x0Swap Whitepaper v1

August 2021

Abstract

This technical whitepaper explains some of the features of x0's liquidity platform for the CBDCs (Central Bank Digital Currency) and global stable coins. It covers x0's methodology to ensure interoperability between multiple blockchain systems including between CBDCs and stable coin pairs. We also attempt to explain how liquidity and pricing is maintained in our platform as well as some of the farms and staking pool features of the x0 platform. This whitepaper describes the mechanics of x0's "core" contracts including the pair contract that stores liquidity providers' funds—and the factory contract used to instantiate pair contracts.

1. Introduction

Global payment systems are neither global nor an actual system. In fact, it is only a messaging system that sends messages about pending transfers from **Sender** to **Recipient**. Transfer settlements for each transfer happen sometimes involving many interactions between financial institutions and can take days for the transaction to be fully settled.

Problem With Money Existing Supply: It's Expensive and Inefficient
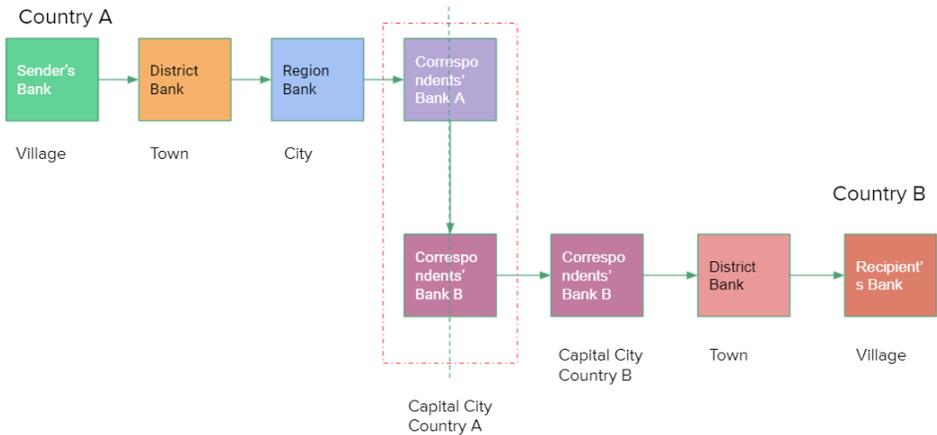
One of the major debilitating hurdles of the current payment system is the non-inclusivity of everyone. Many fintech solutions providers emerge trying to solve this problem with the unbanked but ultimately they end up having to connect to existing systems as well. This is not solving an issue, it is adding another **LAYER** to an already complex system.

Based on Mckinsey & Co's global payments study conducted in 2016, it was found that annually total costs associated with global money transfers topped US$ 1.6 Trillion while average transfers took 3-7 days and up to 4% transactions failed due to inefficiencies in the payments settlement.

2. Cryptocurrencies and CBDCs (Central Bank Digital Currencies)

Crypto entered the global payments scene with Bitcoin, etc. It promises direct payment solutions through decentralization but has struggled with adoption due to highly complex systems, regulatory issues and frequently associated with criminal activities. Governments around the world saw crypto as a huge threat to existing monetary systems and have moved swiftly to issue debilitating curbs, with some countries outright banning and shutting down cryptocurrency operators. This animosity however has not stopped the advance of the adoptio cryptocurrencies with total cryptocurrency valuation hitting US$2.5 Trillion.

Seeing the inevitability to stop the cryptocurrency movement and acknowledging the weaknesses of the existing global payments infrastructures, forward thinking governments have embarked on the journey to introduce CBDCs (Central Bank Digital Currencies). These CBDCs are basically digital equivalent of the existing FIAT currencies, typically issued on a blockchain or other similar platform which allows FIAT currencies to achieve cryptocurrencies' level of efficiency while maintaining the regulatory scrutiny by the central banks.

Central Bank Digital Currencies

	Present	Future
Central Bank	🏛️	🏛️
Real Money	💵	CBDC · 🪙
Banks	🏢	🏢
Services	🏪	🏪
Consumer	🧍	🧍
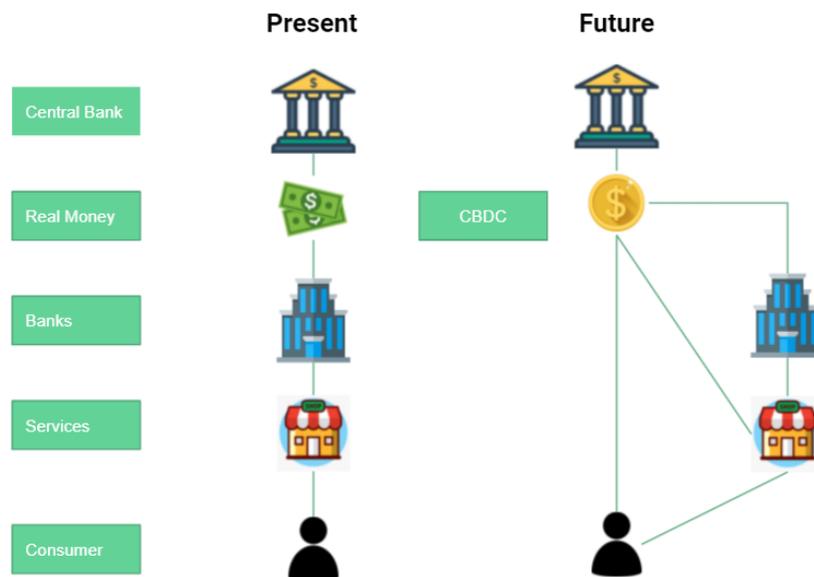
In the present system, banks play a critical role to help central banks distribute money to the economy. All transactions, especially cross border transactions will involve Banks.

In the CBDC world, consumers and services can **settle payments directly** without involving

banks, especially beneficial for cross border payments.

3. Proposed Solution

x0 is a platform that helps financial participants with **interoperability** between CBDCs, existing Digital Assets and Traditional Money in a **transparent** way without a commonly accepted standardization. x0 also helps banks, fintech players and others to **obtain liquidity** in a fast, cheap and democratic way.
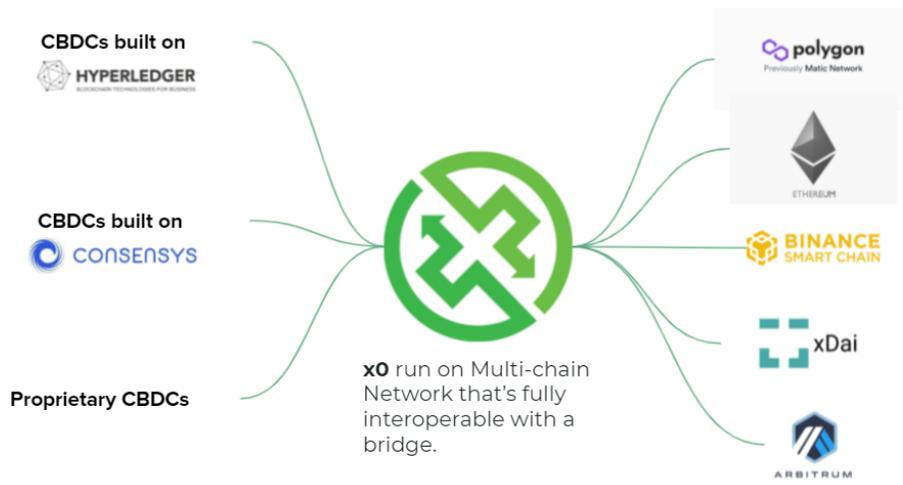
x0 being an interoperability platform, we will allow swapping and exchanging of CBDCs with existing cryptocurrencies and digital assets. Participants will be able to move assets from different blockchains in a more seamless way while allowing for transparent and traceable collaboration.
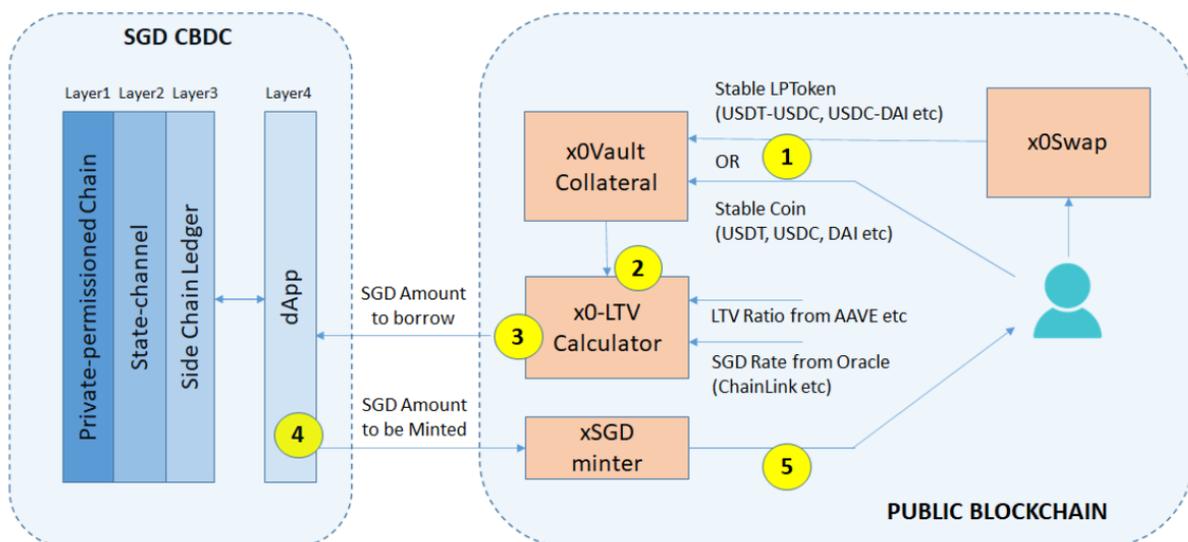
ECOSYSTEM at a Glance
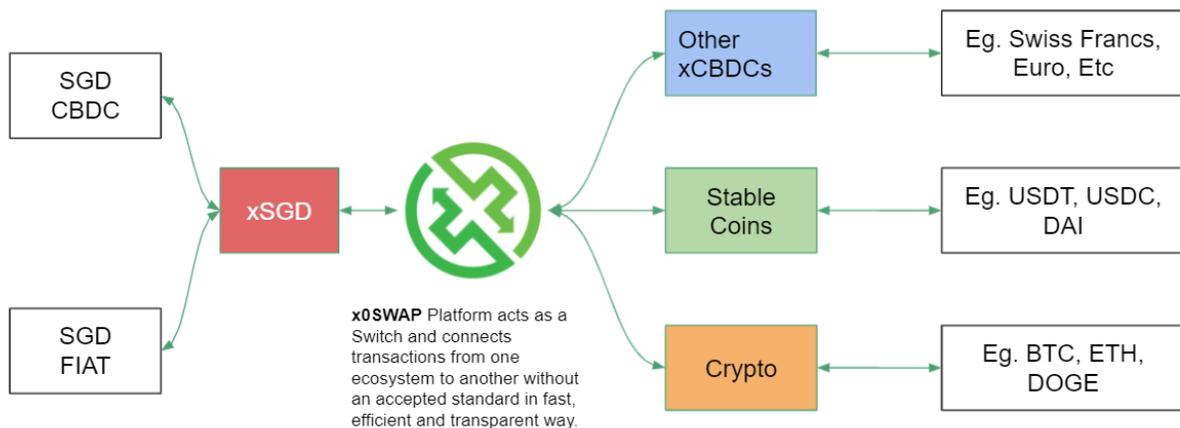
x0 is also a liquidity platform, we allow participants to provide liquidity in exchange for incentives. x0 provides popular liquidity pairs funded by participants which allows almost instantaneous access to liquidity in a fast, cheap and efficient way.

Multi-chain solution at a Glance

CBDCs built on HYPERLEDGER

CBDCs built on CONSENSYS

Proprietary CBDCs

x0 run on Multi-chain Network that's fully interoperable with a bridge.

polygon (Previously Matic Network)

ETHEREUM

BINANCE SMART CHAIN

xDai

ARBITRUM

x0 also has an onboarding platform which allows for CBDCs and other digital assets to be onboarded and allow for global interoperability without border restrictions as well as without prior agreed standards.

CBDC Onboarding: SGD Example

SGD CBDC

Layer1 Layer2 Layer3 Layer4

Private-permissioned Chain

State-channel

Side Chain Ledger

dApp

SGD Amount to borrow — 3

SGD Amount to be Minted — 4

x0Vault Collateral

Stable LPToken (USDT-USDC, USDC-DAI etc) — 1

OR

Stable Coin (USDT, USDC, DAI etc)

x0Swap

x0-LTV Calculator — 2

LTV Ratio from AAVE etc

SGD Rate from Oracle (ChainLink etc)

xSGD minter — 5

PUBLIC BLOCKCHAIN

4. **x0 Platform Features**

Highly Secure

x0 operates systems that are audited by security professionals to ensure that we deliver a stable and secure environment for our participants. We are currently working with several blockchain security auditors to audit our smart contracts to ensure that we are not vulnerable from known hacks and exploits.

Super Fast Transactions

Unlike traditional payments where transaction settlements take days. With x0 transactions are completed within seconds and this constitutes settlement, cutting out middlemen and associated fees. Our direct settlement model will be helpful to allow participants to receive assets directly in their wallets to be used directly.

Low Fees

Since we exist on multiple blockchains, participants can determine which protocol they want to use to send their payments through. Fees start from $0.01 for 500 transactions. x0 tokens exist on multiple blockchains and participants can use this to move assets to multiple blockchains easily and access assets on those blockchains.

On Demand Liquidity

x0 provides participants access to on-demand liquidity. This liquidity is provided by participants themselves as they commit to our liquidity pools in exchange for APRs and yields.

Community Governance

x0 is an open platform supported by our community. The community provides liquidity which powers the x0 platform. Our community will also vote changes to the platform through a voting system.

Liquidity Farms and Pools

x0 platform rewards participants with attractive returns when they participate as **liquidity providers**. Current reward structures include getting **transaction fees** related to the exchange operations.
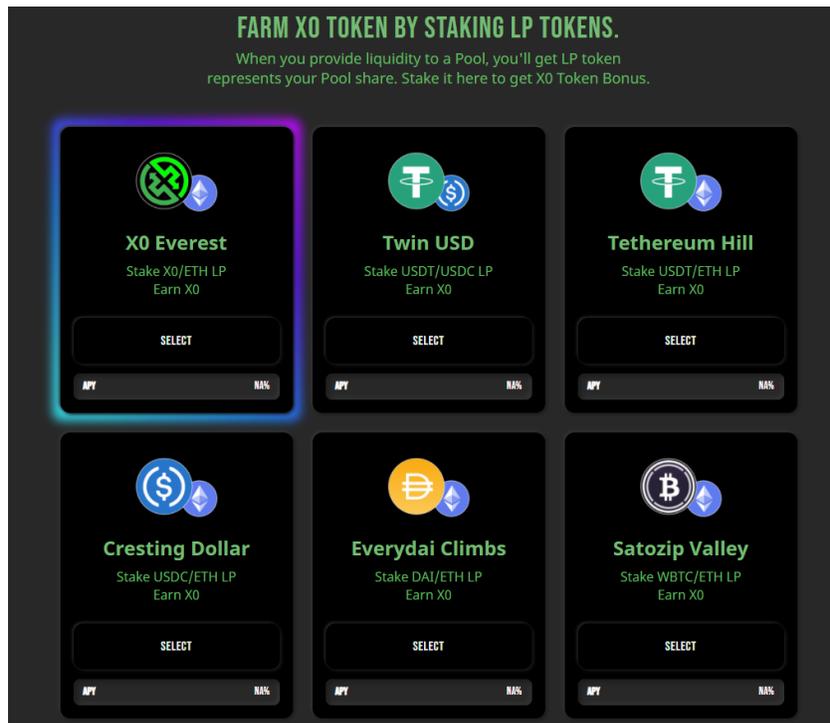
Participants can also choose to commit to **longer duration** as liquidity providers with the reward of x0 Tokens, our platform token. x0 is the first platform which will allow a time-lock period of 3, 6, 9 months staking to unlock higher returns. We encourage our users to put in their liquidity for longer periods and incentivize users that commit to longer lock-in periods.

x0 rewards liquidity providers in a 2-tier incentive structure where liquidity providers earn transaction fees for swap or exchange operations involving their liquidity as well as earning x0 tokens when liquidity providers lock-in their liquidity for our time-lock periods.

5. **x0 Liquidity Concept**

x0's liquidity management process follows closely Uniswap V2's price oracle model. The marginal price offered by the liquidity pool (not including fees) at time t can be computed by dividing the reserves of asset a by the reserves of asset b.

$$p_t = \frac{r_t^a}{r_t^b}$$

Since arbitrageurs will trade if this price is incorrect (by a sufficient amount to make up for the fee), the price offered by the pool tends to track the relative market price of the assets, as shown by Angeris et al [2]. This means it can be used as an approximate price oracle. However, during Uniswap V1, it is not safe to use as an on-chain price oracle, because it is very easy to manipulate. Suppose some other contract uses the current ETH-DAI price to settle a derivative. An attacker who wishes to manipulate the measured price can buy ETH from the ETH-DAI pair, trigger settlement on the derivative contract (causing it to settle based on the inflated price), and then sell ETH back to the pair to trade it back to the true price. This might even be done as an atomic transaction, or by a miner who controls the ordering of transactions within a block.

x0's model improves this oracle functionality by measuring and recording the price before the first trade of each block (or equivalently, after the last trade of the previous block). This price is more difficult to manipulate than prices during a block. If the attacker submits a transaction that attempts to manipulate the price at the end of a block, some other arbitrageur may be able to submit another transaction to trade back immediately afterward in the same block. A miner (or an attacker who uses enough gas to fill an entire block) could manipulate the price at the end of a block, but unless they mine the next block as well, they may not have a particular advantage in arbitraging the trade back.

Liquidity Pair Pricing Curve
Trade Changes Balance of Reserves Resulting in New Price
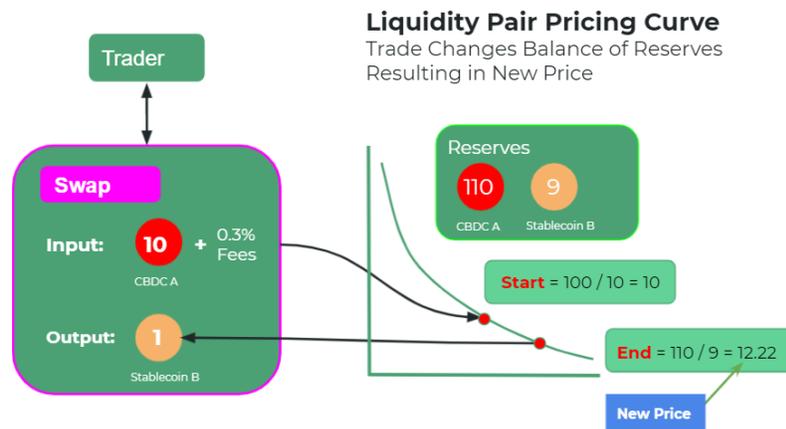
Specifically, it accumulates this price, by keeping track of the cumulative sum of prices at the beginning of each block in which someone interacts with the contract. Each price is weighted by the amount of time that has passed since the last block in which it was updated, according to

the block timestamp. This means that the accumulator value at any given time (after being updated) should be the sum of the spot price at each second in the history of the contract.

$$a_t = \sum_{i=1}^{t} p_i$$

To estimate the time-weighted average price from time t1 to t2, an external caller can checkpoint the accumulator's value at t1 and then again at t2, subtract the first value from the second, and divide by the number of seconds elapsed. (Note that the contract itself does not store historical values for this accumulator—the caller has to call the contract at the beginning of the period to read and store this value.)

$$p_{t_1,t_2} = \frac{\sum_{i=t_1}^{t_2} p_i}{t_2 - t_1} = \frac{\sum_{i=1}^{t_2} p_i - \sum_{i=1}^{t_1} p_i}{t_2 - t_1} = \frac{a_{t_2} - a_{t_1}}{t_2 - t_1}$$

Users of the oracle can choose when to start and end this period. Choosing a longer period makes it more expensive for an attacker to manipulate the TWAP, although it results in a less up-to-date price. One complication: should we measure the price of asset A in terms of asset B, or the price of asset B in terms of asset A? While the spot price of A in terms of B is always the reciprocal of the spot price of B in terms of A, the mean price of asset A in terms of asset B over a particular period of time is not equal to the reciprocal of the mean price of asset B in terms of asset A. For example, if the USD/ETH price is 100 in block 1 and 300 in block 2, the average USD/ETH price will be 200 USD/ETH, but the average ETH/USD price will be 1/150 ETH/USD. Since the contract cannot know which of the two assets users would want to use as the unit of account, it tracks both prices.
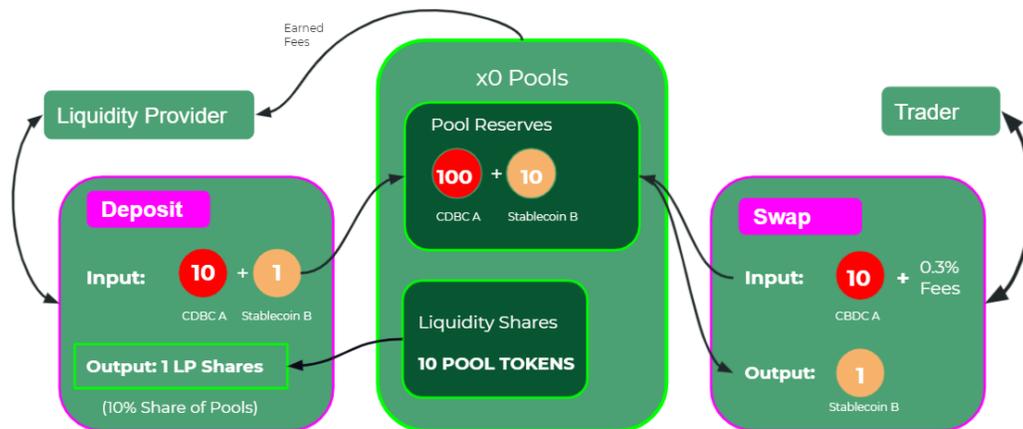
Another complication is that it is possible for someone to send assets to the pair contract—and thus change its balances and marginal price—without interacting with it, and thus without triggering an oracle update. If the contract simply checked its own balances and updated the oracle based on the current price, an attacker could manipulate the oracle by sending an asset to the contract immediately before calling it for the first time in a block. If the last trade was in a

block whose timestamp was X seconds ago, the contract would incorrectly multiply the new price by X before accumulating it, even though nobody has had an opportunity to trade at that price. To prevent this, the core contract caches its reserves after each interaction, and updates the oracle using the price derived from the cached reserves rather than the current reserves.

6. **x0 Tokenomics**

x0 issues our own native token called x0 token (x0 Symbol). We're issuing a total of 153million tokens which will be divided into 3 blockchains:

Matic Polygon	51,000,000 x0
xDAI	51,000,000 x0
BSC (BEP20)	51,000,000 x0

**All x0 tokens will be EVM compatible

x0 tokens on the platform will be minted earned as long as the liquidity pool is filled. x0 tokens minted will follow the block cycle of each of the blockchains stated above with adjustments introduced to ensure that token scarcity is maintained throughout.

x0 tokens will also be used as governance tokens where participants can vote on improvement proposals. Proposals will be introduced at a periodic interval based on community suggestions and general outlook of the ecosystem. Participants who hold x0 tokens can participate in the open governance of the platform allowing them to determine the best path forward.

7. **References**

[1] Hayden Adams. 2018. url: https://hackmd.io/@477aQ9OrQTCbVR3fq1Qzxg/HJ9jLsfTz?type=view.

[2] Guillermo Angeris et al. An analysis of Uniswap markets. 2019. arXiv: 1911.03380 [q-fin.TR].

[3] samczsun. Taking undercollateralized loans for fun and for profit. Sept. 2019. url: https : / / samczsun . com / taking - undercollateralized - loans - for - fun - and - for-profit/.

[4] Mckinsey & Co. Global Payments 2016: Strong Fundamentals Despite Uncertain Times. 2016

[5] Fabian Vogelsteller and Vitalik Buterin. Nov. 2015. url: https://eips.ethereum.org/EIPS/eip-20.

[6] Jordi Baylina Jacques Dafflon and Thomas Shababi. EIP 777: ERC777 Token Standard. Nov. 2017. url: https://eips.ethereum.org/EIPS/eip-777.

[7] Uniswap.info. Whitepaper. url: https://uniswap.org/whitepaper.pdf

[8] Vitalik Buterin. EIP 1014: Skinny CREATE2. Apr. 2018. url: https://eips.ethereum. org/EIPS/eip-1014.

[9] Binance. BSC White Paper. Url: https://github.com/binance-chain/whitepaper

[10] xDAI. POSDAO White Paper. Url: https://www.xdaichain.com/for-validators/posdao-whitepaper

[11] MATIC. Matic network whitepaper: Url: https://github.com/maticnetwork/whitepaper

8. **Disclaimer**

This paper is for general information purposes only. It does not constitute investment advice or a recommendation or solicitation to buy or sell any investment and should not be used in the evaluation of the merits of making any investment decision. It should not be relied upon for accounting, legal or tax advice or investment recommendations. This paper reflects current opinions of the authors. The opinions reflected herein are subject to change without being updated