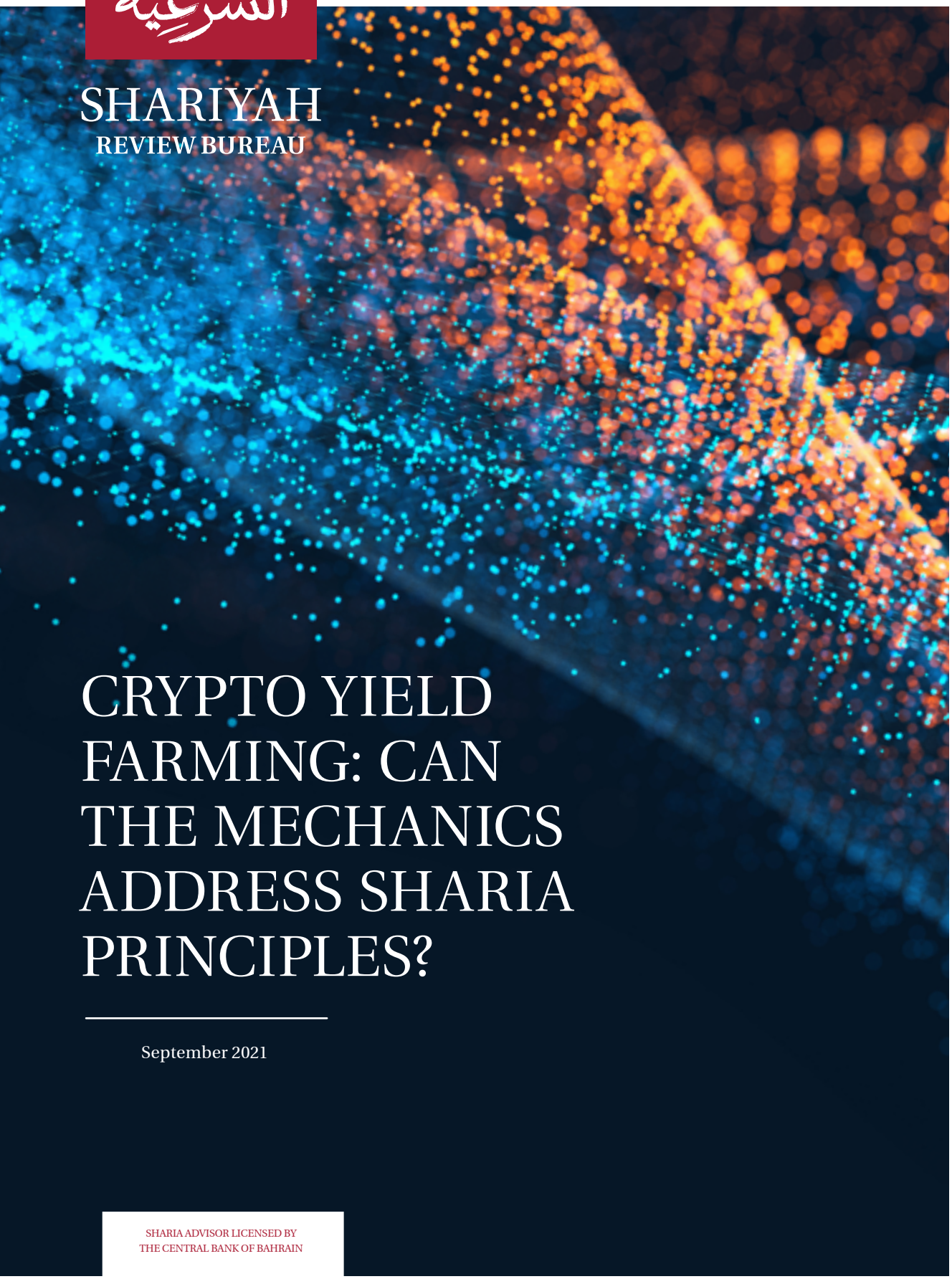
دار المراجعة الشرعية

SHARIYAH
REVIEW BUREAU



CRYPTO YIELD FARMING: CAN THE MECHANICS ADDRESS SHARIA PRINCIPLES?

September 2021

SHARIA ADVISOR LICENSED BY
THE CENTRAL BANK OF BAHRAIN

WHAT IS DEFI?

DeFi is short for "decentralised finance" an umbrella term for a variety of financial applications in cryptocurrency or blockchain geared toward disrupting financial intermediaries[1]. It involves taking traditional elements of the financial system and replacing the middleman with a smart contract. In layman's terms it can also be described as a merger between traditional banking services and blockchain technology.. DeFi relies greatly on cryptography, blockchain, and smart contracts, with the latter being its main building block.

DeFi draws inspiration from blockchain, the technology behind Bitcoin, which allows several entities to hold a copy of a history of transactions, meaning it isn't controlled by a single, central source. That's important because centralised systems and human gatekeepers can limit the speed and sophistication of transactions while offering users less direct control over their money. DeFi is distinct because it expands the use of blockchain from a simple value transfer protocol to a much more complex financial use case.

Before it was commonly known as decentralised finance, the idea of DeFi was often called "open finance." DeFi eliminates the requirement for identification numbers, making it possible for sellers, lenders, buyers, and borrowers to interact directly rather than seeking institutional help for transaction administration.

So, for DeFi to work, it needs a decentralised infrastructure to run on. This is where the Ethereum blockchain comes into play. The Ethereum blockchain is a DIY platform for decentralised applications (DApps). Cutting out middlemen from all kinds of transactions is one of the primary advantages of DeFi. Most applications that call themselves "DeFi" are built on top of Ethereum, the world's second-largest cryptocurrency platform, which sets itself apart from the Bitcoin platform in that it's easier to use to build other types of decentralised applications beyond simple transactions. With smart contracts at the core, dozens of DeFi applications are operating on Ethereum.

DeFi creates an ecosystem of financial applications that are built on top of blockchain networks. DeFi has become a movement that aims to create an open-source, permissionless, and transparent financial service ecosystem that is available to everyone and operates without any central authority. The users would maintain full control over their assets and interact with this ecosystem through peer-to-peer (P2P), decentralised applications (dApps).

The core benefit of DeFi is easy access to financial services, especially for those who are isolated from the current financial system. Another potential advantage of DeFi is the modular framework it is built upon – interoperable DeFi applications on public blockchains will potentially create entirely new financial markets, products, and services[2].

DeFi applications do not need any intermediaries or arbitrators. The code specifies the resolution of every possible dispute, and the users maintain control over their funds at all times. This reduces the costs associated with providing and using these products and allows for a more frictionless financial system.

Another significant advantage of such an open ecosystem is the ease of access for individuals who otherwise wouldn't have access to any financial services. Since the traditional financial system relies on the intermediaries making a profit, their services are typically absent from locations with low-income communities. However, with DeFi, the costs are significantly reduced, and low-income individuals can also benefit from a broader range of financial services.

1 https://www.coindesk.com/what-is-defi
2 https://coreswap.io/the-beginners-guide-to-defi/

APPLICATIONS OF DEFI

Some of the common applications of DeFi are as follows:

1. Monetary Banking Services

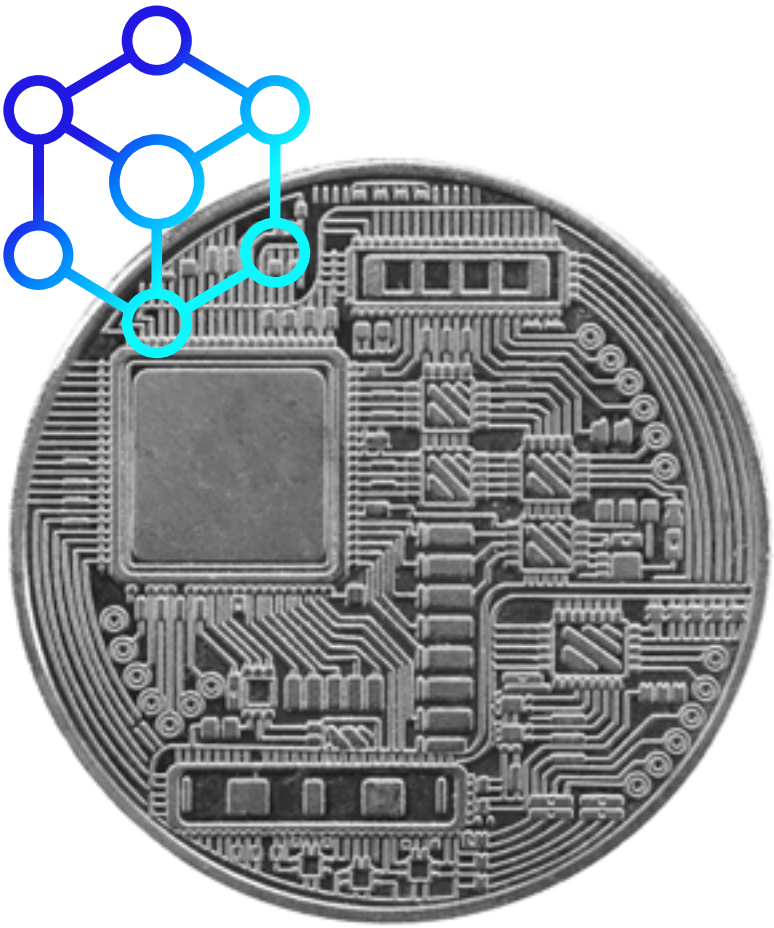
As DeFi applications are, by definition, financial applications, monetary banking services are an obvious use case for them. These can include the issuance of stablecoins, mortgages, and insurance.

As the blockchain industry is maturing, there is an increased focus on the creation of stablecoins. They are a type of cryptoasset that is usually pegged to a real-world asset but can be transferred digitally with relative ease. As cryptocurrency prices can fluctuate rapidly at times, decentralised stablecoins could be adopted for everyday use as digital cash that is not issued and monitored by a central authority.

DeFi also has potential in mortgage provision. Largely because of the number of intermediaries needing to be involved, the process of getting a mortgage is expensive and time-consuming. With the use of smart contracts, underwriting and legal fees may be reduced significantly[3]. Similarly, insurance on the blockchain could eliminate the need for intermediaries and allow the distribution of risk between many participants. This could result in lower premiums with the same quality of service.

2. Decentralised exchanges (DEXs)

Decentralised exchanges are exchanges that operate without an intermediary. They are not as popular as their centralised counterparts. With DEXs, users can connect directly with one another to buy and sell cryptocurrencies in a trustless environment. Assets traded under DEXs are never held in an escrow or third-party wallet, as is done with centralized exchanges. Some common DEXs include Uniswap, Curve and SushiSwap. Centralised exchanges, on the other hand, are trading platforms operated by a central authority. Platforms like Binance and Coinbase are popular examples of centralised exchanges. They are custodial in nature. In other words, the buyers and sellers trust the central authority to keep their digital assets safe.



3 https://coreswap.io/the-beginners-guide-to-defi/

3. Lending Platforms

DeFi proponents say the decentralised lending platforms are democratising the lending ecosystem. These platforms use smart contracts in place of intermediaries like banks — allowing borrowers and lenders to participate in an open system. Lenders can earn interest on their crypto assets by loaning them out, while borrowers can access liquidity without selling off their assets. Of course, from a Sharia perspective, such a use case is problematic.

With the traditional financial system, you need to offer collateral before you can access loans from the bank. This is similar to what happens in DeFi. Borrowers have to over-collateralise their loans by offering assets more valuable than the loan value. Some of the common DeFi lending platforms include Maker, Compound, and Aave. In a nutshell, getting a cash loan with cryptocurrency functions in the following manner:

1. Own cryptocurrency (major digital assets like Bitcoin, Ethereum, or Litecoin).

2. Go to a decentralised finance platform such as Compound.

3. Create a loan offer as a borrower that details your desired loan terms and cash amount.

4. Wait for a lender or group of lenders to match your requirements.

5. Collateralise the loan with your cryptocurrency from step 1.

6. Loan approved and issued.

There are also semi-decentralised crypto loan platforms like Celsius Network, Nexo, and BlockFi that use blockchains for transparency, don't require checks, but do centralise certain processes. Using one of these semi-centralised crypto loan platforms, the process of getting a cash loan backed by your cryptocurrency holdings is even faster.

4. Prediction Markets

A prediction market allows participants to make bets on the outcomes of future events. These platforms function like traditional prediction markets — but with blockchain functionality, which eliminates intermediaries. Examples of DeFi prediction markets are Augur, Gnosis and FTX[4]. Such prediction markets have high non-Sharia compliance risks and depending on the structure, can be a form of gambling.

5. Savings Accounts

A crypto interest account is a place to store your existing cryptocurrency assets and collect interest on them. If you've ever used a savings account with a popular bank or local credit union, then you've dealt with this format for saving and accruing interest on your money. A crypto interest account has three major aims:

- Act as a safe place to deposit and store your crypto
- Loan your crypto to borrowers
- Pay you interest on crypto you deposited

Crypto DeFi platforms, whether it's BlockFi, Celsius, Nexo, or another, are effectively paying you to borrow your money. That's how interest-generating savings accounts work. As these platforms hand out loans to qualified borrowers, they collect fees on the lent funds and use those collected fees to pay back your stipulated APY[5].

BlockFi is a major crypto wealth management platform that offers several services to its clients. Most notable is its generous high-yield crypto savings account. BlockFi calls this product the BlockFi Interest Account. It offers compound interest, institutional backing, interest paid in crypto, and industry-topping interest rates. The BlockFi Interest Account can receive deposits and pay interest in stablecoins that include GUSD, PAX, and USDC, or cryptocurrencies BTC, ETH, and LTC.

4 https://www.nasdaq.com/articles/what-is-defi-and-why-does-it-matter-now-2021-06-04
5 https://www.cryptolendingadvice.com/advice/how-to-earn-interest-on-crypto/

WHAT ARE LIQUIDITY POOLS?

Liquidity pools are one of the foundational technologies behind the current DeFi ecosystem. They are an essential part of automated market makers (AMM), borrow-lend protocols, yield farming, synthetic assets, on-chain insurance, blockchain gaming – the list goes on. The idea in itself, is profoundly simple. A liquidity pool is basically funds thrown together in a big digital pile.

By definition, a liquidity pool is a collection of funds locked in a smart contract. Liquidity pools are used to facilitate decentralised trading, lending, and many more functions.

Liquidity pools are the backbone of DEXs, such as Uniswap. Users called liquidity providers (LP) add an equal value of two tokens in a pool to create a market. In exchange for providing their funds, they earn trading fees from the trades that happen in their pool, proportional to their share of the total liquidity. As anyone can be a liquidity provider, AMMs have made market making more accessible.

YIELD FARMING

Yield farming, also referred to as liquidity mining, is a way to generate rewards with cryptocurrency holdings. In simple terms, it means locking up cryptocurrencies and getting rewards. Some liquidity pools pay their rewards in multiple tokens. Those reward tokens then may be deposited to other liquidity pools to earn rewards there, and so on.

According to CoinMarketCap data, the total locked value of liquidity pools in yield farming projects exceeded $13 billion as of 10th March 2021 (note that the statistics are constantly updated)[6].

Yield farming requires liquidity providers (LPs) and liquidity pools. To become an LP, all you have to do is to add your funds to a liquidity pool (smart contract), which is responsible for powering a marketplace where users carry out several procedures with their tokens, including borrowing, lending, and exchanging. Once you've locked up your funds in the pool, you'll get fees that have been generated from the underlying DeFi platform or reward tokens. In addition, some protocols can even provide payouts in the form of multiple cryptocurrencies, allowing users to diversify their assets and lock those cryptocurrencies into other protocols to maximize yields.

Yield farming is closely related to a model called automated market maker (AMM). It typically involves (LPs) and liquidity pools. LPs deposit funds into a liquidity pool. This pool powers a marketplace where users can lend, borrow, or exchange tokens. The usage of these platforms incurs fees, which are then paid out to liquidity providers according to their share of the liquidity pool. This is the foundation of how an AMM works.

Typically, the estimated yield farming returns are calculated annualized. This estimates the returns that you could expect over the course of a year. Some commonly used metrics are Annual Percentage Rate (APR) and Annual Percentage Yield (APY). The difference between them is that APR doesn't take into account the effect of compounding, while APY does. Compounding, in this case, means directly reinvesting profits to generate more returns. However, be aware that APR and APY may be used interchangeably.

6 https://pixelplex.io/blog/what-is-yield-farming/

Yield Farming Liquidity Pools

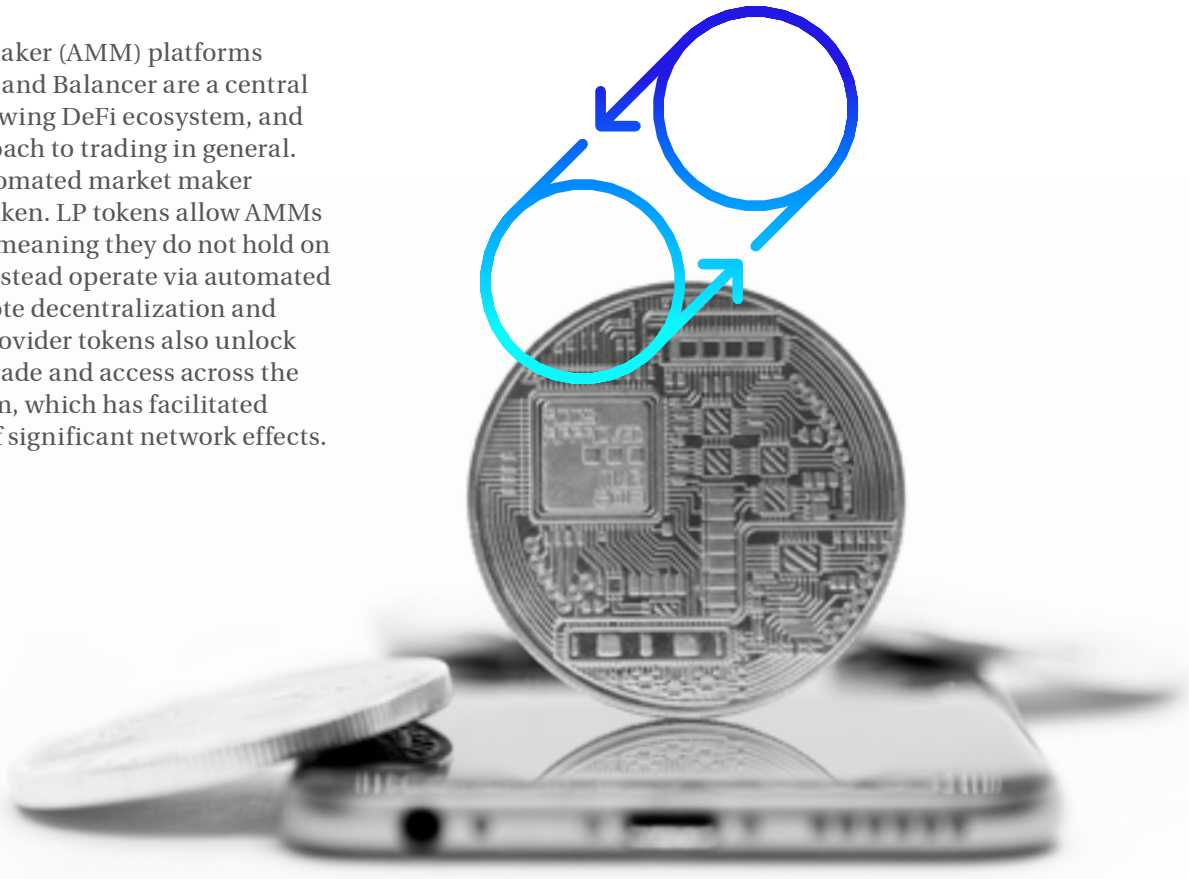
Uniswap and Balancer are the two largest liquidity pools in DeFi, offering LPs with fees as a reward for adding their assets to a pool. Liquidity pools are configured between two assets in a 50-50 ratio in Uniswap. Balancer allows for up to eight assets in a liquidity pool with custom allocations across assets. Every time someone takes a trade through a liquidity pool, LPs that contributed to that pool earn a fee for helping to facilitate this.

Unlike Uniswap and Balancer which function as DEXs, DeFi platforms like Compound, Curve Finance, Aave, and Badger DAO work by letting users deposit cryptocurrency, lending them out to borrowers with interest via smart contracts, then paying yields derived from the interest back to lenders. When you deposit to a DeFi protocol's liquidity pool as a lender, you'll typically earn more of the token you deposited and a reward token (usually the native asset of the platform you're using). So, if you lend on Compound, you'll earn COMP.

Automated market maker (AMM) platforms like Uniswap, Curve, and Balancer are a central aspect of the fast-growing DeFi ecosystem, and present a novel approach to trading in general. A key function of automated market maker platforms is the LP token. LP tokens allow AMMs to be non-custodial, meaning they do not hold on to your tokens, but instead operate via automated functions that promote decentralization and fairness. Liquidity provider tokens also unlock new layers of token trade and access across the entire DeFi ecosystem, which has facilitated growth in the form of significant network effects.

The non-custodial feature of AMM platforms is key to being part of the decentralised finance ecosystem. On AMM platforms, you remain in control of your assets by receiving LP tokens in return for providing tokens like ether (ETH) to the crypto liquidity pool, which is managed by code and not by human operation. LP tokens represent a crypto liquidity provider's share of a pool, and the crypto liquidity provider remains entirely in control of the token.

For example, if you contribute $10 USD worth of assets to a Balancer pool that has a total worth of $100, you would receive 10% of that pool's LP tokens. You receive 10% of the LP tokens because you own 10% of the crypto liquidity pool. The LP tokens become your claim to your share of the pool's assets. Holding these LP tokens allows you total control over when you withdraw your share of the pool without interference from anyone — even the Balancer platform. And since LP tokens are ERC-20 tokens, they can be transferred, exchanged, and even staked on other protocols[7].



7 https://www.gemini.com/cryptopedia/liquidity-provider-amm-tokens

YIELD FARMING POOLS

Some of the common yield farming pools are as follows:

1. Compound Finance

Compound is an algorithmic money market that allows users to lend and borrow assets. Anyone with an Ethereum wallet can supply assets to Compound's liquidity pool and earn rewards that immediately begin compounding. The rates are adjusted algorithmically based on supply and demand[8].

2. MakerDAO

Maker is a decentralised credit platform that supports the creation of DAI, a stablecoin algorithmically pegged to the value of USD. Anyone can open a Maker Vault where they lock collateral assets, such as ETH, BAT, USDC, or WBTC. They can generate DAI as debt against this collateral that they locked. This debt incurs interest over time called the stability fee – the rate of which is set by MKR token holders. Yield farmers may use Maker to mint DAI to use in yield farming strategies.

3. Synthetix

Synthetix is a synthetic asset protocol. It allows anyone to lock up (stake) Synthetix Network Token (SNX) or ETH as collateral and mint synthetic assets against it. The synthetic asset can facilitate anything that has a reliable price feed. This allows virtually any financial asset to be added to the Synthetix platform. Synthetix may allow all sorts of assets to be used for yield farming in the future.

4. Aave

Aave is a decentralised protocol for lending and borrowing. Interest rates are adjusted algorithmically, based on current market conditions. Lenders get "aTokens" in return for their funds. These tokens immediately start earning and compounding interest upon depositing. Aave also allows other more advanced functionality, such as flash loans. As a decentralised lending and borrowing protocol, Aave is heavily used by yield farmers.

5. Uniswap

Uniswap is a DEX protocol that allows for trustless token swaps. Liquidity providers deposit an equivalent value of two tokens to create a market. Traders can then trade against that liquidity pool. In return for supplying liquidity, liquidity providers earn fees from trades that happen in their pool. Uniswap has been one of the most popular platforms for trustless token swaps due to its frictionless nature.

6. Curve Finance

Curve Finance is a DEX protocol specifically designed for efficient stablecoin swaps. Unlike other similar protocols like Uniswap, Curve allows users to make high-value stablecoin swaps with relatively low slippage.

7. Balancer

Balancer is a liquidity protocol similar to Uniswap and Curve. However, the key difference is that it allows for custom token allocations in a liquidity pool. This allows liquidity providers to create custom Balancer pools instead of the 50/50 allocation required by Uniswap. Just like with Uniswap, LPs earn fees for the trades that happen in their liquidity pool. Due to the flexibility it brings to liquidity pool creation, Balancer is an important innovation for yield farming strategies.

8. Yearn.finance

Yearn.finance is a decentralised ecosystem of aggregators for lending services such as Aave, Compound, and others. It aims to optimise token lending by algorithmically finding the most profitable lending services. Funds are converted to yTokens upon depositing that periodically rebalance to maximize profit.

8 https://academy.binance.com/en/articles/what-is-yield-farming-in-decentralized-finance-defi

UNISWAP CASE STUDY

Uniswap is considered as an automated market maker (AMM). An AMM is just a fancy way of describing an exchange that crowdsources its liquidity[9]. Uniswap incentivises liquidity providers to deposit into its pools by paying rewards from transactions using those pools. So, whereas a centralised exchange like Coinbase makes money by keeping exchange fees for itself as profit, Uniswap and other DeFi protocols pay those fees out to users as rewards.

What Compound and Uniswap have in common is this: both rely on liquidity pools as a source of funds for their respective protocols. Uniswap needs liquidity providers to deposit the assets being exchanged by users, and Compound needs liquidity providers to deposit assets being borrowed by users.

Uniswap incentivises liquidity providers by sharing transaction fees between LP's, while Compound incentivizes liquidity providers by paying lenders a floating annual percentage yield rate.

Uniswap is a DeFi protocol built on Ethereum for swapping tokens. DEX solve a multitude of problems that plague centralized exchanges like security breaches and high fees but they struggle with liquidity. Uniswap was created to end the issue of liquidity around DEXs.

Uniswap is an automated liquidity protocol that doesn't require an order book to make trades. It relies on liquidity providers and a decentralised pricing mechanism called the Constant Product Market Maker — which is a variant of the AMM that powers yield farming. AMMs are smart contracts that hold the pool set aside by liquidity providers for traders. Anyone can list an ERC-20 token on Uniswap. Each token has a smart contract, but not every token has a liquidity pool.

Anyone can provide liquidity to Uniswap by depositing funds into Uniswap's liquidity pool. The person depositing the assets is known as a Liquidity Provider (LP). Further, traders use Uniswap to buy or sell crypto tokens, and in exchange for that, Uniswap charges a trading fee. Uniswap distributes this trading fee to its LPs as a reward for providing liquidity to the platform[10]. LPs can create a liquidity pool by depositing an equivalent value of two tokens, say ETH and USDT. Uniswap uses a constant equation: x * y = k to determine pricing. The equation seeks to balance out the value of tokens and their swaps based on how much people want to trade them.

In the equation above, let's look at a simple ETH/USDT pool. Let's represent x with the ETH section of the pool and y represent USDT, while k is a constant value that will never change. k represents the total liquidity in the pool. For example, if Ben decides to buy 1 ETH for 500 USDT. What happens in Uniswap is that the supply of ETH falls, while the supply of USDT goes up and the price of ETH rises since there's less ETH in the pool after the trade and k must always be constant.

The simplest version of a DeFi liquidity pool holds two tokens in a smart contract to form a trading pair. Let's use Ether (ETH) and USD Coin (USDC) as an example, and to make it simple, the price of ETH can be equal to 1,000 USDC. Liquidity providers contribute an equal value of ETH and USDC to the pool, so someone depositing 1 ETH would have to match it with 1,000 USDC. The liquidity in the pool means that when someone wants to trade ETH for USDC, they can do so based on the funds deposited, rather than waiting for a counterparty to come along to match their trade.

Source: coinsutra.com

9 https://blog.shrimpy.io/blog/what-is-yield-farming-defi-basics-explained
10 https://coinsutra.com/liquidity-pools-guide/

Liquidity providers are incentivised for their contribution with rewards. When they make a deposit, they receive a new token representing their stake, called a pool token. In this example, the pool token would be USDCETH. The share of trading fees paid by users who use the pool to swap tokens is distributed automatically to all liquidity providers proportionate to their stake size. So if the trading fees for the USDC-ETH pool are 0.3% and a liquidity provider has contributed 10% of the pool, they're entitled to 10% of 0.3% of the total value of all trades. When a user wants to withdraw their stake in the liquidity pool, they burn their pool tokens and can withdraw their stake.

Liquidity mining originates from two very important concepts in the cryptocurrency world, namely liquidity and mining. The so-called liquidity, we refer to the availability of tokens in a given platform, which is essential for the creation, growth and expansion of the DeFi market. As for mining, we refer to PoW-based technology. By providing computing power, you can obtain new coins just minted by the algorithm. Although these two concepts are far apart, they can be combined with each other, which is undoubtedly conducive to the vigorous development of some DeFi projects[11].

11 https://blockcast.cc/news/liquidity-mining-yield-farming-understand-the-difference-between-the-two/

SHARIA ANALYSIS OF YIELD FARMING

Liquidity Pools

To understand the essence of yield farming, it is necessary to understand liquidity pools from a Sharia perspective. A liquidity pool is simply a smart contract. A »smart contract« is simply a program that runs on the Ethereum blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain.

Smart contracts work by following simple “if/when…then…” statements that are written into code on a blockchain. A network of computers executes the actions when predetermined conditions have been met and verified. These actions could include releasing funds to the appropriate parties, registering a vehicle, sending notifications, or issuing a ticket. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the results.

Within a smart contract, there can be as many stipulations as needed to satisfy the participants that the task will be completed to satisfactory. To establish the terms, participants must determine how transactions and their data are represented on the blockchain, agree on the “if/when...then…” rules that govern those transactions, explore all possible exceptions, and define a framework for resolving disputes. In summary, smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met.

Smart contracts are a type of Ethereum account. This means they have a balance and they can send transactions over the network. However, they're not controlled by a user, instead they are deployed to the network and run as programmed. User accounts can then interact with a smart contract by submitting transactions that execute a function defined on the smart contract. Smart contracts can define rules, like a regular contract, and automatically enforce them via the code.

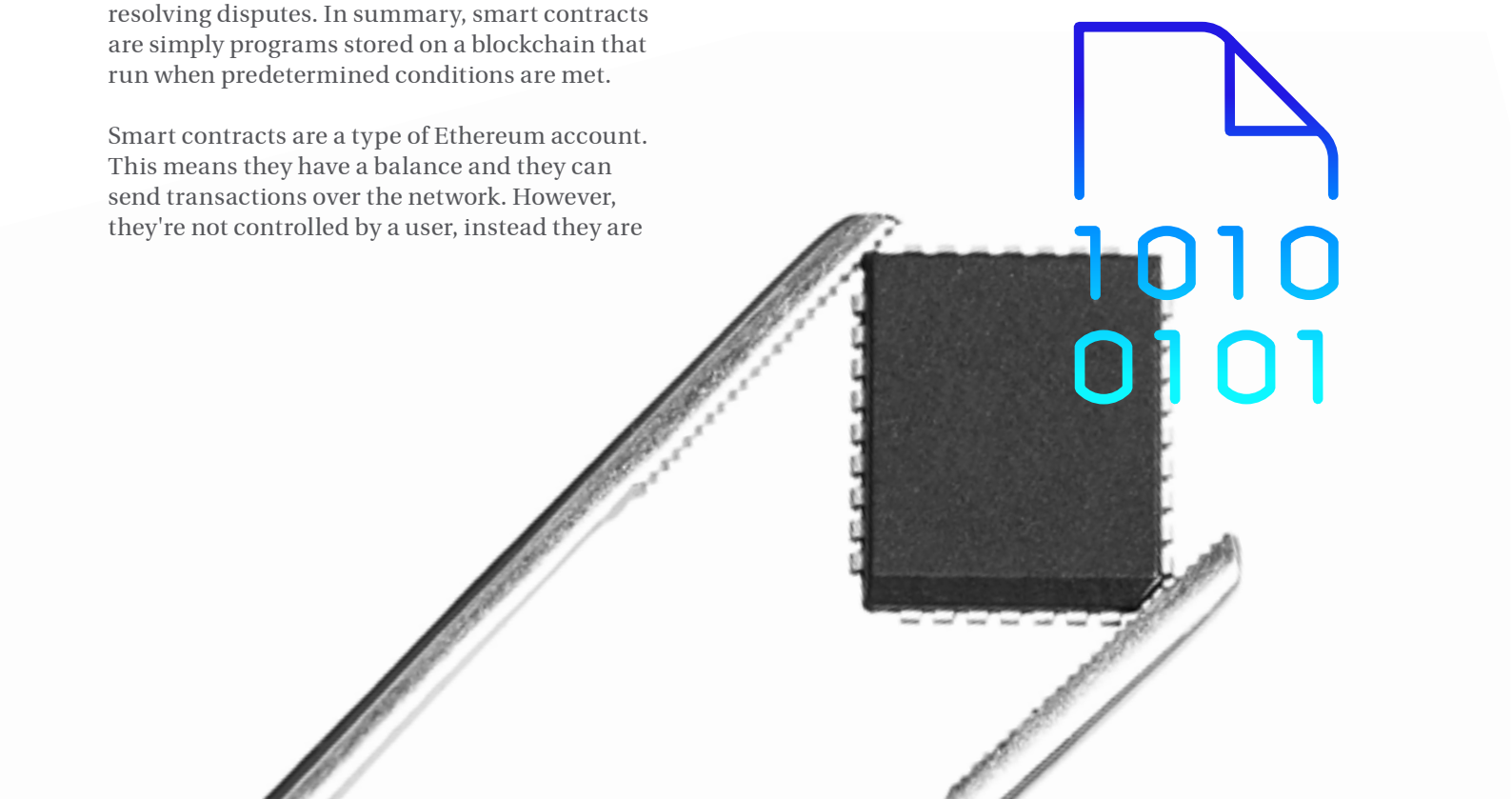
An Ethereum account is an entity with an ether (ETH) balance that can send transactions on Ethereum. Accounts can be user-controlled or deployed as smart contracts.

Ethereum has two account types:
- Externally-owned – controlled by anyone with the private keys
- Contract – a smart contract deployed to the network, controlled by code. Learn about smart contracts

Both account types have the ability to:
- Receive, hold and send ETH and tokens
- Interact with deployed smart contracts

Key differences between externally owned accounts and smart contracts are as follows:

Externally-owned
- Creating an account costs nothing
- Can initiate transactions
- Transactions between externally-owned accounts can only be ETH transfers



Smart Contract

- Creating a contract has a cost because you're using network storage
- Can only send transactions in response to receiving a transaction
- Transactions from an external account to a contract account can trigger code which can execute many different actions, such as transferring tokens or even creating a new contract

Ethereum accounts have four fields:

- **Nonce** – a counter that indicates the number of transactions sent from the account. This ensures transactions are only processed once. In a contract account, this number represents the number of contracts created by the account

- **Balance** – the number of wei owned by this address. Wei is a denomination of ETH and there are 1e+18 wei per ETH.

- **CodeHash** – this hash refers to the code of an account on the Ethereum virtual machine (EVM). Contract accounts have code fragments programmed in that can perform different operations. This EVM code gets executed if the account gets a message call. It cannot be changed unlike the other account fields. All such code fragments are contained in the state database under their corresponding hashes for later retrieval. This hash value is known as a codeHash. For externally owned accounts, the codeHash field is the hash of an empty string.

- **StorageRoot** – Sometimes known as a storage hash. A 256-bit hash of the root node of a Merkle Patricia trie that encodes the storage contents of the account (a mapping between 256-bit integer values), encoded into the trie as a mapping from the Keccak 256-bit hash of the 256-bit integer keys to the RLP-encoded 256-bit integer values. This trie encodes the hash of the storage contents of this account and is empty by default.

If a balance is being forwarded to an account on Ethereum which is what the smart contract is, then this creates a joint account of tokens. A joint account of tokens is created since the tokens are fungibles; one token cannot be distinguished from the other whilst in the account. In reality, these tokens are simply numbers or a balance assigned to a particular account. From a Sharia perspective, this creates a *Shirkat al-Milk* (joint ownership) in the pool. This will be a *Shirkat in an 'Ayn* (specific joint pool), as the account is specific and has a specific code. Every depositor or Liquidity Provider becomes a *Sharik* (shareholder) in the account. Since the nature of the assets in the account are fungibles, one token balance cannot be distinguished from the other. Each sharik simply has a share in this specific account. As such, each Sharik has a share of a percentage or amount of balance in the smart contract. That share can be retrieved from any asset within the account, as it is not possible to distinguish (*Tamyiz*) between the different assets as they are all homogenous and fungibles. Therefore, a liquidity pool creates a *Shirkat al-Milk.*

For the purpose of the Sharia analysis, yield farming can be divided into two operations in light of this paper. However, there could be other methods of yield farming beyond the two below:

1. Lending platforms
2. Decentralised exchanges

1. Lending platforms

DeFi lending platforms such as Compound, Aave and Maker have similar underpinning principles. At their core, they are lending protocols. To understand how they work, let us look at Compound Finance. Compound Finance is a DeFi lending protocol. In more technical terms, it's an algorithmic money market protocol. You could think of it as an open marketplace for money. It lets users deposit cryptocurrencies and earn interest, or borrow other crypto-assets against them. It uses smart contracts that automate the storage and management of the capital being added to the platform[12].

On Compound, suppliers and borrowers don't have to negotiate the terms as they would in a more traditional setting. Both sides interact directly with the protocol, which handles the collateral and interest rates. No counterparties hold funds, as the assets are held in smart contracts called liquidity pools. Like most DeFi protocols, Compound is a system of openly accessible smart contracts built on Ethereum[13].

Positions (supplied assets) in Compound are tracked in tokens called cTokens, Compound's native tokens. cTokens are ERC-20 tokens that represent claims to a portion of an asset pool in Compound. Compound tokens or cTokens are simply ERC20 tokens representing a user's funds deposited in Compound. By putting ETH or another ERC20 like USDC in the protocol, users get an equivalent amount of cTokens. For example, locking up USDC in the protocol generates cUSD–tokens which automatically earn interest for you. At any time, you can redeem your cUSDC for normal USDC plus interest paid in USDC. If you deposit multiple coins, they'll each earn interest based on their individual interest rates. In other words, cDAI will earn the cDAI interest rate, and cETH will earn the cETH interest rate.

Lending on Compound means unlocking the asset that you wish to supply liquidity for, and sign a transaction through your wallet to start supplying capital. The assets are instantly added to the pool, and start earning interest in real-time. This is when the assets are converted to cTokens. Borrowing is a bit more complicated. First, users deposit funds (collateral) to cover their loan. In return, they earn "Borrowing Power," which is required to borrow on Compound. Every asset that is available for supply will add a different amount of Borrowing Power. Users can then borrow according to how much Borrowing Power they have.

The COMP token has a governance feature to it. The token entitles token holders to fees and governance rights over the protocol. As such, token holders can make changes to the protocol through improvement proposals and on-chain voting. Each token represents one vote, and holders can vote on proposals with their token holdings. In the future, the protocol may be completely governed by COMP token holders.

Some of the most common issues that COMP holders vote on include:
- What cToken markets to list.
- Interest rates and required collateralization for each asset.
- What blockchain oracles to use.

Since the balance of a liquidity pool is being borrowed and earning interest for business purposes, the liquidity pool in Compound is Shirkat al-Aqd (joint business venture). The assets held in the liquidity pool are lent on interest and the pool earns income through borrowing. The returns that are generated are though lending contracts. The balance of crypto is lent to others. At any time, a liquidity provider can redeem their cUSDC for normal USDC plus interest paid in USDC.

12 https://academy.binance.com/en/articles/what-is-compound-finance-in-defi#how-does-compound-finance-work
13 https://decrypt.co/resources/compound-defi-ethereum-explained-guide-how-to

Since the yield in yield farming on lending platforms is created through lending contracts, the yield is *Riba*. In Islam, a loan *(Qard)* is a gratuitous contract and lending to people in need is a commendable practice. Both the Qur'an and Sunnah promise reward to a lender who provides a loan to a person in need. The fact that the Shari'ah prohibits the lender to derive any conditional benefit from the loan further emphasises its gratuitous nature. It also implies that a loan contract that is designed for profit should not be used; it is a form of social assistance to keep the community together through hard times. Thus, any profit or additional return in lieu of the loan is impermissible and non-Shari'ah-compliant. Interest is explicitly prohibited in the Qur'an and the Sunnah. We are told:

'Do you who believe! Fear God, and give up what remains of your demand for usury, if you are indeed believers. If you do it not, take notice of war from God and His Messenger. But if you turn back, you shall have your capital sums: Deal not unjustly, and you shall not be dealt with unjustly'

(al-Qur'an, 2:278-279).

A famous juristic maxim states: "Any loan which draws an increment is *Riba*" (Ibn Abi Shaybah).

Riba is more than just simple interest and compound interest; *Riba* is any unjustified excess in a bilateral contract which is stipulated for one of the two transacting parties and is without consideration. Scholars outline two types of *Riba*:

1) *Riba al-Nasi'ah* is the advantage and excess gained without consideration by deferring delivery of any homogenous counter exchange. This excess manifests upon default or delay in payment where time is factored as a consideration.

2) *Riba al-Fadhl* is a contractually agreed excess in units without any consideration in an exchange of homogeneous goods.

Shari'ah has not considered money to be a commodity, but a medium of exchange. When money of the same genus is exchanged, it must be on spot and in equal quantity. Exchanging different amounts at different times brings into effect both forms of Riba: *Riba al-Nasi`ah* and *Riba al-Fadhl*.

Jabir stated that God's Messenger (peace be upon him) cursed the receiver of interest and its payer, as well as the one who records it and the two witnesses; he said, "They are all equal." [Abu Dawud]

2. Decentralised exchanges

As discussed earlier, LPs provide liquidity to a smart contract which is in essence an account. The account is the 'pool' which has rules and protocols by virtue of the smart contract.

The simplest version of a DeFi liquidity pool holds two tokens in a smart contract to form a trading pair, other versions differ. But the underlying Sharia principle would be identical. In a two-token smart contract trading pair, let's use Ether (ETH) and USD Coin (USDC) as an example. Liquidity providers contribute an equal value of ETH and USDC to the pool, so someone depositing 1 ETH would have to match it with 1,000 USDC.

From a Sharia perspective, the following areas are key:

1. Liquidity mining

Any liquidity provider's token pairs in the liquidity pool can be swapped by other traders. The liquidity provider simply has a claim to an amount of tokens initially locked in by the liquidity provider, which is evidenced by the LP token. Users of the DEX basically are trading against the LP, anybody can swap tokens at any point of time.

From a Sharia perspective, since the tokens in the pool are being swapped by other traders, this pool is therefore trading with other traders. What is crucial is the relationship between the pool and the Liquidity Providers. As long as the Liquidity Providers own a percentage of the pool, then the Pool will simply be a *Shirkat al-Milk* (jointly-owned pool of assets) formed for *Shirkat al-Aqd* (business partnership) purposes. In many liquidity pools, Liquidity Providers receive LP tokens as the evidence for their share in the underlying liquidity pool. For example, if you contribute $10 USD worth of assets to a Balancer pool that has a total worth of $100, you would receive 10% of that pool's LP tokens. You receive 10% of the LP tokens because you own 10% of the crypto liquidity pool. The LP tokens become your claim to your share of the pool's assets. Holding these LP tokens allows you total control over when you withdraw your share of the pool without interference from anyone — even the Balancer platform. And since LP tokens are ERC-20 tokens, they can be transferred, exchanged, and even staked on other protocols[14].

For the liquidity mining to be Sharia compliant, the following conditions must be met:

1. The tokens must be Sharia compliant.

2. The return must not be guaranteed. The Liquidity Provider must have the ability to gain or lose their Liquidity.

3. The Liquidity Provider must get a percentage share of the liquidity pool and not a specific amount. If a specific amount of tokens are guaranteed and can be recalled later, then this would not be Sharia compliant. If a specific amount of tokens were always recallable by the Liquidity Provider, then this would mean that the Liquidity Provider does not own a percentage of the pool, rather a fixed amount. That would result in the Liquidity provider not becoming a shareholder in the liquidity pool, but rather a lender to the liquidity pool. As such, the Liquidity Provider would not be bearing risk of loss, and therefore this would be a form of *Qard* (loan) to the pool. As such, any earnings would be *Riba*.

2. The smart contract

Since the smart contract is effectively an account with algorithms, the developer of the smart contract will be an agent of the Liquidity Providers through the use of a smart contract coded with algorithms. If the developer is not a third party but the LP token holders themselves govern the smart contract, there will be no *Wakala* (agency). Rather the LP token holders themselves will be trading through the governance of the liquidity pool. Whether there is a *Wakala* or no *Wakala*, the smart contract, its protocols and the parties involved must be reviewed for Sharia compliance.

14 https://www.gemini.com/cryptopedia/liquidity-provider-amm-tokens#section-how-lp-tokens-enhanced-de-fi-liquidity

3. Transaction fees

LP providers share the fees which are accumulated during every swap through Uniswap, based on the proportion you have contributed to the LP. e.g. if you contributed 10% of the total LP, you shall receive 10% of the total fees. These fees are automatically contributed to the LP, so your total personal LP contribution keeps on increasing according to accumulated fees.

Users of the DEX basically are trading against the LP. Anybody can swap tokens at any point of time. Since you are swapping directly from your own Metamask/Ethereum wallet, your funds are always in your own control, as opposed to centralized exchanges in which the exchange controls your funds[15].

Since the traders are coming onto a platform and are being provided the space and platform to trade tokens, this permits a fee for the transaction to use the DEX. And since the decentralised exchange is primarily dependent on the LP providers, the LP providers are central to the infrastructure and operations of the DEX. Therefore, the transaction fees are permissible to earn for LP providers.

If the LP provider was guaranteed the same number of tokens back rather than a percentage, then the transaction fees would not be Sharia compliant as the pooling would be lending, and that would make the transaction fees *Riba*.

Whenever a trade occurs, a 0.3% fee is charged to the transaction sender. This fee is distributed pro-rata to all LPs in the pool upon completion of the trade.

All LPs must receive and should not be restricted to a few. Similarly, there should be no preference.

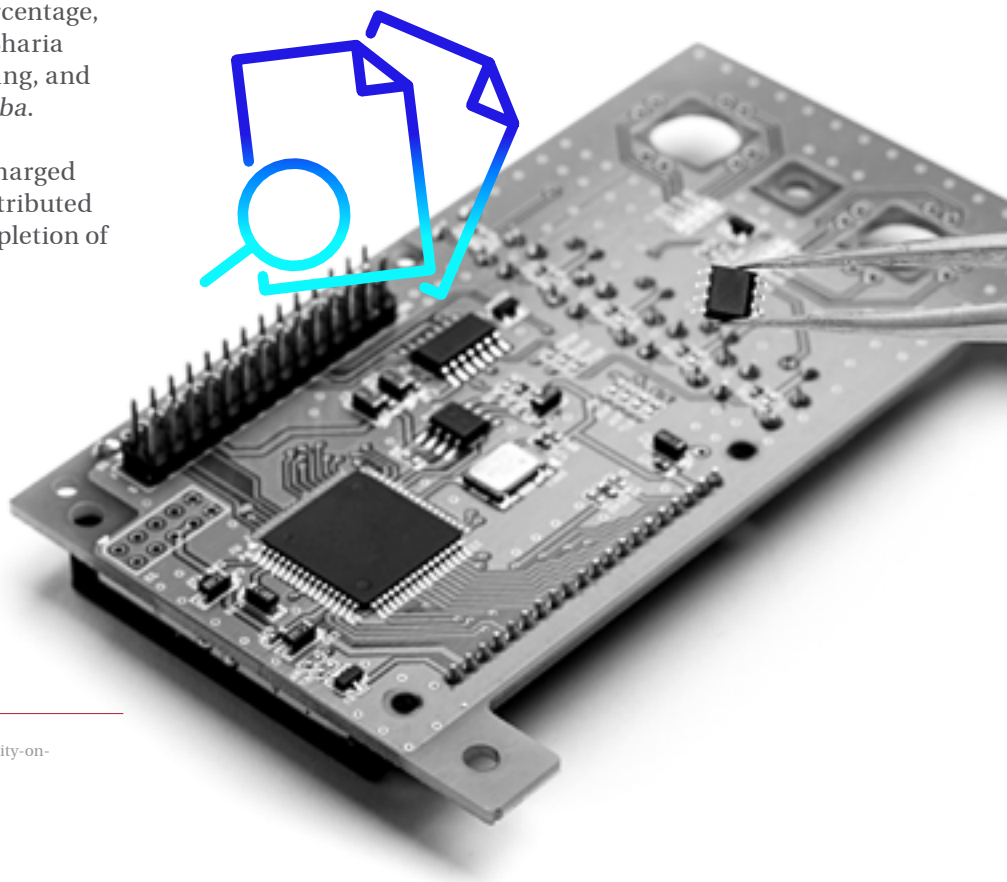
4. LP Tokens

Whenever liquidity is deposited into a pool, unique tokens known as liquidity pool tokens are minted and sent to the provider's address. These tokens represent a given liquidity provider's contribution to a pool.

To retrieve the underlying liquidity, plus any fees accrued, liquidity providers must “burn” their liquidity tokens, effectively exchanging them for their portion of the liquidity pool, plus the proportional fee allocation.

As LP tokens are themselves tradable assets, liquidity providers may sell, transfer, or otherwise use their LP tokens in any way they see fit.

From a Sharia compliance perspective, the LP tokens themselves must have a Sharia compliant utility. Only then will the owning of such tokens be Sharia compliant. Similarly, if any transaction, trading or investing of the LP token must also be reviewed for Sharia compliance. The structure and contracts used in any transaction, trade or investment must satisfy Sharia principles.



15 https://medium.com/phantasticphantasma/providing-liquidity-on-uniswap-ca4415f9534e

CONCLUSION

DeFi is short for “decentralised finance,” an umbrella term for a variety of financial applications in cryptocurrency or blockchain geared toward disrupting financial intermediaries. DeFi relies greatly on cryptography, blockchain, and smart contracts, with the latter being its main building block. The common applications of DeFi include monetary banking services, DEXs and lending platforms. Most DeFi infrastructure use liquidity pools to operate. A liquidity pool is a collection of funds locked in a smart contract. Liquidity pools are used to facilitate decentralised trading, lending, and many more functions. Yield farming is a common method of earning and generating an income through DeFi and liquidity pools. Yield farming involves LPs to pool tokens into the smart contract. The paper concludes that if tokens are provided to a lending platform, then such an activity is not Sharia compliant since interest-lending is involved. Yield farming that involves DEXs have the potential to be Sharia compliant depending on the underlying mechanisms of liquidity mining and the nature of the income. Any such DEX must be reviewed for Sharia compliance before any definitive view can be established for a DEX.

ABOUT SRB

Since our humble beginnings more than 13 years ago we've grown to include more than 100 companies across a host of industries, thousands of transactional programs, multi-disciplinary teams and a combined scholarly workforce of 35 Sharia Scholars from 19 countries. And we're not done yet: our Sharia Advisory and Sharia Audit services will continue to improve—serving local and international businesses to help them maintain and manage Shari'a compliance.

We've been preparing our clients for a new world in which Sharia Advisory rapidly becomes the currency of choice. From faster Certification programs, to direct Sharia Supervisory access, and perhaps most critically, navigating through the economic structures of clients offerings within a matter of days. We've have been working hard to help clients like you capitalize on opportunities in global Islamic financial markets.

Today, scores of institutions across nations, covering public and private businesses, commercial and corporate funds, Sukuks and Islamic equity markets, IPO's and Investment Banking Practices rely on us to run their companies, funds and transactions.

The future of Sharia Advisory and Audit is exciting and we are very lucky to be a part of this business!

ABOUT OUR PEOPLE

RESEARCH AUTHOR

MUFTI FARAZ ADAM

SHARIAH CONSULTANT AT SRB

> Completed his Islamic studies in the six-year Alimiyyah degree at Darul Uloom Leicester.
> Specialised in Islamic law and graduated as a Mufti in South Africa at Darul Iftaa Mahmudiyyah, Durban.
> Accredited with: Masters of Arts in Islamic Theology with specialisation in Juristic verdicts (Iftaa) and a Diploma in Islamic Finance.
> Completed a Master's Degree in Islamic Finance, Banking and Management at Newman University in 2017.

PEER REVIEWER

SHAIKH MUHAMMAD AHMAD SULTAN

SHARIAH ADVISOR AT SRB

> Over 10 years of experience as a Shari'a consultant and academic in various parts of Islamic finance.
> Worked predominantly in the financial services along with retail and investment banking and has expertise in corporate advisory and real-estate funds.
> He procured his Masters (A'alamiyah) in Fiqh and Usool ul Fiqh from Jami'ah Ahsan Ul Uloom and procured Bachelors in Islamic sciences from Jamia Dar-ul-Uloom.

PEER REVIEWER

MUFTI IBRAHIM ESSA

SHARIAH CONSULTANT AT SRB

> Teacher and Member Darulifta Jamiah Darululoom Karachi
> Chairman Shariah Board- Zarai Tarqiyati Bank Limited
> Member Shariah Board- Habib Metropolitan Bank Limited
> Shariah Advisor-EFU Takaful
> Shariah Advisor-Atrium Syndicate Lloyds of London

Disclaimer

This is a preliminary Shariah research and is by no means a definitive conclusion or fatwa on the aforementioned subject. This paper was written to develop knowledge and research on this complex subject from a Shariah perspective. We hope that this paper will prompt and engage global Islamic finance bodies, Shariah scholars and Muslim economists to analyze, comment and build upon the arguments expressed.
Additionally, the views, analysis and opinions expressed in this article are those of the author and Peer Reviewers and do not necessarily reflect the official policy or position of Shariyah Review Bureau or scholars on its network or other practicing scholars of the Islamic Industry. Moreover, the information contained or quoted in this paper are derived from public and private sources which we believe to be reliable and accurate but which, without further investigation, cannot be warranted as to their accuracy, completeness or correctness. Shariyah Review Bureau or its employee, are not liable for any error or inaccuracy contained herein, whether negligently caused or otherwise, or for loss or damage suffered by any person due to such error, omission or inaccuracy as a result of such supply. Shariyah Review Bureau will incur obligation of no kind arising from this document and will not be held responsible for any use of this document.