

DeFiChain

Pink Paper Overview



<https://defichain.com>

@defichain

@uzyn

How far have we come

- First block: May 11, 2020 (Bitcoin halving day)
- Staking ~40% return
 - 20k collateral – simple staking right on the app!
- DEX & Liquidity Mining. >\$250 million TVL

How far have we come

- First bug bounty awarded: \$15,000
- <https://defichain.com/bug-bounty/>

DeFiChain Bug Bounty Program

DeFiChain is engaging with security experts as well as the community to hunt down vulnerabilities. Our bounty program rewards up to USD 50,000.

[Submit vulnerability](#)

[How to participate](#)



Why Pink Paper?

- Lay down the direction of DeFiChain for the next year or so.
- It is a **live paper**, constantly changing as specifications are added to it.
 - PULL REQUESTS are welcomed!
 - Open source. MIT licensed.

DeFiChain Foundation

- It is necessary to kickstart the blockchain.
- It has outlived its general purpose.
- Goal is to be more:
 - **DECENTRALIZED** – no central servers
 - **GENERALIZED** – anyone can utilize the blockchain alike

DeFiChain Foundation

ABOLISHED*

or have its role greatly diminished

* Not a legal obligation.

DeFiChain Foundation

- 2 key addresses:
 - Foundation: 273.7 million DFI
 - Community fund: 11.9 million DFI
- Foundation is merely a **caretaker**.
- Putting DeFiChain into the hands of its users with masternodes taking part in governance decisions.

DeFiChain Foundation

- 2 key addresses:
 - Foundation: 273.7 million DFI
 - Community fund: 11.9 million DFI
- Foundation coins (273.7m): **BURNED!**
- Community fund: UTXO destroyed & placed in consensus-managed smart contract.

Community Projects

- Many great community projects
 - Tracker: <https://www.cakedefi-review.com/DefiChain>
 - Wiki: <https://defichain-wiki.com/>
 - Learning: <https://defichain-explained.com>
 - DeFi Portfolio: <https://github.com/DeFi-PortfolioManagement/defi-portfolio>
 - Mobile app: <https://github.com/DeFiCh-WalletApp>
 - Income Dashboard: <https://defichain-income.com>
 - and many more!



Community Funding Proposal (CFP)

- Today: manual request.
 - Requests are put in.
 - As much as we hate to be one, foundation is the bottleneck and gatekeeper.
- Foundation: to stop being gatekeeper.
 - **Full on-chain CFP**
 - Anyone is free to make one.
 - Part of decentralized governance.

Community Funding Proposal (CFP)

- Fee: 10 DFI per proposal, of which half is burned.
- Simple majority ($\geq 50\%$) by voting masternodes to pass.
- Vote is called out every month – every 70,000 blocks.
- **Tranche** support. Monthly payout.
- Companion website to track and facilitate discussion before voting.
- Masternodes are incentivized to vote.

DFI Issuance

- White paper: 200 DFI per block, guaranteed for the first year.
- Some minor adjustments over DFIPs to incentive anchor and liquidity mining.
- Today's rate: 258.1 DFI per block
 - 58.1 are funded from airdrop fund.
 - Uncertainty over what happens next.

Description	DFI per block
Mining reward	135
Community fund	19.9
Anchor reward	0.1
<i>DeFi incentives</i>	
BTC-DFI	80
ETH-DFI	15
USDT-DFI	5
LTC-DFI	2
BCH-DFI	1
DOGE-DFI	0.1
TOTAL	258.1

DFI Issuance

- Goals:
 - Maintain the same emission rate for the first cycle.
 - Soften the "halving" effect.
 - Maintain the 1.2 billion DFI cap
 - Maintain a steady expected emission rate for foreseeable future. *(this is challenging!)*

DFI Issuance

- First cycle

Description	In use today?	DFI per block	Proportion
Mining reward	Yes	135	33.33% (guaranteed)
Community fund	Yes	19.9	4.91%
Anchor reward	Yes	0.1	0.02%
DEX liquidity mining	Yes	103.1	25.45%
Atomic swap incentives	No	50	12.34%
Futures incentives	No	50	12.34%
Options incentives	No	40	9.88%
Unallocated incentives	No	6.94	1.71%
TOTAL		405.04	100%

DFI Issuance

- Cycle length: 32,690 blocks (2 weeks, 37secs block)
- 1.658% reduction every cycle.
- Proportion is maintained.
 - Cycle 1: Mining reward is 135 DFI per block (33.33% of 405.04 DFI)
 - Cycle 2: Mining reward is 132.76 DFI per block (33.33% of 398.32 DFI)
- Proportion is maintained.
- Unused allocation is burned, not accumulated.

Description	In use today?	DFI per block	Proportion
Mining reward	Yes	135	33.33% (guaranteed)
Community fund	Yes	19.9	4.91%
Anchor reward	Yes	0.1	0.02%
DEX liquidity mining	Yes	103.1	25.45%
Atomic swap incentives	No	50	12.34%
Futures incentives	No	50	12.34%
Options incentives	No	40	9.88%
Unallocated incentives	No	6.94	1.71%
TOTAL		405.04	100%

DFI Issuance

- **In 10 years, 1,188,259,185 DFI is issued**
(inclusive of burned amount). That's **99.02%** issued!
- It'll continue perpetually and never hit the cap 1.2 billion DFI.
- Much more predictable.
- What if allocations are not ideal?
 - Reallocation via governance.
 - Mining is fixed at 33.33%.

Description	In use today?	DFI per block	Proportion
Mining reward	Yes	135	33.33% (guaranteed)
Community fund	Yes	19.9	4.91%
Anchor reward	Yes	0.1	0.02%
DEX liquidity mining	Yes	103.1	25.45%
Atomic swap incentives	No	50	12.34%
Futures incentives	No	50	12.34%
Options incentives	No	40	9.88%
Unallocated incentives	No	6.94	1.71%
TOTAL		405.04	100%

Operator

- Role separation between operator and blockchain.
 - No more foundation.
- Anyone can create operator (*fee TBD*)
 - Creates asset tokens (DAT)
 - Manages DEX
 - Appoints oracles
 - Sets lending rates, etc
- Creates competition

Operator

No security concerns between operators.

**Every offering is secured by
the power of #NativeDeFi**

DeFiChain Fees

- Usage of DeFiChain will consists of the following fees:
 - **Miner fee**
 - For masternodes/miners
 - **Operator fee**
 - For operators
 - e.g. DEX fee, etc. Can be 0.
 - **DeFi fee**
 - For DFI holders. This is already happening today.
 - Fees are burned & tracked.

DeFiChain Fees

- DeFi fees, to be determined.


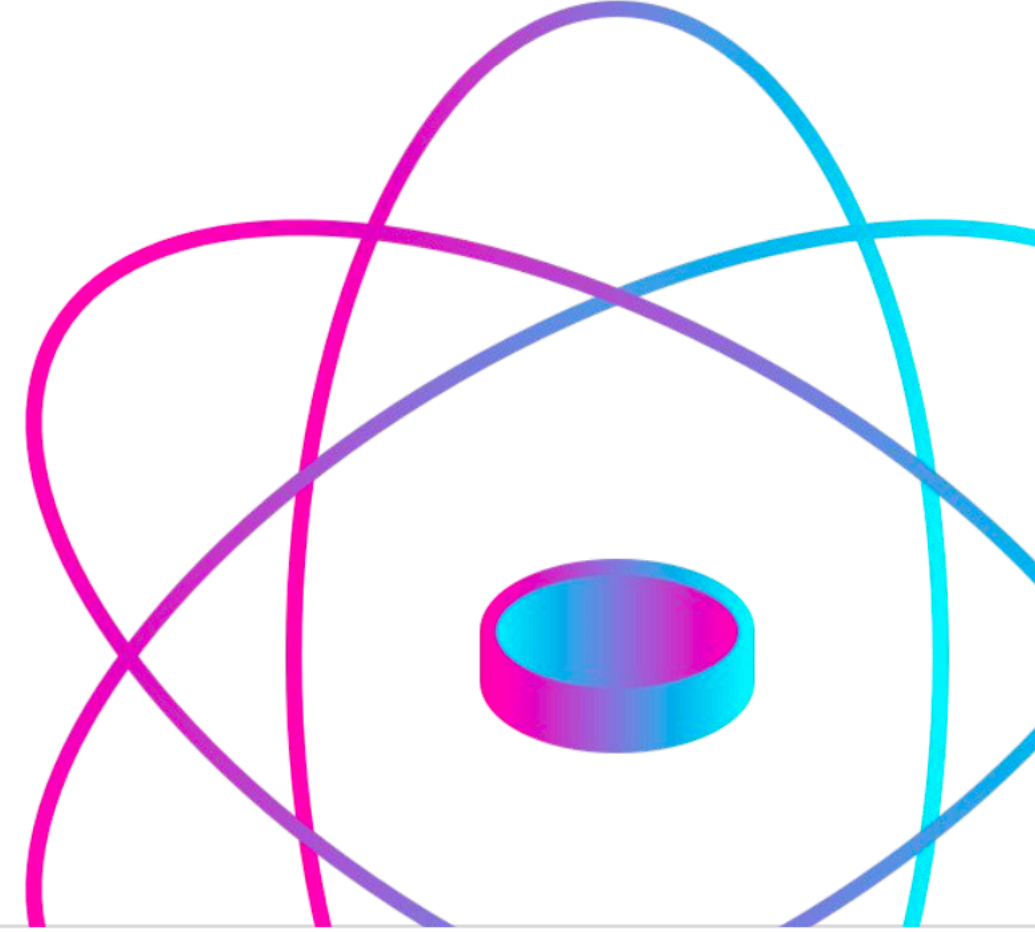
Operations	Burn amount (in DFI)
Masternode	
Registration	10
Operator	
Registration	1000
Tokenization	
Create a new token	100
Liquidity pool	
Create pool	300
Swap (for non-DFI pairs)	0.01
Governance	
Initiate community fund request	5
Initiate vote of confidence	25

Initiate block reward reallocation proposal	250
Interchain exchange	
Atomic swap	0.01
Oracle	
Create price feed	100
Appoint oracle	20
Loan	
Loan interest	TBD
Liquidation fee	TBD
Option pool	
Create pool	300
Option contract creation	0.01

Pink Paper

Decentralized Finance

Interchain Exchange & Atomic Swap

#0	<div>Interchain Exchange and Atomic Swap</div> <div> </div>
17 Feb 21	Decentralized Finance enabled on Bitcoin

Oracle

- Needed for various DeFi applications such as Loan, Future, Option.
- Oracles are appointed by operators, not Foundation.
- Mainly focusing on price feeds: BTC, ETH, TSLA, XAU, etc.
- Multiple oracles, aggregation and weightage support.

Oracle

Price feeds

Price feed should be 8 decimal places

Requires foundation authorization.

1. `createpricefeed BTC_USD_PRICE`
2. `removepricefeed BTC_USD_PRICE`

Oracle appointments

Requires foundation authorization.

1. `appointoracle ADDRESS '["BTC_USD_PRICE", "ETH_USD_PRICE"]' WEIGHTAGE`
 - returns `oracleid`. `oracleid` should be a deterministic hash and not incremental count.
 - `WEIGHTAGE` is any number between 0 to 100. Default to 20.
2. `removeoracle ORACLEID`
3. `updateoracle ORACLEID ADDRESS '["BTC_USD_PRICE", "ETH_USD_PRICE"]' WEIGHTAGE`

Price feeds operations

Requires oracle authorization.

1. `setrawprice TIMESTAMP '{"BTC_USD_PRICE": 38293.12}'`
 - Raw price update should only be valid if timestamp is within one hour from the latest blocktime.
 - timestamp is there so that updates that are stuck in mempool for awhile does not get accepted after timeout.

General usage, requires no authorizations.

1. `listlatestrawprices BTC_USD_PRICE`
 - Also supports `listlatestrawprices` to list across all feeds.
 - Returns an array of all the latest price updates, e.g.

```
[
  {
    "pricefeed": "BTC_USD_PRICE",
    "oracleid": "ORACLEID",
    "weightage": 50,
    "timestamp": "timestamp of the last update",
    "rawprice": 38293.12000000,
    "state": "live"
  }
]
```


Decentralized Loan

- Operator-run decentralized loan – to issue **decentrally-issued price-tracking tokens** such as BTC.
- Secured by DFI/BTC or other tokens determined by operators.
- Over-collateralized loan. Operator sets the parameters:
 - Collateralization ratio
 - Liquidation penalty
 - Interest rates (DFI & other operator-determined fees)

Decentralized Loan

- Loan tokens are supported by Interchain Exchange (ICX) and can be atomically swapped with Bitcoin.
- Loan tokens can also be listed on Decentralized Exchange (DEX) on DeFiChain.

Future

- The primary product that allows DeFiChain to introduce asset tokenizations such as stocks.
- It's a traditional finance derivative that's widely understood.
- Rolled out with decentralized twist.
- Use-case:
 - Allowing traders to LONG or SHORT an asset.
 - Either with **fixed expiry** or **perpetual swap** (*without expiry*)

Future

- Future is provided with price oracles, to allow the token to track the price of a real-world asset.
- **Fixed expiry** future expires at the asset price at settlement time.
- **Perpetual swap** future does not expire. Funding rate will be used to keep the price of token tracking its asset price closely periodically.
- If you LONG TSLA, you can LONG it over the long term, & vice versa.

Future

- Support your position with DFI and operator tokens.
- Boosts TVL.

⌘ Mechanics

1. Margin contract

- Trader is able to fund their Future trading position through this margin contract.
- Contract can be funded with DFI and other tokens that operators decide, e.g. BTC.
- Operator can also define *initial margin* and *maintenance margin* for a margin contract.

2. Asset

- Operator decide assets to list.
- Assets can be stocks, commodities or anything that has a price. It is operator's responsibility to ensure that there are good price oracles for traded assets.

3. Order

- User is able to make an order. It can be a **long** or **short** order.
- Order matching can be automated, if we are able to have good optimization on the node-side. Otherwise it will be an additional transaction call to match orders. Matching daemon can be run by operators.

4. Settlement

- Fixed expiry future will be settled automatically based on settlement oracle price published.
- Perpetual swap future has no settlement. There is instead a **funding rate mechanism**.

5. Perpetual swap funding

- Funding rate is automatically determined by DeFiChain based on fixed algorithm: oracle price, perpetual swap trading price.
- Funding period can be set by operator, but it should be between 1x to a max of 12x per day. For reference, most centralized perpetual swap offerings have a 8h funding interval (3x per day).

6. Liquidation

- When net margin (total margin + unrealized PnL) is less than maintenance margin, forced liquidation would occur.
- TBD: Either automated, operator-run, or community-run with incentives.

Enhancements

1. Future can further be enhanced to allow leverage. DeFiChain will start with no leverage (1x) and will introduce leverage once the mechanisms are stable.

DEFI



Option

- Traditional order-book-based options are boring.
- Introducing AMM-style option. Automated option writer with Option writer pool.
- Participate in automated options pool by providing only 1 token: e.g. BTC, ETH, DFI, USDT
- Liquidity mine by participating in automated options pool.

Option

- **BTC, ETH, DFI**: writing CALL contracts with -USDT.
USDT: writing BTC-USDT, ETH-USDT, etc PUT contracts
- Option buyer can purchase options from pools directly with max expiry of 30 days with automated pricing – *arbitrage!*
- This is still under major design and may be subjected to change.
Also exploring possibility of sweepstake options and paired option pools.

Non-Fungible Token?

- **Native NFT?**
- Offering more integrations and use-case possibilities with NFT, alongside DeFi Standard Token (DST).
- Jellyfish (JS lib) would allow more integration possibility.

Disclaimer

- This is the general blueprint of DeFiChain. Things may change.
- Development takes times – not all features will be available immediately.

Roadmap Checkpoint

Checkpoint

- **Interchain Exchange**
- **Atomic swap**
- Jellyfish & Lightwallet (MetaMask-like UX)
 - Also community light wallet implementation.
- Governance
 - And companion site
- Ledger support

Checkpoint

- Decentralized stocks – futures
- New emission rate and burn tracking

Q&A

Pink Paper is available at

<https://github.com/DeFiCh/pinkpaper>



<https://defichain.com>

@defichain

@uzyn