ILCoin Whitepaper

ILCOIN Development Team March 2019

TABLE OF CONTENTS

What is ILCoin

“WE NEED THINGS THAT DRAW ON THE REVOLUTION OF BITCOIN, BUT BITCOIN ALONE IS NOT GOOD ENOUGH.” - BILL GATES

ILCoin is a modern alternative to Bitcoin using a SHA-256 encryption. ILCoin is a cryptocurrency that is not dependent on the present banking system and has its own independent value. There will be 2.5 billion ILCOIN available. We are looking to expand ILCOIN usage worldwide. In the near future we will be capable of handling smart contracts, also we increase our maximum block size to 25 Mb in order to avoid future problems like hard forking because of SegWit.

Introduction

“KNOW THE BASE WHICH HELPS YOU BUILD YOUR FUTURE!”

ILCOIN is a high-quality cryptocurrency developed by ILCoin Dev Team. It is mined using SHA-256 Proof-of-Work (POW) technology . The ambition of ILCOIN is to evolve and become the foundation of a new, global digital currency-based economic system. Members of this system may earn, accumulate, spend and trade ILCoins for the benefit of themselves and the entire community.

The Background

Digital coins were all but non-existent until 2009 when Bitcoin first appeared from seemingly nowhere. It was, and still is, the most successful cryptocurrency. It also brought blockchain technology into focus, causing a true revolution in the digital world; a game changer.

Cryptocurrencies (and, in a broader sense, blockchains) are digital systems designed to move
information among members directly, through a completely decentralized network of computers (including cell phones). Cryptocurrencies use virtually impenetrable “puzzles” to ensure information remains concealed or locked into a block.

Verifying the cryptographic information is called mining, and miners usually receive a unit of the given cryptocurrency (or a portion of it) for their work. Verifying information contained in a block and adding such blocks to a chain of blocks (the blockchain) are the main elements of how the system works. It is the key to ensuring information is distributed in a decentralized way, without having to originate from, or pass through a central data repository or distribution centre.

This also means that cryptocurrency transfers take place instantly on a peer-to-peer basis - directly from one user to another - without control banks, central banks, card companies, payment processors, etc.

The Outlook

“IN THE NEXT 30 YEARS, 90% OF ALL COMPANIES WILL DO THEIR BUSINESS ONLINE” - JACK MA, FOUNDER OF ALIBABA.COM

In our lifetime, most things have gone or are going digital. Televisions, telephones, typewriters and even information have all gone digital. Clearly, traditional data exchange and payment systems cannot keep up with this fundamental shift in technology. The Internet needs a new form of money, and in order to move fast and virtually at no cost, money needs the Internet.

The crypto movement, although still in its infancy, has demonstrated the superiority of decentralized communication and the voluntary respect of contracts between parties. In other words, information shared and stored is based on a consensus among all parties. The fact that everyone can find and see any type of information publicly - if they know where to look - ensures that information remains untampered and readily available. While there is, of course, a high degree of uncertainty regarding cryptocurrencies and blockchain technology, everybody agrees that it is here to stay. The potential in this groundbreaking technology, together with the acceptance and recognition of cryptocurrencies - even by a growing number of banks and governments - makes new projects extremely appealing for start-ups and investors alike.

The Company

ILCoin has been launched and is mined by IlCoin Dev Team, a young and dynamic start-up company, committed to build and develop a global digital currency-based economic system and community. With long-time programming knowledge for each of our representatives, we are intended to achieve improvements in this cutting-edge technology which is the cryptocurrency world.

Every day we make effort to bring more numerous and improved assets for our users. We are always looking for ways to update with better security and connectivity to our wallets so that we can keep current with the latest technology; providing a better experience for our users. Our support centre is always available to assist you with any issue that might arise during the use of our products. We also have tutorials to help you feel more comfortable and confident when interacting with our products.

The Goal for ILCoin

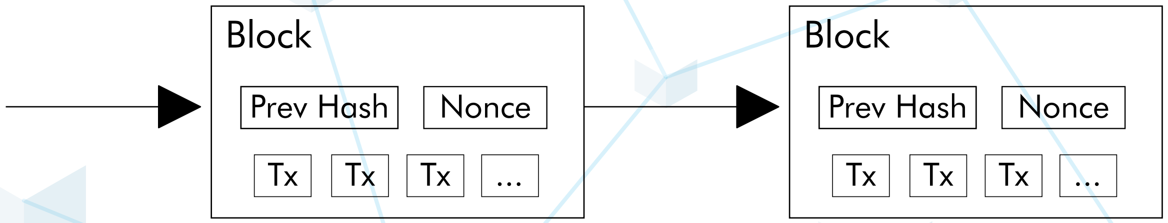
Thanks to the centralized nature of ILCoin mining, developmental work on the blockchain, the wallet and the explorer is a continuous effort kept under tight control. ILCoin can be safely stored in wallets built for the cloud, Android, OSX and PC and it can be transferred directly to anyone instantly at virtually no cost - without banks, without chargebacks. ILCoin users can monitor their transactions throgh our own block explorer. ILCoin is listed and freely traded on several cryptocurrency exchanges.
We are one step away from being able to create "smart contracts", the first blockchain to accomplish this using SHA-256 technology.
The vision is to make ILCOIN available to everyone in the world so that they can enjoy privacy and profit from economic opportunities. The foundations of this new economic community have been laid.

Technical Info

"THIS IS WHY YOU CAN TRUST ILCOIN"

Proof of Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a Proof-of-Work system similar to Adam Back's Hashcash rather than newspaper or Usenet posts. The Proof-of-Work involves scanning for a value that, when hashed, such as with SHA- 256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.
For our timestamp network, we implement the Proof-of-Work by incrementing a nonce in the block until a value is found that gives the block's hash; the required zero bits. Once the CPU effort has been expended to make it satisfy the Proof-of-Work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



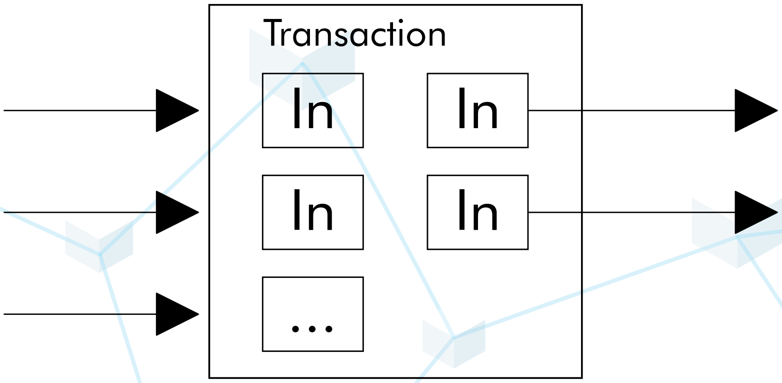
The Proof-of-Work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-Work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest Proof-of-Work effort invested in it.

If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the Proof-of-Work of the block and all blocks after it, then catch up with and surpass the work of the honest nodes.

The probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added. To compensate for increasing hardware speed and varying interest in running nodes over time, the Proof-of-Work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

Combining and Splitting Value

Although it can be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction, or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one for returning the change, if any, back to the sender.



It should be noted that fan-out (where a transaction depends on several transactions and those transactions depend on many more) is not a problem here. There is no need to extract a complete stand-alone copy of a transaction's history.

Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult Proof-of-Work for its block.
4) When a node finds a Proof-of-Work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not spent already.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next Proof-of-Work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

COMPLETED DEVELOPMENTS

"THANKS TO THE OVERALL DEVELOPMENT, ILCOIN IS ONE OF THE BEST MANAGEABLE CRYPTOCURRENCIES ON THE MARKET"

ILCoin Web Wallet

https://ilcoinwebwallet.com/
- Redesign of the Web Wallet, Improving Wallet Security issues; forcing the Encryption of all Wallets
- Implementation of the option of different Fiat Currencies in order to know the Actual Price of ILCoin
- Implementation of a Dynamic Graph in order to know the Historical Price of ILCoin
- Upgrade the Security of the Site and also added a SSL Certificate to assure the Connection Security
- New Graph Options
- Improved Security
- Upgraded Server Back-End Security

ILCoin Blockchain Explorer

https://ilcoinexplorer.com/
- Redesign of the ILCoin Block Explorer
- 1.0 Security Upgrade: Implementation of SSH Keys, Firewall, VPN, Public Key Infrastructure and SSL/TLS
- Encryption, SSL Certificate with 256 bits of encryption
- Activation of the Message Verification
- Creation of the Login Module
- Update of the outdated ILCoind to the newest ILCoin Core

Android/IOS ILCoin Wallet

https://play.google.com/store/apps/details?id=wallet.ILCOIN&hl=hu
- Layout Design
- Encryption of the Wallets and Mnemonic phrase for Wallet Recovery
- Multi-Address System
- Implementation of a Label and Password for every wallet in your device
- Possibility to see the Unconfirmed Balance
- QR Code Reader for Sending ILCoin and QR Generator for Receiving ILCoin
- Transaction History
- Dynamic Graph with Historical ILC/USD price
- Transaction Fee Configuration
- Sign and Verify Message
- Set Default Wallet (every time you open the app, that will be the default wallet to open)

ILCoin Source Code

- Update of the Boost Version from 1.54.0.1 to 1.63.0, the Latest Version at the beginning of this year
- 14 New Libraries
- Update Node Version from 70001 to 70015
- Faster Synchronization
- Improved Signing Security
- Watch-Only Wallet Support
- Mining and Relay Policy Enhancements
- Memory Usage Optimization
- Block File Pruning
- Database Cache Memory Increased
- Sensitive Data No Longer Stored in Debug History
- 5 Consensus Changes
- 227 RPC and REST Changes
- 56 Command Line Changes
- 193 Blockchain Handling and Storage Changes
- 210 P2P Protocol and Network Code Changes
- 154 Wallet Changes
- 14 Mining Changes
- 32 Protocol and Network Changes
- 49 Validation Changes
- 173 Build System Changes
- 250 GUI Changes
- 291 Tests Changes
- 360 Miscellaneous and Documentation Changes
- 2 Dependency Changes

ILCoin Windows/Mac Qt

- Update of the QT Version
- Redesign of the Layout
- Wallet Advanced Encryption
- Transaction History
- Possibility to see the Unconfirmed Balance
- Transaction Fee Configuration
- Implementation of the ILC/USD, and ILC/BTC Price Dynamic Graph
- Brand New QT Versions
- Connectivity Issues Solved
- Improved Security
- Faster Connectivity and Transactions
- New Interactive Graph Connected Directly with the Markets

ILCoincrypto.com

- Design of the Site
- Implementation of Security for the Site
- SSL Certificate
- Contact Form
- Creation of the Buy ILC with BTC Module (upcoming)

SegWit Problem Solved

The original SegWit problem took place in the Bitcoin network and in all subsequent coins that used the Bitcoin technology. Due to this, a 1MB limit existed, which caused delay in the system if many transactions were made within a short amount of time. The Bitcoin system was not very flexible to cope with this issue and thus it became a problem. ILCoin instead increased the block size to 25MB meaning that we have greatly increased the capacity and electronic limits of the amount of transactions our miners are able to close. SegWit or BIP148 will be available for Bitcoin if at least 95% of the miners accept the new source. However, until then Bitcoin cannot do this because the miners have to accept the bigger block size and be setup for them. Since we control the network of ILCoin, we simply adjust it to our needs. From 170,000 transactions per block, we can handle 15 million transactions per day or more depending on the blocks we mine. At the moment, Bitcoin can handle 375 thousand (data is from https://www.coindesk.com/).

Android ILC/BTC Wallet

- Layout Design
- Encryption of the Wallets and Mnemonic Phrase to Recover the Wallet
- Multi-Address and Multi-Wallet System
- Implementation of a Label and Password for every wallet in your device
- Possibility to see the Unconfirmed Balance
- QR Code reader for Sending ILCoin and QR Generator for Receiving ILCoin
- Transaction History
- Dynamic Graph with Historical ILC/USD and BTC/USD Price
- Transaction Fee Configuration
- Sign and Verify Message
- Set Default Wallet (every time you open the app, that will be the default one to open)
- The Recovery Phrase can be checked after the wallet its created

Block Explorer 2.0

- Upgrade ILCoin Insight Block Explorer
- Separates from Insight to Insight-API and Insight-UI.
- German language
- Fee Rate per kB
- ILCOIN to USD, ILCOIN to BTC in Real-Time
- Connection of BTC Explorer and ILCOIN Explorer

Command Chain Protocol (C2P)

Command Chain Protocol (C2P) was created in order to prevent one of the biggest concerns in the crypto world “the 51% attack to the network”, as the name announce we have a set of rules and policies carve in the source code which allow or block different type of activities, this also help us prevent any blockchain corruption like the double spending issue and prepare our chain for having smart contracts safer and solid. The implementation of 3 different levels of security create a safe environment to the user, took the solid SHA-256 and we put a hack-proof vest so no one can double spend, roll back, or corrupt the network. Also, with these 3 levels we spread the stress of the network by giving different tasks to complete to every full node therefore our chain can be more stable, strong and faster. C2P is the actual next step of security in the cryptocurrency world, in order to turn down the page for all the non-ethical hackers who always try to take advantage on some back doors for some faulty codes, or lack of hashing power for example and in the same moment hurt a specific cryptocurrency and the trust of still cutting-edge technology.

In C2P every block non-only contains the hash of the last block but also contains a set of certificates which the nodes can read in order to double or even triple check the origin of the block and inputs, therefore if that container it’s a valid or a corrupt one, in the second case that block and its inputs will be rejected for all the network. This new protocol prevents the 51% attack with it unique certificate stamp in every block since only non-malicious nodes can deliver that certificate, in addition to this it has implemented a unique blocking mechanism who allows to prevent the stealing of the coins and spending in case of a lost wallet from a user. C2P is a unique asset of ILCoin and with these add on this cryptocurrency became the most secure coin ever existed.

Future Plans and Developments

“ILCOIN WILL BE ABLE TO PROVIDE THESE INNOVATIVE SERVICES TO ITS USERS.”

Expand Exchange Market

ILCoin Development Team is working hard to be inside of new crypto exchanges. At this moment, we are on Bit-Z, IDAX, Fubt, Bitker, DobiTrade, Stex, CoinExchange.io, TradeSatoshi, FreiExchange, Graviex, Crex24 but in the near future we are looking forward to expand greatly within the marketplaces.

Smart Contracts (Q4 of 2019)

- Blockchains can run code. While the first blockchains were designed to perform a small set of simple operations - mainly transactions of a currency- like token - techniques have been developed to allow blockchains to perform more complex operations defined in full-fledged programming languages.
- First, the program itself is recorded on the blockchain which allows it a blockchain’s characteristic permanence and censorship resistance.
- Second, the program itself can control blockchain assets - i.e., it can store and transfer amounts of cryptocurrency.
- Third, the program is executed by the blockchain, meaning it will always execute as written and no one can interfere with its operation.
- ILCoin Blockchain is capable of making smart contracts
- Contracts between parties.
- Define rules and penalties for each type of contract.
- Up to 5 types of contracts to define, each with its own rules and penalties.
- Example type of contract exchange properties.
- Example type of contract exchange shares.

Conclusion

We believe that ILCoin is a high-quality cryptocurrency which will be available to everyone who would like to enjoy privacy and profit from economic opportunities.

References

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf. Oct 2008

[2] https://www.coindesk.com/making-sense-smart-contracts/