Defi Basics and Cross-Chain
(Draft October 30, 2021)

Disclaimer

Defi, yield farming and liquidity mining are the most risky ways to "invest" because one can lose 100% overnight for all types of reasons. Please read other articles such as Defi, Yield Farming and Liquidity Mining.

Background

Defi has evolved rapidly over the last ten months. According to DefiLlama at https://defillama.com/chains, total value locked (TVL) has increased from $30 billion in January 2021 to $260 billion in October 2021. In addition to BTC, ETH, BSC and Polygon, many new chains have marched into the top 100 market cap category. It is increasingly challenging for any beginner to understand cryptocurrencies and defi. I have hosted several webinars for friends, and decide to write down the content so I don't have to repeat.

Information Sites

The two largest sites about cryptos are:

1. Coinmarketcap: https://coinmarketcap.com/
2. Coingecko: https://www.coingecko.com/

Taking Coinmarketcap for example, it lists the top centralized exchanges (CEXs) and top coins/tokens. The largest spot exchange, Binance, is operating through a smaller entity Binance US in U.S., which has a much smaller list of markets. Coinbase is the 2nd largest, and is definitely not the cheapest. I have been using Bittrex for a long time, which is a U.S.-based firm. From time to time, I also use MEXC, as explained below.

Chains and Smart Contracts

Surprisingly there isn't a good list about blockchains. Blockchains are public databases jointly hosted by many participants, and cannot be stopped unless all participants stop service. In general, blockchains can be grouped as Ethereum-Virtual-Machine (EVM) compatible ones and others. As discussed below, we can use the same web wallet for all EVM-compatible chains.

Smart contracts are programs running on the blockchain and are immutable. Once they are deployed and verified, the program cannot be revised, although (a) the program may include an upgradable component and (b) variables in the smart contracts can be revised.

Top EVM-compatible chains include:

1. Ethereum (ETH)
2. Binance Smart Chain (BSC)
3. Avanlanche (AVAX)
4. Polygon (Matic), which is a layer-2 solution for ETH
5. Fantom (FTM)
6. Harmony (One)
7. Celo (Celo)
8. And many smaller ones coming every month, like Velas

Top non-EVM-compatible chains that can run smart contracts include:

1. Cardano (ADA)
2. Solana (SOL)
3. Polkadot (DOT) – a side chain Moonriver is EVM compatible
4. Terra (Luna)
5. Secret Network (SCRT)
6. Fusion (FSN)
7. And many others

Bitcoin is the largest chain but is not currently capable of running smart contract. The transaction fee is probably prohibitive anyway. The abbreviated name for each chain is typically the name of the coin. BSC is the only exception – the coin on BSC is BNB.

Secret Network and Fusion are way smaller chains than others named above; they are very unique chains:

1. On almost all chains, activities related to one address are public information and can be viewed on the block explorer. For example, https://www.polygonscan.com is the explorer for Polygon. Secret Network is the only chain that enables smart contracts but requires an encrypted viewing key to view token activities
2. Fusion focuses on cross-chain, as further explained later.

Coins and Tokens

Technically a coin is the currency of a particular blockchain, e.g., ETH is the only coin on the Ethereum chain; tokens are the assets on each blockchain. To execute a smart contract, we need to pay transaction fees or “gas,” which are measured in the coin driving each blockchain. The transaction fee is the product of two components:

- Gas limit, which is the amount of work we want the blockchain to run, estimated by the web wallet and is typically accurate. If the swap price has not changed but the transaction fails, we may need to manually modify the gas limit

- Gas price, which is the price per unit of work that we are willing to pay. Paying higher gas price than estimated may result in faster execution

Gas for each chain is significantly different: one transaction on ETH may cost hundreds of USD, while one transaction on Polygon or IOTX costs far less than one cent.

Coinmarketcap and Coingecko no longer separate coins from tokens, so this article will use the word “token” for both coins and tokens. We may be able to view the tokens by chain at some sites, such as: https://coinmarketcap.com/view/binance-smart-chain/.

Because most tokens are only issued on one chain (such as BTC), and are desired by other chains, a special version, wrapped token, is created. The token name and ticker, such as Ethereum (ETH), are not unique. A scammer may create a new worthless token called ETH and lists the token for sale.

- This is not an issue for CEXs, which only list established tokens
- For most decentralized exchanges (DEXs) such as https://www.uniswap.org, they build a default list of established tokens

When a token is not on the default list of a DEX, the only way to ensure we are buying the right token is to use the token address for that chain. For example, wrapped BTC on polygon has the address ending bfd9: https://polygonscan.com/token/0x1bfd67037b42cf73acf2047067bd4f2c47d9bfd6. If we input this address at https://quickswap.exchange/#/swap, it will automatically be translated to WBTC. Scammers like to spam their fake tokens with different addresses, so do not import the address at DEXs unless we obtain it from the official website. The same wrapped token always have different addresses on different chains. For example, the same WBTC on ETH has an address ending c599: https://etherscan.io/token/0x2260fac5e5542a773aa44fbcfedf7c193bc2c599

Stablecoins

Token price is subject to high volatility – it is common to see a 10% daily swing on major cryptos. There is a special group of tokens that aim to maintain the peg to something stable, such as USD. Those tokens have significantly different risks:

1. Over- or fully-collaterized stablecoins. Major stablecoins include:
    a. USDT. There are many articles that USDT may not be fully collaterized, but USDT has been very stable near $1
    b. BUSD, which is backed by $1 USD
    c. USDC, which is backed by $1 USD
    d. DAI, which has maintained peg for years

2. Partially-collaterized stablecoins. Risks get incrementally higher as we go down the categories. FRAX is an example with 90% collateral and has been stable for months. However, there is no guarantee that it will remain peg. UST/MAI/MIM are some other examples that are relatively smaller. Iron Finance tried to create one on Polygon and reached $1 billion minted tokens, which collapsed in 24 hours.
3. Algostablecoins. Those tokens are Ponzi schemes and mostly collapsed this year, such as Basis Cash. They are not true stablecoins.

Stablecoin is a key component of defi, because (a) the value is stable, and (b) the swap cost is much lower. While most DEXs charge 0.3% for swapping tokens, Curve Protocol exists on many chains and charge 0.04%, such as https://polygon.curve.fi/.

Moving Funds to Defi

To start investing in crypto, we need to convert our fiat money to crypto. A centralized exchange (CEX) receives deposits in USD and offers many market pairs to trade to cryptocurrencies. For us to participate in defi on any chain, those are the two critical items to obtain: gas and stablecoins. Once we have both on a chain, we can then use DEXs to swap into any other tokens, without using CEXs anymore.

Other than being a critical gateway between fiat and crypto, a CEX may have the following advantages:

1. Customer service if we run into problems – there is no customer service in defi
2. Withdrawal of gas to many chains. It is hard to get gas money on many chains, but CEXs may allow withdrawal. For example, I don't recall anyway to get SCRT without using a CEX.
3. Market depth. Some tokens such as FSN have very poor depth on DEXs: $1,000 buy may move the price up by 1%, compared to 0.1% on CEXs
4. Tokens listed are relatively safe. Comparatively, you can add liquidity for any token on a DEX

A CEX has the following disadvantage:

1. A CEX may have hundreds of markets, but DEXs have thousands. Some tokens can only be purchased at some DEXs, because many CEXs require a hefty fee to list a token
2. A CEX, especially smaller ones, may suspend withdrawal or even disappear. In defi, we have 100% of control of the crypto

I have been using Bittrex since 2018, but unfortunately Bittrex only support the ETH chain, which has high transaction costs. If we must use the ETH chain, Bittrex is a good choice. Otherwise https://www.mexc.com seems to cover much more chains and

markets. For example, withdrawing Matic, the gas for Polygon, to Polygon costs 1 Matic, or $2. Withdrawing Matic to ETH costs about $100. For the example below, we will avoid ETH and use Polygon as an example. Once we have Matic for gas and USDT on Mexc, we are ready to withdraw to Polygon.

Wallet

To withdraw funds from CEX to an address that we control, we need a web wallet. https://metamask.io/ is the most popular web wallet for all EVM-compatible chains and there is no reason to use anything else. To start, it will ask you to create a seed phrase of pass-phrase.

The top safety rule is: never give your seed phrase to anyone or any website.

When we create a web wallet using tools such as MetaMask or Phantom, the seed phase is not the account number – it is the money itself. For every month into defi, we would see dozens of people faking as customer support personnel asking for the seed phase – do not do that in any circumstance. Some legitimate sites may ask for the seed phrase or key files – do not do that as a beginner.

The best practice is to write down a variation of your seed phrase on a piece of paper. For example, if your seed phrase includes apple and you like banana in real life, write down banana instead of apple. This ensures that no one else can restore your wallet and take away your funds.

We need to add Polygon to Metamask as an additional network. Please see guide at: https://medium.com/stakingbits/setting-up-metamask-for-polygon-matic-network-838058f6d844

Once a wallet is established, it can include unlimited numbers of addresses. If we own an address on one EVM-compatible chains, we own that address on all EVM-compatible chains. If we accidentally send fund to the right address on a wrong chain, we can still recover the fund.

Once we have the address, we are ready to withdraw funds from Mexc or other CEXs. The fund transfer on Polygon is extremely cheap – if you transfer between two addresses on Polygon, the cost is way less than one cent. Withdrawing from Mexc will cost $1 Matic, so we should always test a small withdrawal. If the small withdrawal is successful, we can proceed to withdraw the rest of the funds. Remember, we are withdrawing to Polygon, not ETH – there is a wrapped version of Matic on ETH.

Any Matic sent to an address will be shown in Metamask. If we don't see USDT withdrawn, we may need to manually add USDT to the token list. On https://www.polygonscan.com, if we search USDT, we will find the address is

0xc2132d05d31c914a87c6611c10748aeb04b58e8f, which we can put under “Import Tokens.”

Liquidity Mining and Token Approval

There are at least three ways to lose all money in defi:

1. Losing seed phrase
2. Sending funds to an address we don’t own
3. Allowing a contract to spend our tokens

The first two ways can be avoided if we exercise common sense, and the third way requires some education. Smart contracts cannot handle the coin on a chain, such as Matic on Polygon, so our Matic is always safe (the wrapped version, wmatic is not). Some smart contracts are malicious – if we approve them to use our tokens, it may drain all tokens we have, even if we do not take any action after approval.

How do we know a smart contract is safe or not? We may trust a website and related smart contract if the website has been operating for a long time without glitch. Even this is not reliable – Pancakeswap is the largest DEX on BSC, and had its DNS hijacked in early 2021. A better approach is to write down the contract address or make a note in Metamask. https://www.rugdoc.io is a very useful site. It compares a smart contract to the original version of the smart contract, to make sure there is no malicious content. As a random example, https://rugdoc.io/project/bouje-finance/ reviewed a contract ending D8B5, and concluded that contract is the same as the original version. A webpage can change its link to the smart contract. The contract we interact with is noted on the top right corner of the Metamask pop-up window.

Since the transaction cost on Polygon is so cheap, let us test a $20 liquidity mining.

1. Go to https://quickswap.exchange/#/swap
2. Click “Connect Wallet” on the top right corner and select Metamask. It will then ask you which address to connect and receive approval
3. Select USDT on top, and Matic at the bottom
4. Type in “10” on the top box. The box at the bottom will calculate the Matic you will receive, which is 4.863 today. Each Matic is then $2.056 USDT
5. Click “Approve USDT,” and a window will pop up, asking whether we allow Quickswap to spend our USDT token. This is an important step. If we don’t know about the contract, we should never grant unlimited approval to a smart contract. Instead, we should click “View full transaction details” to see whether the contract address is the right address, then click “Edit Permission” and type in “10” in “Custom Spending Limit”

    a. In the entire Polygon universe, I only grant infinite permission to Quickswap and 1inch, a price aggregator. 1Inch breaks down a large transaction into smaller pieces and find the best deal for us, but requires a VPN to use for the first time
6. There is no need to edit "Transaction Fee," but we can
    a. The gas limit is estimated by the website or Metamask, and typically does not need to be changed
    b. The gas price should be at least 30. Changing to a higher number will cost more, but may accelerate the transaction. https://polygonscan.com/gastracker provides the real-time gas price.
7. Within a few seconds, we will receive the approval. We can either refresh the page, or wait for the page to reflect, so "Swap" button is enable
8. The clog icon on the top right corner allows us to change some transaction settings. We can leave slippage at 0.5% or 1%
9. After clicking "Swap" button, we will receive some Matic, which is within 0.5% of 4.863 shown

Then we need to provide liquidity

10. We can go to https://quickswap.exchange/#/pool, and click "Add Liquidity"
11. Select "Matic" on the top and "USDT" at the bottom. Please see prior articles about liquidity mining risks.
12. Type "10" in the USDT box
13. If we grant only $10 permission above, we may need to grant permission again
14. Click "supply," which will trigger a pop-up window to confirm transaction. We will then receive some wmatic-usdt liquidity provider tokens (the LP tokens)

Then we can stake the LP tokens to earn reward:

15. We can go to https://quickswap.exchange/#/dual
16. Under the box of Matic-USDT, we can see "reward + fee APY: 98.12%"
17. Click "Deposit" and follow the instruction, until we see approximately $20 under "your liquidity deposit."
18. We can unstake, remove liquidity, and sell Matic to USDT any time.
19. To remove/revise token permissions, we can use https://debank.com/

Stuck Transactions

Occasionally a transaction can be stuck in Metamask activity section. It is primarily due to two reasons:

1. The RPC, which is used to broadcast your transaction, is congested. https://polygon-rpc.com is online since August 2021, so this is no longer a problem for Polygon, but could be an issue for other chains.
2. The chain is too congested. We can see how congested the chain is by looking at https://polygonscan.com/gastracker, and decide whether to increase gas price

Sometimes a transaction has gone through and can be checked at the block explorer, but shown as stuck in Metamask. In that case, try to send 0.1 Matic to ourselves. If that doesn't work, we may need to go Metamask – Settings – Advanced – Reset Accounts. It sounds scary, but will only empty the transaction history instead of erasing our account.

Bridging to BSC

As discussed above, we only need two things to use a new chain: gas for transaction fee, and funds. If we have access to Mexc, we can buy some BNB there and withdraw to Binance Smart Chain (BSC), which is the gas month. There may be three other ways to get gas money:

1. Some bridges may give you a little bit gas money, such as https://app.relaychain.com/. However, that may or may not be enough. If we bridge funds to Fantom using spookyswap bridge, that will provide some gas money too
2. We can check whether the network has a faucet. https://matic.supply/ may still be working.
3. We can find some admins in a telegram channel, send a small amount to him on other chains, and receive the gas money on another chain

We can also use CEXs to bridge fund from one chain to another, if we trust the CEX will not suspend or steal the fund. For example, we can withdraw USDT from Mexc to 10 different chains, with a daily limit of $300,000.

Both BSC and Polygon are major chains, so there are plenty of Defi bridges available:

1. https://anyswap.exchange/#/router is the largest cross-chain bridge projects, with several billions locked. However, all defi bridges are subject to capacity limit from time to time. Between the two boxes on this website, we will see USDC as

   Pool: MATIC Polygon: 60,048.13, BNBBSC: 1,988.06

   This means we can only bridge $60,048 USDC from BSC to polygon, or $1,988 USDC from Polygon to BSC. When the bridge has limited capacity, we have two choices: swap USDC into other stablecoins, or use other bridges. Fortunately, there are $7M USDT capacity into Polygon and $13M USDT capacity into BSC.

It is appalling that ANY only has a market cap of $200 million at $11-12, which is one of my holdings.

2. https://www.binance.org/en/bridge is the official bridge operated by Binance
3. https://app.allbridge.io/ is getting popular but I only used it once
4. https://www.xpollinate.io/ is one of the earliest bridges between Polygon and BSC. However, capacity is getting very limited nowadays
5. https://cbridge.celer.network/ belongs to Celer Network, which has a market cap exceeding $600M. This bridge is quite reliable
6. There are many official bridges that are less frequently used:
    a. BSC: https://www.binance.org/en/bridge
    b. Polygon: https://wallet.polygon.technology/bridge

1Inch is also the DEX aggregator on BSC. Alternatively, we can swap stablecoins at curve forks: https://ellipsis.finance/, https://nerve.fi, or https://app.acryptos.com/stableswap/.

Information on Selected Other Chains

AVAX

Transaction cost: $0.10

Main DEX: https://traderjoexyz.com/ it flipped Pangolin to become the main DEX. It is probably the only main DEX that issued a Ponzi memecoin – it is shameful.

Dex Aggregator: https://paraswap.io/#/?network=avalanche

Primary bridge: https://anyswap.exchange/#/router

Primary stablecoin: USDC, USDT, Dai

Primary stablecoin swap: https://avax.curve.fi/

Primary vault: https://app.beefy.finance works on almost all chains. https://yieldyak.com/ is another one

FTM

Transaction cost: $0.15

Main DEX: https://spookyswap.finance/swap

Dex Aggregator:

Primary bridge: https://anyswap.exchange/#/router

Primary stablecoin: USDC

Primary stablecoin swap: https://ftm.curve.fi/

Primary vault: https://app.beefy.finance

Moonriver

Transaction cost: $0.15

Main DEX: https://app.solarbeam.io

Dex Aggregator: Unknown to me

Primary bridge: https://anyswap.exchange/#/bridge

Primary stablecoin: USDC, Dai, BUSD, USDT

Primary stablecoin swap: unknown to me

Primary vault: unknown to me

Secret Network

Transaction cost: $1

Main DEX: https://app.secretswap.io

Dex Aggregator: unknown to me

Primary bridge: https://bridge.scrt.network/. This is the only bridge and breaks down from time to time.

Primary stablecoin: USDC. This network separates USDC bridged from ETH and BSC

Primary stablecoin swap: unknown to me

Primary vault: unknown to me

Fusion

Transaction cost: unknown

Main DEX: Chainge app

Dex Aggregator: unknown to me

Primary bridge: https://anyswap.exchange/#/router

Primary stablecoin: Unknown to me

Primary stablecoin swap: unknown to me

Primary vault: unknown to me

Safety Rules

As always, we should stick to the safety rules until we know what we are doing:

1. Never give seed phrase or private keys to anyone or any website
2. When we ask a question in a Telegram Channel, there is always scammers faking as customer support or admin to message you – no exceptions. That is why most admin names are “xxx – will never DM first”
3. Be helpful but not gullible. If someone asks for gas money in a Telegram but does not want to pay first, he is a scammer
4. Do not be greedy. When someone gives you a seed phrase, showing some money in the address, do not transfer gas to that wallet – a contract will grab it
5. If you find some unknown tokens in your wallet, ignore them. They are either scam tokens, trying to entice you to click some links on a website, or message tokens, such as token named like “GoBuyDoge”
6. Spread out funds over multiple addresses
7. Spread out funds over multiple tokens and projects
8. Do not grant token permission more than necessary – additional permission only takes seconds and costs one cent
9. Do not tell anyone your wallet address unless necessary
10. Make friends or email me questions; do not blindly trust strangers