Ducatus Coin - White Paper

*By Ducatus Swiss Pte limited in consultation with Trammell Ventures**

What Is Ducatus?

Ducatus provides the world's strongest combination of cryptocurrency infrastructure and a network marketing distribution system. Leveraging the distribution power of carefully structured network marketing system with the scalability, security, and durability of a robustly designed cryptocurrency gives your Ducatus coins real and lasting value.

Members of Swissmine.club can buy and sell Ducatus mining credits and digital coins from the Swissmine.club website. The coins can be securely stored in a digital wallet on a phone, desktop computer, or on the Swissmine.club website. When a member wants to make a purchase using their Ducatus coins, they make a simple transfer from the wallet of their choosing to the vendor. This will work not only for online shopping but eventually for compatible point-of-sale systems as well.

How It Works

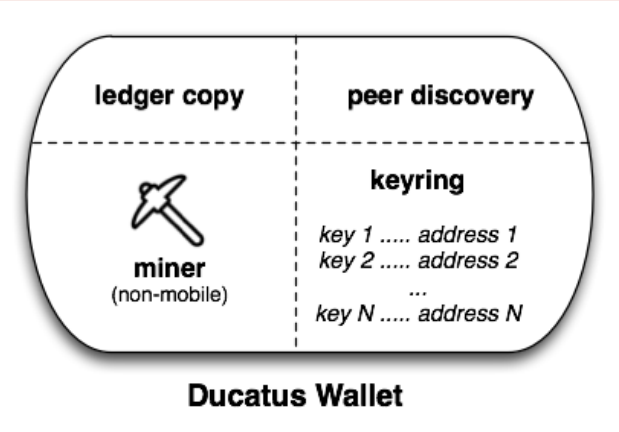
Cryptocurrencies rely on a distributed ledger called a "blockchain". This ledger keeps track of all of the transactions between digital "wallets" in the network. Wallets are apps that run on club member smartphones and desktop computers. When a member wants to send Ducatus coins from one wallet to another, they enter the recipient's "public address" and the amount. The network of all member wallets then joins forces to verify and validate the transaction, which, once verified, is written to the shared ledger.

Blockchains are the secret sauce that make cryptocurrencies work. They contain a database of all transactions that have taken place involving that cryptocurrency. It's referred to as a "blockchain" because it is made up of a series of "blocks", each of which is a set of transactions in the ledger which took place over a short period of time. In order to generate the next block, wallets compete to solve a challenging cryptographic problem that they only learn of when the preceding block is completed. When a wallet thinks that it has solved the problem, other wallets work to validate that it is in fact accurate. Once enough wallets have confirmed the accuracy of the block, it is added to the blockchain of all wallets. This process is called "mining".

While the block is being mined, wallets report transactions to each other. A transaction is simply a transfer of cryptocurrency coin from one wallet to another, based on their public addresses. Assuming that sufficient wallets agree that a transaction has been made during mining, these transactions are added to the ledger in the blockchain, at which point all wallets in the network recognize that the transfer of coins has taken place. As your wallets participate in the mining operation and successfully mine blocks, they will receive a number of small Ducatus coin

payments from other members in the form of transaction fees. Wallets running on desktops may receive more significant rewards since they have higher processing capability than wallets on mobile phones.

Wallets contain a set or “keyring” of public addresses that give them a way to publicly identify themselves in the ledger. For each public address, a wallet has a corresponding secret or “private” key that only the member has access to. A wallet may generate multiple public addresses in order to distinguish between different reasons for transacting with coins. This is somewhat akin to the trailing digits in a bank account number that let you know whether it’s for your checking or your savings account. If a Swissmine.club member wants to use different platforms, say, one on their iPhone and one on the website, they will need to create a wallet and addresses for each platform. Members will easily be able to transfer coins between their wallets using the Ducatus coin network.



Ducatus Wallet

Making a purchase with a cryptocurrency is as easy as it is to use a credit card, but the way the ledger works means that the process may feel a little backwards at first. Ducatus’s partner vendors host their own wallets which accept Ducatus coins for purchases. When a club member wants to make a purchase from a store, they send their coins to the wallet address that the store gives them and fill in their own public address. The member will tell their wallet app to send the appropriate amount of coins to the address, and then the Ducatus coin network takes care of the rest of the transaction. So, instead of sending a vendor a code as you would with a credit card number, the vendor gives you a code to type into your wallet.

Since all of the wallets in the network work together to create a ledger without needing to connect to Swissmine.club, members are able to use their coins as long as there are wallets connected to the Internet. This means that any vendor that supports Ducatus coins can accept them forever. The ledger is distributed between all wallets, so any member can easily see all validated transactions that have been made on the Ducatus coin network. There is no need to worry about a third-party like Swissmine tracking your club credit - it’s all right there for everyone to see and is cryptographically and permanently secured.

Altcoin Technology

At Ducatus we use industry standard cryptographic algorithms and blockchain technology in order to provide a secure and reliable experience. As a result, we have decided to follow tried and tested industry best practices to create an “altcoin”, that is, an alternate cryptocurrency to Bitcoin which is created based upon the code underlying Bitcoin. We have forked the source code of open source Bitcoin wallets and modified the parameters of the network in order to create a new coin, the Ducatus coin, with characteristics that we believe will work best for the members of Swissmine.club. A fork is a variation to the an existing body of code which renders it distinct from previous versions. In this case the ‘hard fork’ of the Bitcoin code allows us to create a coin which uses all the best features of Bitcoin and omits or fixes those features which have proved to have issues or weaknesses.

One of the most important changes that we have made to standard Bitcoin parameters is that we have modified the time that it takes to mine blocks. Bitcoin blocks take on average ten minutes to mine, which is fairly long for applications like e-commerce, not to mention selling items at a point of sale like a restaurant or a store (imagine that a shop assistant asked you to wait while they processed your credit card ... and it then took ten or more minutes for them to get back to you!).

Since the majority of the original tried and tested code is retained, forking source code is considerably more stable and secure than independently developing an entirely new (and thus untested) body of code for a new coin. The information security community has a saying, “don’t roll your own crypto”. In almost all major cases where a cryptographic product has been compromised it has been because that team did not seek independent testing and verification of the cryptographic algorithms used in their product. Using Bitcoin as a basis for our technology means that Ducatus benefits from all of the hard work and analysis that has already been done on the Bitcoin system. We have engaged industry-leading experts in information security to ensure that our new code is also very secure, but by forking Bitcoin we have already built on the world’s most solid cryptocurrency foundation.

Another major benefit of a Bitcoin fork is that partner vendors are able to much more easily support the Ducatus coin. There are many existing code libraries that allow e-commerce sites to support Bitcoin on a plug-and-play basis, and since we are using a nearly identical API, web stores and crypto-currency exchanges will be able to very easily adapt them for use with Ducatus. Where appropriate we will also work with vendors and the open source community in order to ensure that relevant libraries will continue to be compatible with Ducatus in the years to come.

Creating a Wallet

Swissmine.club will provide and host “web wallets” which members can use to perform transactions with Ducatus coins. For members who want the convenience of having a wallet at their fingertips, we will also offer mobile apps for iOS and Android. Power users and members who are interested in receiving transaction fees for mining blocks may choose to use a desktop

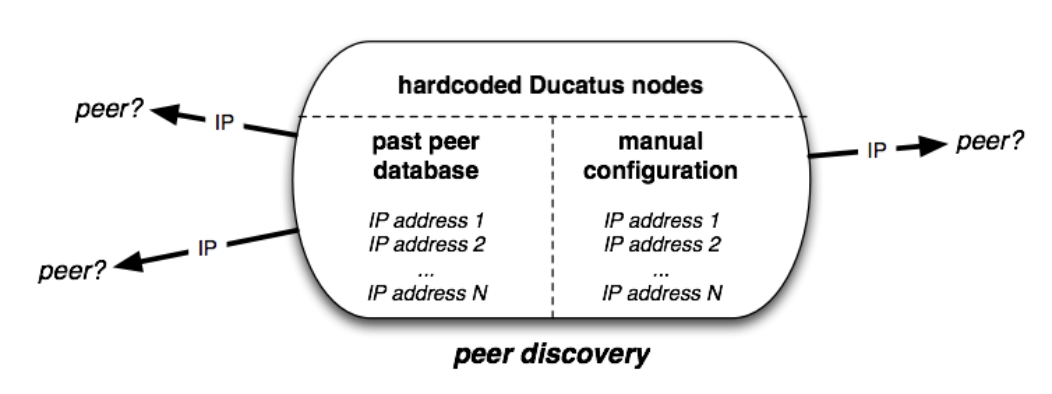
wallet, which we will offer for Windows, OS X, and Linux. Any of these wallets can join the Ducatus coin network and send and receive coins.

A member wishing to use a wallet app starts out simply by downloading it and setting it up on their device. When the wallet initializes itself it will create a private key as well as a public address to receive coins at. The user can then add more keys to their wallet as desired. It is a good idea for a member to create a backup of their private keys - if they lose them, neither they nor anybody else will be able to access the contents of their wallet. Our recommendation for our members to backup private keys is to print them out and store the paper copy in multiple locations, including their home safe and ideally also in a separate safety deposit box.

Connecting to the network

Once the wallet is set up with keys and addresses, it's time to connect to the Ducatus coin network. This network is made up of all Ducatus wallets that are connected to the Internet - it can be seen as a virtual layer on top of the Internet. This technology is similar to that of the peer-to-peer networks that are used for applications like BitTorrent.

Wallets find each other through a process called "peer discovery". A freshly created wallet that is connecting to the internet for the first time, will use the DNS system to lookup a Ducatus wallet server that contains a list of active wallets. Each wallet maintains its own list of peers, and will share that peer list with other wallets. After a wallet has connected the first time it will first refer to its own saved list of peer wallets that it has successfully connected to in the past. There is also the option to manually add wallet IP addresses into the Ducatus wallet in case neither of these approaches is successful.



Your First Coins

As a Swissmine.club member you'll get your first coins from the Swissmine.club website through the purchase and subsequent conversion of mining credits. You can then associate a public wallet address with your membership profile on the website. That way Swissmine will know where to send your coins.

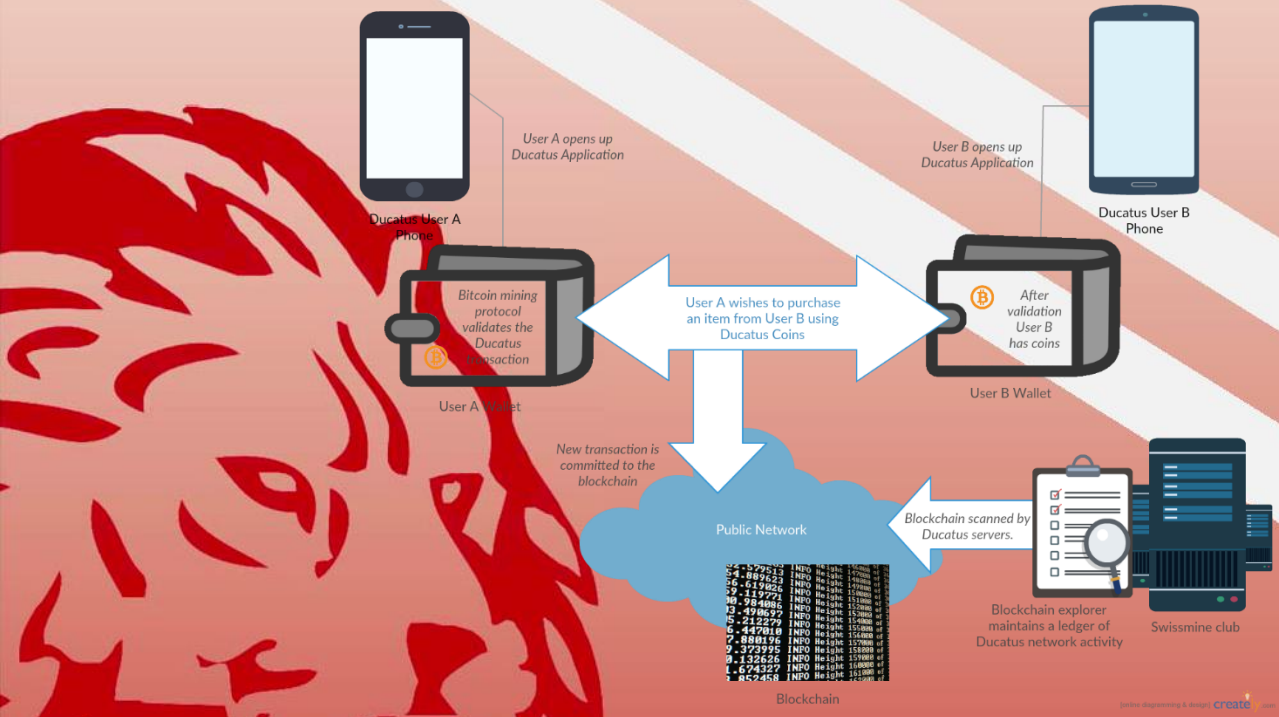
Once your profile is set up, you can then just click to send coins to your wallet. Swissmine will then use its own wallet to initiate a transaction on the Ducatus blockchain. Wallet nodes on the network will mine a block, and then that transaction is added to the ledger. At that point your wallet will recognize that your Ducatus coins have been added to it.

Making a Transaction

At this point, your coins are yours and it's up to you what you want to do with them. You may want to make a purchase from one of our vendor partners. To do this you would use their online web shop like any other e-commerce site and when you checkout you simply select 'Ducatus' as your payment method.

At this point, vendor implementations can vary quite a lot from store to store, but it will be something like the following: first, they use their wallet to generate a unique public address for your transaction, then they share that public address with you and state the amount that they are going to ask you to pay, at which point, if you're using a desktop wallet, you can just copy-paste the address into your wallet and initiate the transaction. Many vendors also will give you their wallet address as a QR code so that you can easily scan it with the wallet app on your mobile device without having to type it in by hand.

Once you have initiated the payment process, the vendor will scan the Ducatus blockchain for the transaction. Once it's been posted to the ledger and validated by enough peers, the vendor will approve your payment and continue the process just as they would if you use any other form of currency.



Mining blocks

If you're running a desktop wallet then once it has established peer-to-peer connections with other wallets, it's ready to help mine some blocks and earn transaction fees. As a user you need to do very little to enable this - as long as your machine is on and connected, and if mining is enabled, the wallet will mine in the background with whatever extra computational resources that your machine has available.

What is mining, really? Each block in the Ducatus blockchain must be validated with a cryptographic hash. This hash is derived mathematically by combining all of the prior block hashes with all of the pending transactions that need to be validated. Creating a hash is a one-way operation, so it's cryptographically challenging to find what the new one is; *i.e.* you need to crunch through large numbers of complex computations in order to find the answer. Miners all work by processing calculations to find the hash, and once one announces a solution, the rest can quickly check and validate that solution. With enough validations that block is then added to the distributed Ducatus blockchain which is recognized by all wallets and then cannot be changed. This puzzle-solving approach is used to validate all Ducatus transactions at a steady rate.

Fund Recovery

As long as a member has created a paper or electronic backup of their private keys they will always be able to access their coins on the Ducatus blockchain, no matter what happens to their wallet app, computer, or phone. This is because the coins aren't really stored "in the wallet" - their storage in the wallet is recorded in the ledger on the blockchain. So if something goes wrong, all the member needs to do is download the wallet app and give it the private keys that they backed up. The wallet will then check its keys against addresses in the blockchain and then it will automatically have access to its Ducatus coins again and know how much value is associated with each key.

Pre-Mining

Ducatus is unusual amongst altcoins because our cryptocurrency coins are all pre-mined. Historically, most coins have used block mining as a way to provide rewards for the mining of new blocks and the building of the blockchain. Using the Ducatus approach however, miners will still earn rewards in the form of transaction fees, but we will instead start with a known pool of Ducatus coins and distribute them to our members through our network marketing and the associated compensation system to ensure rapid widespread adoption all around the world.

Stockpile Management

While we have made Ducatus as decentralized and distributed as possible, there are still some considerations with regard to managing the pre-mined coin stockpile. Fortunately, handling large wallets is a known challenge in the cryptocurrency industry and the industry has evolved to support a fairly secure and robust process. Cryptocurrency exchanges face a similar problem

as they have many members who buy coins from and sell coins to them. When a user has coins on an exchange to convert between currencies the coins are temporarily held by the exchange's wallet. This makes the exchange a tempting target for adversaries.

Best-practices have evolved to ensure wallet security for exchanges and systems like Ducatus. The problem is not just a technical one but that of following sound security policy. The greatest threat to any company that holds significant volumes of cryptocurrency coins is that an attacker will compromise their wallet security either by obtaining their private keys or by taking over the wallet software itself. We use a two-pronged approach to mitigate this threat.

Hot and Cold Wallets

The first approach to securing wallets is to simply not make them available to attackers online. It is impossible to do this for all wallets on an exchange or a system like Ducatus because they must be online in order to send coins to members. But that doesn't mean that Ducatus needs to keep its entire coin bank online at any given moment. This has led to the concept of "hot wallets" and "cold wallets".

Recall that a wallet has two components - private keys and public addresses. The private keys are required to process blockchain ledger transactions on behalf of the wallet. Any wallet that has an Internet-connected component that knows its private keys is referred to as a "hot wallet" for these purposes. It's live, online, and something that we don't want an attacker to get at. The wallets used by Ducatus to transfer funds to members must be hot in order to send transactions to the blockchain. Ducatus hot wallets will be highly secured when operating.

A "cold wallet" is a wallet that is not connected to the Internet but just because a wallet isn't connected to the Ducatus coin network doesn't mean that it can't *receive* transactions. Cold wallets are any wallets that don't have a live connection, but that we do know one or more public address for. The private keys might be in a safe deposit box, but the public addresses are known to the ledger. Therefore, a cold wallet can receive funds over the blockchain even though it is not actively connected.

Industry best practice is "wallet splintering" - breaking the funds that are available to an exchange up between a set of hot and cold wallets. This means that, even if one wallet is successfully attacked, most of the funds are still intact in all of the other wallets. Spreading items across many wallets decreases the value of any one wallet, making the attack far more difficult to obtain any items of significant value. Cold wallet private keys are stored in a physically secure location off of the Internet, and hot wallets are configured to only have as much coin as is expected to be needed on a day-to-day basis. By using this approach we ensure that at any given time our threat profile is minimized.

Code Quality

Our security is only as good as our software, and the software used to connect the Swissmine.club website to its hot wallets is a key target for attackers; the hot wallets are where an electronic attacker could get directly at Ducatus coins. We have engaged with industry experts in information security to ensure that our process and technology is security-centric, especially when it comes to our hot wallets.

We use a combination of human review (both third-party audits as well as the use of an internal change management board whenever significant source changes are made) as well as electronic analysis tools that can help uncover potential issues such as command injection points and possible logic flaws. This is not something that we will do once - security is an ongoing concern and is built in to our process.

Next Steps

Following the formal acceptance of this white paper we will move immediately to execution. This will involve a number of steps:

1. Confirmation of specifics regarding the forked code-base including identifying a target Bitcoin branch and establishing proper parameters.
2. Fork and deployment of our initial Ducatus wallet for internal mining.
3. Establishment of the Ducatus blockchain followed by commencement of pre-mining Ducatus coins for Swissmine.club.
4. Final selection of code bases for key member components (web / desktop / mobile wallets, blockchain explorer, etc.)
5. Development and launch of Ducatus web wallet and block explorer and integration with Swissmine.club.
6. Coin integration with Ducatus shop.
7. Launch of Ducatus member desktop and mobile wallets.
8. Finalization of API for Ducatus integration with third-party vendors and shop POS systems.
9. Internal Ducatus coin exchange for member-to-member trades
10. Finalization of API to support third-party cryptocurrency exchanges

Key deliverables, in sequence, will be:

- Linux wallet (used for blockchain initation)
- Pre-mined Ducatus coins.
- Web-based wallet and block explorer; integrated with Swissmine.club
- Windows, OS X, Android, and iOS wallets
- Third-party vendor integration instructions/examples/libraries.
- Internal Ducatus coin trading exchange
- Third-party exchange integration API

Conclusion

Ducatus is poised to deliver a robust cryptocurrency solution for Swissmine.club's member network. We have devised a well-thought out architecture based on industry best practices, which means that we have a realistic way forward to deliver a great experience for users. As we have developed our coin network we have engaged with domain experts in blockchain and information security in order to ensure that we have delivered a reliable and secure solution for our members.