# DeFi Talents

## Merged session material - Ignas Aničas

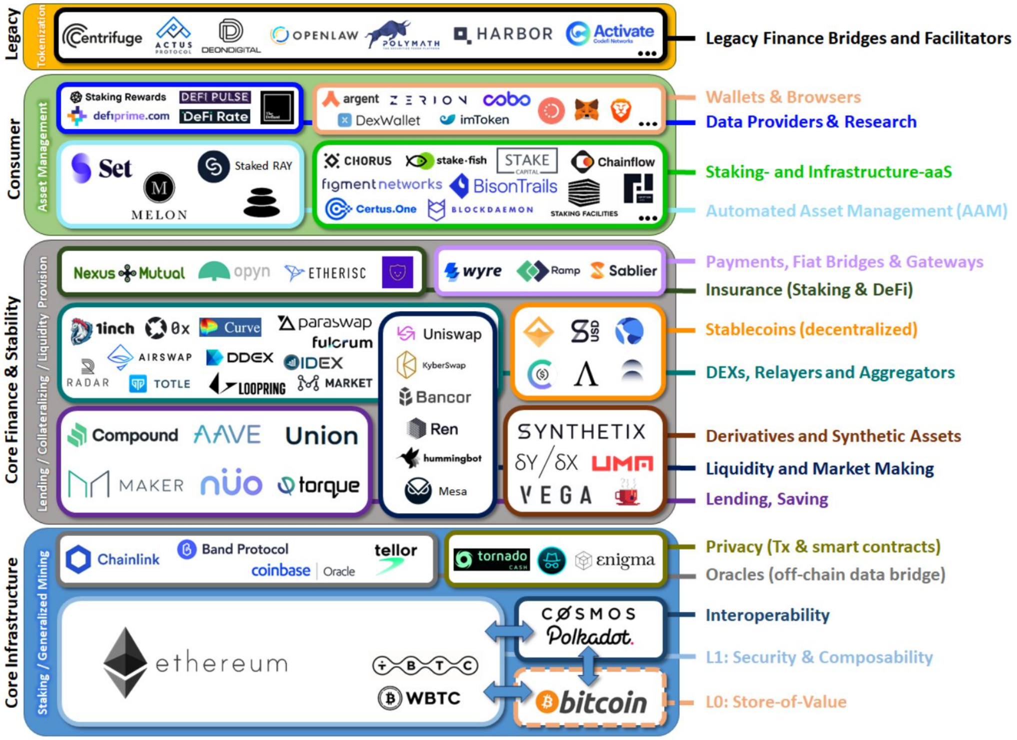
March, 2022

Powered by

BLOCKSIZE CAPITAL    Capgemini    LEDGER ENTERPRISE SOLUTIONS

# Visualizing the “DeFi stack”

Decentralized Finance (DeFi) Stack: Product & Application View



Legacy Finance Bridges and Facilitators

Wallets & Browsers

Data Providers & Research

Staking- and Infrastructure-aaS

Automated Asset Management (AAM)

Payments, Fiat Bridges & Gateways

Insurance (Staking & DeFi)

Stablecoins (decentralized)

DEXs, Relayers and Aggregators

Derivatives and Synthetic Assets

Liquidity and Market Making

Lending, Saving

Privacy (Tx & smart contracts)

Oracles (off-chain data bridge)

Interoperability

L1: Security & Composability

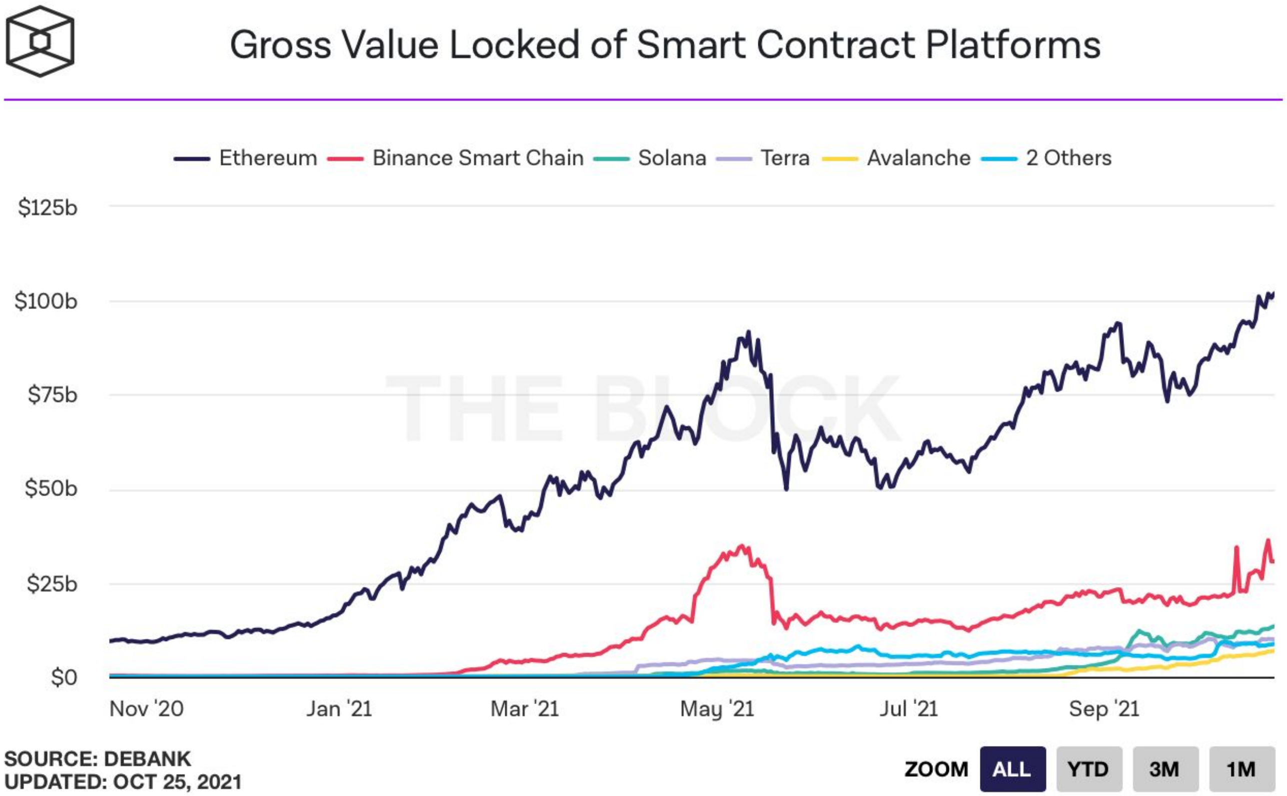
L0: Store-of-Value

Source: StakingRewards

- Ethereum ecosystem depicted on the left
- Rapidly changing and expanding:
    - Other blockchains (especially Solana)
    - DeFi 2.0 (Olympus DAO, FIRP protocols (Pendle, APWine), Rari Capital, Abracadabra)
    - L2 natives (e.g. Klima DAO on Polygon)

# Which blockchain are you most likely to use to participate in DeFi and why?

- Ethereum is the dominant blockchain / smart contract platform when it comes to DeFi.
- All the blue chip protocols have been launched on Ethereum with other platforms following along / trying to catch up.

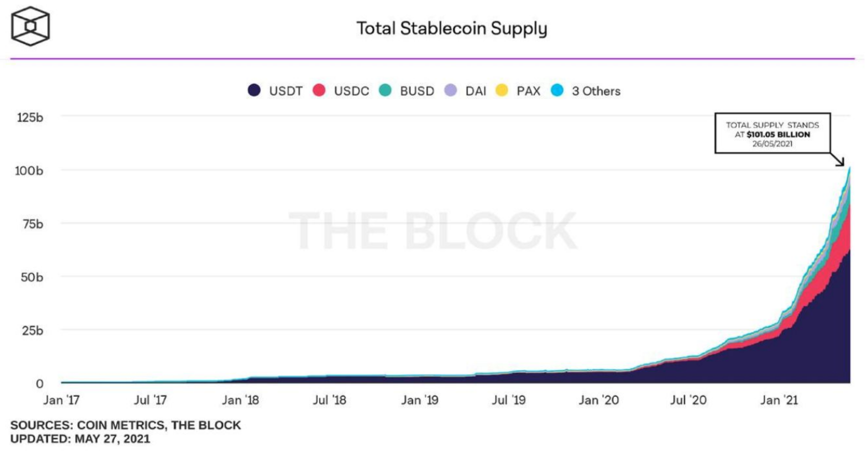


Gross Value Locked of Smart Contract Platforms

SOURCE: DEBANK
UPDATED: OCT 25, 2021

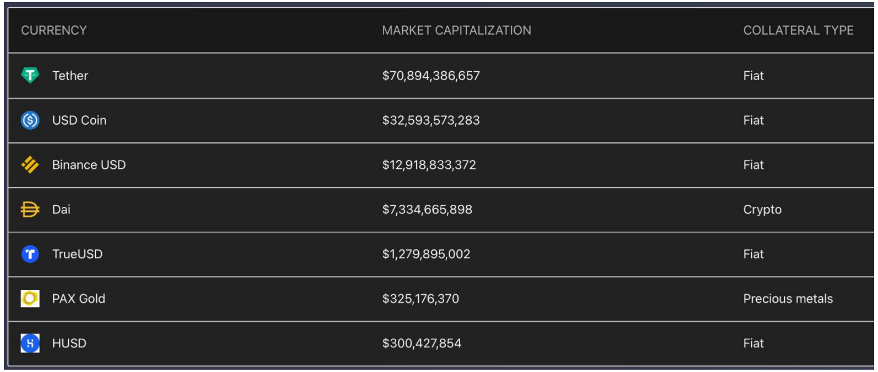
# Which stablecoin are you most likely to use to park your funds and why?

- Ethereum stablecoins dominate.
- Current stablecoin market is mostly using USD peg (crypto native stable store of value alternatives yet to emerge / gain significant market cap).
- Tether the largest one by market cap although questions regarding its collateral are being raised (https://www.bloomberg.com/news/features/2021-10-07/crypto-mystery-where-s-the-69-billion-backing-the-stablecoin-tether).
- Dai is the largest most crypto native / collateral backed alternative adhering to values / ethos of the ecosystem (governed by a DAO) with recent news of Societe Generale wishing to provide collateral (https://blockworks.co/major-french-bank-wants-to-back-the-dai-stablecoin-with-40m-in-bonds/).



TOTAL SUPPLY STANDS AT $101.05 BILLION 26/05/2021

SOURCES: COIN METRICS, THE BLOCK
UPDATED: MAY 27, 2021



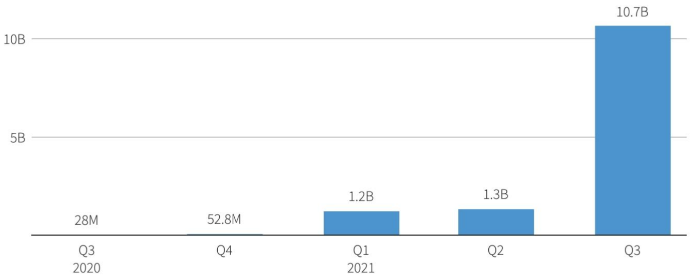
| CURRENCY | MARKET CAPITALIZATION | COLLATERAL TYPE |
|---|---|---|
| Tether | $70,894,386,657 | Fiat |
| USD Coin | $32,593,573,283 | Fiat |
| Binance USD | $12,918,833,372 | Fiat |
| Dai | $7,334,665,898 | Crypto |
| TrueUSD | $1,279,895,002 | Fiat |
| PAX Gold | $325,176,370 | Precious metals |
| HUSD | $300,427,854 | Fiat |

# What is the significance of NFTs? Use-cases beyond art?

- NFTs are becoming the ICOs of 2021.
- “Exotic” spins on the initial use cases being developed (rewarding holders with native ERC20 tokens, community co-creation (e.g. loot boxes), riddle based drops (e.g. neotokyo.codes)).
- Gaming use cases emerging fast as it allows users / players to own in game assets creating a whole new dynamic.
- Other use cases include identity, specific asset management (e.g. NFTs to represent ownership of real world assets - real estate, vehicles, art).

**NFT sales surge to $10.7 billion in Q3 - DappRadar**

Quarterly non-fungible token sales volumes across multiple blockchains, in U.S. dollars



# Most popular lending platforms

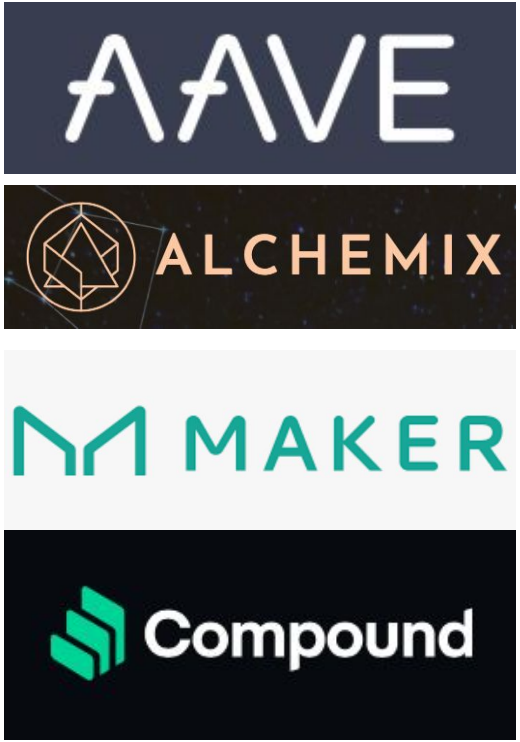
## Decentralized vs centralized - what is the difference?

### CeFi Platforms

CeFi or centralized finance platforms generally serve as intermediaries for the execution of the crypto lending process. A centralized cryptocurrency lending platform would take control of the assets of lenders and collateral of borrowers for the period of the loan. In addition, a centralized crypto lending platform would also require a KYC process, thereby excluding anonymity.

### DeFi Platforms

DeFi or decentralized finance platforms, on the other hand, present a decentralized approach for crypto lending. DeFi platforms use smart contracts for the execution of lending procedures. Most important of all, DeFi lending platforms could ensure complete automation of the lending process alongside the execution of the contract upon fulfillment of specific conditions.



# Compound V2 vs. Aave V2

| Protocol | Compound | AAVE |
|---|---|---|
| **Minimum collateralization ratio** | 133% | 133% |
| **Maximum LTV** | 75% | 75% |
| **Liquidation point (LTV)** | >75% | >80% |
| **Liquidation penalty** | 8% | 5% |
| **Flash loans** | No | Yes |
| **Available assets** | 17 | 31 |
| **Fixed borrowing rate** | No | Yes |
| **Current Dai APY (borrow)** | 4,18% | 2,89% (12.10% stable) |

**How are lending and borrowing interest rates determined?**

Interest rates are determined based on the supply and demand ratio of the asset in a specific market (Compound, AAVE).

**Is one better than the other?**

Both protocols have widespread adoption and have proven themselves from the security standpoint as well. AAVE seems to be positioning itself as a more innovative alternative (flash loans, fixed short-term borrowing rates, more assets) but both are good alternatives and the main decision factor when choosing among both protocols should be interest rates for a specific asset.

# Flash Loans

Flash loans are a new financial instrument which can be used to exploit inefficiencies across decentralized financial markets. No collateral is needed to get a flash loan (a  fee is paid in proportion of the flash loan size). They must be repaid within  the same block before a next one is mined.

Flash loans can be used for a variety of different things, including the following items:

- Arbitrage: Traders might earn by spotting price discrepancies across several different exchanges and exploiting them. Assume that the price of a pizza coin varies between two markets. Prices on Exchange A are one dollar and prices on Exchange B are two dollars. The user can utilize a flash loan and a separate smart contract to purchase 100 pizza coins at Exchange A for $100 and subsequently sell them at Exchange B for $200, generating $200 in revenue. Following that, the borrower pays back the loan and keeps the difference.
- Collateral swaps: Collateral swaps quickly replace another type of collateral for the collateral used to secure the user's loan.
- Reduced transaction fees: The transaction fees are reduced since flash loans combine several transactions into a single transaction in some cases. The cost of a transaction is deducted from the loan amount. Therefore rapid loans may result in lower fees.

Overall flash loans help to make decentralize financial markets more efficient, but are also being used as an instrument to exploit / hack various protocols with the aim of stealing funds or manipulating markets in a way which allows the attacker to exploit specific protocol users.

# Risks associated with DeFi Lending

- **Interest rate fluctuations.** Lending / borrowing rates can be volatile for less liquid assets or in case of “shallow markets” in certain protocols. This is both - protocol and specific asset risk. While certain protocols offer fixed rate borrowing (e.g. AAVE, Notional Finance) the rates are fixed for a comparatively short time (3-12 months) for limited number of assets (e.g. only DAI and USDC available for a 12 month fixed rate contract).
- **Protocol security.** While top lending / borrowing protocols have been around for a while, the sector as a whole is experiencing hacks / exploits quite frequently with potential for users to lose part or all of their funds (e.g. in October 2021 Cream Finance was hacked for over $130 million). This risk needs to be taken into account when making any decisions regarding protocol choice and caution should be exercised when it comes to newer, yet to be time tested / audited  protocols.
- **Asset price fluctuations - liquidation risk.** Lending / borrowing protocols usually offer up to 70% LTV ratio for borrowing. While such ratio should be fine for stablecoins (USDC, DAI, USDT), in case of providing more volatile assets as a collateral and taking out other assets as a loan (e.g. providing Ethereum and taking out USDC loan) increases the risk of liquidation drastically. Other users might also use leverage - provide collateral, take out maximum loan, provide it as a collateral, take out a loans against it and so forth. This can leverage up the position increasing APY while also increasing the risk of liquidation. Caution should be exercised and educated risk management approaches taken when dealing with volatile assets and using leverage in the above described way.

# DEXs risks

1. **For liquidity providers (LPs)**

   a. Impermanent loss. In case of a larger price move, LPs can experience impermanent loss due to constant product AMM mechanics. When one asset experiences large moves against the other asset in the pool, it attracts arbitrage traders who buy up the asset which appreciated in price or sell the asset which depreciated in price. This can result in situation where it could be more beneficial just to hold the cryptocurrencies in question rather than providing liquidity, but AMM protocols usually provide additional incentives in the form of governance tokens or similar to avoid situations where hodling is more attractive than providing liquidity.

   b. Protocol risk. DEXes can be hacked / exploited in various ways. There are countless stories with such cases therefore caution needs to be exercised when choosing specific protocols. The most well known and used ones have clear benefits while newer protocols might be providing better incentives for LPs while also bearing more protocol risk.

2. **For traders who engage in token swaps?**

   a. Slippage. This is basically the difference between expected and actual price at which swap was executed. It can, depending on the swap to available pool liquidity ratio, to a varying degree affect the price of assets being bought / sold. The larger the swap and the shallower the pool used for the swap, the more slippage will be experienced resulting in money lost as the assets would be swapped in a suboptimal price different to the one available elsewhere in the market.

   b. Potential MEV exploits - sandwich attacks, frontrunning, etc.

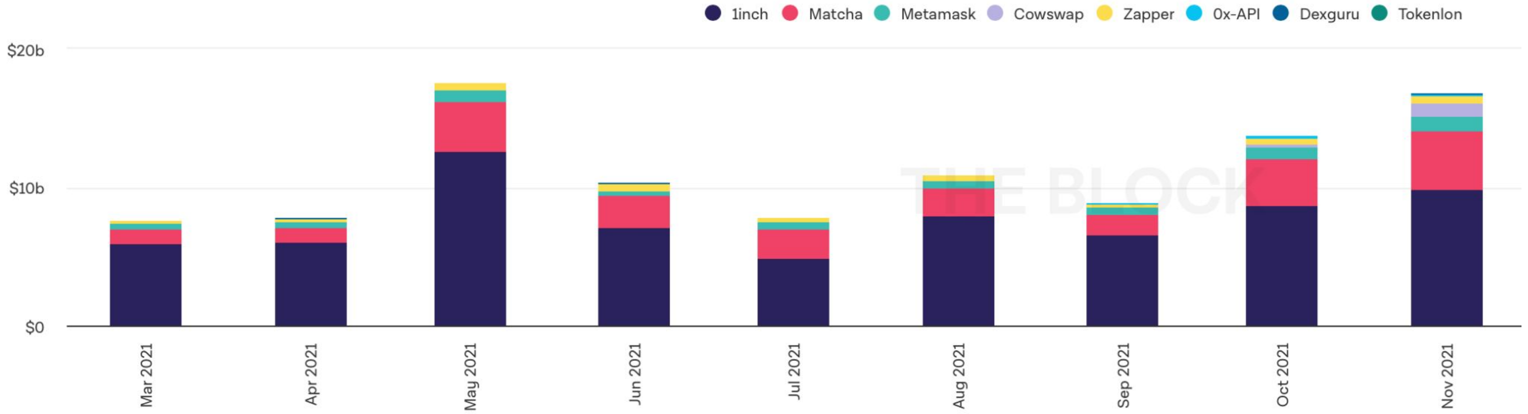
   c. Hacks / scams using fake front end or other attack vectors. Due to irreversible nature of blockchain transactions, hackers / scammers go out of their way to try and trick people into using fake websites / smart contracts and scam them out of their money.

# DEX aggregators

## 1. What are examples of DEX aggregators and what do they do?

DEX aggregators allow users to find the best available swap rates while also minimizing potential slippage and MEV exploits (in some cases). 1inch is currently dominating the market with runner up Matcha growing fast as well. Each of the well established market players have their own differentiating value offerings:

- 1inch, Matcha are most straightforward aggregators with limited additional functionality.
- Metamask is mainly a wallet provider having DEX aggregation function built in as a means to generate additional revenue.
- Zapper promotes itself mainly as a portfolio / asset tracker across web3 while also having DEX aggregator functionality.
- Dexguru in the meantime positions itself more like a trading, research and analytics hub.



Source: The Block (https://www.theblockcrypto.com/data/decentralized-finance/dex-non-custodial/dex-aggregator-trade-volume)

# Cross-chain DEXs?

1. **Are there any cross-chain DEXs existing or in development? How do/could they work?**

- Currently there are a limited number of cross-chain DEXes due to various aspects, mainly:
    - LP positions. Traditional concept is that a LP provides 2 tokens which originate from the same chain while cross-chain DEX model complicates this and makes it more difficult to maintain balanced pools throughout.
    - The need for a trusted party. Due to technical reasons it is not possible or very difficult to make a fully trustless cross-chain DEX due to the fact that one cannot write a smart contract which would span across several blockchains. This makes it technologically difficult to develop cross-chain DEXes with trust issues arising along the way as if one wants to automate it, back end code needs to be developed and run on some server (not on the blockchain) meaning someone would be able to make changes to it.
- Currently, most well known cross-chain DEX is AnySwap.
- At the current stage, most common solution to cross chain bridges / swaps is to have a chain specific bridge provider (usually tied to one of the bridged chains, like Binance or Polygon tools allowing to bridge) with more “traditional” DEXes operating on different chains. This seems to be a more sustainable model currently while as the sector grows and develops there should certainly be more cross-chain DEX providers coming.

# DAOs

1. **Main differences between current DAOs.**

Differences across DAOs lie in their aims and governance models. Some pool together funds in order to achieve specific goals (VC funding, acquiring a public good, etc.) with the ability to vote on the use of acquired goods (e.g. putting a copy of US constitution on display in a museum - choosing a specific museum for that), others use governance tokens provided to the users of specific protocols (e.g. to LP providers in DeFi protocols / AMMs) to vote on various aspects of the protocol - fee distribution, introducing new asset pairs, etc.

a. **Which model is the most interesting?**
The most interesting model is one which uses DAO model as an enabler for “real world” assets / organisations. Constitution DAO is one such example where people have pooled their assets in order to acquire a privately held copy of US constitution with the aim of putting it on display in a museum. This brings about a new and novel ways for people to organize themselves in order to work together for a greater good while benefiting participants at the same time (e.g. a DAO owned good could be for example displayed somewhere while DAO members could still sell their shares of the mentioned good to other people).

b. **Potential new DAO example.**
DAO for urban mobility. Current ride / scooter, bike sharing market is highly monopolized / oligopolized with platforms trying to capture as large share of the market as possible and then switch to the usual user exploitation strategy once incumbent position is reached. I believe that current ride sharing models can be improved through the use of DAOs and cryptocurrency as it would allow DAO participants to earn passive income through providing their own assets. The people providing their assets to the platform would earn fees in the form of native protocol token which could then be staked with rewards paid in governance tokens allowing for voting regarding ride fees and other aspects.

# Role of derivatives in finance

Derivatives enable price discovery, improve liquidity of the underlying asset they represent, and serve as effective instruments for hedging.

The size of derivatives market in traditional finance is gigantic and the easiest way to comprehend this is through visuals - https://www.visualcapitalist.com/all-of-the-worlds-money-and-markets-in-one-visualization-2020/

1. **Different forms of derivatives.**
   a. **Futures:** These are arrangements to buy or sell a fixed quantity of a particular security or currency for a fixed price and date in the future.
   b. **Option:** The owner of an option does not have the obligation but the option to buy or sell a particular security, currency on or before a predetermined date.
   c. **Swap:** A derivative is a financial instrument that derives its value from an underlying asset. The underlying asset can be equity, currency, commodities, or interest rate. Thus, a change in the underlying asset leads to an equivalent change in the derivative. Derivative markets are investment markets where derivative trading takes place.
2. **Forward commitments vs. contingent claims.**
   a. While a forward commitment contains an obligation to carry out the transaction as planned, a contingent claim contains the right to carry out the transaction but not the obligation. As a result, the payoff profiles between these derivatives vary, and that affects how the contracts themselves trade.
   b. The value of a derivative with a forward commitment will move more or less in lockstep with the price of the underlying product. In contrast, a contingent claim derivative will increase or decrease with the likelihood of the right being exercised for a profit.

# Synthetics in traditional finance vs. DeFi

1. **Synths Creation process.**

   Users mint (create) synthetic assets by depositing collateral (SNX for Synthetix, UST for Mirror). The collateral is used to back the minted synthetic asset with real value.

2. **Difference between sXAU and iBTC.**

   sXAU tracks gold price while iBTC tracks BTC price inversely.

3. **Oracles and Synths.**

   Oracles provide reliable information to the blockchain. The data is then used (in case of Synths) to price synthetic assets.

4. **Inverse Synths.**

   Inverse synths inversely track the price of a specific asset. Once they are created, they have an initial price based on the price of an underlying asset at the time of synth creation. After the creation, as the price of the underlying asset changes, the synth is priced inversely based on the price movement. E.g. iBTC was created at the price of 50000$ and the price of BTC moves to 49000$, then the price of iBTC will become 51000$.

# Getting to know stakeholder domains (Entrepreneurs, Investors, Influencers)

1. **Top startups in DeFi.**

   OlympusDAO (Maven11), Uniswap (Paradigm, Andreessen Horowitz), Alchemix (Alameda Research), SushiSwap (Blokchain Capital, Pantera Capital), AAVE (Three Arrows Capital, Maven11), Yearn Finance (Andre Cronje), Balancer (Blockchain Capital), MakerDAO (Paradigm, Andreessen Horowitz), Curve Finance (Vulcan Capital and many others).

   Pretty much all of the above mentioned startups are bringing new and innovative solutions to the DeFi space with crypto VCs allowing them to scale faster than they otherwise could. There is also a clear trend towards more distributed funding models surpassing VC funding as it being seen as benefiting a handful of people instead of the whole community / users.

2. **VCs/investors in DeFi.**

   Paradigm (dYdX, FTX, OpenSea, Optimism), Andreessen Horowitz / a16z (Coibase, Celo, MakerDAO, Uniswap), Pantera capital, Digital Currency Group, Polychain Capital, Sequoia Capital, Coinbase Ventures.

3. **Top influencers in DeFi.**

   Crypto Twitter is the main channel for DeFi influencers. The community ir really vibrant and there are loads of quality content creators not just for DeFi but for the blockchain / cryptocurrency sector as a whole. Main influencers in this sphere have been thoroughly laid out in the Messari crypto thesis for 2022 report - https://messari.io/pdf/messari-report-crypto-theses-for-2022.pdf.

# Insurance & Decentralization

1. **Benefits of a decentralized insurance system.**
   a. Protection of DeFi deposits, protection against volatility & flash crash.
   b. Immediate redemption of tokenized crypto.
   c. Protection against the risk of theft & attack on crypto wallets.
   d. Protection of funds from hack on exchange platforms.
2. **Primary things insurance needs to address in relation to the DeFi-ecosystem.**
   a. Potential protocol hacks.
   b. Liquidation risk.
3. **Top 5 biggest DeFi exploits.**
   a. Poly Network ($611m) - attacker had found a way to 'unlock' (ie buy) tokens on the Poly Network protocol without 'locking' (ie selling) the corresponding tokens on other blockchains.
   b. Coincheck ($547m) - NEM stolen from a hot wallet.
   c. Mt. Gox ($480m) - exchange hack by an outsider.
   d. KuCoin ($285m) - hackers obtained private keys to exchange's "hot wallets".
   e. BitGrail ($170m) - hackers stole $170m in niche cryptocurrency Nano.

# Current Insurance Platforms and Potential Improvements

**Nexus Mutual**

Nexus Mutual is creating decentralized insurance on Ethereum by using a risk-sharing pool. The pool is governed by its members where membership rights are represented by the NXM token. The mutual is initially launching with smart contract cover, allowing anyone to purchase insurance on any public Ethereum smart contract. This means that DeFi users can now get protection on their funds being lent out on Compound or Dharma or their assets deposited in a Uniswap pool.

**Unslashed Finance**

Insurance available through Unslashed Finance covers a variety of events including exchange and smart contract hacks, validator slashing, stablecoin pegs, and oracle failures. The team behind the project is dedicated towards building a DeFi insurance product that is easily accessible to individuals, developers, and institutions alike but that also rewards users for their participation with an average yield of 24%.

**Etherisc**

Etherisc is building a platform for decentralized insurance applications. The core team developed some common infrastructure, product templates and insurance license-as-a-service that allows anyone to create their own insurance products. With this, the Etherisc community has designed a suite of basic insurance products ranging from flight delay insurance and hurricane protection to crypto wallet and lending collateral protection.

**CDx**

CDx is a platform for tokenized, tradable insurance swaps. Crypto investors can now protect their funds from hacks on popular exchanges. Exchange insurance is likely one of the more needed insurance products given the numerous hacks over the past decade. Hacks which have ended in the loss of hundreds of millions in investor capital. CDx Swaps can be used for a range of use cases including trading swaps for a profit, protecting your crypto assets, betting against exchange security, and others.

**InsurAce**

Insurance available through Unslashed Finance covers a variety of events including exchange and smart contract hacks, validator slashing, stablecoin pegs, and oracle failures. The team behind the project is dedicated towards building a DeFi insurance product that is easily accessible to individuals, developers, and institutions alike but that also rewards users for their participation with an average yield of 24%.

*The main area of improvement for current state of DeFi insurance market remains market depth and overall sector maturity which would result in smaller insurance premiums as well as expanded product range. It is estimated that only 3% of DeFi TVL is currently insured which presents a huge opportunity for new market players as well as startups which are already working in this space.*

# Smart Contract Auditing

**A smart contract audit usually includes the following stages:**

- An overall analysis of the code and application.
- Documentation review.
- Brief code overview: quick analysis of the smart contract functionality, main .sol classes, etc.; analysis of cryptography, third-party modules, and library structure.
- Detailed analysis of the application, each of its actions, all requests, input fields, and nested modules.
- Bug scanning: scanning the application on appropriate binary and source-code levels to identify potential deviations from coding guidelines and security practices.
- Scanner results verification: in this phase, the team reviews the scan results to identify which of them are false positives and which of them can affect the application’s security.

**Most common mistakes / vulnerabilities include:**

- Inconsistency between specification and implementation.
- Flawed design, logic, or access control.
- Arithmetic overflow operations (integer overflow and underflow).
- Reentrancy attacks, code injection attacks, and Denial of Service attack.
- Exceeded limits on bytecode and gas usage.
- Race conditions, other known attacks, and access control violations.

Source: https://blockgeeks.com/guides/audit-smart-contract/

# Getting to know stakeholder domains (Technologists and Regulators)

### L1’s compared

| L1 | Ethereum | Solana | Avalanche | Fantom |
|---|---|---|---|---|
| Tx/s | 13 | 2000 | 4500 | 4500 |
| Block time | 12-14 seconds | 0.4 seconds | ~3 seconds | ~1 second |
| Avg tx cost, USD | $23.07 | $0.00025 | $0.0001 | <$0.1 |
| # of validators | >300 000 | >1000 | >1000 | 78 |
| # of Dapps | >2900 | >350 | >320 | >100 |
| # of active wallet addresses, monthly | >16 000 000 | >1 800 000 | >800 000 | >400 000 |

# Getting to know stakeholder domains (Technologists and Regulators)

1. **Pros and Cons of different Layer 2 Rollups (Optimistic vs ZK).**

   A ZK Rollup has the advantage of being significantly quicker than an Optimistic Rollup since it is considerably lighter on Layer 2 because the validation occurs on the mainchain rather than on the sidechain. Because mainchain validation occurs almost instantly, ZK Rollups are quicker and more scalable than previously.

   Optimistic Rollups take a bit longer to validate since they rely on smart contracts at the second layer. As a result, Optimistic Rollups are less scalable than ZK Rollups.

   Although zero-knowledge proofs take more computer resources than other options, ZK Rollups allow ten times as many transactions as Optimistic Rollups. This is the only drawback one can find with ZK Rollups.

2. **Existing regulations vs “native DeFi regulations”.**

   Due to such a disruptive and “digital native” nature of DeFi, existing regulations make little sense in the space as the actors at play are decentralized and anonymous for the most part. Regulators houls come up with DeFi native set of regulations.

# Thank you! 👋

**Ignas Aničas**

+37062674402
ignasanicas@gmail.com
https://www.linkedin.com/in/ignasanicas/