocol, and lay the foundation for the Aurora network. The immediate priority is expanding the team of four into a team of around ~10, adding at least four more developers to the team. The anticipated use of funds is as follows:

- 70% Development Expenses - Contributions allocated for development expenses will be utilized to cover all costs associated with the further development of IDEX, the Snowglobe protocol, and the boreal and Aurora network. This includes improvements to and security audits for the existing network, and the launch of the decentralized Aurora platform.
- 15% Operational Expenses - Contributions allocated for operational expenses will be utilized to cover costs associated with accounting, business development, community management, people operations, recruiting, support, and other administrative tasks.
- 8% Marketing Expenses - Contributions allocated for marketing expenses will be utilized to cover costs associated with the promotion of IDEX, the Aurora project, the Snowglobe protocol, and the boreal stable currency.
- 7% Legal Expenses - Contributions allocated for legal expenses will cover any legal costs associated with the establishment and operation of the Aurora project entity and any unforeseen legal costs necessary to address issues that could threaten the success of the Aurora project.

8. Development Timeline

The semi-decentralized implementation of IDEX launched on the mainnet in early Q4 2017. Post-launch the team's focus has turned to the development of Snowglobe.

- October 2017 - IDEX launch on the mainnet. Semi-decentralized architecture consists of Ethereum smart contract plus central trading engine and transaction arbiter.
- October 2017 - API integration. Opening the platform via API access has enabled the development of trading bots, increasing liquidity and improving market efficiency.
- December 4th 2017 - IDXM membership sale starts
- January 2018 – AURA airdrop on IDXM holders
- Q3 2018 - Boreals go live with market making to stabilize the price
- Q3 2018 - Deploy childchain architecture, allowing IDEX to increase transaction throughput.
- Q4 2018 - Decentralization of the orderbook and transaction arbiter. This completes the transition of the current IDEX product to a decentralized childchain exchange.
- Q1 2019 - Margin trading support. Including this functionality in the protocol will put the UX on par with existing centralized exchanges.
- TBD - Launch the Snowglobe MVP, allowing other exchanges are now able to build on the protocol. This is dependent on the development of scaling solutions such as sharding.
- TBD - Fully decentralized Aurora mvp with Decentralized Capital boreal loans

9. Team

We have a qualified team with a healthy mix of business and development experience.

Alex Wearn - CEO (https://www.linkedin.com/in/alexwearn/)
Alex is an expert at leading teams in the design and delivery of software products. He has managed a wide range of operations, marketing, and sales analytics products for Amazon, Adobe, and IBM, and most recently led a product management team in re-platforming their application to operate on a private Ethereum blockchain (project still in stealth mode). Alex is a graduate of the Kellogg MMM program, a dual MBA in Finance and Operations and MS in Design and Innovation.

Phil Wearn - COO (https://www.linkedin.com/in/philwearn/)
Phil is a Co-founder of EtherEx and has been building blockchain based companies since the time when Ethereum was little more than a white paper. While developing EtherEx he identified the pressing need for a high performance decentralized exchange protocol, an insight which served as the basis for IDEX. Phil has a background in aerospace engineering.

Raymond Pulver - CTO (https://www.linkedin.com/in/raymond-pulver-iv-9504038a)
Ray is an avid mathematician, cryptographer, and software developer with over a decade's worth of development experience. An expert in multiple languages, Ray has been designing secure systems on Ethereum since its inception. His preliminary designs led to the IDEX transaction arbiter and trading engine enabling high transaction throughput and true market orders, features which were previously unavailable on Ethereum exchanges.

Brian Fernalld - Full Stack Developer (https://www.linkedin.com/in/brianfernalld/)
Brian is a full stack developer with over 10 years experience in startups. In addition to engineering, Brian has worked for many years in the fields of blockchain technology, product management, marketing, and design. Brian uses his passion for fintech and blockchain technology to build the best user experiences possible.

Supplemental Information

https://www.youtube.com/watch?v=wXQ-W_DlI3c

http://oll.libertyfund.org/titles/selgin-the-theory-of-free-banking-money-supply-under-competitive-note-issue

https://mises.org/library/denationalisation-money-argument-refined