Global DeFi Whitepaper

James Li, Philip Fan, Alex Tham

Abstract

From exchange of goods, barter trading, to animal-skin based currency, to the metal coins, and finally paper currency, it is a natural development that tends to move to the more lightweight and convenient, secure way of trading and doing business. Eventually, the paper currency will be replaced by digital tokens completely. Traditional banks are slowly replaced by online banks, then slowly replaced by decentralized finance (DeFi) platforms. DeFi is not just a trend, it is the future and it is happening now.

Global Defi is a DeFi platform that will address the shortcoming of the current DeFi platform, which most of the platforms only allows ERC20 tokens for borrowing/lending. We not only allow ERC20 tokens for borrowing and lending, we also use the technology of TSS for cross chain assets management, and thus support other major blockchains like BTC, BCH, TRON, EOS, etc on our platform. We also address the issue of high hardware requirements for nodes, we use anti ASIC/GPU algo so that a relatively low end computer or a Raspberry PI 4 can be used to run a node, which is very cost effective, reliable and simple to set up. Validators will be elected during each epoch, to do transaction verifications and mining purposes. We do not intend to run an ultra high TPS network which will require a tremendous amount of hardware resources. There is no need for a 100,000 TPS for DeFi. We believe the DeFi platform should be business oriented and focus, and not technology focus only.

1. Introduction and Problem Statement

Current problem for the blockchain has too many incompatible native networks that result in inability to exchange tokens or assets easily without using an exchange. DeFi for example, most of it is focusing on Ethereum blockchain only. BTC, BCH, TRON, EOS and others cannot easily be integrated into the platform for DeFi purposes. There are few blockchain projects that try to address these issues but none of them prove to be successful at least at this moment.

2. DeFi Overview

Defi is a very hot topic recently. What is DeFi actually? DeFi is an acronym for Decentalized Finance. For laymen, it is simply the blockchain version of traditional banks, but without centralized authority to control, and monitor and trust. A DeFi is a trustless, decentralized, in other words, no one or party is in control, and trustless platform. You don't need to trust anyone or any party because all the rules and regulations are clearly visible and verifiable via smart contract. You can see for yourself what is in the smart contract that controls the whole platform execution. And no one or no authority can confiscate or freeze your assets.

DeFi works like a bank. A DeFi platform like us, allows you to borrow/lend assets to other parties without a middleman. There is no need for trust, as all the rules and regulations (payback, interest, collateral, terms and conditions) all spelled out clearly in the smart contract. You can borrow for example $1000 USDT to fund your mining rig, and agree to pay for some interest say 5% for 6 months. Another party will then lend you the $1000 USDT and collect some collateral from you. Failure to pay back within the said period will render your collateral to the lender.

The future of DeFi is bright as more and more assets and property are being made digitally tokenized. Think in the future, a house is digitally tokenized, and it can be used as a form for collateral purposes, similar to what happens now to banks. Of course, issues related to legal, authority for property still need to be solved before it can be realized. Currently there are attempts and efforts to digitize the value of painting/art work using tokens.

3. Design Approach

DeFi is a wonderful idea that addresses the current problem in our traditional banking approach, which is strictly under the control of a central authority usually is the country's central bank. It has absolute power to freeze your assets if it thinks that it deserves to protect its monetary issues, and under the legal framework. DeFi makes the traditional banks absolute the same way that digital photography makes Kodak obsolete. DeFi however, majority of facing a main issue, it is blockchain specific. We need a DeFi that is blockchain agnostic, that accepts and connects to all the major native networks, which includes BTC, ETH, BCH, EOS, TRON, etc.

4. Our Solution

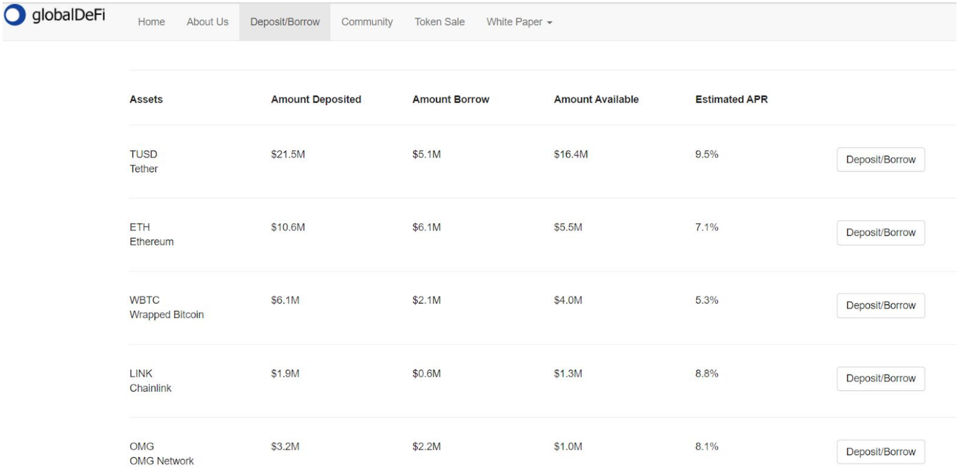
We propose to develop a platform as a front end interface and a native network that forms the backbone which is serving as a bridge that connects to all different blockchains via a method called TSS (Threshold Signature Scheme).

Using TSS and our own network as a bridge, any blockchain can safely and easily move around for asset exchange and trading, lending and depositing. The following sections will describe in more detail how TSS works and how our network forms as a middleman to mediate the transfer of assets from different networks securely.

Phase 1: Only Ethereum and ERC20 tokens DeFi platform

Phase 2: Ethereum, ERC20 and BTC, BCH, EOS, TRON DeFi platform

Please check our roadmap for more details.



Assets	Amount Deposited	Amount Borrow	Amount Available	Estimated APR	
TUSD Tether	$21.5M	$5.1M	$16.4M	9.5%	Deposit/Borrow
ETH Ethereum	$10.6M	$6.1M	$5.5M	7.1%	Deposit/Borrow
WBTC Wrapped Bitcoin	$6.1M	$2.1M	$4.0M	5.3%	Deposit/Borrow
LINK Chainlink	$1.9M	$0.6M	$1.3M	8.8%	Deposit/Borrow
OMG OMG Network	$3.2M	$2.2M	$1.0M	8.1%	Deposit/Borrow

Figure 1: Global Defi Platform for ERC20 tokens only (Phase 1)

5. TSS and GlobalDeFi Nodes

Threshold Signature Scheme (TSS)

Threshold Signature Scheme (TSS), Multisig and Secret Sharing Scheme (SSS) all share very common properties and thus it is discussed here.

Multisig is used in Bitcoin wallets to enable control by not just 1 party but several parties. Multisig wallets such as Armory can have a setup of 2of3, for example, which means any 2 out of the 3 signatures can sign the transaction. Most of the exchanges also use multisig to protect their wallet from single point of failure and to increase security. Multisig requires blockchain support technology and more bytes for additional signatures.

Secret Sharing Scheme (SSS) on the other hand, will break down a normal private key into many pieces, and each piece is stored by one party. In order to sign a transaction, all parties need to sign it in the proper order. SSS does not require blockchain support and does not use any additional bytes for signatures. However, it has a dealer when the key is generated and also when signing a transaction, the whole private key is reassembled and vulnerable to a single point of attack.

Threshold Signature Scheme (TSS) is similar to Multisig and SSS but with certain key differences. With TSS, each party creates a key independently, there is no single dealer unlike SSS. It does not add more bytes to signature, which appears as it is the same as normal single signature. However, TSS requires all parties to be present during the action of unlocking. One can now use TSS to enable cross chain support in a secure way. We can theoretically use a single private key in a node to do cross chain support, but it is vulnerable to attack. By using TSS, cross chain support is enabled with no compromise in security.

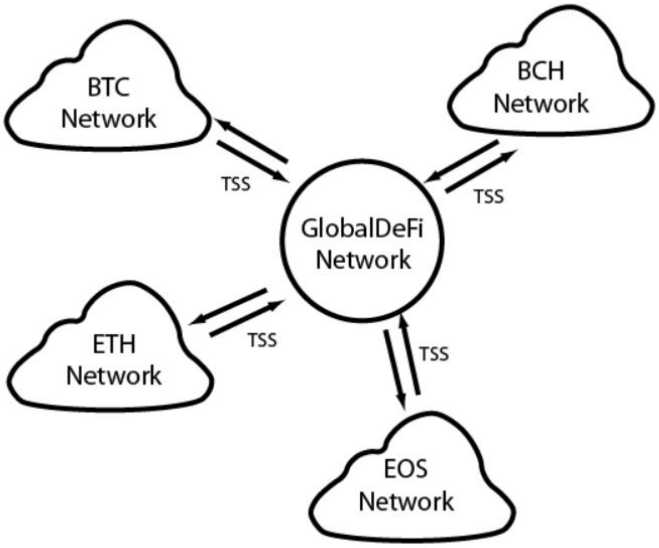


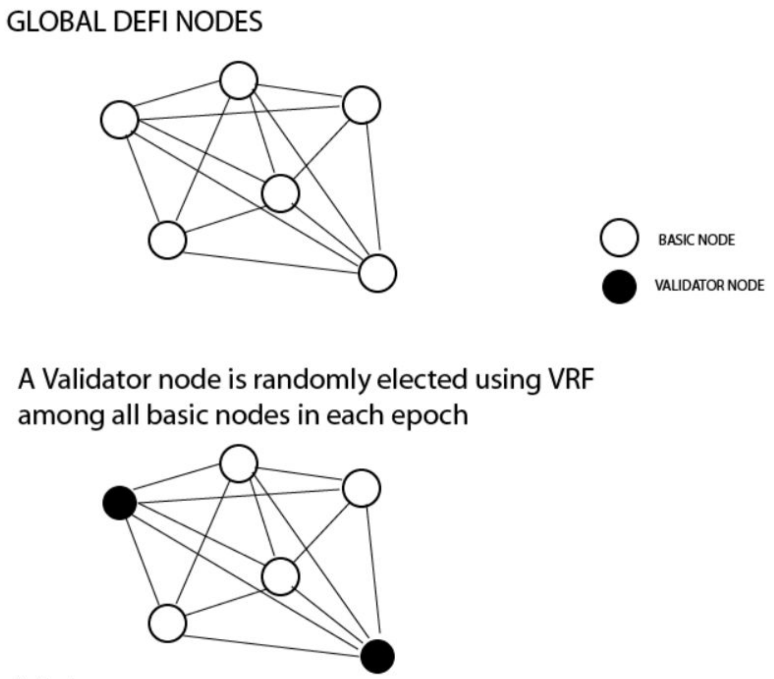
Figure 2: GlobalDeFi Network acts as a bridge to connect many different blockchains

Global Defi nodes

To be clear, we do not plan to reinvent the wheel. Thus, we will use an established and reliable TSS library as our main source (currently we are working to port Binance TSS library) and adapt and port to our network for cross chain assets management and movement. We will also use some of our previous knowledge in other projects especially PCHAIN tech in VRF to randomly elect validators.

Global Defi Network will have 2 types of nodes. Basic nodes and validator nodes. All basic nodes will need to deposit a certain amount of GDF native tokens to participate in the VRF election. Basic nodes will be light weight, and can be run on Raspberry Pi 4 or above, or on any Ubuntu computer. We will add an ASIC/GPU resistant algorithm so that any computer without GPU will be able to use it as a node. By using affordable hardware like Raspberry Pi 4, we can reach a wider audience and more nodes from the public will be activated. We plan to sell Raspberry Pi 4 pre-installed with our node so that anyone can just plug and play (only need to do minor settings) to run as a node. Or alternatively anyone can download from our github to install as a node.

Validator node is elected using VRF (verifiable random function) from the basic nodes during each epoch. For EOS, each epoch is approximately 126 seconds while PCHAIN is about 1 month. Our epoch will be around 1 day. Any transactions need to have at least 2/3 of the validators to be verified. The deposit of GDF is used as a security deposit. Any malicious attempt from the node will be confiscated and the deposited GDF will be burned.


GLOBAL DEFI NODES

A Validator node is randomly elected using VRF among all basic nodes in each epoch

Figure 3: GlobalDefi Basic Nodes and Validator Nodes

Basic Node
To synchronize blocks and broadcast TX only. Basic nodes do not involve mining.

Validator Node
To validate transactions, synchronize blocks, and produce blocks. Validator nodes will perform mining.

6. Token Usage and Economics

Our token GDF, initially will be released as ERC20 until we launch our mainnet with 1:1 ratio for swapping to our native GDF token. GDF token will be used for governance of our network, and also as an incentive to lower commission/fee in our trading platform. Once our native network is launched, GDF will be needed to be used as a gas/tx fee for swapping assets.

All our nodes will require GDF staking to run as a deposit against malicious attack. The more GDF a node has staked, the higher the chance it will be selected as a validator via random voting process (VRF).

We will use 10% of our revenue to buy back and burn GDF each quarter until only 10% of GDF (100,000,000 GDF) remains.

7. Token Release Schedule

We have decided we don’t need seed investors. Initial investments are all coming from the team. We try to avoid having seed investors due to the concern by investors of their much lower price of purchasing the tokens, that may cause an unhealthy valuation of our GDF.

Token symbol: GDF
Total max supply: 1,000,000,000 tokens
TGE: September 2020
Token type: ERC20 (to be converted 1:1 to native token once mainnet launch)

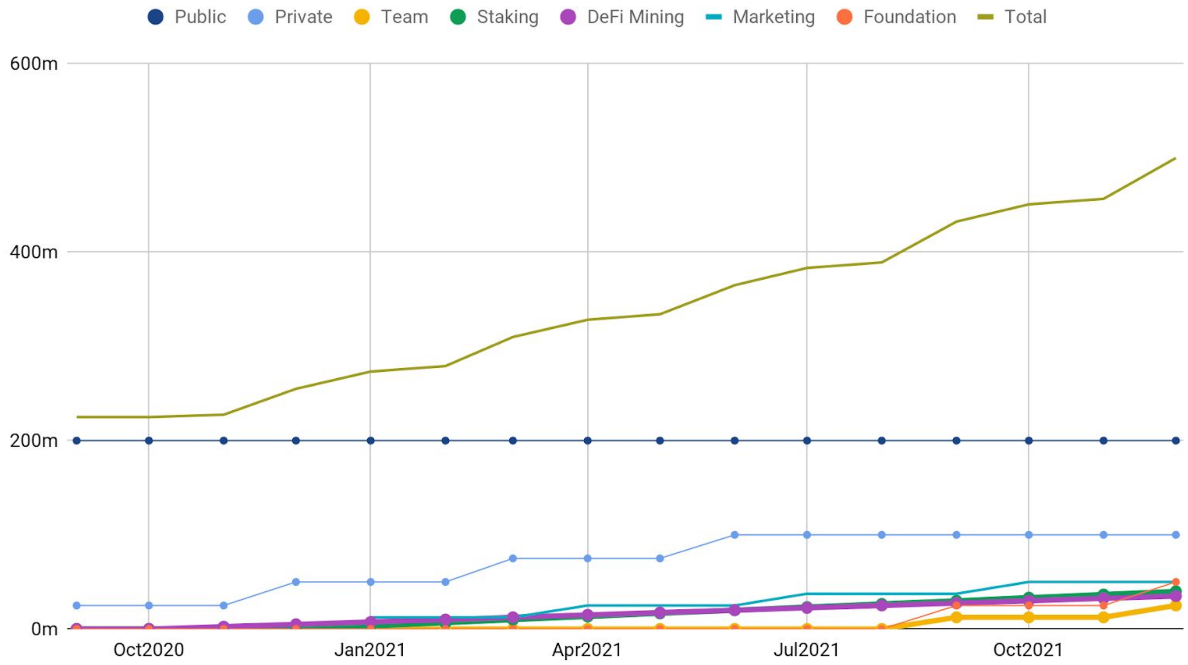


Figure 4

Seed Round: None

Private Round
Token Price: $0.009
Total tokens allocated: 100,000,000
Amount to raise: $900,000
Vesting: 25% unlocked during TGE, thereafter 25% each quarter.

Public Round
Token Price: $0.01
Total tokens allocated: 200,000,000
Amount to raise: $2,000,000
Vesting: None

Total Hardcap (assuming fully subscribed): $2,900,000

Token Allocations

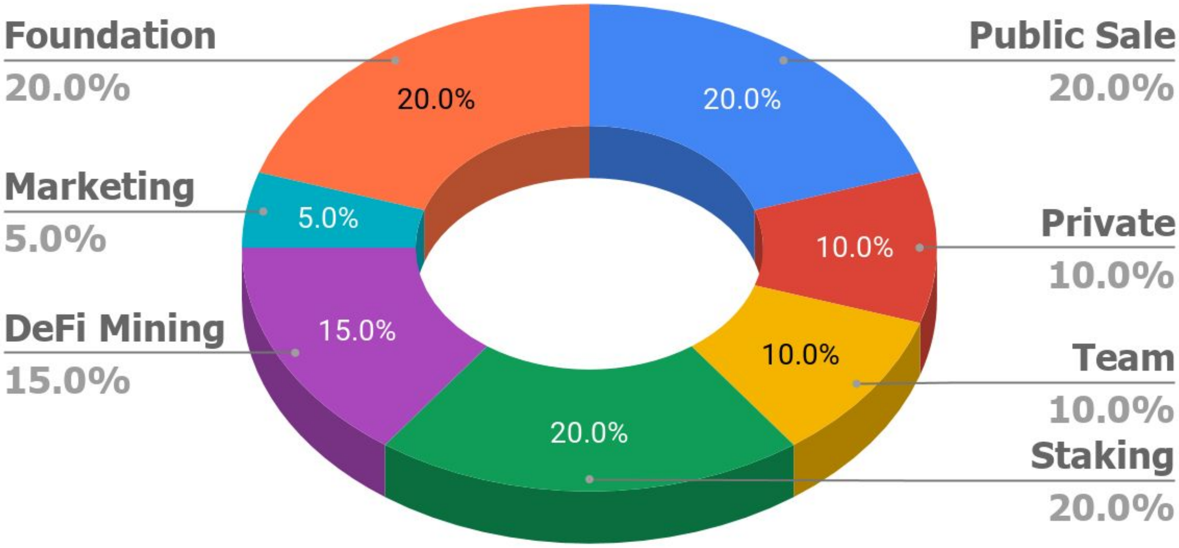


Figure 5

Public Sale	20% (200,000,000 GDF)
Private Sale	10% (100,000,000 GDF)
Team	10% (100,000,000 GDF)
Staking	20% (200,000,000 GDF)
DeFi Mining	15% (150,000,000 GDF)
Marketing	5% (50,000,000 GDF)
Foundation	20% (200,000,000 GDF)

Vesting

Public Sale :None

Private Sale:25% unlocked during TGE, thereafter 25% each quarter

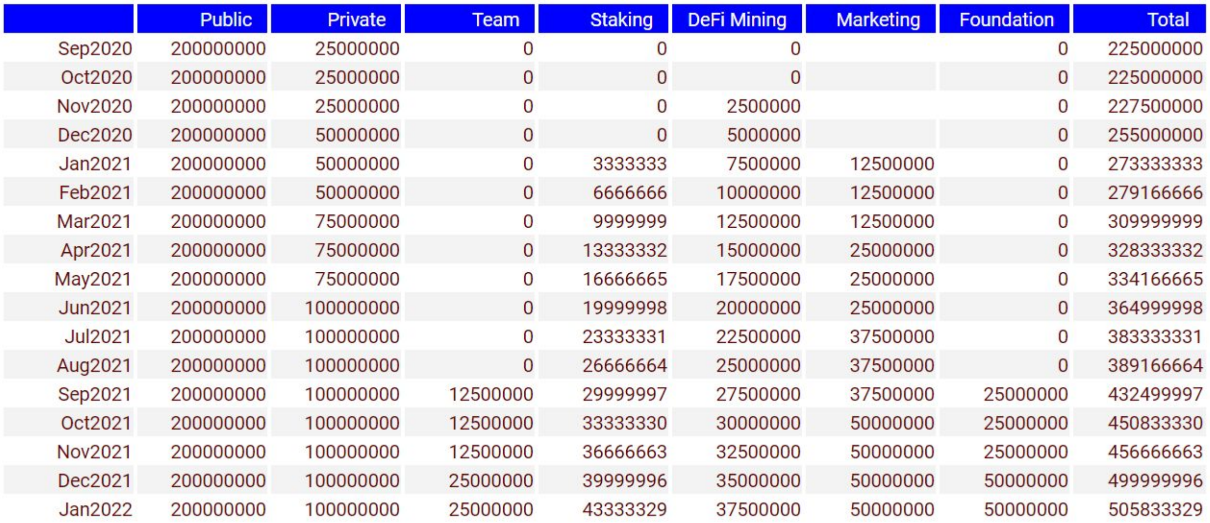
Team :Locked 1 year, 12.5% each quarter thereafter

Foundation :Locked 1 year, 12.5% each quarter thereafter

Staking :After mainnet launch (estimated 4 months after TGE)

DeFi Mining :After platform launch (estimated 2 months after TGE)

Marketing :Locked 4 months



	Public	Private	Team	Staking	DeFi Mining	Marketing	Foundation	Total
Sep2020	200000000	25000000	0	0	0		0	225000000
Oct2020	200000000	25000000	0	0	0		0	225000000
Nov2020	200000000	25000000	0	0	2500000		0	227500000
Dec2020	200000000	50000000	0	0	5000000		0	255000000
Jan2021	200000000	50000000	0	3333333	7500000	12500000	0	273333333
Feb2021	200000000	50000000	0	6666666	10000000	12500000	0	279166666
Mar2021	200000000	75000000	0	9999999	12500000	12500000	0	309999999
Apr2021	200000000	75000000	0	13333332	15000000	25000000	0	328333332
May2021	200000000	75000000	0	16666665	17500000	25000000	0	334166665
Jun2021	200000000	100000000	0	19999998	20000000	25000000	0	364999998
Jul2021	200000000	100000000	0	23333331	22500000	37500000	0	383333331
Aug2021	200000000	100000000	0	26666664	25000000	37500000	0	389166664
Sep2021	200000000	100000000	12500000	29999997	27500000	37500000	25000000	432499997
Oct2021	200000000	100000000	12500000	33333330	30000000	50000000	25000000	450833330
Nov2021	200000000	100000000	12500000	36666663	32500000	50000000	25000000	456666663
Dec2021	200000000	100000000	25000000	39999996	35000000	50000000	50000000	499999996
Jan2022	200000000	100000000	25000000	43333329	37500000	50000000	50000000	505833329

8. Roadmap

Roadmap

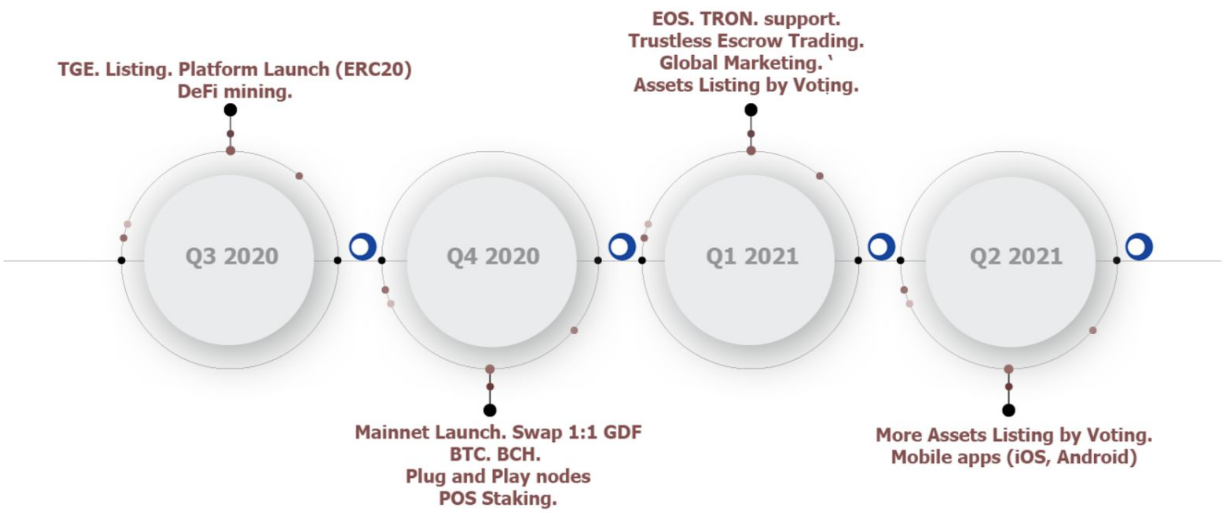

TGE. Listing. Platform Launch (ERC20)
DeFi mining.
EOS. TRON. support.
Trustless Escrow Trading.
Global Marketing. `
Assets Listing by Voting.
Q3 2020
Q4 2020
Q1 2021
Q2 2021
Mainnet Launch. Swap 1:1 GDF
BTC. BCH.
Plug and Play nodes
POS Staking.
More Assets Listing by Voting.
Mobile apps (iOS, Android)

Figure 6

Q3 2020
TGE- Token Generation Event
Listing of GDF on 1-2 popular centralized exchanges.
Platform Launch (ERC20)
DeFi mining starts once the platform launches.

Q4 2020
Mainnet Launch
Swap GDF ERC20 to native GDF, 1:1 ratio
Platform support BTC and BCH
POS Staking.

Q1 2021
Platform includes TRON and EOS assets support for DeFi.
Launching of Trustless Escrow trading (for locked/unlocked tokens).
Global marketing initiative.
Assets Listing by community voting. To vote, you need to hodl GDF tokens.

Q2 2021
Mobile apps for the platform in Android and iOS launch.
Support for more other blockchain assets in our platform via community voting. To vote, you need to hodl GDF tokens.

9. Team

The team consists of young and mature founding members, who are very enthusiastic in building and developing blockchain projects. We believe technology alone will not drive adoption, we need a solid business and marketing plan, together with good technology for success. We do not intend to reinvent the wheel. We will adopt reliable and tested libraries for our projects to shorten time to deliver and reduce cost.

The team is committed to develop chain agnostic and efficient DeFi solutions for all. We believe a good tech is necessary but a user friendly, investors driven approach is also necessary to achieve good success. Tech alone will not solve the problem. We will focus on tech, development and business and marketing.

James Li
CEO

James Li has an extensive and diverse background in the blockchain industry, as well as in the corporate world. She has in-depth knowledge and know-how in leading blockchain companies. James was in the PCHAIN team before she left to found Global Defi. She has good problem solving skills and the ability to solve complex problems, coupled with good connection with the business world. Graduated with a degree in computer science from ECNU university.
Email: james@globaldefi.io

Philip Fan
CTO
Email: philip@globaldefi.io

A passionate and very experienced blockchain developer, with excellent knowledge and skills in blockchain core development, SQL, Oracle Database, Agile Methodologies, Spring Framework and jQuery. Graduated with a Bachelor of Science in Computer and Information Sciences from Murdoch University. He was a PCHAIN core blockchain developer in 2018-2019.

Alex Tham
CMO
Email: alex@globaldefi.io
Alex has many years of experience in marketing and business relation in the crypto sphere as early as 2016. He knows the market well and has many contacts, for marketing, exchange listings, and promotions. Graduate with a bachelor degree in Engineering.

10. Contact

You can reach us via several methods as shown below:

Official website: https://globaldefi.io
Official telegram:https://twitter.com/global_defi
Official twitter: https://twitter.com/defi_global
Github: https://github.com/globaldefi
Email: **contact@globaldefi.io**

If anyone is keen in participating in our private sales, please contact us via contact@globaldefi.io

11. References

[1] The Decentralized Financial Crisis
https://arxiv.org/abs/2002.08099

[2] Decentralized Finance (DeFi)
https://dx.doi.org/10.2139/ssrn.3539194

[3] The Decentralized Financial Crisis
https://arxiv.org/pdf/2002.08099.pdf

[4] Threshold Signatures Explained
https://academy.binance.com/security/threshold-signatures-explained

[5] Bridges between Islands: Cross-Chain Technology for Distributed Ledger Technology
https://ssrn.com/abstract=3452714

[6] Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities
https://arxiv.org/abs/1902.04471

[7] Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme
https://www.iacr.org/archive/pkc2003/25670031/25670031.pdf

[8] Practical Threshold Signatures
https://www.iacr.org/archive/eurocrypt2000/1807/18070209-new.pdf

[9] Fully Distributed Non-Interactive Adaptively-Secure Threshold Signature Scheme with Short Shares: Efficiency Considerations and Implementation
https://csrc.nist.gov/CSRC/media/Events/NTCW19/papers/paper-LJYM.pdf

[10] Threshold Signatures: Current Status and Key Issues
http://isrc.asia.edu.tw/www/myjournal/P269.pdf

[11] A Directed Threshold - Signature Scheme
https://arxiv.org/ftp/cs/papers/0411/0411005.pdf

[12] A New Threshold Signature Scheme to Withstand the Conspiracy Attack
https://ieeexplore.ieee.org/document/5696295

[13] Forward-Secure Threshold Signature Schemes
https://www.di.ens.fr/~mabdalla/papers/amn01-full.pdf

[14] An Efficient Code-Based Threshold Ring Signature Scheme with a Leader-Participant Model
https://www.hindawi.com/journals/scn/2017/1915239/

[15] New threshold-proxy threshold-signature schemes
https://www.sciencedirect.com/science/article/abs/pii/S0045790605000182

[16] Privacy and Anonymity Protection with Blind Threshold Signatures
https://www.jstor.org/stable/27751059?seq=1

DISCLAIMER

This material is provided on an "as is" basis and to the fullest extent permitted by law is without warranty of any kind whatsoever, whether express or implied, including without limitation any implied warranties of merchantability, fitness for use, fitness for a particular purpose and/or non-infringement of third party rights. In addition, any warranties, whether express or implied, statutory or otherwise, in relation to use, access, operation, availability, continuity or non-interruption of this material are hereby excluded to the fullest extent permitted by law. While the information and content on this material is believed to be accurate, it may contain errors or inaccuracies.