fotocoin

WHITEPAPER

Whitepaper

(v 1.0)

This whitepaper is a living document and will be improved and edited on a regular basis. The strategies and ideas you will read about will continue to be added, revised, and improved as we move the project forward. However, in doing so, we will attempt to maintain the original objectives of this project.

This paper is divided into three sections. First section will cover about the ItsFoto platform and its features and benefits. Second and third section will discuss about the technical details of cryptocurrency in general and FotoCoin in particular.

Contents

ItsFoto

Introduction

ItsFoto is an image uploading and downloading platform that is first of its kind to provide privacy and income to its users at the same time. The project's aim is to provide anonymous uploading of images and royalty free downloading of images. We also aim to provide creators and photographers bounty for their creativity and innovations without revealing their privacy to the world. We will also try to protect the system from misuse and make it stable and usable by common users.

Features

This section will shed light on few of the many features of this system. We will also try to cover the benefits of this system and talk about how this platform is one of its kind and better than the existing ones.

Royalty Free Images

Royalty-free, or RF, refers to the right to use copyright material or intellectual property without the need to pay royalties or license fees for each use, per each copy or volume sold or some time period of use or sales. The most basic concept you must know to work with stock photos is that you are acquiring the right to use a photo in a certain way, not the property of the photo itself. Unlike many existing photo platforms, you won't have to pay any money upfront for using individual images. All images on ItsFoto will be available for free download and will be free to use for personal and commercial purposes.

CC0 License

Most of the Images made available for download on ItsFoto will be subject to and licensed under the Creative Commons Zero (CC0) license ("CC0 Content"). The CC0 Content on the Service is marked with the reference "CC0 License" next to the respective image made available for download. This means that to the greatest extent permitted by applicable law, the uploader(s) of the image(s) have dedicated the work to the public domain by waiving all of his or her rights to the CC0 Content worldwide under copyright law, including all related and neighboring rights. Subject to the CC0 License Terms the CC0 Content can be used for all personal and commercial purposes without attributing the author or content owner of the CC0 Content or ItsFoto.

Be aware that the patent or trademark rights of any person, nor the rights that other persons may have in the CC0 Content or in how the CC0 Content is used, such as publicity or privacy rights, are not affected by CC0. Therefore, depending on the intended use of the CC0 Content (in particular commercial purposes), in the case of the depiction of identifiable people, logos, trademark or copyrightable work depicted in the CC0 Content, you therefore may still need the permission or consent from third parties.

Furthermore, when using the CC0 Content, you may not imply endorsement of products and services by the author of the CC0-Content and/or any person, company or brand depicted in the CC0-Content.

Anonymous and Private

ItsFoto does not track or store any of user’s private information, whether it be personal or non-personal. ItsFoto takes special care of user’s privacy, anonymity and security at the same time providing awesome services better than the existing platforms. ItsFoto does not require any logins or signups while downloading or even uploading images, while still earning bounties for uploaded images, which makes it stand out of existing similar platforms. We will try to make better this privacy and anonymity feature in future while still providing the same service and more.

Bounty for Uploading Images

The image upload bounty on ItsFoto will be divided in two parts. First one will be a competition in which we will aim to distribute bounty to top 50 image uploaders based on total number of images uploaded by the user. We will track total number of images uploaded by the user by the donation address provided while uploading the image. Second phase of the bounty will start after the end of first phase in which we will provide bounties for every uploaded images whether the image gets downloaded or not, which makes it stand out of other systems. We have planned to pay bounty for 1,000,000 (one million) images. More detailed information on the working and terms for both the bounties will be announced on the project website.

Strategy

In order to create a highly efficient platform capable of possessing the above mentioned features (especially security, privacy and anonymity) at the same time, we will try to escape tracking, and implement highly advanced yet easy to use payment system for donations and bounty distribution (for uploading images). Crypto coins always takes the first place to handle this case, so we will implement cryptocurrency in this platform to achieve high security, anonymity and privacy, all at the same time.

FotoCoin Implementation

At the very heart of ItsFoto lies FotoCoin to power the platform and make it simple for use by everyone. FotoCoin will be used for giving and accepting donations and for bounty distribution to uploaders. FotoCoin makes the system reliable, safe, secure, private, anonymous and free from third party interventions (like payment systems etc). The many features of FotoCoin will be discussed in details in the later sections of this paper.

Benefits

The combination of ItsFoto and FotoCoin will benefit the image uploaders (artists, creators, photo enthusiasts etc), image downloaders (designers, developers etc) and the crypto world in terms of usage, implementation and adaptation. ItsFoto will try to educate the common people (who are still unaware of crypto revolution), will try to boost the cryptocurrency adaptation by common people (who are not yet using the power of crypto) and will show them the power and usage of cryptocurrency in real world innovations.

Technical Background

This section of the white paper is intended for readers with a strong technical background and some experience with blockchain technologies and cryptocurrencies.

What is a cryptocurrency?

Standard definition

A cryptocurrency is a medium of exchange that uses hash-based algorithms or cryptography to provide more secure transactions and a better protocol as a medium of exchange. Most currencies are peer-to-peer and utilize decentralized communication between networks. They run with a proof-based algorithm that makes the network possible.

The usefulness

Cryptocurrency is useful in a number of ways, including but not limited to:

- More profitable
- Transactions are faster and more secure
- Less prone to inflation
- Gives users more control over currency due to less government interference

Main bottlenecks to Bitcoin

1. Centralization
2. Network capacity
3. Anonymity

Any decentralized payment system that wishes to achieve universal adoption and solidify itself as a viable global currency must be built in such a way that its very infrastructure addresses and solves all bottlenecks early on.

Economically speaking, the exponential price appreciation of Bitcoin from under $0.01 to about $20k clearly demonstrates an increasing global market demand for the solution that Bitcoin offers, however, we believe that until a comprehensive solution arises that fully answers the challenges faced by the Bitcoin network, a full capitalization of the global multitrillion-dollar financial industry cannot be reached.

With this philosophy and unmet public use cases in mind, we have decided to create FotoCoin (FOTO). FotoCoin is a community driven, open source and fully autonomous cryptocurrency that places a strong emphasis on the very building blocks required to create a complete empowering solution to images, artists, photographers and photo enthusiasts: it is secure, anonymous, trustless, scarce and fungible with a very low transaction fees. It is designed to embody all that Bitcoin as well as more advanced cryptocurrencies have grown to become as well as to capture the economic value that is thus far inhibited by the systemic constraints outlined above.

We will expand on these 3-main adoption and growth barriers and outline why FotoCoin's unique architecture was necessarily created to power ItsFoto.

Centralization

A network is considered centralized when either vast or absolute decision-making power is vested in the hands of few individuals. We believe that in recent years, the Bitcoin network has taken on a path of evolution that is incompatible with its founders' original vision.

The first is the question of mining. Mining is the process by which individuals dedicate computational resources to solving difficult mathematical problems. Upon solving the aforementioned, a new block is found on the blockchain and with it newly pending transactions are confirmed and cleared through. This process is known as Proof of Work (or PoW) as it forces the miner to prove that they have done the necessary work to verify the block, and the first miner to find a new block is compensated for their efforts. This introduces an element of economic competition between miners and prevents the network from being attacked as attacks become too costly and thus, economically unviable.

Unfortunately, the Bitcoin protocol has introduced a mining algorithm that allows for ASICs (Application-Specific Integrated Circuit) devices that can create a very large number of hashes per second. This has created an unfair status quo whereby those who can afford to purchase ASIC devices have a clear upper hand and those who cannot are effectively excluded from participating in the network. Since every bitcoin protocol enhancement needs to be approved with a 95% majority of miners, the top X% of miners who own 95% of the mining power can either accept or veto any suggestion that is brought before the community. This effectively overrules the democratic nature that a decentralized network should be characterized by and creates a disproportionate centralization of decision-making power. In order to prevent such an occurrence, FotoCoin utilizes an advanced and fair hashing algorithm known as POS. POS is well known for being a lightweight algorithm which processes new blocks by the process of minting and anyone having FotoCoin can participate in the minting network (more on POS will be discussed later). With it, we seek to eliminate any barrier to entry for the average FotoCoin end user in terms of network governance and promote absolute decentralization and democracy.

Network Capacity

Transaction data is permanently recorded in files called blocks. They can be thought of as the individual pages of a city recorder's recordbook (where changes to title to real estate are recorded) or a stock transaction ledger. Blocks are organized into a linear sequence over time (also known as the block chain). New transactions are constantly being processed by miners into new blocks which are added to the end of the chain.

Originally, Bitcoin's block size was limited by the number of database locks required to process it (at most 10000). This limit was effectively around 500-750k in serialized bytes, and was forgotten until 2013 March. In 2010, an explicit block size limit of 1 MB was introduced into Bitcoin by Satoshi Nakamoto. In 2013 March, the original lock limit was discovered by accident (Bitcoin Core v0.8.0 failed to enforce it, leading to upgraded nodes splitting off the network). From this point forward, the 1 MB limit became the effective limiting factor of the block size for the first time. The limit was not changed again before 2017 and was believed to require a very invasive hard fork to change.

Another issue is the mining difficulty which is increasing exponentially and producing blocks very slowly. Difficulty is a measure of how difficult it is to find a hash below a given target. The Bitcoin network has a global block difficulty. Valid blocks must have a hash below this target. Mining pools also have a pool-specific share difficulty setting a lower limit for shares. The difficulty is adjusted every 2016 blocks based on the time it took to find the previous 2016 blocks. At the desired rate of one block each 10 minutes, 2016 blocks would take exactly two weeks to find.

The block size limit combined with the block time of 10 minutes and exponentially increasing mining difficulty is leading to slow transactions.

It once happened that tens of thousands of unprocessed transactions queued up, and bitcoin-accepting vendors started opting out of the network.

“It’s like trying to fit more cars on the highway where the highway needs to be widened at some point”

FotoCoin solves these issues by introducing many new features not available in Bitcoin. First, the average block time is set to 90 seconds which will produce super fast blocks. Second, the difficulty retargeting algorithm is Dark Gravity Wave (DGW) which retargets difficulty better than the default Bitcoin difficulty retargeting algorithm.

Anonymity

Bitcoin is not anonymous, but, rather, pseudo-anonymous. While the Bitcoin technology can support strong anonymity, the current implementation is usually not very anonymous. The main problem is that every transaction is publicly logged. Anyone can see the flow of Bitcoins from address to address. Alone, this information can't identify anyone because the addresses are just random numbers. However, if *any* of the addresses in a transaction's past or future can be tied to an actual identity, it might be possible to work from that point and guess who may own all of the other addresses. This identity information might come from network analysis, surveillance, or just Googling the address. The officially encouraged practice of using a new address for every transaction is designed to make this attack more difficult.

The FotoCoin network has a focus on the anonymity of payments through the implementation of Dash’s Protocol. This provides a level of privacy by mixing various amounts of FotoCoin within the masternode network. More about this feature will be discussed in “DarkSend”.

FotoCoin

Introduction

FotoCoin is a next-generation, hybrid cryptocurrency based on proof-of-stake (POS) mining and masternodes. This project is a fork of the open-source project of PIVX (which is ultimately a fork of the open-source project, Bitcoin) and leverages the innovations of previous generations of cryptocurrencies.

FotoCoin is distributed within a two-tier, hybrid network for securing the blockchain by (a) confirming transactions, (b) ensuring the privacy of transactions, and (c) facilitating instant transactions. As in other masternode networks, owners of FotoCoin are compensated by the network through a dynamic allocation of rewards based upon FotoCoin owner contributions to the network as confirmation nodes and masternodes. This incentive structure encourages FotoCoin owners to utilize the digital currency for securing the FotoCoin payment network; this is conceivably more profitable than selling the cryptocurrency on the open market. In addition to being a cryptocurrency, the primary mission of the FotoCoin project is to create an easy-to-use contactless payment system for ItsFoto website and more of its likes to come in future.

Features

Proof-of-Stake

At the heart of the proof-of-stake algorithm is the storage of all the operations in the FotoCoin wallet with the distributed database. Synchronization of the wallet nodes of FotoCoin running on proof-of-stake is carried out through the peer-to-peer network, P2P. Thanks to proof-of-stake, it is possible to implement cryptocurrency with high security conditions to avoid hacker attacks and fraudulent actions. Moreover, it is more efficient and environmentally friendlier than proof-of-work, which utilizes lots of energy with application specific integrated circuit (ASIC) machines. The system using the proof-of-stake method is based on the principles of decentralized management in the absence of a single controlling authority, which does not allow a malicious actor to know exactly which version of the block is valid. In simple terms, the definition of the principle of the proof-of-stake algorithm can be given as follows: The more FotoCoin possessed in a wallet, the more credibility that wallet node will be given in the permission- less network. Thus, the wallet will likely receive a block reward because of the relative weight that wallet contributes to the protection of the network. The amount of time a wallet participates in protecting the network is also a factor. From a security standpoint, proof-of-stake is not only mining, but the wallet also stakes the FotoCoin amount to ensure against the validity of the transactions placed in blocks. By having a wallet with a large amount of FotoCoin and staking that amount, this decreases the probability that the owner of the wallet is acting in a malicious manner to harm the network. Thus, wallets with high FotoCoin amounts are given a greater preference in confirming transactions than wallets with smaller FotoCoin amounts. A FotoCoin wallet node serves in the first layer of the hybrid cryptocurrency network by confirming transactions on the blockchain, selecting a network masternode for instant transactions, and creating the next block for storing future transactions. A discussion of the second layer of FotoCoin network is described next.

Masternodes

Masternodes play an important part of the FotoCoin network. A masternode network is the second layer of the FotoCoin network that donates processing power to confirm transactions instantly utilizing the InstantX technology inherited from PIVX. A masternode then receives a reward for the work performed – one reward per block every 90 seconds. These rewards are directly paid to the FotoCoin wallet that is linked to the masternode. Using masternodes also ensures the stability and security of the entire network. These nodes serve a special purpose within the network to mix various transaction amounts to increase fungibility and anonymity of transactions. This is done by the process of obfuscation, which is also inherited from the open source PIVX codebase.

DarkSend

The FotoCoin network has a focus on the anonymity of payments through the implementation of Dash's Protocol. This provides a level of privacy by mixing various amounts of FotoCoin within the masternode network. This protocol consumes sent funds through a special algorithm and goes through several iterations, thus providing a high level of anonymity. The implementation of the preliminary algorithm makes the transactions completely unknown to everyone except the sender and the receiver of funds. This makes attacks on the network increasingly difficult. Here is a brief description of how the technology works: A user determines through the wallet the depth of anonymization and the amount of funds s/he wishes to send. The wallet then "shreds" the transaction into predetermined smaller amounts. These smaller amounts are then sent across the masternode network and intermixed with other users' coin transactions also being anonymized, using the master registry for coordination. These coins are not processed but will be mixed in again with another round of transactions, depending on how many mixes the FotoCoin user has selected. The maximum amount of mixes the wallet can generate is eight; however, FotoCoin can be mixed again by following the same procedure. These mixed coins will show up on a separate balance sheet for the anonymous payment to be made.

InstantX

FotoCoin uses InstantX technology, which allows users to conduct a transaction without waiting for traditional confirmations on the blockchain. The technology uses a network of second-level master logs, which detects transactions marked as "InstantX". These master logs then lock the transaction input and sends a confirmed transaction message to the network. As a result, the transaction takes about 2-5 seconds, while ensuring that no double spending can occur. After sending a confirmation message, the transaction is recorded in the network, as usual. This means that FotoCoin can compete with the ease, convenience, and speed of traditional debit or credit card payments today.

Block Reward Distribution

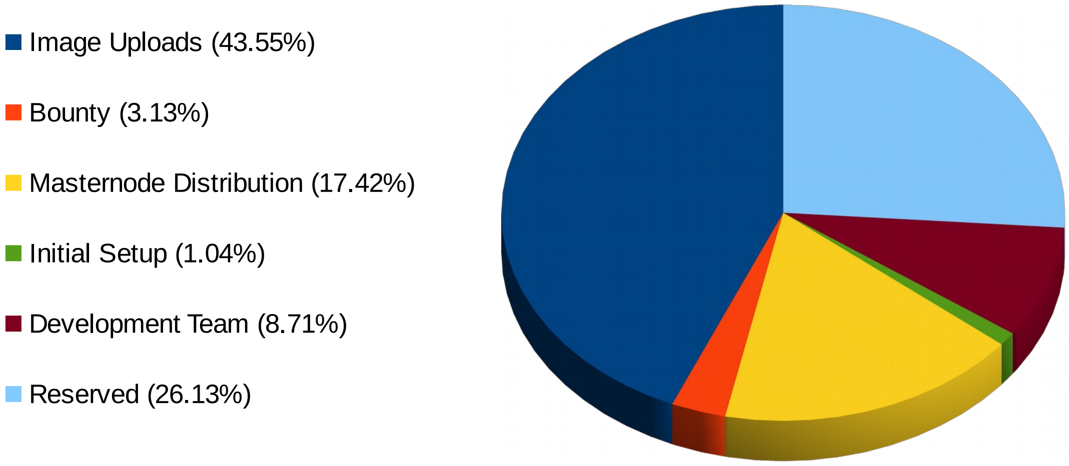
Phase	Block Range	Reward Per Block	Masternode Reward %	Staking Reward %
1	12001-22000	1.5	70	30
2	22001-32000	1.75	75	25
3	32001-42000	2	76	24
4	42001-52000	2.15	77	23
5	52001-62000	2.25	78	22
6	62001-72000	2.5	79	21
7	72001-82000	2.75	80	20
8	82001-92000	3	81	19
9	92001-112000	3.15	82	18
10	112001-142000	3.25	83	17
11	142001-172000	3.5	84	16
12	172001-210000	3.75	85	15
13	210001-250000	4	86	14
14	250001-300000	3.75	87	13
15	300001-380000	3.6	88	12
16	380001-500000	3.45	89	11
17	500001-700000	3.3	90	10
18	700001-900000	3.15	90	10
19	900001-1200000	3	95	5
20	1200001-1500000	2.75	95	5
21	1500001 & above	2.5	95	5

Premine

A very small percentage of FotoCoin has been mined by the developer and reserved to process certain initial necessary tasks. Prime purpose of the premine is to support ItsFoto Platform both in present and in future. This premine will prove helpful in initial boost, distribution and establishment of the project. It will also help in future advancement and expansion of the project.

Premine Distribution

Premined FotoCoin will be used for many progressive tasks necessary for development and boost of ItsFoto. Premined FotoCoin will be distributed among the development team, image uploaders and as bounty to many other users promoting the platform. The perfect overview of the distribution is shown in the chart below.



Roadmap

The following roadmap is an initial plan set up for 2019, which may be revised later as we progress the project forward.

Color conventions used:

🟩 - Completed

🟦 - Ongoing

🟪 - Planned

🟨 - Pending (not yet confirmed)

Q1 2019
🟩 Plan and release fotocoin
🟦 List fotocoin on exchanges
🟩 Alpha version release of itsFoto
🟩 anonymous upload and download of images
🟩 Free CC0 License for all resources
🟩 sorting images by categories
🟦 get paid for uploading images
🟩 get donations for uploaded images

Q2 2019
🟪 Update fotocoin if necessary
🟪 List fotocoin on more exchanges as per user demand
🟦 Beta version release of itsFoto
🟦 UI/UX improvement
🟪 star rating or adding to favourites
🟪 sharing images to social media
🟪 improved search functionality
🟪 bundle downloads

Q3 2019
🟪 Stable version release of itsFoto
🟨 commenting feature on images
🟨 API releases
🟨 multiple download options

Q4 2019
🟨 photo collections
🟨 account registration
🟨 photo management by users
🟨 multiple uploads for registered users

Conclusion

The FotoCoin Team prepared this document to provide a brief overview about cryptocurrencies in general and FotoCoin in particular. We discussed our primary goal of creating an anonymous and private photo sharing platform to empower creators and photo enthusiasts and a private, safe, secure and easy to use currency to power images. From a technology perspective, evidence supports the view that proof-of-stake/masternode technology is not only secure, but also environment friendly and more efficient than proof-of-work consensus models. FotoCoin is based on next-generation technology such as InstantX, DarkSend, proof-of-stake and second-layer masternodes inherited from proven, open-source technologies. The contribution of FotoCoin to the cryptocurrency revolution is to facilitate mass adoption of cryptocurrency to power photos and empower creators, photographers and photo enthusiasts. We will do this through a combination of first-of-a-kind platform and unique business models. A long-term goal of this project to position FotoCoin as a medium of power for ItsFoto, store of value, and a unit of account, ultimately satisfying the defining characteristics of cryptocurrency in this digital age. This process is a natural evolution in Internet technology in which cryptocurrencies will conquer every field of the Internet making our life easier and better, giving back to us our privacy, security and freedom.

References

https://itsfoto.com

https://bitcoin.org/bitcoin.pdf

https://github.com/dashpay/dash/wiki/Whitepaper

https://pivx.org/wp-content/uploads/2017/03/PIVX-purple-paper-Technincal-Notes.pdf

https://en.bitcoin.it/wiki/Block

https://en.bitcoin.it/wiki/Block_size_limit_controversy

https://en.bitcoin.it/wiki/Difficulty

https://www.coindesk.com/bitcoins-2018s-bottleneck

https://www.ccn.com/transaction-bottleneck-kill-bitcoin-nyu-academic-warns/

https://bitcoinmagazine.com/articles/is-bitcoin-anonymous-a-complete-beginner-s-guide-1447875283/

fotocoin
itsfoto