LEOcoin

White Paper

Foreword

Historically, digital currencies have been the preserve of technologically minded individuals with supercomputers. As the founders of LEOcoin, we have an ambition to bring digital currency to everyone.

We think digital currencies like LEOcoin can do so much more than the sector has managed to date. Finding a way of making this sector appeal to local businesses and people, includes removing the need to understand the technical details of the technology.

New and improved technology, combined with more user friendly interfaces can now make this possible. We have major ambitions for this sector, as it has the potential to fundamentally transform the way business is done across the world. We want LEOcoins accepted in local corner shops - when that happens, digital currencies will start to meet their potential.

At the heart of LEOcoin's approach is the desire to make a currency for entrepreneurs, businesses of all shapes and sizes, and the everyman.

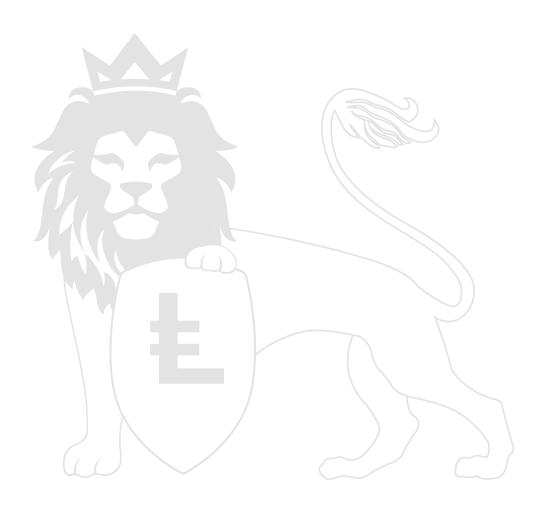This whitepaper sets out how LEOcoin works, and our vision for the future of digital currency.

Founders of LEOcoin

Our vision for the future of digital currency.

Contents

Introduction

LEOcoin was created in June 2014, and has been backed by a dedicated digital currency exchange (www.LEOxChange.com) since April 2015. It is the first digital currency to be launched in the UK that is designed for small business owners; allowing individuals to make fast, secure and cost effective transactions through a decentralised peer-to-peer network. The usability and accessibility of the currency positions LEOcoin as a world currency and the currency of choice for entrepreneurs.

The opportunity for digital currencies is significant: the world's largest 'cryptocurrency,' Bitcoin, has around 13.5m coins in circulation, used by around 2.6m individuals in up to 100,000 transactions per day.

This paper sets out to introduce LEOcoin, the underlying technology that supports it, and its business support philosophy.

It explores the principles of digital currency and the potential it offers to businesses and consumers; including increased security, privacy and flexibility.

From low transaction fees to instant trading, we explain the advantages offered to both consumers and business owners, as well as the support network offered by LEO and the LEOcoin Foundation. The LEOcoin Foundation has been created as an open and participatory standards body for the LEOcoin project. It is a non-profit organisation that funds the development of LEOcoin and the LEOcoin infrastructure.

Why digital currency?

Digital currencies leapt onto the scene in 2009 bringing a new dynamic to the speed, security and privacy of financial transactions. The fallout of the world banking crisis, combined with concerns over the privacy and security of money and new restrictive regulations, led people to look for new and innovative ways to transact.

Conventional banking works in such a way that many third parties have sight of and access to a person's financial and personal information throughout a transaction, which has associated costs and privacy issues. With LEOcoin there is not the multitude of third party transferring agents who want their share of the action. The cost of sending LEOcoin is practically zero compared to the high costs associated with credit card and payment processing agents most businesses are used to.

The rate of inflation that can potentially diminish the purchasing power of fiat – or traditional - currencies (such as Sterling) does not affect the value of a digital currency to the same degree, as there is a fixed amount of the currency produced over a fixed period of time – and no governments or institutions to manipulate the quantity or price.

> With LEOcoin, there is not the multitude of third party transferring agents who want their share of the action.

LEOcoin

Bitcoin was the trailblazer for digital currencies. It has achieved a huge amount in a short time, but has also opened up an opportunity to do things in a very different way. Many experts believe that the future's leading digital currency will not be Bitcoin. There have been many lessons learned from the journey of Bitcoin - and LEOcoin has implemented these lessons. The early days of digital currency encountered many technical problems due to the platforms being used; many of these are still an issue. These include excessive processing energy consumption, 51% attack, and manipulation of the ASIC computer chip that drives the technology.

The leading standard digital currency will be the one that resolves these challenges and makes it as user friendly as possible. This aim is at the heart of LEOcoin's creation.

Initially LEOcoin used a hashing algorithm (Scrypt-Jane) that gradually increases the demand in RAM (a computer's processing power). This method is known as Proof of Work, and in essence it meant the more powerful a computer you had, the more digital currency you could mine.

But not any longer. LEOcoin has now moved to a Proof of Stake model which, rather than rewarding LEOcoin investors for the power their computer lends to the network, it instead rewards LEOcoin users based on the number of LEOcoin's they currently hold and 'stake'. Essentially this means the more LEOcoin's you have, the more you will earn.

This method is far less demanding on computer power and in practical terms that means the consumer and small business owner does not need to invest in an expensive and powerful machine to mine LEOcoin. This makes LEOcoin mining available to a wider mass market audience.

Who is Using LEOcoin?

LEOcoin has been designed to appeal to the enterprise community: small businesses who are penalised by transaction fees, domestic and international.

There are already 33,000 Merchants offering goods and services priced in LEOcoin and 206,000 LEO Members who hold LEOcoin.

This is where LEOcoin diverges from digital currencies that have been seen to date. Capitalising on LEO's existing membership of hundreds of thousands, LEOcoin offers instant access to a mobilised user-base.

Pervious digital currencies have started from a zero-base, relying on word of mouth and the technical knowhow of the 'cryptocurrency' community. LEOcoin is different. LEO Members have been involved from the start of the LEOcoin development process, and as such they were a ready and waiting community of merchants, consumers and traders when the LEOxChange launched. This has added stability to the exchange price as well as faster uptake than previous coins.

However, communicating the opportunity presented by digital currencies is still in its early stages. LEOxChange conducted a YouGov survey in 2015 that found almost 50% of small to medium sized enterprises who trade internationally said transaction fees were a key concern; and 43% who transacted using debit or credit cards were also worried about the associated costs. Yet 85% said they would consider using a digital currency. LEOcoin wants to capitalise on that mindset.

How does it work?

A mathematical computer-based process called mining generates LEOcoins. The mining itself is a very complex mathematical problem, which is solved by a computer executing difficult number-crunching tasks.

The difficulty of the mining increases over time making it harder to obtain the coins. This acts as a deflationary brake on the currency, therefore creating stability in the price. This is the opposite of a conventional fiat currency which decreases in value each time a Government prints more.

LEOcoin was designed by experts using the latest technology and techniques in cryptocurrency and blockchain. LEOcoin is at the cutting edge in digital currency, designed for use by the world's entrepreneurs as well as private individuals.

The total number of LEOcoin is finite. There are only 1 billion LEOcoins in the network that will be mined over the next 100 years. This gives leverage, robustness and long-term sustainability to LEOcoin as a digital currency.

Furthermore, LEOcoin pre-mined 50 million coins ahead of the exchange going live. This was designed to nurture the early development of the LEOcoin economy and add stability.

The total number of LEOcoin is finite. There are only 1 billion LEOcoins in the network that will be mined over the next 100 years. This gives leverage, robustness and long-term sustainability to LEOcoin as a digital currency.

Consumer Advantages

As discussed above, the major advantage of LEOcoin is the existing user-base and community that supports it. LEO members are already trading amongst themselves using the currency, creating a readymade economy. Furthermore, the LEOcoin Foundation's mission is to educate the untapped audience of the business community and drive uptake of digital currency.

Other benefits include:

Privacy - Payments with LEOcoin can be made and finalised without any personal information being tied to any transactions; and due to this enhanced privacy of personal information, there is greater protection against identity theft.   Due to the way the blockchain works, the identity of the user is not important. This means it is secure and kept hidden at all times unless someone chooses to reveal it. Because all the transactions and information are highly encrypted, even extreme computational power would require thousands of years to crack it.

Transparency - Using the blockchain technology, all finalised transactions are available for everyone in the network to see, however all personal information is hidden, i.e. you can tell when a coin was spent, but not by whom. While a public address may be visible, personal information is not tied to it, giving it the transparency of a public ledger whilst at the same time maintaining personal information security.

Control - Accounts that hold traditional currency can be requisitioned or frozen completely by a host of authorities, often through no fault of the consumer. Since digital currencies exist outside the traditional regulatory frameworks that allow this to

happen, it is very rare for a holder to be rendered unable to access their coins, unless illegal activity is proven to have taken place.

Secure - LEOcoin's Proof of Stake (POS) model reduces the risk of 'Selfish Miner flaw' and '51% attacks'. Transactions in any digital currency have to be approved and verified by the peer-to-peer network. This community approval means everyone has a stake in the currency, so it is in the community's interest to ensure security.

Value - there are no 3rd party transferring agents (like a bank) who want their share. The cost of sending LEOcoin is practically zero compared to the bank transfer costs most people are used to.

As every coin is accounted for in your ledger, merchants cannot charge extra hidden fees without being noticed. They must communicate fees to the consumer before adding charges.

Accessibility – Digital currencies have the potential to provide the unbanked with a low-cost financial refuge. Peer-to-peer transactions and digital currency denominated banks will allow the unbanked to have a safe, low-cost way to manage their wealth. In theory, assuming the backing of a financial system, digital currencies could ultimately help bring many out of poverty by letting capital flow more easily.

Untapped Audience

Businesses could potentially have access to millions of customers who have 'unbanked' money; as these are people who do not use banks or financial institutions to manage and save their money – through digital currency they would have a new option. Without access to a bank, these people rely on cheque cashing services and cash-only transactions to survive. Aside from the danger of operating exclusively in cash, cheque cashing services can charge fees anywhere between 1.5 percent and 10 percent for each transaction. People who do not use banks typically cannot afford to open savings accounts or have a credit card. According to the World Bank, 3/4's of the world's poor are unbanked. Even some who can afford to open a bank account abstain because of the associated costs.

Access to low cost, secure tender, could allow for the 'unbanked community' to constructively participate in the economy again.

International Trading

Using credit cards or bank accounts for international transactions can be problematic; since they are linked to the legal tender of a specific government, exchange rates, interest rates, and country-to-country transaction fees. This adds levels of bureaucracy that have associated costs.

Trading across currency lines forces people to pay taxes at both ends, as well as any additional costs from using wire transfers or services like Western Union and exchange fees. Digital currency bypasses this confusion, dismantling barriers between markets.

Digital currencies are not bound by the rules or status of any one government's currency, so international transactions tend to go a lot more quickly and smoothly when they are used. They bring competition to the remittance and payment markets.

Merchant Advantages

Many of the features above apply to merchants as well as consumers. Digital currency transactions, such as LEOcoin, are not reversible, do not carry personal information and are secure, therefore merchants are better protected from potential losses that occur from fraud. Merchants are able to do business where crime rates and fraud rates may be high and credit or debit cards may not be accepted.

Digital currency makes transaction fraud harder due to the public ledger (blockchain) and the peer network encourages cooperation against fraudsters.

LEOcoin also benefits from having an existing large membership base of over 206,000, (plus 33,000 merchants) who all receive promotional material about LEOcoin's marketplace, which is in effect additional free advertising.

The merchant programme means LEOcoin can reach out to more people through training, in turn making them ambassadors of LEOcoin – this will perpetuate the LEOcoin user community and strengthen it.

Energy and cost efficient

Proof of Stake (POS) requires much less energy than other digital currencies in the longer run, making LEOcoin attractive from a sustainability perspective.

By design, it will take approximately 100 years to distribute all of the LEOcoins to the community. Meanwhile owners of LEOcoin will be rewarded with more coins on the basis of their stake, as follows (correct at July 2016):

1,000 LEOcoin	10% each year
5,000 LEOcoin	15% each year
50,000 LEOcoin	20% each year

This allows LEOcoin to have a very low inflation rate that no bank can change. The Proof of Stake basis, offers a significant reward encouraging people to hold LEOcoin and benefit from these rewards. Additionally, Proof of Stake, truly democratises the way that new LEOcoin are spread among users.

As part of our ambition to be a coin for everyone, we were keen to have a coin that did not rely on excessive technical knowledge or require significant financial investment in GPUs and mining rigs. Instead, a simple desktop wallet is all that is needed to fully benefit from the rewards offered by Proof of Stake

The block chain

The blockchain

The 'blockchain' is the name for the system that governs transaction administration in digital currency. The transactions in the system are recorded in a public ledger, processed by decentralised computers in an operation referred to as mining. It uses its own unit of account, in this case LEOcoin.

LEOcoin has no central repository and no single administrator; the US Treasury refers to digital currencies like LEOcoin as 'decentralised virtual currency.'

Once you start mining, the pool uses the following payout systems.

A Share - Finding blocks is not an easy task. Since it would take a long time on some coins, finding a block is broken down into shares. Depending on the server side setting, each share can be a certain difficulty. The more difficult each share is to find by miners, the fewer total shares are required to eventually find a block.

Simplistically, this could be compared to premium bonds. The more you buy, the better chances you have to win the award. With LEOcoin you can participate in this process by keeping your wallet open and using your stake.

Stratum, a protocol used by a miner to request work from a server, is used for share submission and getting new work. On the server side, each share is checked against the coin daemon (a server side wallet with more features) if it is indeed a valid block solution. Every share computed has the potential to be a block solution.

Pay Per Last N Shares (PPLNS) - Block rewards are distributed among the last shares, disregarding round boundaries. Essentially this means the 'miner' is rewarded for solving a block of code.

In the accurate implementation, the number of shares is determined so that their total will be a specified quantity of score (where the score of a share is the inverse of the difficulty). Most pools use an implementation based on a fixed number of shares or a fixed multiple of the difficulty.

Orphan block - Coins generated by a block will not be available to you right away. They will take some time to be confirmed by the entire network before you are allowed to transfer them out of the pool. This is to minimise the risk of fraudulent activity and 'double-spending' of coins.

Usually coins have a confirmation set to 120. What that actually means is that the network (not the pool) has to discover 120 additional blocks on top of the one found by the pool to confirm it.

Estimated payout - this is your estimated payout if a block is found at that time. This is an estimate according to your amount of shares submitted for the round(s).

Regulation

Currently there are few regulations imposed on digital currencies, other than standard money laundering regulations. Because of their international trading potential, and the anonymity of the currencies, regulations would be difficult to impose without altering some of the fundamental benefits of them.

However, not all regulation is bad, and LEOcoin supports the development of steps that can be taken to create more confidence within the mainstream population without severely hampering innovation or the privacy of users. In fact, LEOcoin has made a number of approaches to the UK Treasury and regulators in the USA, regarding the shaping of their own plans for regulation.

If a government were to intervene in a heavy handed fashion then digital currency would lose its core benefits of privacy, security, low to no fees, and free marketability. Over-regulation would obviously make it no different from current currencies. This could in fact dissolve the benefits of digital currency.

Outlawing digital currencies would simply restrict legitimate business and drive the criminals further underground, depriving the private sector of the significant benefits of digital currencies. However, with government approval, or at least acquiescence, legal businesses and users can take advantage of the potential speed, low costs, flexibility, and privacy offered by digital currency.

Over-regulation could simply drive the creation of another black market, while denying the substantial benefits of legitimate digital currencies to the law-abiding citizen everywhere.

LEOcoin Foundation

The LEOcoin Foundation has been created as an open and participatory standards body for the LEOcoin core project.

It is a non-profit organisation that funds the development of LEOcoin and the LEOcoin infrastructure, creating new avenues for people to participate in the LEOcoin project.

It undertakes research, provides education and acts as an enabler for public participation. It fosters efficient cooperation between private and corporate stakeholders, governmental and non-governmental organisations and commercial and non-commercial entities.

Cryptography and the power of online networks have made possible the existence of decentralised, purely digital currencies, and by promoting the use of such digital currencies the LEOcoin Foundation will support improvements to existing monetary systems.

Through participating in the wider digital currencies ecology, the LEOcoin Foundation aspires to be thought leaders and a respected contributor to the development of this nascent technology.

Through economic support the LEOcoin Foundation will aid worthy contributors irrespective of currency affiliation.

Through robust engagement with official bodies the LEOcoin Foundation will become an established supporter and contributor of public dialogue, seeking to inspire, educate and engage both the public and regulatory bodies.

The Government Are Banking on Digital

There is much evidence that public and regulatory bodies are coming round to the view that digital currencies are the way forward.

In 2016, Circle, a pay-app, was granted an e-money issuer licence by the UK Financial Conduct Authority (FCA), despite the fact that the UK Treasury had yet to decide on its stance on regulation of the digital currency market. They were supposed to have done that by the end of 2015.

Why does this matter? It matters because this is the start of the process of normalizing a technology that until recently was seen as the 'reserve of cyber criminals'. In essence the FCA have just given the green light to the sort of technological step that not long ago was seen as pure science fiction.

Circle started out in 2013 as a bitcoin 'wallet' and has since expanded into broader currency payments. It uses blockchain technology to make international payments from one currency to another, transferring into bitcoin en route, then turning back into fiat currency at the other end. This means they make it possible to transfer British Pounds to Russian Rubles via a momentary conversion to bitcoin. The important point is that this payment avoided the government regulation and international currency bureaucracy that governs the fiat currencies.

Now Circle are taking the same instant service that we have come to expect from Facebook messenger and WhatsApp and applied it to cash payments. The concept of being able to text your friend money securely was fanciful not long ago; and doing it with a license from Government would have been unthinkable. But that's the world we're now starting to live in.

What makes this development all the more interesting is that it's not just some young entrepreneurial upstarts taking it to market, it's actually backed by one of the world's largest banks, Barclays.

Barclays' involvement is intriguing because, not least of all, blockchain technology has been regularly cited as one of the biggest threats to the financial status quo. The reason why blockchain could be a threat is because, used properly, it takes out the middleman; and what are banks if not middlemen.

Blockchain technology itself is nothing new, it's just an encrypted database that's distributed across a computer network. What makes it possibly revolutionary is that it can only be updated when everyone on that network agrees and once entered, the information can't be overwritten. That's why people are looking at it for purposes such as electronic voting and healthcare records. The collective responsibility and encryption makes it incredibly secure and reliable.

Banks have dined out for centuries on being that reliable secure connection for our money; take that away from them and make it an instant automated process and, at least in theory, you're taking away their reason to exist.

Perhaps then that's why it should be no surprise that, in 2015, nine of the world's biggest banks joined forces to create a framework for using blockchain. This group of banks, including Goldman Sachs and Barclays, have come together with New York-based financial tech firm R3 in the hope of utilising the technology to strip out processing costs and save money.

Governments are looking at ways they can utilise it too - the cynically minded might say that banks and governments are doing this to gain some control of the technology.

So the future looks bright for those who view digital currencies as the new transmitter of value; as the way to mobilise an economy without interference from middlemen who add no value; and without the heavy burden of irrelevant legislation.

Glossary

ASIC (Application-Specific Integrated Circuit)

An ASIC is a microchip designed for a special application, such as a particular kind of transmission protocol or a hand-held computer. You might contrast it with general integrated circuits, such as the microprocessor and the random access memory chips in your PC. ASICs are used in a wide-range of applications, including auto emission control, environmental monitoring, and personal digital assistants (PDAs).

An ASIC can be pre-manufactured for a special application or it can be custom manufactured (typically using components from a "building block" library of components) for a particular customer application.

Block Reward

The reward given to a miner which has successfully hashed a transaction block.

CPU (Central Processing Unit)

The CPU is the part of a computer system that is commonly referred to as the 'brains' of a computer. The CPU is also known as the processor or microprocessor. The CPU is responsible for executing a sequence of stored instructions called a program.

Fiat Currency

Currency that a government has declared to be legal tender, but is not backed by a physical commodity. The value of fiat money is derived from the relationship between supply and demand rather than the value of the material that the money is made of. Historically, most currencies were based on physical commodities such as gold or silver, but fiat money is based solely on faith. Fiat is the Latin word for *"it shall be".*

GPU (Graphics Processing Unit)

A silicon chip specifically designed for the complex mathematical calculations needed to render millions of polygons in modern computer game graphics. They are also well suited to the cryptographic calculations needed in cryptocurrency mining.

Hash

A hash algorithm turns an arbitrarily-large amount of data into a fixed-length hash. The same hash will always result from the same data, but modifying the data by even one bit will completely change the hash. Like all computer data, hashes are large numbers, and are usually written as hexadecimal.

Hash Rate

The number of hashes that can be performed by a bitcoin miner in a given period of time (usually a second).

Mining

Mining is a metaphor to describe the process where someone has a computer and they use the hardware storage space of that computer to support the processing power needed to maintain a digital currency ledger. In other words, if I were to pay you a sum of LEOcoins, that transaction needs to be recorded and verified. This needs computer hardware storage space and processing power; when someone participates and shares their computer, this is called mining.

LEOcoin operates a straightforward 'plug and play' system, meaning the mining requires little input from the user.

P2P (Peer to Peer)

Decentralized interactions that happen between at least two parties in a highly interconnected network. An alternative system to a 'hub-and-spoke' arrangement, in which all participants in a transaction deal with each other through a single mediation point.

POS (Proof of Stake)

An alternative to proof of work, in which your existing stake in a currency (the amount of that currency that you hold) is used to calculate the amount of that currency that you can mine.

POW (Proof of Work)

A system that ties mining capability to computational power. Blocks must be hashed, which is in itself an easy computational process, but an additional variable is added to the hashing process to make it more difficult. When a block is successfully hashed, the hashing must have taken some time and computational effort. Thus, a hashed block is considered proof of work.

RAM (Random Access Memory)

The main memory in a computer, smartphone or tablet. RAM is the temporary workspace where instructions are executed and data are processed. What makes RAM "random access" is its capability of reading and writing any single byte. This "byte addressability" differs from storage devices such as hard disks and flash memory chips, which read and write sectors containing multiple bytes. In addition, RAM is used as a temporary space for the software, while storage is permanent until deleted by the user.

Selfish Miner Flaw

The result of a miner keeping their block discoveries private to their own pool, and cautiously revealing them to the rest of the honest miners, thus forcing the honest miners to waste their resources on blocks that are not part of the blockchain.

Wallet

A secure digital application that is used to store LEOcoins. This can be downloaded from the LEOcoin website for Windows, Linux, Android, IOS or Mac OS operating systems.

LEOcoin Foundation

Battle Barns
112 Preston Crowmarsh
Oxfordshire, OX10 6SL
United Kingdom
www.LEOcoinFoundation.org

www.LEOcoin.org

www.digitalchamber.org