

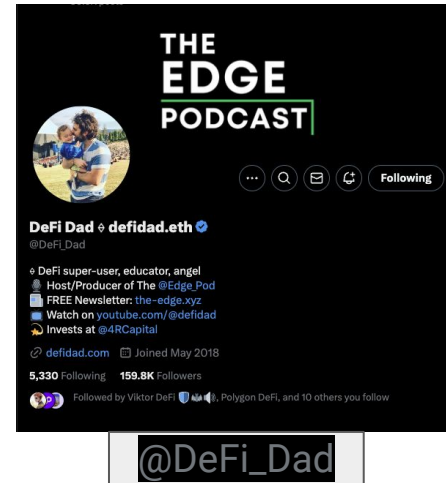
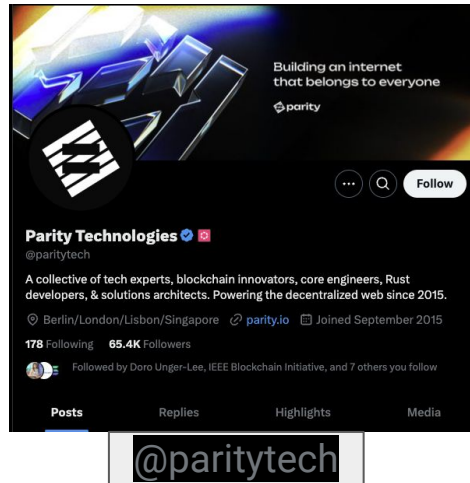
Session 1

Assignment Solution

by
Manjiri Birajdar

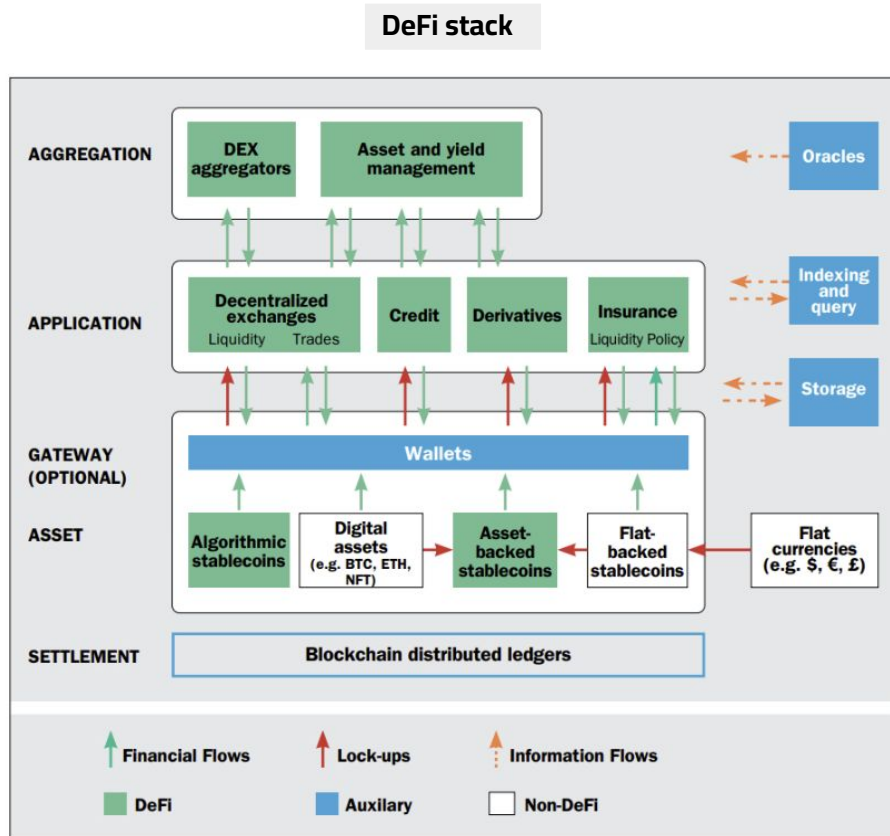


0. Practical (Bonus) : *Share your Twitter handle and recommended DeFi accounts you follow*



Defining DeFi

Visualize the “DeFi stack” in a nice slide:
What are the elements
and layers of DeFi and
how are they related
to each other?



Source: World Economic Forum - defi policy maker

Defining DeFi (Decentralized Finance)

In 5 sentences, how would you define DeFi?

- a. A global, peer-to-peer, pseudonymous (Identification of users is not necessary in DeFi), open to all and permissionless financial ecosystem built on blockchain technology
- b. By using smart contracts and decentralized protocols (dApps), DeFi allows users to borrow, lend, trade, and invest without needing intermediaries like banks
- c. Financial systems based on DLT, instead of relying on centralized authorities, DeFi platforms operate through code (smart contracts), providing transparent and automated financial services
- d. Anyone with an internet connection can access these services, enabling financial inclusivity
- e. Its decentralized nature also makes it resistant to censorship and restrictions imposed by traditional financial systems











Defining DeFi

What are potential security risks related to DeFi?

1. **Smart Contract Vulnerabilities:** Bugs or exploits in the code of smart contracts can lead to loss of funds, as they govern all operations autonomously.
2. **Oracle Manipulation:** DeFi protocols rely on oracles for price feeds, and a compromised oracle can feed incorrect prices, leading to significant financial losses.
3. **Rug Pulls and Exit Scams:** Developers can create malicious projects that gain users' trust and investment, then disappear with the funds.
4. **Governance Attacks:** Decentralized governance in DeFi projects may be vulnerable to majority attacks, where malicious entities gain control and alter the protocol's behavior.
5. **Flash Loan Attacks:** Bad actors use flash loans to manipulate markets or exploit protocol logic in ways that result in financial gain at the expense of the system.

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

What are the top 5 stablecoins by market capitalization?

#	Name	Price ⓘ	1H ⓘ	24H ⓘ	7D ⓘ	Market Cap ⓘ ▾	24H Volume ⓘ	7 Day Chart ⓘ
1	 Tether (USDT) ⓘ	\$1.00	+0.01%	-0.02%	-0.01%	\$120.04B	\$32.33B	
2	 USDC (USDC) ⓘ	\$1.00	+0.05%	-0.04%	0.00%	\$34.47B	\$5.09B	
3	 Dai (DAI) ⓘ	\$1.00	+0.18%	-0.06%	-0.05%	\$5.84B	\$77.58M	
4	 First Digital USD (FDUSD) ⓘ	\$1.00	+0.43%	-0.41%	-0.34%	\$2.63B	\$3.57B	
5	 Ethena USDe (USDe) ⓘ	\$1.00	+0.20%	+0.10%	+0.27%	\$2.60B	\$86.78M	

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

What are the different methods of how stablecoins achieve their stability?

Crypto-backed:

- A cryptocurrency (like Bitcoin) is utilized as collateral
- most well-known stablecoin in this category is DAI, issued by MakerDAO, a protocol built on Ethereum

Fiat-backed:

- Stablecoins that are directly backed by fiat currencies at a 1:1 ratio
- Tether (USDT), the Gemini Dollar (GUSD), and True USD (TUSD) are some of the most widespread examples

Algorithmic:

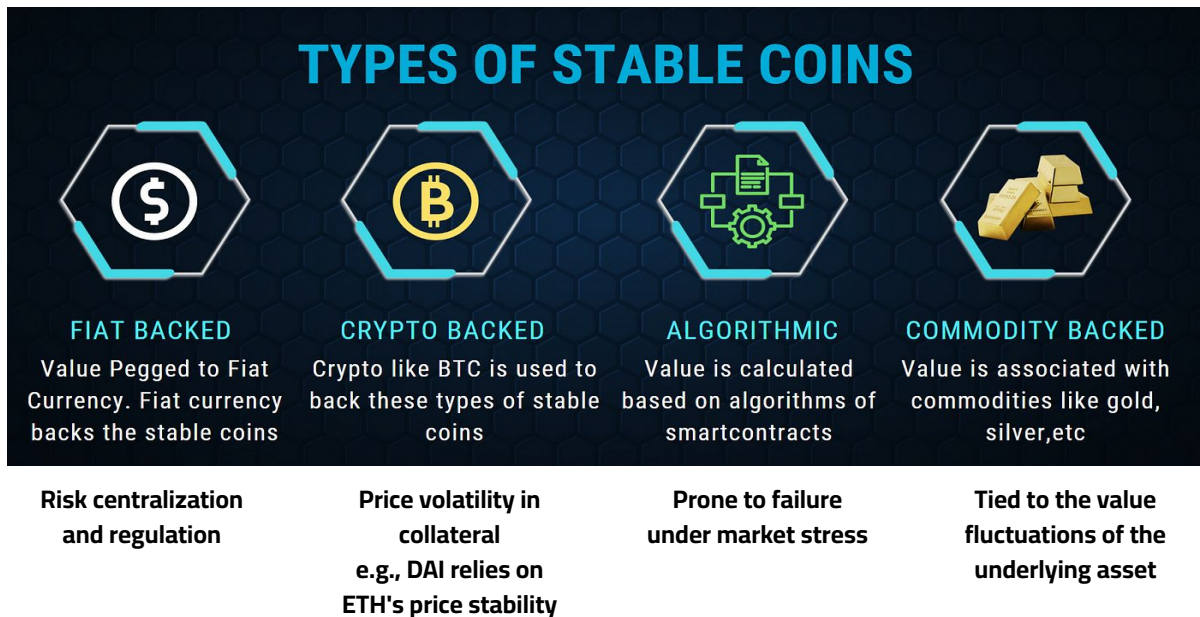
- Stablecoins supported by algorithms are not backed by fiat or cryptocurrency
- Empty Set Dollar (ESD) and Ampleforth (AMPL) are the leading algorithmic stablecoins in terms of market capitalization

Commodity-Backed:

- Cryptocurrencies that are pegged to the market value of commodities such as gold, silver, or oil
- One of the most popular commodity-backed tokens is Tether Gold (XAUt), a cryptocurrency backed by gold reserves

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

What are the risks associated with the different methods? Centralization, Regulation, etc.?



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

Does a stablecoin pegged to the official currency of your country exist yet?

- Yes, a stablecoin pegged to the official currency of Germany (EURO) does exist
- [Circle's](#) stablecoin, **Euro Coin (EUROC)**, which is fully backed by reserves of euros held in regulated financial institutions
- EURC is the leading euro stablecoin for crypto capital markets, and is commonly used in DeFi for FX (Forex - foreign exchange market) trading, borrowing and lending
- Designed for stability, EURC is **compliant with MiCA** (The Markets in Crypto-Assets) and backed 100% by euro
- Euro reserves are transparently held at regulated financial institutions in the EEA with published monthly attestations
- The EURC smart contract and token primitives are modeled after USDC, making it easy for developers to integrate into existing apps.



Euro Coin

I would park my
funds in
Euro Coin!

Wallets

What types of wallets are you familiar with?

How do they differ in terms of use case and security?

Make a one-slide overview.

Wallet Type	Description	Use Case	Security Considerations
Hardware Wallets	Physical devices (e.g., Ledger, Trezor) that store private keys offline.	Long-term holding and high-value storage	Highest security, immune to online attacks, but can be lost.
Software Wallets	Apps for desktops or mobile devices (e.g., MetaMask, Trust Wallet).	Everyday transactions	High convenience, but vulnerable to malware or hacks.
Web Wallets	Wallets accessed via a web browser (e.g., Coinbase, Binance Wallet).	Quick access and easy setup	Custodial (on exchanges), risk of hacks and centralized control.
Paper Wallets	Printed QR codes or private keys on paper, stored securely offline.	Cold storage for long-term savings	Secure offline, but physical damage or loss is possible.
Multisignature Wallets	Requires multiple keys from different parties to authorize transactions.	Corporate or shared funds	Enhanced security through multiple approvals, but complex setup.
Smart Contract Wallets	DeFi wallets that enable programmable transactions using smart contracts.	Advanced DeFi use cases	Security depends on smart contract code, risk of exploits.

Wallets

Beyond personal wallets, how do institutions, organizations, or DAOs store and manage digital wallets? Hint: Explore Qredo, Gnosis Safe, and the concept of multi-signature (multi-sig) wallets. Also, check out Multi-Party Computation (MPC) wallets.

Multi-Signature (Multi-Sig) Wallets	Multi-Party Computation (MPC) Wallets	Custodial Wallets
require multiple private keys to authorize a transaction , increasing security by distributing signing authority among several parties	splitting a private key into multiple pieces across different parties without ever combining them into one complete key	Institutions often opt for custodial solutions where a third-party custodian manages private keys on their behalf
Gnosis Safe	Qredo	Coinbase Custody
Focus on decentralized, shared control for security	Advanced cryptography ensures no single entity holds the full private key at any moment	Ease of use and strong regulatory compliance
useful in DAOs and collaborative environments	Best suited for institutions needing the highest levels of security and regulatory compliance	Ideal for large institutions with regulatory concerns or who prefer outsourcing key management