White Paper
Fellas Cryptocurrency (FELLAS)

(English)

Whitepaper Version 1.0
12 August 2018

Disclaimer

PLEASE READ THIS DISCLAIMER SECTION CAREFULLY. IF YOU ARE IN ANY DOUBT REGARDING THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL, FINANCIAL, TAX, OR OTHER PROFESSIONAL ADVISOR(S).

The information within this document is an inclusive list and does not imply any part of a contractual relationship. While we make every effort to ensure that any material in this white paper is accurate and up-to-date, such material in no way constitutes the provision of professional advice. The Fellas team does not accept legal liability whatsoever arising from or connected to the accuracy, reliability, currency, or completeness of any material in this whitepaper.

Investors and potential Fellas (FELLAS) token holders should seek independent professional advice prior to relying on or entering any commitment or transaction based on this whitepaper; material within is purely published for reference purposes alone. FELLAS tokens are not intended to constitute securities in any jurisdiction. This whitepaper does not constitute a prospectus, and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction.

The Fellas team does not provide any opinion or advice to purchase, sell, or otherwise transact with FELLAS tokens. Presentation of this whitepaper shall not form the basis of, or be relied upon in connection with, any contract or investment decision.

No person is bound to enter into any contract or binding legal commitment in relation to the sale or purchase of FELLAS tokens, and no cryptocurrency or another form of payment is to be accepted on the basis of this white paper.

What is Blockchain?

The simple explanation is a 'chain' of blocks. A block is an aggregated set of data. Data are collected and processed to fit in a block through a process called mining. Each block could be identified using a cryptographic hash (also known as a digital fingerprint). The block formed will contain a hash of the previous block, so that blocks can form a chain from the first block ever (known as the Genesis Block) to the formed block. In this way, all the data could be connected via a linked list structure.
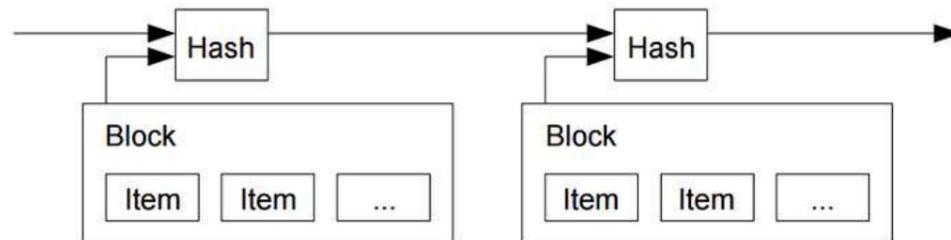
What is inside a block?

In simple words, data are contained inside blocks as well as an arbitrary integer (called nounce) that is necessary for producing the proof-of-work. In bitcoin blockchain, the block contains a header and relevant transaction data. A merkle tree of transactions is created and the hash of the root is included in the header.

A merkle tree is a full binary tree of a hash values. At the bottom level of the tree, each transaction has a node containing its hash value. After that, the tree is constructed in a way such that the parent node has a value of the hash of the data contained in its children concatenating together.

The merkle tree data structure allows fast validation by constructing a merkle tree path from the bottom level of the tree up to the root node. Since each bitcoin transaction output can be spent once only, as long as the output is spent, it could be erased out of the tree structure using some pruning algorithms. In this way, disk usage could be reduced while the validation functions preserve.
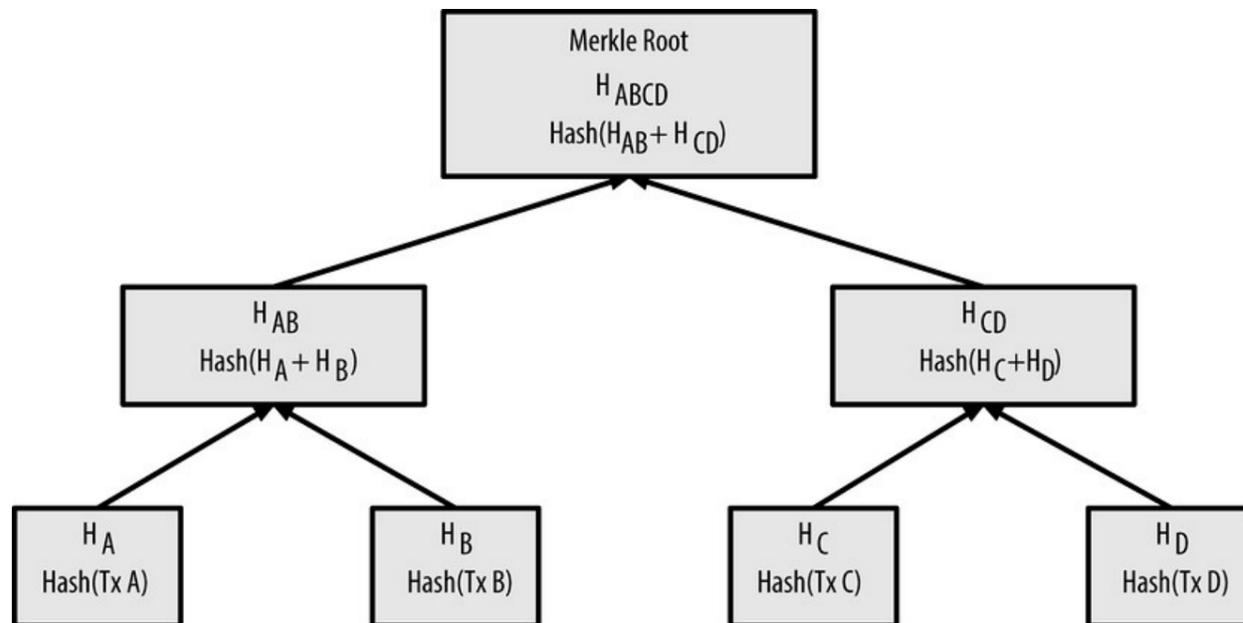
How are blocks chained together?

Each block contains a hash of its previous block. In bitcoin blockchain, the block header has a field for previous block hash. Hence, all blocks will contain a reference of its previous block, and this could build up a chain of blocks.

Sometimes, a fork on the block chain may occur. This is due to two blocks computed at a very short time interval. The subsequent blocks may build upon both blocks and both of the chain remain valid. In subsequent process of mining, one fork would be longer than the other fork, in

this case, the longer chain would be accepted by the network and the short would not be used unless its length exceeds the the longer chain in the future.

Features of blockchain

Controlled block generation time

The blockchain is designed in a way such that the average time for a block to be generated remains fairly constant. In the bitcoin blockchain, the average time for a block to generate is 10 minutes. Other blockchains may have a different time, e.g. 30 seconds, 5 minutes, etc.

The controlled block generation time is achieved by adding a difficulty value inside the block. In bitcoin, the hash of the block must be strictly smaller than a given value to be accepted. The given value varies according to the total computation power of the network. The more powerful the network is, the more smaller the given value, and hence the more difficult it is to generate the block.
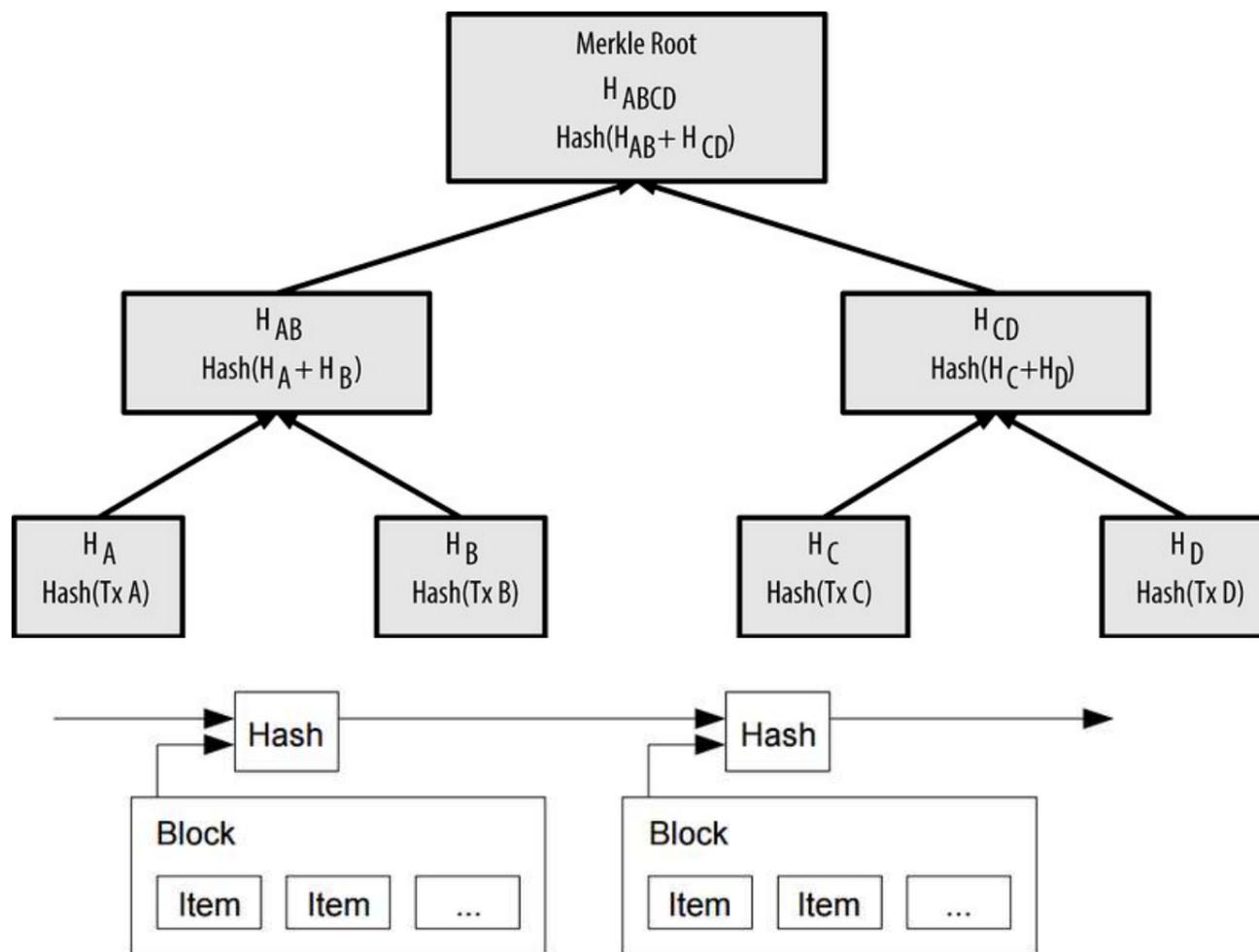
Information storage

Bitcoin Transactions support a function such that messages could be sent with bitcoins in a transaction (via OP_RETURN operator in the unlocking script). This feature extends bitcoin blockchain to more uses than handling transactions. A sender to choose to include a text in a transaction, as the transaction is included in a block attached to the blockchain. The message can be retrieved from the block by everyone and it could hardly be modified unless the whole block is re-written (see below). This can provide reliable storage for short texts.

For example, a hash of a file could be included in a transaction. The users of the file could check the message field attached and verify whether the file in his hand has not been comprimised and has remained original.

Access control

Bitcoin blockchain is a shared public chain. It means that everyone would have access to the chain, not only read the information on the chain, but also append new blocks on the chain, i.e. everyone have full access over the chain. This is known as unpermissioned chain. The chain could also be modified so that stricter access control applies. The strictest access control is that only the owner of the chain could have full access of the chain whereas others have no access at all. This may be similar to the way a central database stores confidential data.

However, in many scenarios somewhere between a shared public chain and a private chain should be the cases resembling real world uses. Through public key cryptography, access control could be implemented during setting up of the chain so that different access control could apply. An example would be the health information of individual. This should be accessed only by the patient or anyone who have been granted access by the patient; only trusted body could append new data to the chain. This is known as permissioned chain.

Merkle Root
H_{ABCD}
$Hash(H_{AB} + H_{CD})$

H_{AB}
$Hash(H_A + H_B)$

H_{CD}
$Hash(H_C + H_D)$

H_A
$Hash(Tx\ A)$

H_B
$Hash(Tx\ B)$

H_C
$Hash(Tx\ C)$

H_D
$Hash(Tx\ D)$

Hash

Hash

Block

Item | Item | ...

Block

Item | Item | ...

Consensus method

Bitcoin blockchain uses a proof-of-work algorithm for reaching a consensus. The cryptographic hash function of each block must be smaller than a specific value in order to be considered value. A nonce is thus included in the block for this feature. By using the proof-of-work method, in order to change the data in one block, all successors of that block must be re-written and a huge amount of calculation is necessary. In addition, the longest chain would be accepted by the network whereas the shorter ones would be discarded at the situation of branches of the chain. This made the data in blocks practically unmodifiable, and moreover, the more blocks built upon the block in which the data is contained, the harder the processing of overwriting the data.

However, the blockchain may use other methods of consensus. For example, a blockchain may use Scrypt for proof-of-work algorithm instead of hash functions. In addition, the blockchain could be extended for scientific computation where a correct solution to a certain problem could act a

validation method. In this way, the computation power may be used to help solving scientific problems and contribute to scientific researches.

Distributed computation

Bitcoin blockchain is a shared public ledger. Each user running a full node on the computer will download a full copy of the whole blockchain, which will include data of all transactions of the bitcoins recorded on the blockchain. After that, each node can run independently to process any incoming transactions and propagate the transaction further. The node can also contribute to the establishment of the consensus by mining - to include transaction data in a block and then to find a proof-of-work for the block. There is not a central node processing the data and distribute the data, but every node can run independently and broadcast any work that is proved. This model of distributed computation could be extended to many other services such as Domain Name Server.

Figure 1: Different ledger technologies vary in their 'degrees of centralisation'

| Permissionless, Public, Shared Systems (eg Bitcoin) | Permissioned, Public, Shared Systems | Permissioned, Private, Shared Systems | Today's Typical Systems |

100% Decentralised ← Distributed Ledger Technology Covers a Broad Set of Usages / Centralised Ledgers → 100% Centralised

What is Ethereum?

In order to fully understand Ethereum, what it does and how it can potentially impact our society, it is important to learn what its core properties are and how they differ from standard approaches.

First of all, Ethereum is a decentralized system, which means it is not controlled by any single governing entity. An absolute majority of online services, businesses and enterprises are built on a centralized system of governance. This approach has been used for hundreds of years, and while history proved time and time again that it's flawed, its implementation is still necessary when the parties don't trust each other.

A centralized approach means single-entity control, but it also means a single point of failure, which makes apps and online-servers utilizing this system extremely vulnerable to hacker attacks and even power outages. Moreover, most social networks and other online servers require users to provide at least some degree of personal information, which is then stored on their servers. From there, it can be easily stolen by the company itself, its rogue workers or hackers.

Ethereum, being a decentralized system, is fully autonomous and is not controlled by anyone at all. It has no central point of failure, as it is being run from thousands of volunteers' computers around the globe, which means it can never go offline. Moreover, users' personal information stays on their own computers, while content, such as apps, videos, etc., stays in full control of its creators without having to obey by the rules imposed by hosting services such as App Store and YouTube.

Secondly, it is important to understand that even though constantly compared to each other, Ethereum and Bitcoin are two completely different projects with entirely different goals. Bitcoin is the first ever cryptocurrency and a money-transfer system, built on and supported by a distributed public ledger technology called the Blockchain.

Ethereum took the technology behind Bitcoin and substantially expanded its capabilities. It is a whole network, with its own Internet browser, coding language and payment system. Most importantly, it enables users to create decentralized applications on Ethereum's Blockchain.

Those applications can either be entirely new ideas or decentralized reworks of already existing concepts. This essentially cuts out the middleman and all the expenses associated with the involvement of a third party. For example, the only profit that comes from users 'liking' and 'sharing' their favorite musician's posts on Facebook is generated from an advertisement placed on their page and it goes directly to Facebook. In an Ethereum version of such social network, both the artists and the audience would receive awards for positive communication and support. Similarly, In a decentralized version of Kickstarter, you won't be getting just some artifact for your contribution to the company, you will be receiving a part of the company's future profits. Finally, Ethereum-based applications will remove all sorts of payments to third parties for fascinating any kind of services.

As it was mentioned before, Ethereum is a decentralized system, which means it utilizes a peer-to-peer approach. Every single interaction happens between and is supported only by the users taking part in it, with no controlling authority being involved.

The entire Ethereum system is supported by a global system of so-called 'nodes.' Nodes are volunteers who download the entire Ethereum's Blockchain to their desktops and fully enforce all the consensus rules of the system, keeping the network honest and receiving rewards in return.

Those consensus rules, as well as numerous other aspects of the network, are dictated by 'smart contracts.' Those are designed to automatically perform transactions and other specific actions within the network with parties that you don't necessarily trust. The terms for both parties to fulfill are pre-programmed into the contract. The completion of these terms then triggers a transaction or any other specific action. Many people believe that smart contracts are the future and will eventually replace all other contractual agreements, as the implementation of smart contracts provides security that is superior to traditional contract law, reduce transaction costs associated with contracting and establish trust between two parties.

Moreover, the system also provides its users with the Ethereum Virtual Machine (EVM), which essentially serves as a runtime environment for smart contracts based on Ethereum. It provides users with security to execute an untrusted code while ensuring that the programs don't interfere with each other. EVM is completely isolated from the main Ethereum network, which makes it a perfect sandbox-tool for testing and improving smart contracts.

The platform also provides a cryptocurrency token called 'Ether.'

Who did create Ethereum?

In late 2013, Vitalik Buterin described his idea in a white paper, which he sent out to a few of his friends, who in turn sent it out further. As a result, about 30 people reached out to Vitalik to discuss the concept. He was waiting for critical reviews and people pointing out critical mistakes in the concept, but it never happened.

The project was publicly announced in January 2014, with the core team consisting of Vitalik Buterin, Mihai Alisie, Anthony Di Iorio, Charles Hoskinson, Joe Lubin and Gavin Wood. Buterin also presented Ethereum on stage at a Bitcoin conference in Miami, and just a few months later the team decided to hold a crowdsale of Ether, the native token of the network, to fund the development.

How does Ethereum works?

As it was mentioned before, Ethereum is based on Bitcoin's protocol and its Blockchain design but is tweaked so that applications beyond money systems can be supported. The two Blockchains' only similarity is that they store entire transaction histories of their respective networks, but Ethereum's Blockchain does a lot more than that. Besides the history of transactions, every node on Ethereum network also needs to download the most recent state, or the current information, of each smart contract within the network, every user's balance and all the smart contract code and where it's stored.

Essentially, the Ethereum Blockchain can be described as a transaction-based state machine. When it comes to computer science, a state machine is defined as something capable of reading a series of inputs and transitioning to a new state based on those inputs. When transactions are executed, the machine transitions into another state.

Every state of Ethereum consists of millions of transactions. Those transactions are grouped to form 'blocks,' with each and every block being chained together with its previous blocks. But before the transaction can be added to the ledger, it needs to be validated, that goes through a process called mining.

Mining is a process when a group of nodes apply their computing power to completing a 'proof of work' challenge, which is essentially a mathematical puzzle. The more powerful their computer is, the quicker it can solve the puzzle. An answer to this puzzle is in itself a proof of work, and it guarantees the validity of a block.

A lot of miners around the world are competing with each other in an attempt to create and validate a block, as every time a miner proves a block new Ether tokens are generated and

awarded to said miner. Miners are a backbone of the Ethereum network, as they not only confirm and validate transactions and any other operations within the network but also generate new tokens of the network's currency.

What can Ethereum be used for?

First and foremost, Ethereum allows developers to build and deploy decentralized applications. Moreover, any centralized services can be decentralized using the Ethereum platform. The potential of Ethereum platform for building apps not limited by anything other than the creators' creativity.

Decentralized applications have a potential of changing the relationship between companies and their audiences completely. These days there are a lot of services that charge commission fees for simply providing an escrow service and a platform for users to trade goods and services. On the other hand, Ethereum's Blockchain's can enable customers to trace the origins of product they're buying, while the implementation of smart contracts can ensure safe and fast trading for both parties without any intermediary.

The Blockchain technology itself has a potential of revolutionizing web-based services as well as industries with long-established contractual practices. For example, an insurance industry in the US possesses more than $7 bln inclined life insurance money, which can be redistributed fairly and transparently using Blockchain. Moreover, with the implementation of smart contracts, clients can be able to simply submit their insurance claim online and receive an instant automatic payout, considering that their claim met all the required criteria.

Essentially, the Ethereum Blockchain is capable of bringing its core principles - trust, transparency, security and efficiency - into any service, business or an industry.

Ethereum can also be used to create Decentralized Autonomous Organizations (DAO), which operate completely transparently and independently of any intervention, with no single leader. DAOs are run by programming code and a collection of smart contracts written on the Blockchain. It is designed to eliminate the need for a person or a group of people in complete and centralized control of an organization.

DAOs are owned by people who purchased tokens. However, the amount of purchased tokens doesn't equate equity shares and ownership. Instead, tokens are contributions that provide people with voting rights.

Advantages of Ethereum

Ethereum platform benefits from all the properties of the Blockchain technology that it runs on. It is completely immune to any third party interventions, which means that all the decentralized apps and DAOs deployed within the network can't be controlled by anyone at all.

Any Blockchain network is formed around a principle of consensus, meaning that all the nodes within the system need to agree on every change made within it. This eliminates possibilities of fraud, corruption and makes the network tamper-proof.

The whole platform is decentralized, which means there is no possible single point of failure. Hence, all the apps will always stay online and never switch off. Moreover, the decentralized nature and cryptographic security make the Ethereum network well protected against possible hacking attacks and fraudulent activities.

Abstract

We are living in the digital era. Social networking has become second nature to us and is a seemingly unavoidable part of our everyday life. In a similar manner, adoption of blockchain technology and cryptocurrencies is growing exponentially and will soon be paramount in our daily financial exchanges. We believe that a well-crafted and readily accessible cryptocurrency should allow for the same range of user adoption as social networking, and therefore, it is only natural for the next phase of blockchain implementation and cryptocurrency adoption to take place on social networks.

The time and effort users invest in social media platforms can become a real asset for crypto-powered exchange scenarios. The Fellas (FELLAS) team believes the innate usability of social networking can be matched with an equally usable peer-to-peer currency exchange platform, overriding the necessity of lengthy technical explanations to non-crypto users. Our technology seeks to aid people in the use of cryptocurrency and value transfers through their already polished knowledge of multiple social networks, blending blockchain technology architecture and functionality with established communication networks.

The market for FELLAS is enormous. Approximately one third of the world's population, or 2.6 billion people, use social media. In contrast, there are only about 3 million users of cryptocurrency in the world. Social networks are the next frontier for cryptocurrency because they provide a launching pad for cryptocurrency adoption through instant access to one third of the world's population.

Yet, we recognize that simply introducing a cryptocurrency to social media users is not enough to capitalize on this market. Recently, The Fellas team conducted a survey of 4,000 people from around the world and found that only 15% were crypto literate. Hence, although we expect to fill a key role in the adoption of cryptocurrency using our technology as the medium to tap into the limitless potential of social and crypto interaction, we envision serving also as a bridge between early and late adopters of cryptocurrency by pioneering simplicity in the crypto-sphere with a social media based cryptocurrency platform, the mission of which is to facilitate the most straight-forward, user friendly, and intuitive peer-to-peer cryptocurrency transfers.

Background

In 2018, a team was formed to study how cryptocurrency technology and the blockchain network could be integrated with social networks. The main focus was to provide a feasibility study for a global social platform for the sending of cryptocurrency via social networks.

During a trip to South Asia (Nepal, India, Bangladesh, Srilanka), we gained insight that most people are well connected and aware of social networks, but have little to no understanding of cryptocurrencies. Most people are crypto illiterate. Sending Bitcoin, or any other altcoin, is complicated for most people as they do not have knowledge of blockchain technology, wallets, and cryptocurrency as a whole.

We decided to make the use of cryptocurrencies as easy as using social networks, so that every person in the world who can use a cellphone or computer will be able to use cryptocurrencies. Our study proved the feasibility of the concept "Fellas token".

Visition

Social media is the place where people spend most of their time these days. The influence of social media on people can not be denied. Our goal as our team is to introduce as many social media users as possible to the crypto world, to increase the validity of the crypto money and spread the word "GET SOME FELLAS" all over the social media.

What Is Fellas Token (FELLAS)?

Fellas token (FELLAS) is a blockchain project advancing and integrating cryptocurrency into/with social networks. FELLAS is integrated in a Global Social Network Platform, which is a simple and universal integration system with user experience in mind.

Sending and receiving funds on any social network is achievable with only a novice level of expertise. It is as easy as posting a message on a social media platform. The user may not even realize that he or she is utilizing blockchain technology.

It allows family and friends to send funds to one another over social networks by just using their username or an email address rather than a long wallet address. The most interesting thing is that someone who has never even heard of cryptocurrency can receive a payment with no prior knowledge or setup.

For Example, John from the Australia has a friend named Kate who lives in the US. They are friends on Facebook and John owes Kate some money. He could use PayPal, a global remittance company, a swift transfer, or another centralized method, but these options are slow and cost a lot of money. With FELLAS token, John can easily send his friend funds instantly with the tap of his finger while interacting with him on a social network. Kate will receive the funds within seconds.

Hence, FELLAS is the catalyst that puts cryptocurrency into the hands of the masses via the power of social networks.

Token Specification

FELLAS is an Ethereum token based on the ERC223 standard and is the first cryptocurrency developed in Japan. While ERC20 is currently the most popularized form of Ethereum tokens,

ERC233 is gaining attention as an upwardly compatible standard that revises on ERC20's -aws, such as xing the issue in which tokens can no longer be transferred in the event one sends funds to an incorrect or invalid contact address. Additionally, with the specication change, tokens can also be transferred at half the cost of the ERC20. ERC223 is backwards compatible with ERC20, making it available for use in ERC20-supported service tools and wallets such as MyEtherWallet, MetaMask, and Mist. ERC233 also carries the big plus of being scheduled for used with revolutionary services like Raiden and Plasma in the near future. Using the ERC233 standard as a base, FELLAS comes mounted with many features. For example, using the Airdrop feature included, users can distribute tokens to multiple people simultaneously via Airdrop while keeping transfer fees low. Furthermore, since this feature is available to everyone, FELLAS holders can user Airdrop at any time. On top of that, account freeze and lockup features are also included. The ability to freeze the addresses of malicious users and temporarily lock management-held tokens allows us to both maintain and increase FELLAS's value. Additionally, the number of tokens in circulation can be adjusted through the Burn (decrease) and Mint (increase) features. The Mint feature can also be turned off forever.

Social Transfer

The most important and unique feature of FELLAS coin is social sending. FELLAS is the only token in the market which implements the concept of social sending over numerous social networks. FELLAS token will be integrated with various social networks via its Global Social Network Platform, allowing users to FELLAS tokens to their friends and families within their social network, even without having technical knowledge of cryptocurrency. The following chart shows how it works.

SENDER

- Sign up with the Global Social Network Platform via Facebook, Twitter or Email
- Receive an address to upload funds (Web Wallet)
- Send FELLAS coins to Web Wallet

PLATFORM
- Connect with friends and family on different social networks
- The Global Social Network Platform collates a list of family and friends from the sender's various social networks
- Send funds to friends and family via the Global Social Network Platform

RECEIVER
- Receive instant notification of transfer of funds
- No need of any crypto knowledge or registration in order to receive notification of the reception of funds
- Receiver receives funds as soon as he or she is registered with the Global Social Network Platform

The Road to Becoming the Most Popular One Cryptocurrency

The Road to Becoming the Most Popular Cryptocurrency With the motto of becoming the number-one used cryptocurrency, FELLAS token plans to remain proactive in seeking out collaborations and developing systems in the interest of building an economic bloc within the social media industry. We hope to aim for a world where the Blockchain platform is ready for use in everyday life. We strive to create an ideal environment in which anyone is free to participate and contribute to the FELLAS token project. As passionate users of social media platforms, we first intend to form business relationships with various organizations within the industry to pave the way for FELLAS to be used for social media related goods and services. Finally, creating a chat platform (as seen on the roadmap) is end goal. With that fully of token gifted chat platform will push other social platforms to get integrate with FELLLAS.

Token Allocation

Most of the virtual currencies thus far have vague denitions of the requirements, such as possessing a "majority", to become the "management team". Therefore, for clarity, the minimum required possession percentage of FELLAS to function as the aforementioned management team is set to be 10% of the total. The benet of declaring this percentage is that even if the management team sells out, the market will not collapse because the managing team does not hold the majority. Certainly, there will be a secondary countermeasure of requiring the holder to clearly state that it is not their intent to disturb the market by undercutting or overselling. Following the opening game, we plan to sell 900 million FELLAS for 2 sat as an ICO, which is less than 2% of the total issued volume. Likewise, after the opening, burns and lockups will be implemented for unsold tokens.

Team

As a community run project, the Fellas team is comprised of many creative people. The team is truly decentralized, and in the spirit of Satoshi Nakamoto, most contributors have chosen to remain anonymous. However, several central members of the team can be contacted directly via Discord:

@Kutenbas – Administrator
@FellC0d3 – Administrator
@WhiteLion – Administrator
@TheWhizardOz – Administrator

Website and Social Media Accounts

- **Website:** https://www.fellas.io/
- **Email address:** mymoneyfellas@gmail.com
- **Facebook:** https://www.facebook.com/The-Big-Fellas-447632539049197

- **Twitter:** https://twitter.com/TheBigFellas1
- **Discord:** https://discord.gg/A8YDbY8
- **Telegram (chat):** https://t.me/FellasChat
- **Telegram (announcement):** https://t.me/Fellascoin
- **Instagram:** https://www.instagram.com/fellascoin/

Miscellaneous

This first whitepaper for FELLAS token includes all relevant information currently. Yet, it might require update from time to time in the future, with changes to the roadmap and release of products. However, access to this original version (Version 1.0.0.0) will remain available through the download of this .pdf even though there may be updates in the future.

Thank You

The Fellas team would like to take this chance to thank you for your interest, your trust in the Fellas token project, and for taking the time to read our white paper. We are very thankful to our community and their support.

If you have any question or doubts, feel free to reach out to us via our website https://www.fellas.io or social media accounts noted above. The Fellas team hopes that you will share in its vision and mission to put blockchain technology into the hands of every ordinary person who uses social networks.