LEOcoin Foundation

Digital Currency Whitepaper

LEOcoin's new privacy settings

Contents

Our vision for the future of digital currency

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.

LEOcoin has now undergone a significant technological innovation, which will give its users access to a unique level of privacy – setting LEOcoin apart from other digital currency competitors.

This Whitepaper sets out the new functionality of LEOcoin and the key debates on the capability of digital currencies to be anonymous and private.

Foreword

The Western world has undoubtedly embraced digital exchanges of currency, but the question now is whether it will entirely embrace digital currency itself.

Our digital currency combines development skills, international infrastructure, real-world entrepreneurial know-how, and a global network and user base, creating a platform for growth.

Sending LEOcoin is a fast and simple way to transfer money globally, without the need for transaction fees, middlemen or banks. Through the use of advanced cryptography and encryption methods, LEOcoin has managed to create a truly private digital currency.

When the idea of cryptocurrencies emerged, one of its purposes was to create a truly anonymous system that requires no bank or centralised operator.

LEOcoin leaves banks out of the money transfer process. This means there are no third party transferring agents who want their share. So the cost of sending LEOcoin is practically zero compared to the bank transfers most people are used to.

This is an efficient way to send money to family and friends as well as pay for products and services worldwide; and is much simpler to use than online banking, as the user is entirely in control of their wallet.

Sending LEOcoin is as easy as typing in the address of the receiver and clicking the send button. Everything else is done by a very advanced programme that requires no further user interaction.

Here we set out to answer a number of questions around the security and secureness of digital currencies (also known as cryptocurrencies) and blockchain technology, as well as an introduction to LEOcoin's new unique privacy function.

Dan Andersson

Founder of LEOcoin, and Chairman of the LEOcoin Foundation

Digital currency anonymity and privacy

Digital currencies are often referred to as private or anonymous currencies. In the context of financial transactions, digital currency has the potential to be private and anonymous with new technological solutions now available on the market to protect the users' right to privacy – in this regard digital currencies are no different to the use of cash.

Digital currencies, like LEOcoin, are anonymous in terms of programming, and provide anonymity in practice thanks in large part to advancements in the capability to protect the users' details — name, home address or bank details — from all kind of snooping. LEOcoin's new privacy option within the latest 'Upgrade' feature augments this further.

Identities are not recorded in the LEOcoin protocol itself, but every transaction performed with LEOcoin is visible on the distributed electronic public ledger known as the blockchain. However, outward transactions do contain a privacy feature that protect user's privacy and their identity from unwanted surveillance.

The privacy provided by digital currencies is a point of attraction and a challenge for financial regulation (see Jason Weinstein's comments on page 4).

Yet the practical reality for the vast majority of digital currency users is that they are not operating anonymously. For many users of digital currencies, who access the currency through one of the popular online wallet or exchange services (like LEOxChange), their participation at the outset entails linking their personal identity to their digital currency holdings. A digital currency for this type of user is effectively no more anonymous than a bank account. For example, to open a digital currency wallet an individual must conform to the same proof of identity checks that an individual would go through to open a bank account, i.e. proof of ID, address, etc.

Digital currency transactions can then be anonymous, since real-world identities are not recorded on the blockchain ledger: the only identifying information recorded there are the Bitcoin addresses, whose corresponding private keys are held by the owners as proof of ownership.

A further source of potentially deanonymizing information is available to every computer that participates in the decentralized transaction network by hosting a digital currency 'node'. This information is the set of Internet Protocol (IP) addresses of the computers that announce new digital currency transactions. So the computer where the coin was generated could be traced back to its IP address, however not necessarily the user.

LEOcoin's new privacy settings

The new encryption features of LEOcoin's blockchain means that every move that is recorded in the ledger is encrypted. It is written in a way that would take all the computers in the world thousands of years to decrypt and brings with it the highest level of security. Every identity and every transaction is turned into a series of letters and numbers that make no sense unless you know how to turn it back to its original state. Think of it as a locked chest, we can see that there is a chest but not what's inside it.

LEOcoin is spearheading a new direction for digital currencies. LEOcoin users now have access to a unique level

Is digital currency the criminal's friend or foe?

Jason Weinstein, a partner at Steptoe & Johnson LLP and a former deputy assistant attorney general in the US Department of Justice, in charge of cybercrime and organized crime, gave a recent speech on digital currency in relation to criminal use.

He says a user's Bitcoin address is like an account number that stays with the user; if you can connect that address to a user, you can identify and trace all of the transactions in which that individual has participated using that address.

As with banks, law enforcement would be able to obtain information about the address user by serving a subpoena or following other lawful process. There are existing and rapidly improving techniques to help link those users to their Bitcoin addresses and transactions using, among other things, analysis of transaction patterns to make connections among multiple addresses used by the same individual; mining of data from social media and public sources; and analysis of IP addresses used to conduct transactions.

He added that there's also a real attribution advantage: the traceability, search ability, and permanence of the blockchain. Whether a law enforcement agent identifies the owner of an address tomorrow or two years from tomorrow, the agent will then be able to trace back every transaction involving that address, all the way back to the beginning.

Moreover, because the ledger is publicly accessible, law enforcement does not have to worry about what type of legal process is required to access the data, and because the ledger is borderless, law enforcement can get the data without having to go through a foreign government. That gives law enforcement the data it needs to 'follow the money' in a way that would never be possible with cash.

Law enforcement is still on a learning curve with Bitcoin, although the case against Carl Force IV, the former Drug Enforcement Administration (DEA) agent convicted of stealing bitcoins during the Silk Road investigation, demonstrates that even at this early stage, law enforcement has already developed an impressive capacity to follow the money using the blockchain.

of functionality that will allow them to use these new encryption features to 'go private'. This method will allow the user to choose to trade their currency in an even more secure form – something that no other digital currency offers.

Every wallet will start with two addresses, one public and one private (also known as Stealth address). The public address will work in exactly the same way that other digital currency transactions work - publicly recording the user's pseudonymous information and the transaction history of every LEOcoin. However, choosing the private option, launches 'Ring of Trust Technology', which essentially creates and confirms the transaction on the blockchain without publishing potentially identifiable details. This model is called Dual-key Stealth Addresses and it keeps users' information safe by not recording any pseudonymous information.

Stealth addresses are generated in a different way than normal 'Bitcoin' addresses, but they have a similar structure. A dual-key stealth address contains a lot more information because it requires the sender of a transaction to know the public scan key and the public spend key, which is not stored on the blockchain. All data required to perform such a transaction is derivable from the stealth address itself.

The payer derives a new, normal address from the Stealth address, to which the funds will be sent and in that process only allows the payee to compute the corresponding private key. This is based on the mathematical principle called the 'Diffie-Hellman Key Exchange'. It allows two entities to generate a shared secret based on their keypairs. Like with the famous Enigma machine, it did not matter if you had the code for either end of the transmission, if you didn't have the source code the Enigma machine was using, you could not translate it. With the Stealth address system even a super computer like Colossus cannot crack it.

Essentially, the coins are destroyed after they are sent from the original wallet and created anew before they arrive with the recipient (meaning the process cannot be reverse engineered).

What's more, LEOcoin's new privacy functions include a private messenger function so that traders can communicate with the utmost privacy as well as trade privately.

All messages are encrypted by the proven AES-256-CBC algorithm, and distributed between nodes. Even if the 'assailants' could view the entire network the message information would remain private due to the aforementioned encryption.

Conclusion

Average users and regulators should be aware that trading in digital currency using standard functionality is certainly less 'anonymous' than cash, but more so than conventional online fiat transaction. However, dedicated users can make specific transactions anonymous through the use of LEOcoin's new privacy settings. However, the open nature of the transaction ledger makes it extremely difficult for the user to achieve absolute anonymity, unless on a limited scale using LEOcoin's new technology.

In summary, the consumer advantages of instant, secure, international transaction are considerable. - Yes, there are opportunities to exploit the system, much as there are with existing forms of fiat transaction, but the security concerns presented by the supposed anonymity of digital currencies are largely overblown.

Furthermore, law enforcement agencies have largely caught up with people using it for criminal purposes and have been able to discover information about transactions where relevant to a criminal act.

However the new level of privacy offered by LEOcoin's upgrade, will offer our users an added level of protection. The right for consumers to privacy must always be considered – and that is why LEOcoin has introduced this new feature for its users.

Our private feature 'The Upgrade' protects our users' identities at a time when identity theft, the right to anonymity and privacy in the digital age is at the forefront of public attention.

The rapid pace of technological development enables individuals all over the world to use new information and communications technologies (ICTs) to improve their lives. At the same time, technology is enhancing the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy.

Article 8 of the European Convention on Human Rights legislates for an individual's 'private and family life, his home and his correspondence', subject to certain restrictions that are 'in accordance with law' and 'necessary in a democratic society'. This article clearly provides a right to be free of unlawful searches, and mass surveillance campaigns. Therefore anonymity in conducting your financial affairs is very much within the letter and spirit of international laws. LEOcoin's new offering exemplifies this right.

Furthermore, a 2014 report to the General Assembly of the United Nations (UN) by the UN's top official for counter-terrorism and human rights condemned mass electronic surveillance as a

clear violation of core privacy rights guaranteed by multiple treaties and conventions and makes a distinction between 'targeted surveillance' – which 'depend[s] upon the existence of prior suspicion of the targeted individual or organization' and — 'mass surveillance', by which 'states with high levels of internet penetration can gain access to the telephone and e-mail content of an effectively unlimited number of users and maintain an overview of internet activity associated with particular websites'. Only targeted interception of traffic and location data in order to combat serious crime, including terrorism, is justified, according to a decision by the European Court of Justice. This should not include legitimate businesses only seeking to trade. Our new privacy settings will give those traders a new level of security.

A new resolution on the right to privacy in the digital age, adopted on 21 November 2016 at the UN General Assembly of the UN, comes at a time when the rapid pace of technological development is enhancing the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy.

The UN policy links the right to privacy with the exercise of freedom of expression, as well as participation in political, economic, social, and cultural life, a framing that challenges increasing identification of security and surveillance by governments and corporations.

At LEOcoin we have given our users the ability to go private – because that's their right. 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 LEOcoin and our contemporaries.

Glossary

Digital anonymity

Digital currencies are pseudonymous; that is, sending and receiving digital currency is like writing under a pseudonym. If an author's pseudonym is ever linked to their identity, everything they have ever written under that pseudonym will be linked to them. In digital currency, your pseudonym is the address at which you receive it, and every transaction involving that address is stored forever in the blockchain. However, technology is now available to undertake a financial transaction anonymously by creating and confirming the transaction on the blockchain without publishing the original sending address. Essentially, the coins are destroyed after they are sent from the original wallet and created anew before they arrive with the recipient.

Blockchain

Blockchain technology itself is nothing new, it is just an encrypted database that is 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 cannot be overwritten.

Proof of Stake

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 (POS) model, which rather than rewarding LEOcoin investors for the power their computer lends to the network, 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.

LEOcoin's POS model also 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.

LEOcoin Foundation

Battle Barns
112 Preston Crowmarsh
Oxfordshire, OX10 6SL
United Kingdom

www.LEOcoinFoundation.org

www.LEOcoin.org

www.digitalchamber.org