UNIVERSITY of NICOSIA

Session 4.2

Blockchain-based Derivatives, Oracles, Insurance

BLOC 611: Introduction to Decentralized Finance

Objectives

- Introduce the concept of financial derivatives and their use cases
- Provide an overview of oracles, their use-cases, and the oracle problem
- Provide an overview of blockchain insurance and its applications

Agenda

1. Financial Derivatives
2. Blockchain-based derivatives
3. Popular blockchain derivative dApps
4. DEXes for Derivatives
5. Oracles
6. Insurance
7. Conclusions
8. Further reading

Session 4.2: Blockchain-based Derivatives, Oracles, Insurance

1. Financial Derivatives

Financial Derivatives

As already established, DeFi **replicates** concepts of traditional finance, but with a different set of benefits and trade-offs. DeFi often **iterates** on those concepts, producing innovations unattainable by centralised systems.

- **Financial derivatives** is another concept adopted, and then iterated upon, by DeFi
- Financial derivatives are securities* whose value follows, or is derived from an underlying asset, group of assets, or even benchmark.
  - Derivatives **emulate** the cashflows of another security or securities but **are not** the security itself.
  - Importantly for DeFi, they don't require the **consent** or **participation** of the issuer.

In essence, derivatives are **contracts** between one or more parties, with set conditions that pertain to the underlying asset of assets. Their value relies on the value of the underlying asset(s), which traditionally include either stocks, bonds, commodities, interest rates, or market indexes.

Securities are tradable financial assets.

Uses for derivatives (simple example)

- Consider the example of the dairy farmer, Jamie who sells milk at the price of €1 per litre at the local supermarket. Jamie's milk costs her €0.50/litre, as her cows consume 1 kilo of wheat per litre of milk they produce and wheat currently costs €1.10/kilo.
- While Jamie currently enjoys a healthy 50% profit margin, she fears that due to unstable weather conditions, the price of wheat will rise in within the next 6 months. As a result, she might have to pay €1.10/kilo of wheat. She knows that the supermarket will not accept a higher price for her milk, which will render her business unprofitable.
- To mitigate this risk, Jamie enters a contact with her supplier to buy a 1,000 kilos of wheat at the price of €0.75/kilo in 6 months from now. While she loses out on the possibility of the price remaining the same, or even decreasing, she is at least safe from a risk that would threaten her business.

Financial Derivatives, Examples

The previous slide offers a simplfied example of a type of financial derivative, the **Forward Contract**.

- A **Forward** is an agreement to buy or sell of an asset at a certain time in the future for a certain price.

Examples of other derivatives include:

- **Futures**, which are standardized versions of forwards traded on formal exchanges instead of OTC.
- **Options**, are similar to forwards and futures, however, the option holder is not obligated to exercise their agreement to buy or sell. Instead of a requirement, options can be seen as an opportunity to buy or sell at a specific price, at some point in the future.
- **Swaps** are agreements to exchange cash flows in the future,
  - usually interest rates or interest rates and principal in once currency, for another.
- Unlike the previous example, assets rarely change hands; derivatives are mostly settled in cash
  - Contracts can also be sold before their settlement date in the open market.
  - A contract can change hands many times, but the (cash) settlement happens only once

Uses for derivatives

As demonstrated derivatives can be used as a hedge against risk, other use cases include:

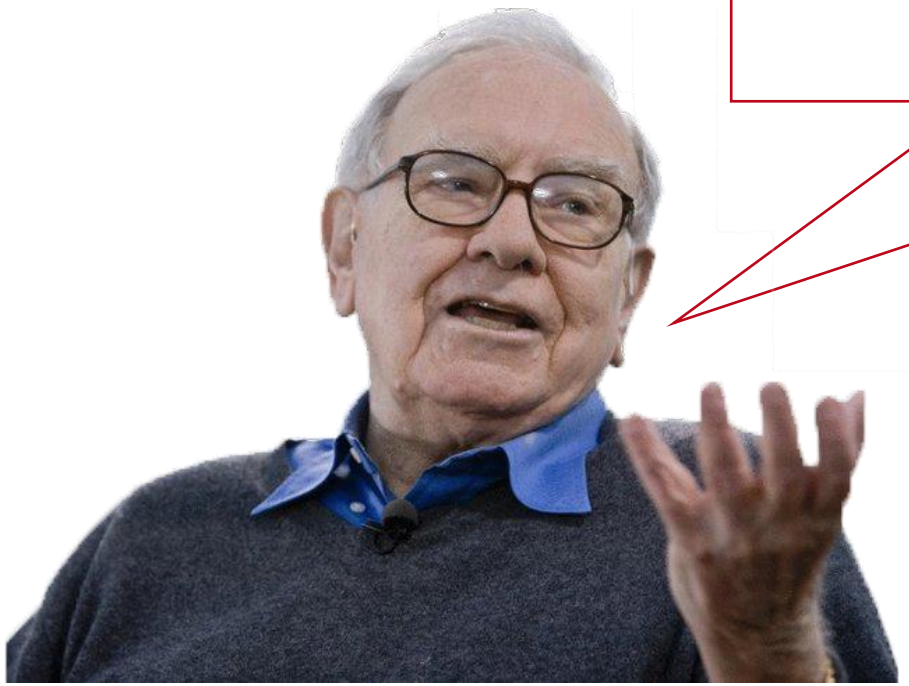
- **Hedge against risk,** price volatility, external dangers, etc.
- **Leverage and speculation**, by betting on the future prices of an asset with today's money
- **Access to unavailable markets**, as derivatives can represent assets otherwise unavailable to investors
- **Complex investment strategies**, by using a combination of financial derivatives

Derivatives have become very popular, yet they come with many pitfalls, including:

- High risk even at the smallest investments, as small price movements can result in loss of capital due to leverage
- The "Derivatives time bomb", which refers to the possibility of many positions unwinding* simultaneously (more on that in the next slides)
- Counter-party risk for OTC products.

"Unwinding" refers to the abrupt closing of a trading position.

Size of the derivatives market



Derivatives are financial weapons of mass destruction

Warren Buffett,
Investor

Size of the derivatives market

- Derivatives are an integral part of modern finance.
  - The **low-end** estimate for their notional value is $558.5 trillion. This number comes from the Bank of International Settlements and covers OTC derivatives such as commodity futures and swaps that can be measured precisely.
  - The **high-end** estimate is $1.2 quidrillion; while unofficial, it is widely cited.
  - The gross market value is calculated at approximately 12 trillion, still 20% of the world's wealth
  - Notional value is theoretical value of a derivative whereas market value is the price of the security now.

Session 4.2: Blockchain-based Derivatives, Oracles, Insurance

2. Blockchain-based Derivatives

Blockchain-Based Derivatives

When we talk about blockchain-based derivatives, we usually mean one of three things:

- **Synthetic Assets**
  - A way for representing on-chain and off-chain assets through tokens.
  - They make use of collateral in the form of a platform's own token (see next slides)
- **Wrapped tokens**
  - Wrapped tokens utilize collateral in the form of the asset they represent.
- **Special types of DEXes for derivatives trading**
  - Which, like their traditional counterparts, can include futures, swaps, etc.

Synthetic Assets

Synthetic assets are a new type of derivative that relies on **smart contracts** instead of traditional contracts.

- Synthetic assets are essentially **tokens** that represent customizable exposure to another underlying asset.
- They do so by creating a blockchain record of the relationship between the underlying asset and the token.
- This relationship is enforceable **programmatically** by smart contracts and is **verifiable** on the blockchain.

Synthetic assets allow investors to tokenize anything, including:

- Real and financial assets, such as gold and stocks
- Cryptocurrencies, cryptocurrency pairs, and indexes
- Even built-in trading strategies and rebalancing pairs

They are not to be confused with traditional derivatives of cryptocurrencies, such as Bitcoin futures

Size of the blockchain derivatives Market

How blockchain synthetic assets work

- Blockchain-based derivatives require three main components:
  - An **oracle**
  - An **algorithm** for for achieving price parity between the derivative and the underlying asset(s)
  - An **issuer**
- Users mint (create) synthetic assets by depositing (locking) collateral in the form of a token to a derivative platform.
  - Similarly to decentralized loans, synthetic assets are usually overcollateralized, meaning that the value of the collateral exceeds the value of the synthetic asset.
- Users can then trade, or simply hold the asset.
- Oracles, algorithms, and arbitragers collectively ensure that the price of the derivative matches the price of the underlying asset(s).

Wrapped Tokens

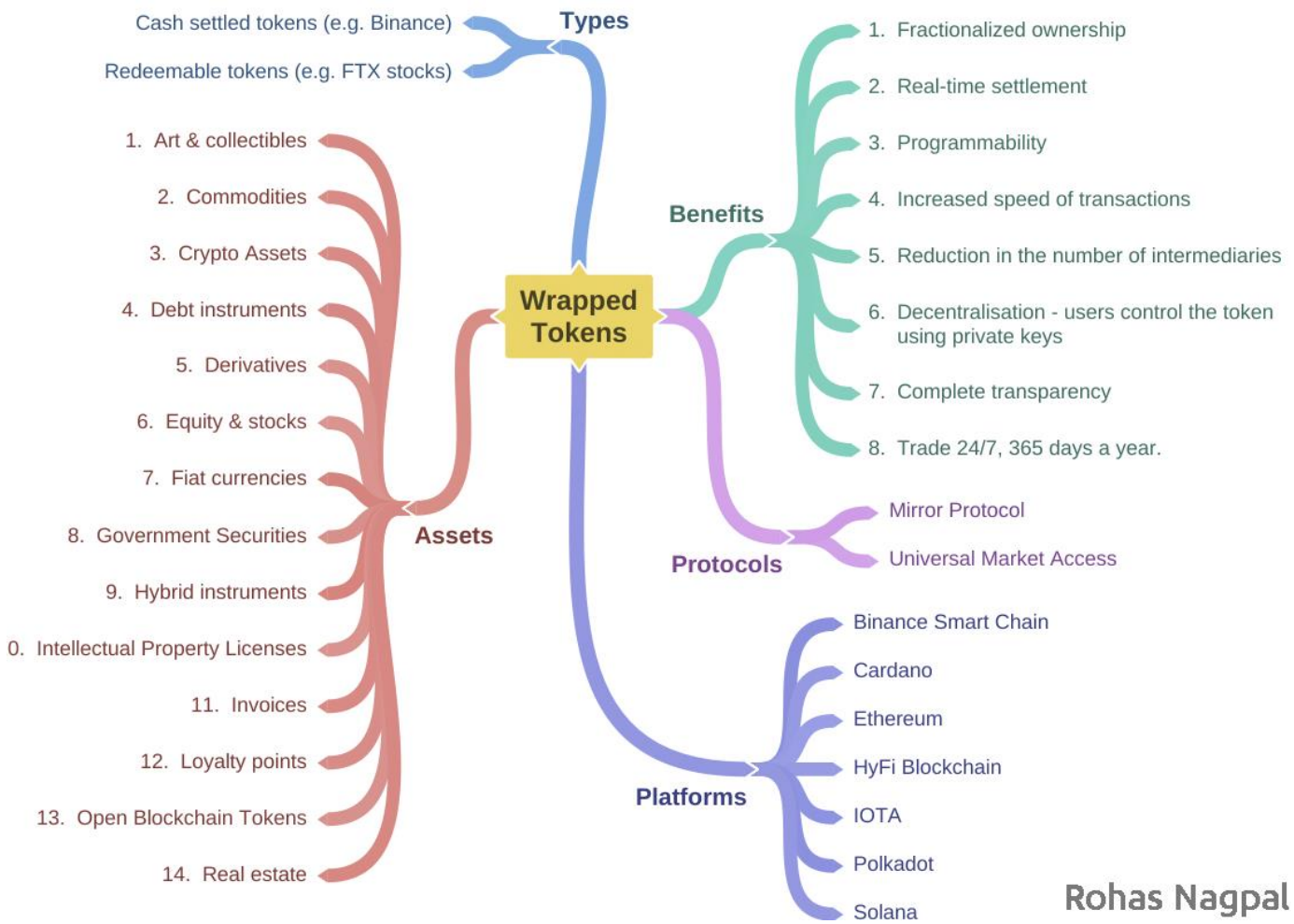
An example of a practical application for synthetic assets is wrapped cryptocurrencies, the most popular of which is wrapped ETH or wETH. The word “wrapped”, refers to a cryptocurrency that is represented 1:1 in the form of an ERC-20 token so that 1 wETH = 1 ETH in value.

- The obvious question then becomes, why do we even need wETH?
  - The ERC-20 standard defines certain specifications for tokens including how they are transferred and recorded.
  - Ether, as the native currency of Ethereum, does not comply to the ERC-20, since it was built before it.
  - To interact with many DeFi apps, ETH needs to be wrapped into an ERC-20 token.
- New token standards and advances to Ethereum will likely render wETH redundant.
- Yet, wrapped tokens are here to stay, as they present a convenient way for brining non-native cryptocurrencies to any blockchain.
  - For example, wrapping Bitcoin to be used in the Ethereum network.

How Wrapped Tokens Work

- Wrapping usually requires a **custodian** or an entity that holds the reserves of the asset that is being wrapped. Custodians come in different types, they can be:
  - (Centralized) Merchants
  - Smart Contracts
  - dApps governed by DAOs
- Wrapping essentially refers to the process of giving an asset to a custodian, in exchange for a proportional amount of the wrapped asset. The wrapped asset can be redeemed again for the original asset.
  - After receiving the asset, e.g. Ether, the custodian mints a proportional amount of the wrapped asset, in our case wETH, and sends it back to the original address
  - To “unwrap” the asset, wETH need to be burned, before the merchant releases the locked Ether.
- Besides Ether (wETH), wrapped assets are also popular with Bitcoin (wBTC, renBTC, and more)

Examples of wrapped assets



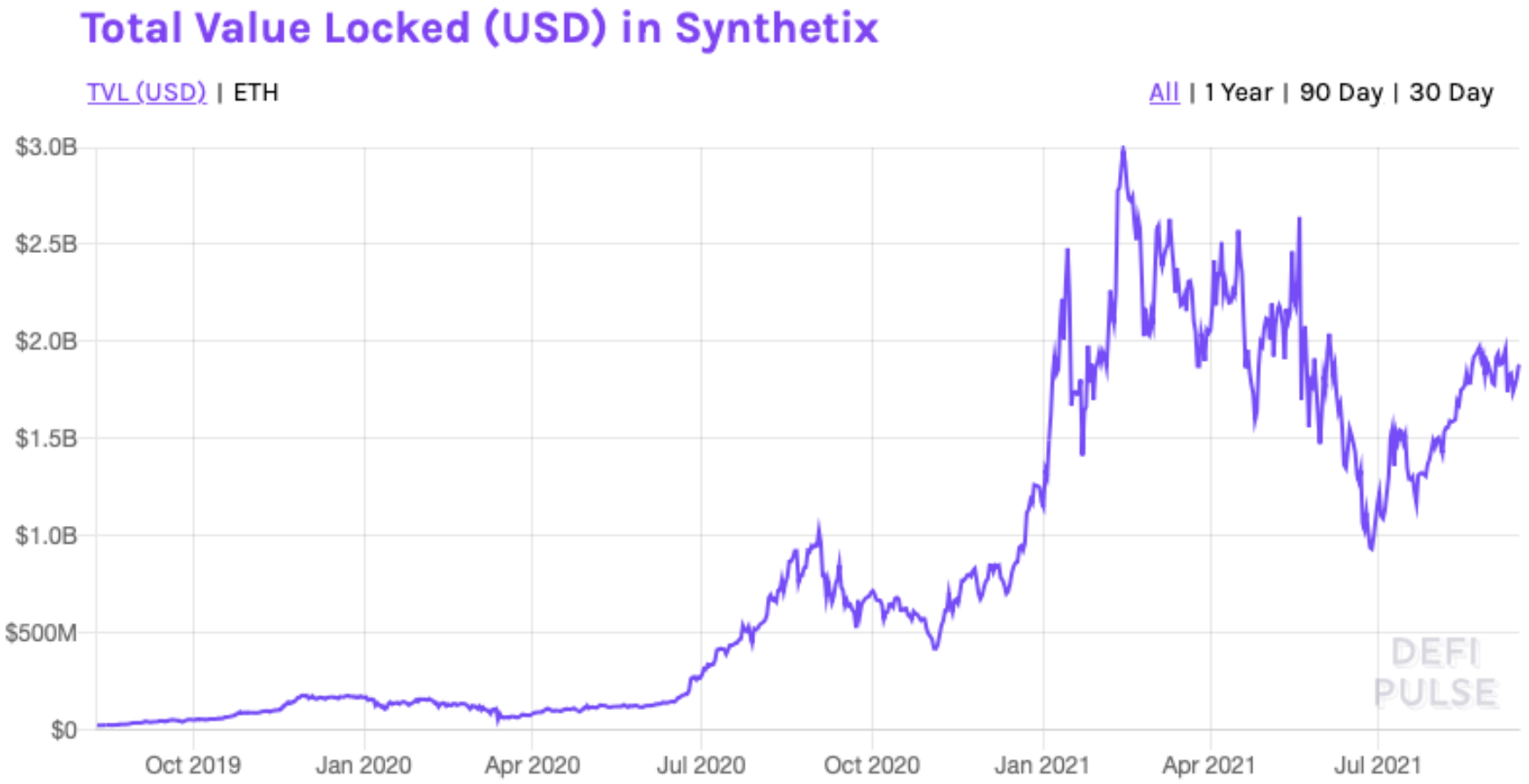
Session 4.2: Blockchain-based Derivatives, Oracles, Insurance

3. Popular Blockchain Derivative dApps

Example: Synthetix

- **Synthetix** is the largest and one of the oldest projects of the space.
  - It is a decentralized synthetic asset platform built on Ethereum, where anyone can mint (create) **synths**.
  - Users mint new synths by provide collateral in the form of the platform's native SNX token in a debt pool.
  - Positions in Synthetix are overcollateralized, at a ratio of 5:1 (used to be 7:1).
  - This means that for every €1 worth of a derivative, a user would have to provide €5 worth of SNX as collateral.
  - Synths, represent a variety of assets including USD, EUR, JPY, BTC, ETH, BNB, TSLA, AAPL, GOOG, FB, OIL, etc.
  - Users that wish to retrieve their collateral from the debt pool must pay back this debt by "burning" their synths
  - Transaction fees from synths exchanged on Synthetix's DEX go to SNX holders and synth minters, incentivizing synth creation and providing value to the underlying collateral (i.e., the SNX token).

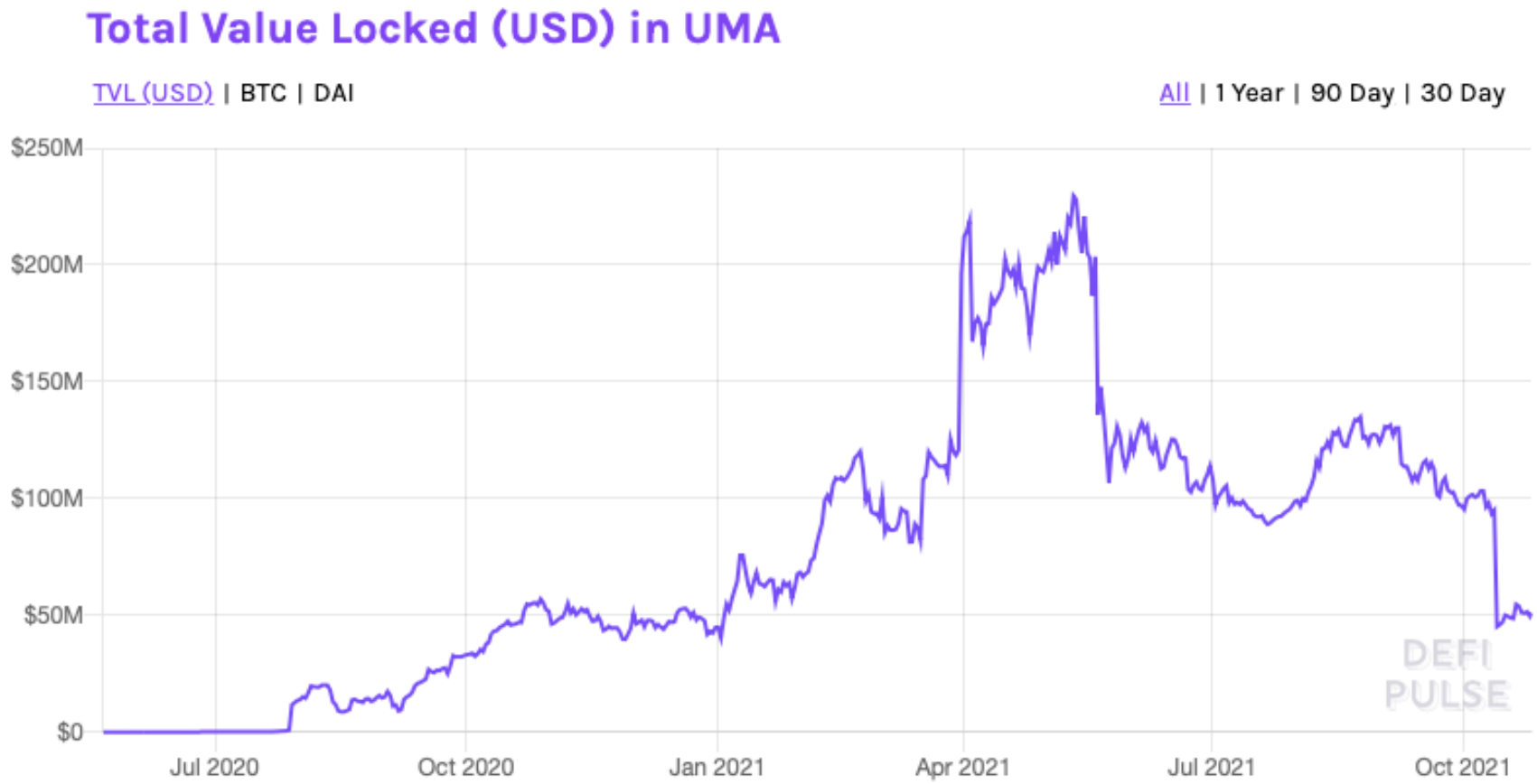
Synthetix TVL



Example: UMA

- Similarly to Synthetix, Universal Market Access, or UMA is another protocol for blockchain derivatives
  - It allows developers to create and manage derivatives using open-source templates
  - The primary difference between Synthetix and UMA, is that the latter does not rely on overcollateralization
  - It instead incentivizes liquidators to identify and liquidate improperly collateralized positions for a profit.
  - Liquidators pay back the debt and reclaim the collateral for themselves.
  - For that reason, UMA does not use oracles, since liquidators use their own price feeds when monitoring positions
  - In a sense, the liquidators serve as oracles-by-proxy for UMA.
  - When a liquidation happens, disputers have some time to determine whether a liquidation was valid.
  - When a dispute is raised, UMA holders vote on the price of the asset, based on their own price feeds, in exchange for rewards.

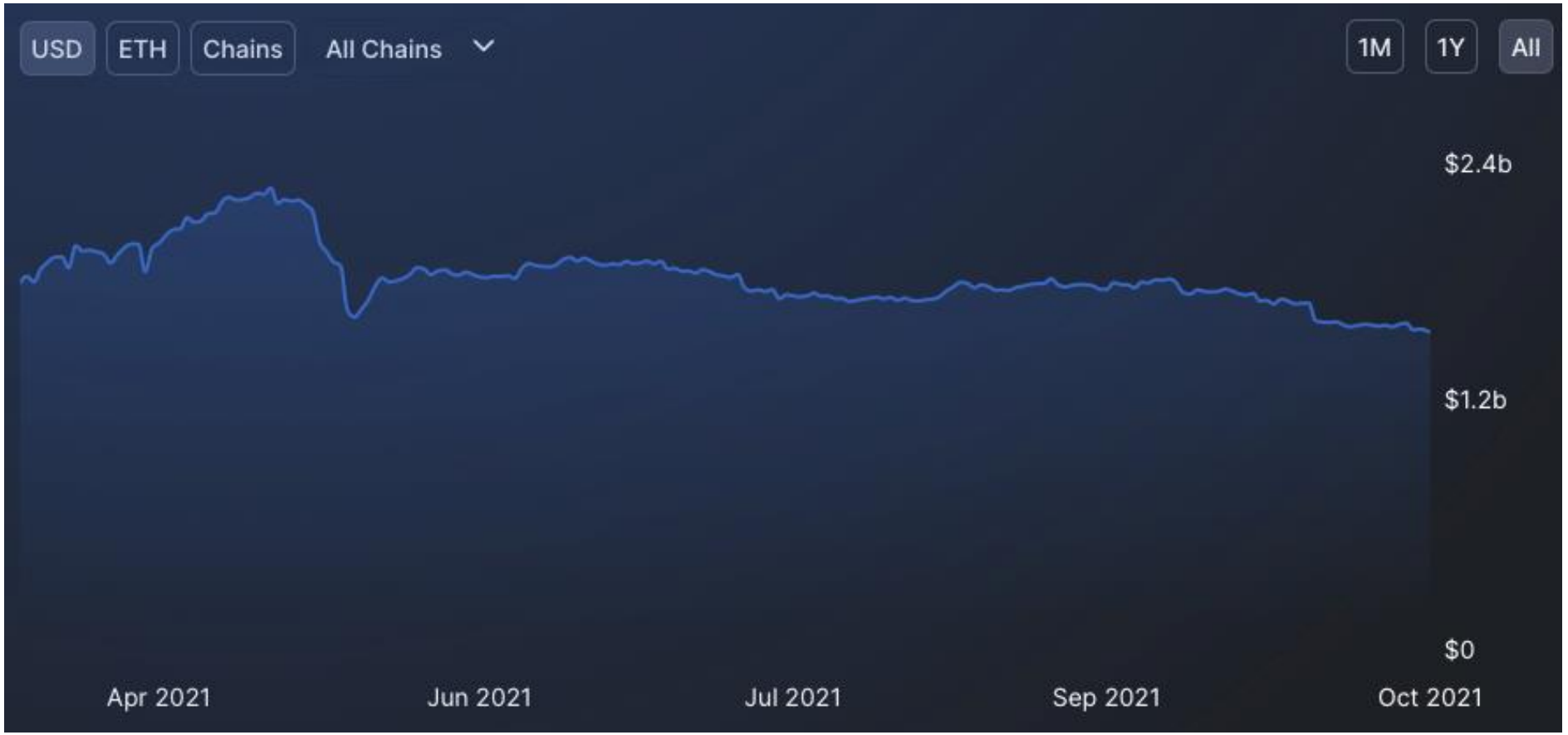
UMA TVL



Example: Mirror

- **Mirror** is another protocol for synthetic assets.
  - Unlike Synthetix or UMA, it is built on the Terra blockchain.
  - Similarly to Synthetix, users can lock the protocol's native token, MIR, to mint synthetic assets for a plethora of financial assets.
  - Mirror is governed by a DAO that, among other things, determines the synthetic assets that can be minted.
  - Utilizing a bridge solution known as Terra Shuttle, Mirror assets can be traded on the Ethereum and Binance Smart Chain, too.

Mirror TVL (DeFi Llama)



Session 4.2: Blockchain-based Derivatives, Oracles, Insurance

4. DEXes for Derivatives

dYdX

dYdX is a decentralized derivatives exchange and one of the first to offer decentralized perpetual contracts

- It offers a plethora of financial products including:
  - Spot, margin, perpetual, and swap trading
  - Lending and borrowing.
- In contrast to many other decentralized applications, it utilizes an off-chain matching mechanism for faster speeds and order books. However, settlement happens on-chain.
- The perpetual trading takes place on a layer-2 solution developed by StarkWare
- The contracts can change hands various times but the settlement happens only once, at the delivery date.

Perpetual Protocol

As the name suggests, Perpetual Protocol offers on-chain perpetual futures.

- It currently supports the trading of over 15 trading cryptocurrency pairs, for up to x10 leverage
- The platform utilizes the stablecoin USDC to fund and settle all trades
- Relies on the xDAI instead of the Ethereum blockchain. Currently some fees are subsidized by the protocol
- It utilizes a special form of AMM for pricing its assets called a Virtual AMM or vAMM.
  - vAMMs do not rely on liquidity pools or liquidity providers, hence the name ”virtual”
  - The collateral is stored in a smart contract
  - The constant product formula is used to determine the price of each trade

Perpetual Contracts

Perpetual contracts are an example of a DeFi innovation.

- Like futures or forwards, they are a (smart) contract to buy or sell an asset at a specific price in the future.
- However, unlike futures or forwards, perpetual futures don't have a specific settlement date.
- Instead, they can be held in perpetuity (forever) until a trader closes their position.
- They were popularised for the cryptocurrency market following their introduction by BitMEX.

Blockchain Derivatives Risks

Blockchain–based derivatives pose many of the generic DeFi risks:

- Hacks and Exploits
- Loss of Private Keys
- Admin Key Risk
- Protocol and Platform risks

In addition:

- Leverage presents its own risks as small price movements can result in huge losses for derivatives traders
- Oracle failures
- Lack of liquidity may lead to skewed pricing compared to real-world assets

Session 4.2: Blockchain-based Derivatives, Oracles, Insurance

5. Oracles

The Oracle Problem

- Blockchain nodes need to reach an agreement (consensus) on the state of the network at any point in time
- Since all nodes must always, under same inputs, come to the same agreement, the execution environment of smart contracts must be **deterministic**.
  - For an environment to be deterministic, it has to operate by very strict requirements and limitations.
  - Blockchains in particular are completely **isolated** and **sandboxed** from the outside world.
  - They cannot even access the node's hardware, file system, etc.
- As such, and for the sake of security and immutability, blockchains are inherently **closed systems**.
- This brings us to the simple fact: the only 'world' a smart contract sees, consists of other contracts and transactions directed towards it. In other words, all the data a certain contract needs, must come from inside the blockchain.
- However, in many cases, a smart contract will require access to non-blockchain information to function correctly, e.g. 'what is the current exchange rate of ETH in USD", "what is the current price of TSLA stock"
- This is often referred to as **the blockchain oracle problem**

*The bid-ask spread, or the distance between the maximum price someone is willing to pay (bid) and the minimum price someone is willing to sell (ask) is an indicator of market liquidity

Blockchains and Oracles

To be of any real-world value, many decentralised applications, including those in the DeFi space, require access to data that is not native to blockchains. Indicatively, this includes information such as:

- Price feeds
- Data from IoT sensors
- News items, such as election results or sport scores

Retrieving this information requires **a third-party "bridge" to the outside world, known as an oracle**.

Oracles operate on behalf of smart contracts predominately by:

1. Retrieving and delivering off-chain data to smart contracts (dApps, DeFi applications)
2. Writing data from smart contracts to external systems
3. Executing off-chain computations

Blockchains and Oracles (continued)

- Those functions are integral to many aspects of DeFi and even beyond:
  - DEXes
  - Stablecoins
  - Blockchain Derivatives
  - Insurance
  - Most enterprise blockchain applications
- As oracles are essentially "black boxes" for smart contracts, ideally they would need to be as secure as them – or even more secure than the system relying on them for information.
  - That is because a smart contract cannot know how an oracle has come up with a certain output (the black box) and has no option but to trust it (e.g. when the oracle reports that the current price of BTC is $60, instead of $60,000)

Relevant Quote

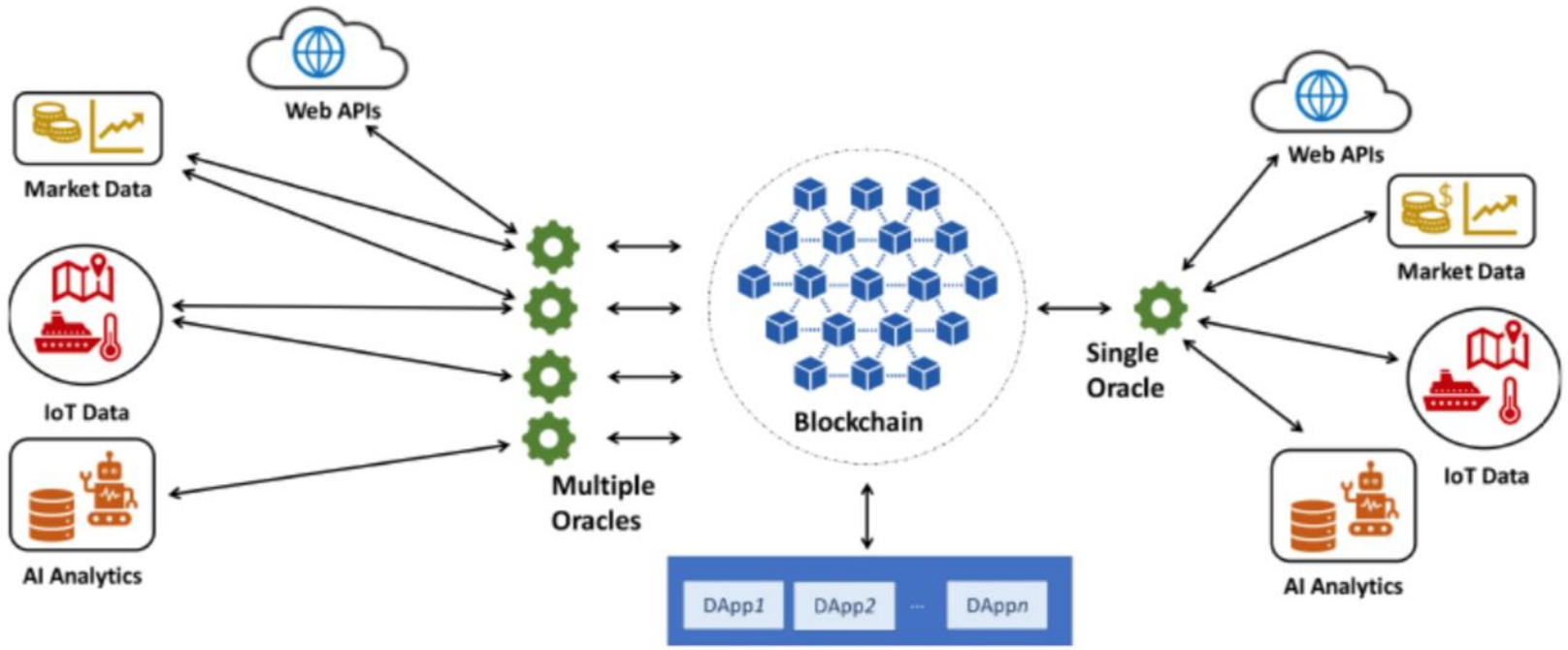
"Imagine the ideal protocol. It would have the most trustworthy third party imaginable — a deity who is on everybody's side.

All the parties would send their inputs to God. God would reliably determine the results and return the outputs. God being the ultimate in confessional discretion, no party would learn anything more about the other parties' inputs than they could learn from their own inputs and the output”

Nick Szabo,
Computer Scientist

How Oracles Work

- When a smart contract requires external data, it submits a request in a transaction to the oracle's contract.
- The oracle is an off-chain application that monitors the transactions sent to its contract. When it detects a new request, it is responsible for executing all necessary steps to come up with an answer. This can include fetching external world data, doing computations and more.
- The oracle then submits its response to the smart contract, again in the form of a transaction.



Types of oracles

There are two main types of blockchain oracles, depending on the way that they allow blockchains to interact with the real world:

- **Inbound oracles** provide data from the external world to blockchains and smart contracts.
- **Outbound oracles** provide smart contracts with the ability to send data to the outside world.

Depending on where their data comes from, we can distinguish oracles into:

- **Software oracles** that handle information data coming from the internet (e.g. asset prices from websites).
- **Hardware oracles** used when smart contracts need information directly from the physical world (e.g. IoT sensors).
- **Consensus-based oracles** that get their data from human consensus. For example, to avoid market manipulation, prediction markets implement a rating system where different users vote on the outcome in question and their weighted-by-rating average is transmitted to the enquiring smart contract.

Oracle example: Chainlink

One of the most popular oracle implementations is Chainlink. Studying Chainlink will give us a good sense of how many oracle solutions operate.

- Chainlink is a decentralised network of nodes that provide data and information from off-blockchain sources to on-blockchain smart contracts via oracles. It works in the following way:
  1. **Request**: A smart contract (dApp, DeFi application) submits a request to the Chainlink protocol for specific information (e.g. the price of the BTC/ETH pair). The Chainlink protocol receives the request and creates a smart contract with three sub-contracts:
  2. **Selection**: The **reputation contract** checks the oracle provider's track record and past performance, among other factors, to match the smart contract with appropriate and reliable oracles
  3. **Reporting**: The **order matching contract** sends the smart contract's request to Chainlink's nodes and receives bids, before selecting the right number and type of nodes to fulfil the request
  4. **Results**: The results are tallied and returned to the **aggregation contract**. The aggregation contract receives data from the nodes and reconciles them in a final result before feeding the weighted sum score to the requesting smart contract
- Some amount of decentralization is achieved in Chainlink by utilizing numerous nodes and data sources.

Session 4.2: Blockchain-based Derivatives, Oracles, Insurance

6. Insurance

Decentralized Insurance

- We have already discussed about the size and value of the DeFi ecosystem
- It is important to remember that DeFi is still an embryonic and highly experimental industry that often utilizes novel and untested technologies to implement existing or novel financial concepts.
- This can result in many of the risks that we have discussed in the previous sessions.
- As DeFi explodes in popularity, so do hacks, exploits, rug-pulls and more.
- **Decentralized Insurance** is a way for DeFi users to secure their assets against unexpected events for a fee.
  - In that sense it akin to traditional insurance.
  - But, it is also decentralized!

The world of DeFi is Dangerous – for more details see here

1. **Poly Network - REKT**
   $611,000,000 | 10 Aug 2021
2. **EasyFi - REKT**
   $59,000,000 | 19 Apr 2021
3. **Uranium Finance - REKT**
   $57,200,000 | 28 Apr 2021
4. **PancakeBunny - REKT**
   $45,000,000 | 19 May 2021
5. **Kucoin - REKT**
   $45,000,000 | 29 Sep 2020
6. **Alpha Finance - REKT**
   $37,500,000 | 13 Feb 2021
7. **Meerkat Finance - BSC - REKT**
   $32,000,000 | 04 Mar 2021
8. **Spartan Protocol - REKT**
   $30,500,000 | 02 May 2021
9. **StableMagnet - REKT**
   $27,000,000 | 23 Jun 2021
10. **Paid Network - REKT**
    $27,000,000 | 05 Mar 2021
11. **Harvest Finance - REKT**
    $25,000,000 | 26 Oct 2020
12. **XToken - REKT**
    $24,000,000 | 12 May 2021
13. **Popsicle Finance - REKT**
    $20,000,000 | 03 Aug 2021
14. **Pickle Finance - REKT**
    $19,700,000 | 22 Nov 2020
15. **Cream Finance - REKT**
    $18,800,000 | 30 Aug 2021
16. **bEarn - REKT**
    $18,000,000 | 17 May 2021
17. **Furucombo - REKT**
    $14,000,000 | 27 Feb 2021
18. **Compounder Finance - REKT**
    $12,000,000 | 02 Dec 2020
19. **Value DeFi - REKT 3**
    $11,000,000 | 7 May 2021
20. **Yearn - REKT**
    $11,000,000 | 05 Feb 2021
21. **Rari Capital - REKT**
    $10,000,000 | 8 May 2021
22. **Value DeFi - REKT 2**
    $10,000,000 | 5 May 2021
23. **Cover - REKT**
    $9,400,000 | 29 Dec 2020
24. **Punk Protocol - REKT**
    $8,950,000 | 10 Aug 2021
25. **THORChain - REKT 2**
    $8,000,000 | 22 Jul 2021
26. **Hack Epidemic (Origin Protocol - REKT)**
    $8,000,000 | 17 Nov 2020
27. **Anyswap - REKT**
    $7,900,000 | 10 Jul 2021
28. **Warp Finance - REKT**
    $7,800,000 | 18 Dec 2020
29. **BurgerSwap - REKT**
    $7,200,000 | 28 May 2021
30. **Value DeFi - REKT**
    $7,000,000 | 14 Nov 2020
31. **Alchemix - REKT**
    $6,500,000 | 16 Jun 2021
32. **Belt - REKT**
    $6,300,000 | 29 May 2021
33. **Bondly - REKT**
    $5,900,000 | 15 Jul 2021
34. **Roll - REKT**
    $5,700,000 | 14 Mar 2021
35. **THORChain - REKT**
    $5,000,000 | 15 Jul 2021
36. **X-Token - REKT X2**
    $4,500,000 | 29 Aug 2021
37. **Eleven Finance - REKT**
    $4,500,000 | 22 Jun 2021
38. **ChainSwap - REKT**
    $4,400,000 | 11 Jul 2021
39. **DAO Maker - REKT**
    $4,000,000 | 04 Sep 2021
40. **JayPegs Automart - REKT**
    $3,100,000 | 17 Sep 2021
41. **PancakeBunny - REKT 2**
    $2,400,000 | 16 May 2021
42. **DODO - REKT**
    $2,000,000 | 09 Mar 2021
43. **Akropolis - REKT**
    $2,000,000 | 12 Nov 2020
44. **Levyathan - REKT**
    $1,500,000 | 30 Jul 2021
45. **The Big Combo (Growth DeFi - REKT)**
    $1,300,000 | 09 Feb 2021

Decentralized Insurance Example: Opyn

Opyn is a permissionless, decentralized insurance platform allowing users to protect their DeFi deposits from financial and technical risks

- Opyn uses blockchain-based **option derivatives** to provide insurance. In theory, any blockchain derivative can be used for hedging risk, and thus is a form of insurance.
- Options are similar to forwards or futures. **Call/Put options** give the option holder the option (but not the obligation) to buy/sell an asset at a specified price at a specified future date. Call options are bought by individuals that think the price will rise, whereas put options are bought if the price would fall.
  - Require collateral
  - Similarly to other DeFi applications they are capital inefficient – WE NEED TO EXPLAIN HOW OPYN USES OPTIONS FOR INSURANCE

Opyn TVL

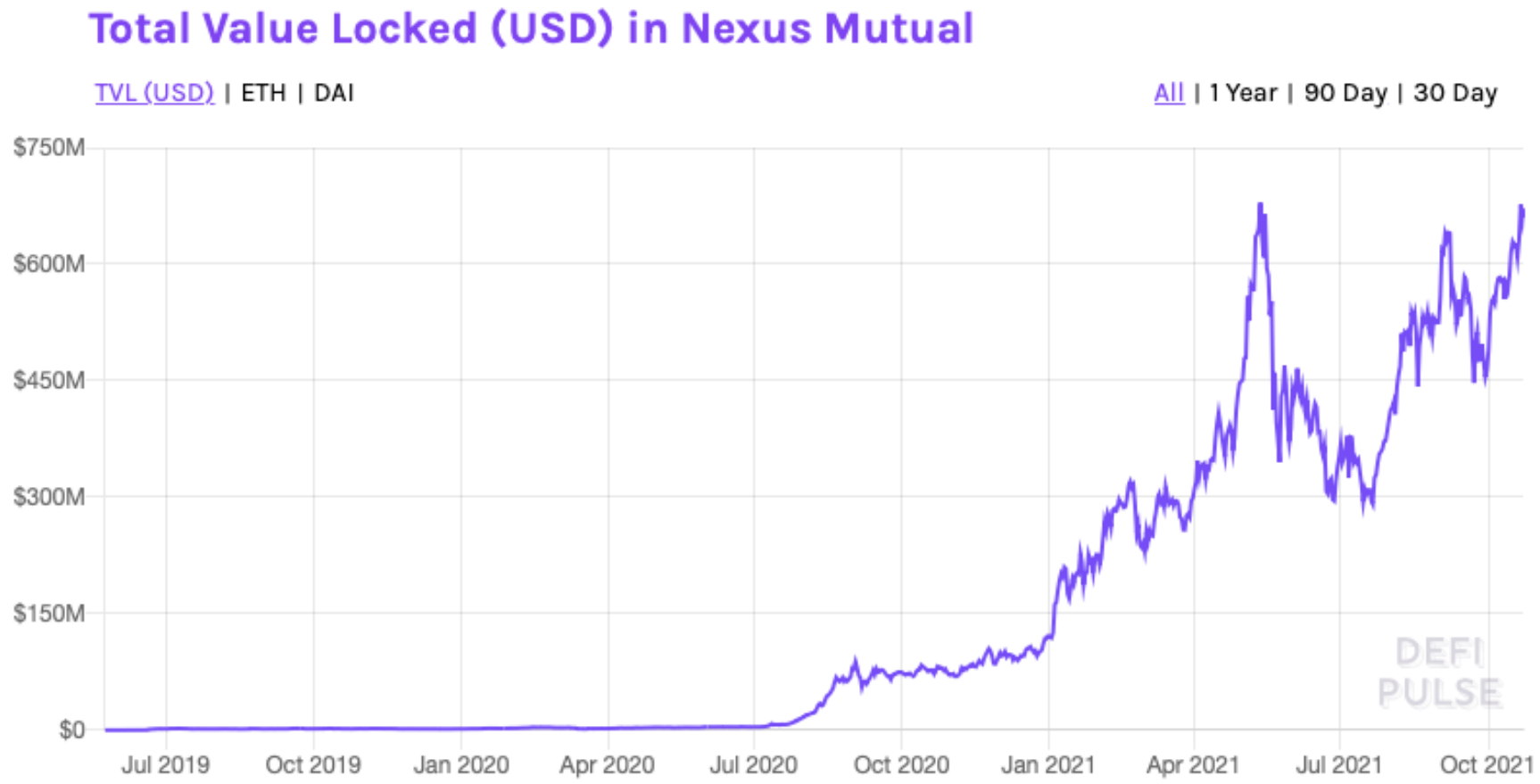
Decentralized Insurance Example: Nexus Mutual

Nexus Mutual is more akin to traditional insurance, covering smart contract failures, including:

- Economic design failure
- Oracle failures
- Governance failures
- Hacks, exploits and more.

- It works in the following way:
  - Users who want to take out insurance specify the smart contract address that they want cover for.
  - They then specify the **cover amount** (payable in DAI or ETH) as well as the **cover period**.
  - Importantly, anyone can buy cover on any smart contract and redeem it in case of a covered event. This goes against some of the basic principles of traditional insurance, namely that of insurable Interest, and indemnity, and in that sense is more akin to gambling.
- The price of the insurance is determined by:
  1. The characteristics of the smart contract that is insured
  2. Cover amount and period
  3. Value staked by **risk assessors** against the smart contract

Nexus Mutual TVL



Session 4.2: Blockchain-based Derivatives, Oracles, Insurance

7. Conclusions

Conclusions

- In this session you have learned about the various types of financial derivatives, their use cases and dominance in the finance space. You should now have an understanding of the importance of financial derivatives for the entire financial system
- We have also explored how traditional derivatives can be brought on-chain through various techniques. You should now understand that the term “Blockchain Derivatives” is broad, and encompasses various derivative-related functions.
- You have been introduced to the concept of oracles, through the oracle problem and you have examined the basic characteristics of oracles. You should now be able to explain the basic function of oracles, as well as their importance for building DeFi applications that are relevant in the real world.
- Finally, you have learned how insurance can be brought on-chain through derivative applications.

Session 4.2: Blockchain-based Derivatives, Oracles, Insurance

8. Further Reading

Further Reading

Oracles

- A First Look into DeFi Oracles
- Town Crier: An Authenticated Data Feed for Smart Contracts
- The God Protocols, Nick Szabo

Blockchain Insurance

- DeFi Llamma, overview of insurance
- Opyn.co website
- Nexus Mutual Whitepaper

Tip: Clicking while pressing Ctl key opens a new tab in Chrome browser on non-Apple devices

Join our discord server!

https://discord.gg/r6FrHbsfSJ

UNIVERSITY *of* NICOSIA

Questions?

Contact Us:

Twitter: **@mscdigital**
Course Support: **defi@unic.ac.cy**
IT & Live Session Support: **dl.it@unic.ac.cy**