



UNIVERSITY *of* NICOSIA

Session 7

Cryptocurrency Taxonomy

DFIN 511: Introduction to Digital Currencies

Objectives

- Provide a framework for classifying existing cryptocurrencies and tokens.
- Learn some key characteristics and differences in each category, and understand why they are important.
- Explore some notable cryptocurrencies in each category.

Boundaries between categories are not always 100% clear in an area of constant innovation, experimentation, and practically infinite combinations of characteristics and functionalities that a cryptocurrency might have.

Disclaimer: As usual, the inclusion of any particular blockchain project or organisation is for educational purposes only. This should not be construed as an endorsement or investment advice.

Agenda

1. Cryptocurrency Classification
2. Cryptocurrencies
3. Platform Tokens
4. Utility Tokens
5. Security Tokens
6. Natural Asset Tokens
7. Cryptocollectibles
8. Crypto-Fiat Currencies and Stablecoins
9. Conclusions
10. Further Reading

Session 7: Cryptocurrency Taxonomy

1. Cryptocurrency Classification

How many Cryptocurrencies are there?

- As of March 2021, over 8,700 coins / tokens are listed on popular chart sites, with an estimated total market capitalization of \$1,6 trillion. (Note: Capitalization equals the listed price x the circulating supply)

Cryptocurrencies: 8.794 Markets: 36.267 Market Cap: \$1,683,597,525,369 24h Vol: \$135,061,719,874 Dominance: BTC: 61.7% ETH: 11.9%

Today's Cryptocurrency Prices by Market Cap

The global crypto market cap is \$1.68T, a ▼ 3.04% decrease over the last day. [Read less](#)

The total crypto market volume over the last 24 hours is \$135.06B, which makes a ▲ 3.73% increase. The total volume in DeFi is currently \$12.66B, 9.38% of the total crypto market 24-hour volume. The volume of all stable coins is now \$106.83B, which is 79.10% of the total crypto market 24-hour volume.

Bitcoin's price is currently \$55,767.98.

Bitcoin's dominance is currently 61.71%, an increase of ▲ 0.49% over the day.











- FUN FACT:** only the first ~2,000 listed coins / tokens usually have any measurable market capitalization.

Source: <https://coinmarketcap.com/> <https://www.coingecko.com/en>

Session 7: Cryptocurrency Taxonomy

Top 20 Cryptocurrencies' ranking by market capitalization

- As of September 2021, over 11,500 coins / tokens are listed on popular chart sites, with an estimated total market capitalization of \$2 trillion. (Note: Capitalization equals the listed price x the circulating supply)

#	Name	Price	24h %	7d %	Market Cap
1	 Bitcoin BTC	\$47,463.85	-1.49%	-0.97%	\$893,405,970,904
2	 Ethereum ETH	\$3,402.61	-4.13%	-7.56%	\$399,006,495,594
3	 Cardano ADA	\$2.78	-1.66%	-5.68%	\$89,485,724,727
4	 Binance Coin BNB	\$471.06	-0.83%	-0.88%	\$79,432,797,376
5	 Tether USDT	\$1.00	-0.07%	-0.02%	\$65,503,422,544
6	 XRP XRP	\$1.20	-5.77%	-4.05%	\$55,936,796,212
7	 Dogecoin DOGE	\$0.2805	-0.79%	-2.43%	\$36,996,100,335
8	 Solana SOL	\$113.70	-7.57%	-61.28%	\$33,179,059,822
9	 Polkadot DOT	\$30.89	-21.31%	-22.96%	\$30,984,171,575
10	 USD Coin USDC	\$1.00	-0.03%	-0.02%	\$27,487,520,452

Source: <https://coinmarketcap.com/>

Classifying Cryptocurrencies

- All cryptocurrencies and tokens will not share many of the same key characteristics.
- First we should classify the most notable examples based on a variety of criteria.
- For the purpose of this course, we will use the [Blockchain Research Institute Taxonomy of Cryptoassets](#).
- This should provide the background to understand whether a given cryptocurrency or token falls within the purview of national and/or international regulations.

Classifying Cryptocurrencies



Source: Blockchain Research Institute

Session 7: Cryptocurrency Taxonomy

2. Cryptocurrencies

Bitcoin

- Cryptocurrencies (in the taxonomy, 'payment tokens') are the native cryptographic asset of a particular blockchain protocol, designed and intended to 'serve as a general purpose store of value or medium of exchange.' These are two of the main functions of money that we covered in Week 1: A Brief History of Money.
- Bitcoin (BTC) is the leading example in this category.
 - Genesis Block: 3 January 2009
 - Consensus Mechanism: Proof-of-Work
 - Average Block Time: 10 minutes
 - Total Supply Limit: 21 million bitcoin
 - Current Circulating Supply: 18.802 million
 - Market Capitalization: \$893.4 billion (31 August 2021)



Source: https://www.gdf.io/wp-content/uploads/2019/02/0010_GDF_Taxonomy-for-Cryptographic-Assets_Proof-V2-260719.pdf#

<https://coinmarketcap.com/>

Bitcoin Cash and forks



- 1 Aug 2017: Bitcoin Cash (BCH), emerged out of a hard fork of Bitcoin (BTC) prior to SegWit activation, due to a disagreement about the scaling roadmap.
 - BTC: Segwit (increased block size theoretical limit to 4 MB), Lightning Network
 - BCH: No Segwit, increase base block size limit to 32 MB
- 24 Oct 2017: Bitcoin Gold (BTG) emerged as a hard fork of Bitcoin (BTC).
 - BTG Rank: #79, market capitalization of \$1.3 billion
- 15 Nov 2018: Bitcoin Cash hard forked into Bitcoin ABC and Bitcoin Satoshi Vision (BSV).
 - BCH Rank: #15, market capitalization of \$12 billion
 - BSV Rank: #44, market capitalization \$3.19 billion (31 August 2021)

Source: <https://bitcoinmagazine.com/articles/bitcoin-cash-or-bcash-whats-name> <https://coinmarketcap.com/>

Litecoin



- 13 Oct 2011: Litecoin (LTC) went live as a Bitcoin fork.
- Rank: #16 with total market capitalization of \$11.5 billion (31 August 2021).
- Maximum supply: 84 million compared to Bitcoin's 21 million.
- Average block time: 2.5 minutes compared to Bitcoin's 10 minutes.
- Consensus Mechanism: Proof-of-Work utilizing the 'Script' algorithm which is an alternative to SHA-256 used in Bitcoin. Both hash functions are computationally intensive as they both require raw computational power to generate a large number of possible solutions for their respective functions.
- Litecoin was often referred to as the 'silver' to Bitcoin's digital 'gold.'

Source: https://www.litecoin.info/index.php/Main_Page <https://coinmarketcap.com/>

Privacy Coins – Monero

- Monero is one of the most well-known privacy coins. In contrast to Bitcoin's transparent blockchain, Monero makes it harder to trace transaction history without highly specialised tools and resources.
- Rank: #29 with a total market capitalization of \$5.2 billion (31 August 2021).
- Monero uses three techniques to make tracing difficult: Ring signatures, Stealth Addresses and RingCT (short for Ring Confidential Transactions).
- Ring Signatures is a type of group signature that obfuscates/hides the transaction history by associating each transaction input to not just one, but many possible equally valid outputs. This number of possible outputs is called the Ring Size of the transaction, while an outside observer cannot tell which of the possible signers in a signature belongs to your account.
- Stealth Addresses are used to hide recipient addresses. While the recipient can always give the same address to every sender, this address is used to generate a different, one-time address to use each time a transaction is made. Thus, transactions are unlinkable, as nobody can prove that two transactions have the same recipient.



Source: <https://getmonero.org/resources/moneropedia/ringsignatures.html>

Privacy Coins – Monero



- In Jan 2017 RingCT (Ring Confidential Transactions) was introduced.
- RingCT introduces an improved version of ring signatures called “A Multi-layered Linkable Spontaneous Anonymous Group Signature”, which allows for hidden amounts, origins and destinations of transactions with reasonable efficiency and verifiable, trustless coin generation.
- This modification is based on the Confidential Transactions which are used on the Liquid sidechain in Bitcoin, except it allows for their use in ring signatures. Therefore, the modification is given the obvious name of Ring Confidential Transactions for Monero. After Sept 2017, this feature became mandatory for all transactions on the network.
- As of Oct 2018, Monero hark forked again to add bulletproofs for range proving RingCT values. A range proof allows anyone to verify that a commitment represents an amount within a specified range, without revealing anything else about its value. Monero uses the range proof in RingCT to secure the amount being sent in a transaction. Bulletproofs are a more efficient type of range proofs.
- Regulators opposed to such financial privacy have issued guidance about the "risks" of privacy coins such as Monero, leading many exchanges to de-list or avoid listing it.

Source: <https://www.getmonero.org/resources/moneropedia/ringCT.html> <https://eprint.iacr.org/2015/1098>

Privacy Coins – Zerocoin/Zerocash

- Privacy coin Zcash, also tries to make it harder to trace transaction history, in contrast to Bitcoin's transparent ledger.
- Zcash used secure cryptographic techniques called zero-knowledge proof (ZKP), obfuscating / hiding a payment's origin and user identities, but not its destination or amount.
- Zcash employs a special iteration of Zero-Knowledge-Proof is called zk-SNARKs (Zero Knowledge Succinct Non-Interactive Argument of Knowledge) that allow native transactions to remain fully encrypted while still being verified under the network's consensus rules, in which no interaction is necessary between prover and verifier.
- Rank: #66 with total market capitalization of \$1.8 billion (31 August 2021).



Image Source: Wikimedia Foundation

<https://cointelegraph.com/explained/zero-knowledge-proofs-explained>

<http://zerocoin.org/>

<https://z.cash/technology/>

Privacy Coins - GRIN

- GRIN is another privacy coin, launched on January 2019 as an implementation of the MimbleWimble protocol.
- Rank: #565 with market capitalization of \$30 million (12 March 2021).
- MimbleWimble is a blockchain protocol that mixes several innovative technologies (zero knowledge proofs and ring signatures). Transactions in a block are not listed separately (inputs and outputs); instead all inputs and outputs are mixed and aggregated into a single transaction.
- MimbleWimble with this process reduces the size of the blockchain, needing only to store 10% of the data requirements compared to Bitcoin. This means that the blockchain could be smaller, more scalable, and significantly faster to verify, while the coin can be mined with your CPU at home.
- Like Bitcoin, Grin uses Proof of Work (PoW) mining, but with a different algorithm called Cuckoo Cycle, which is intended to be ASIC resistant.



Source(s): <https://cryptobriefing.com/grin-coin-mimblewimble-introduction/> <https://www.coindesk.com/whats-really-private-in-crypto-research-on-grin-raises-questions> <https://blockonomi.com/grin-mimblewimble>

Session 7: Cryptocurrency Taxonomy

3. Platform Tokens

Ethereum

- Platform tokens (in the taxonomy, 'consumer tokens') are designed to support blockchain platforms on which decentralized applications may be built. These “DApps” will have tokens of their own that can be used in the application.
- Ethereum and Ether (ETH) are the leading example in this category.
 - Genesis Block: 30 July 2015
 - Consensus Mechanism: Proof-of-Work; planned shift to Proof-of-Stake
 - Average Block Time: 13 seconds
 - Total Supply Limit: None
 - Current Circulating Supply: 117.33 million ether
 - Market Capitalization: \$401.3 billion (31 August 2021).

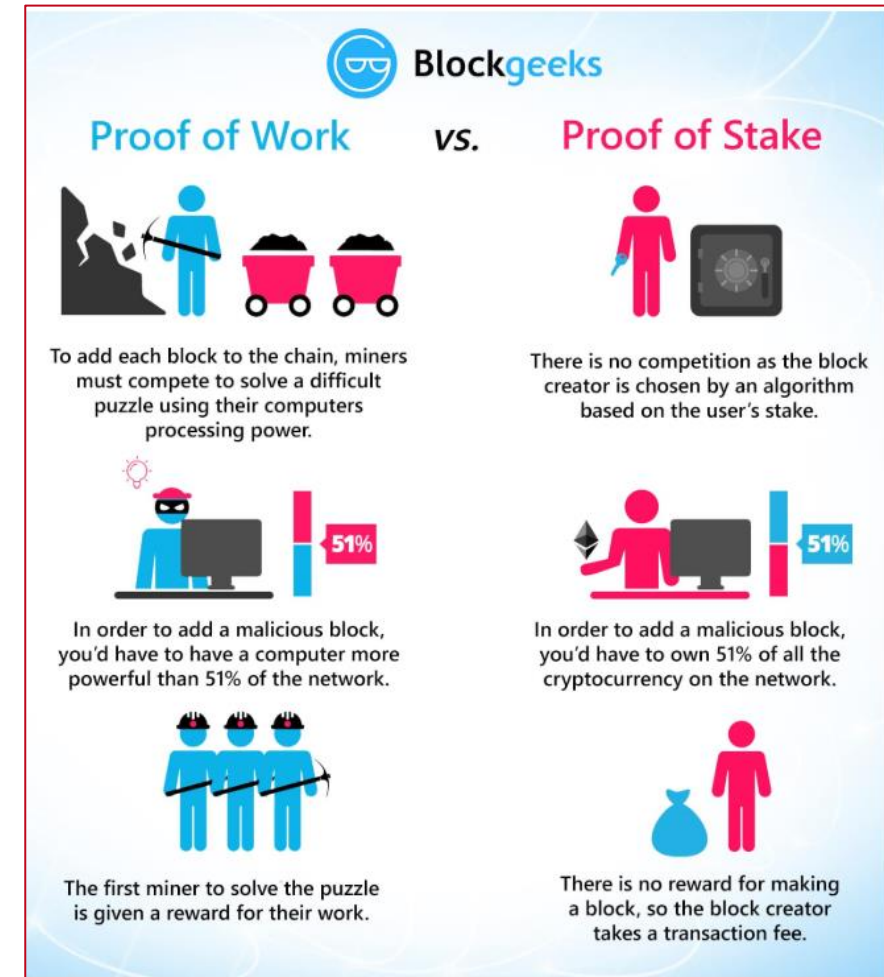


Source(s): https://www.gdf.io/wp-content/uploads/2019/02/0010_GDF_Taxonomy-for-Cryptographic-Assets_Proof-V2-260719.pdf

<https://coinmarketcap.com/>

Proof-of-Stake versus Proof-of-Work

- Proof of Stake (PoS) depends on a validator's economic stake in the network.
- Proof-of-Stake is framed as more environmentally friendly because it does not depend on an external thermodynamically intensive process.
- There is no need to issue as many new coins in order to motivate network participants (no block reward in PoS).
- In order to conduct a 51% attack, you would need to control 51% of the total stake; in proof-of-work, you would need more than 51% of the total hash power.



Source(s): <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#what-are-the-benefits-of-proof-of-stake-as-opposed-to-proof-of-work>

<https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/>

Binance Chain

- **Binance Smart Chain** (BSC) also supports smart contracts, is now the biggest platform chain after Ethereum.
- **Binance Coin** (BNB) is the native token powering the Binance ecosystem.
 - Genesis Block: 18 April 2019
 - Consensus Mechanism: Tendermint BFT (Byzantine Fault Tolerance)
 - Average Block Time: 1 second
 - Total Supply Limit: 170.5 million BNB
 - Current Circulating Supply: 168.1 million BNB
 - Market Capitalization: \$77.8 billion (31 August 2021)



Source(s): https://www.gdf.io/wp-content/uploads/2019/02/0010_GDF_Taxonomy-for-Cryptographic-Assets_Proof-V2-260719.pdf

<https://coinmarketcap.com/>

Polkadot

- Polkadot is a blockchain aiming to provide for multiple blockchains to connect with each other. Polkadot is powered by its native token DOT.
 - Genesis Block: 26 May 2020
 - Consensus Mechanism: Polkadot has a hybrid consensus model, enabled by two tools working together: GRANDPA (GHOST-based Recursive Ancestor Deriving Prefix Agreement) which helps achieve blockchain finality, and BABE (Blind Assignment for Blockchain Extension) helps produce blocks. There are three different distinct node types in the Polkadot blockchain network which ensures operational efficiency (validators, collators, and fishermen)
 - Average Block Time: Polkadot uses Parachains (parallel processing chains) and can go from 100K transactions per second, up to 1 million transactions per second
 - Total Supply Limit: 1.1 billion DOT
 - Reported Circulating Supply: 987.5 million DOT
 - Market Capitalization: \$29.7 billion (31 August 2021)



Source(s): <https://eprint.iacr.org/2020/641.pdf> <https://coinmarketcap.com/>

EOS

- EOS also aims to provide smart contract functionality and be the preferred platform for dApp development, like Ethereum.
- 26 June 2016: EOS tokens are distributed on the Ethereum platform.
- Rank: #32 with market capitalization of \$4.7 billion (31 August 2021).
- Circulated supply: 956.9 million EOS
- Consensus mechanism: Delegated Proof of Stake (DPoS): Unlike Proof-of-Work or Proof-of-Stake in which anyone can verify transactions and produce blocks, in EOS token holders vote for a select set of 21 delegated nodes, who then become block producers, validating transactions.
- The advantage of a DPoS blockchain is its scalability. The 21 EOS delegate nodes, for instance, validate transactions much more efficiently than the over several thousand nodes on Ethereum or Bitcoin. However, this is also more centralized.



Source(s): <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#what-are-the-benefits-of-proof-of-stake-as-opposed-to-proof-of-work> <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/>

Cardano

- Cardano (ADA) is a promising 3rd generation blockchain which is similar to Ethereum.
- It aims to develop more advanced features through ‘a scientific philosophy and a research-first driven approach’.
- Rank: #3 with a market capitalization of \$89.1 billion (31 August 2021).
- Circulating supply: 32.1 billion ADA.
- Consensus mechanism: Proof-of-Stake (PoS).
- Distribution of Cardano tokens started Oct 2015.



Source(s): <https://www.cardano.org/en/genesis-block-distribution-timeline-preview/>

Stellar

- Stellar is a distributed project focused on developing a financial payment infrastructure to facilitate cross-border and multi-currency transactions globally.
- Stellar's native token is 'Lumens' (XLM).
- 31 July 2014: Stellar Lumens initially released.
- Rank: #21 with market capitalization of \$8 billion (31 August 2021).
- Circulating supply: 23.6 billion Lumens
- Maximum supply: Stellar Foundation has **burned** (send to unspendable address without a private key) 55 billion Lumens (XLM) of its previously 105 billion SLM in existence.
- Consensus Mechanism: Proof of Stake.



Source(s): <https://www.coindesk.com/stellars-foundation-just-destroyed-half-the-supply-of-its-lumens-cryptocurrency>

<https://support.blockchain.com/hc/en-us/articles/360018796912-What-is-the-difference-between-Stellar-and-lumens->

Session 7: Cryptocurrency Taxonomy

4. Utility Tokens

Utility Tokens

Utility tokens are intended to provide digital access to an application or service. After the application is completed, utility tokens may give holders perks such as access to the network or voting rights.

Examples include:

- Brave Software's Basic Attention Token (BAT), for a digital advertising exchange ecosystem.
- Golem Network Token (GNT), facilitating a decentralized market for computing power.
- FunFair Token (FUN), an online gaming and casino platform using smart contracts.
- Filecoin (FIL), for a decentralized storage system. The mainnet launched in October 2020.



Source(s): <https://www.merriam-webster.com/dictionary/utility%20token> <https://blockgeeks.com/guides/utility-tokens-vs-security-tokens/> https://www.gdf.io/wp-content/uploads/2019/02/0010_GDF_Taxonomy-for-Cryptographic-Assets_Proof-V2-260719.pdf#

Session 7: Cryptocurrency Taxonomy

5. Security Tokens

Security Tokens

- A classic security is a **fungible** (identical cannot be distinguished from another), negotiable (can be owned and traded) financial instrument that holds some type of monetary value.
- Security Tokens introduced the important concepts of ‘Tokenization’ or ‘Digitization’ or ‘Fractional Ownership’, meaning that an asset (tangible or intangible) can be divided into fungible (identical) tokens, which can be issued, tracked and transferred via the blockchain. This allows for an investor to have ‘fractional’ ownership of an underlying asset.
- Following the Howey Test (a test created by the US Supreme Court for determining whether certain transactions qualify as “investment contracts” or securities), a token will be an investment contract (and therefore subject to securities registration requirements) if:
 - It is an investment of money;
 - There is an expectation of profits from the investment;
 - The investment of money is in a common enterprise; and
 - Any profit comes from the efforts of a promoter or third party.

Source(s): <https://www.investopedia.com/terms/s/security.asp>

https://www.gdf.io/wp-content/uploads/2019/02/0010_GDF_Taxonomy-for-Cryptographic-Assets_Proof-V2-260719.pdf#

ERC-20 Fungible Tokens

- The term 'ERC' stands for Ethereum Request For Comments and the number 20 stands for a unique ID number to distinguish this standard from others.
- ERC-20 is a protocol standard that defines certain rules and standards for issuing tokens on Ethereum's network, recreating the attributes of a security (fungible, transferable, having an intrinsic value).
- The ERC-20 token standard was the first token standard on the Ethereum network.
- Most of the other token standards try to remain ERC-20 compatible, and most wallets implement ERC-20 standards, allowing them to hold and transact compatible tokens.
- The standard implements two fundamental items:
 - the ability to associate token balances with Ethereum addresses
 - the ability to transfer the tokens between addresses

Source(s): <https://coinsutra.com/what-is-erc20-token/>

<https://github.com/ethereum/EIPs/blob/master/EIPS/>

ERC-20 Fungible Tokens

- A key disadvantage with the ERC-20 standard is that it is easily possible to send tokens to addresses that can't handle them (eg, smart contract addresses). Since there is no process for identifying whether an address can support ERC-20 tokens, sending them to such an address will mean that they will be 'burned' (rendered unspendable).
- An extension of the ERC-20 standard, ERC-777, tries to address some of these disadvantages:
 - Tokens can only be sent to smart contracts that are able to receive them.
 - Sending and receiving contracts are notified when a transfer is happening and can cancel it.

Source(s): <https://coinsutra.com/what-is-erc20-token/> <https://github.com/ethereum/EIPs/blob/master/EIPS/>

Session 7: Cryptocurrency Taxonomy

6. Natural Asset Tokens

Natural Asset Tokens

- Natural Asset Tokens represent tangible goods in established markets (like gold, oil, natural gas, base metals) or in frontier markets (like carbon, water, air).
- Earth Token is a decentralized Natural Asset Exchange blockchain platform with accompanying Earth Token (EARTH).
- Power Ledger is a blockchain-based, peer-to-peer energy platform that lets users buy and sell electricity, using Power Ledger Token (POWR) ERC-20 tokens.
- SunContract is a similar blockchain platform for trading energy, using the Sun Token (SUN).
- Note: the boundaries in classifying Natural Asset Tokens are not completely clear. Depending on the details of how it is structured, it could be seen as a Security token or a 'Stablecoin' (next chapter).



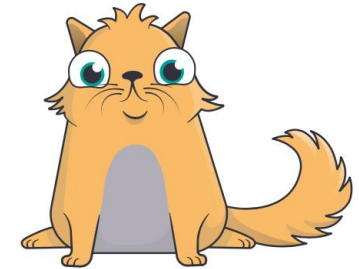
Source(s): <https://www.royalmint.com/invest/bullion/digital-gold/> <https://cryptobriefing.com/what-is-power-ledger-network-introduction-to-powr-and-sparkz-tokens/> <https://thefintechtimes.com/royal-mint-gold-british-blockchain/>

Session 7: Cryptocurrency Taxonomy

7. Non-Fungible Tokens - Crypto Collectibles

Non-Fungible Tokens – Crypto-collectibles

- Non-Fungible Tokens (NFTs) have unique properties, meaning they can be distinguished from another and cannot be duplicated.
- The ERC721 standard on Ethereum is fundamental for non-fungible tokens.
- “CryptoKitties” are unique virtual cats that people can purchase, trade, raise, and even breed with other CryptoKitties.
- Non-Fungible Tokens can also be used in gaming to create unique gaming characters.
- They may also be linked to unique real-world assets such as art or rare cars, and can allow investors to own a fractional interest in such a unique asset.



Source(s): <https://www.royalmint.com/invest/bullion/digital-gold/>

<https://cryptobriefing.com/what-is-power-ledger-network-introduction-to-powr-and-sparkz-tokens/>

<https://thefintechtimes.com/royal-mint-gold-british-blockchain/>

Session 7: Cryptocurrency Taxonomy

8. Crypto-fiat currencies and Stablecoins

Stablecoins

- Stablecoins (as the term indicates) were introduced to address the high price volatility of Bitcoin, Ethereum and other altcoins and designed to maintain a relatively stable value (at least short-time).
- A stable coin is tied or 'pegged' to an underlying asset or currency, can take many forms and can reference the following assets:
 - Fiat currencies. A crypto-asset can be related to one or more fiat currencies.
 - Other real-world assets such as securities, commodities, real-estate, financial instruments and/or other assets.
 - Other crypto-assets. A crypto-asset can be related to one or more other crypto-assets.
 - Algorithmically controlled. A crypto-asset can use an algorithm that attempts to mimic monetary policy and adjust the supply of tokens to match demand.
- Regarding how stablecoins are implemented we may classify two broad categories:
 - Centralized custodial stablecoins: the underlying asset(s) are held by a centralized custodian.
 - Decentralized non-custodial stablecoins: managed in a decentralized fashion, operated through smart contracts, that has reserves in cryptocurrency, rather than fiat.

Source(s): <https://en.wikipedia.org/wiki/Stablecoin>

<https://www.iosco.org/library/pubdocs/pdf/IOSCOPD650.pdf>

Centralized Custodial Stablecoins: FIAT-backed

- Fiat-backed were the first type of stablecoins in the market and the most common.
- They may be backed by only one fiat currency (usually USD) or more fiat currencies (Euro, Swiss Franc) in a fixed ratio.
- The amount of currency used for backing the stablecoin has to reflect the circulating supply of the stablecoin, and is usually held by a regulated entity.

Examples:

- Tether (USDT) : Rank: #5 with total market cap. \$65.5 billion as of 31 August 2021.
- USD Coin (USDC) by Coinbase: Rank: #10 with total market cap. of \$27.4 billion.
- Paxos (PAX): Rank: #98, with total market cap. \$945 million.
- Stablecoins are now used by financial institutions to facilitate fast and low cost cross-border transfers.



Source(s): <https://www.coindesk.com/jpmorgan-to-start-customer-trials-of-its-jpm-co>

<https://cryptoslate.com/cryptos/stablecoin/in-crypto>

Centralized Custodial Stablecoins: Commodity backed

- Stablecoins can be backed by one or more commodities (i.e gold, silver).
- The amount of commodity used to back the stablecoin has to reflect the circulating supply of the stablecoin. Examples:
 - Digix Gold Token (DGX): 1 DGX = 1 gram of gold
 - Tether Gold (XAUT): 1 XAUT= 1 troy fine ounce of gold, being able of being fractionalized up to six decimal places (i.e. in increments as small as 0.000001 troy fine ounce).



Source(s): <https://digix.global/#/> <https://gold.tether.to/>

Centralized Custodial Stablecoins: Basket – Weighted currencies backed

- Libra was initially announced to be a basket of currencies (bank deposits and government debt) referred to the 'Libra Reserve'.
- The launch has been delayed, after various concerns were raised by financial regulators and consumer advocates.
- Libra has now been renamed to Diem, aiming to debut as a single USD pegged coin, in its attempt to get regulatory approval.
- It is intended to be used as a means of payment.
- Novi will be the digital wallet for Diem, available in Messenger, WhatsApp, and as a standalone application.



Decentralized non-custodial stablecoins

- Decentralized non-custodial stablecoins are managed in a decentralized fashion, operated through smart contracts, that has reserves in cryptocurrency, rather than fiat.
- Makerdao is a smart contract platform on the Ethereum blockchain that backs and dynamically stabilizes the value of the Dai stablecoin.
- The goal is to have a pegged value of 1 DAI = 1 USD, entirely backed up by one or more cryptocurrencies (DAI can be backed by ETH, BAT or even USDC).
- Explanation: Since last year DAI is multi-collateral DAI and can now be backed by a basket of coins, including some stablecoins that are custodial (Coinbase's USDC). The original DAI is now called SAI for "Single-collateral DAI" and is backed only by ETH.
- A smart contract controls a 'Collateralized Debt Position' (CDP) which is practically a vault in which you invest a cryptocurrency (ETH). Based on how much ETH you put in, you can choose a collateralization ratio and have the smart contract issue DAI against your ETH collateral.



Decentralized non-custodial stablecoins

- There are no central operating actors at MakerDAO - both its code (or protocol) and governing community are decentralized.
- DAI is also part of a broader and growing Decentralized Finance (DeFi) ecosystem, which focuses on building financial services separate from the traditional financial system.
- So far DAI has remained relatively stable, being able to maintain a 95-98% peg versus a full 1 DAI = 1 USD peg.
- The concept is still being tested and significant risks are still involved in terms of investing.



<https://makerdao.com/en/>

Session 7: Cryptocurrency Taxonomy

9. Conclusions

Conclusions

- In this session, you have learned about various categories of cryptographic digital currency and tokens, including: cryptocurrencies, platform tokens, utility tokens, security tokens, colored coins, natural asset tokens, crypto-collectibles, crypto-fiat and stablecoins.
- We explored one or a few examples of each, highlighting the distinguishing features and data points such as novel signature schemes, ranking, and circulating supply.

Session 7: Cryptocurrency Taxonomy

10. Further Reading

Further Reading

List of cryptocurrency market capitalizations:

- <https://coinmarketcap.com/all/views/all/>

Cryptocurrencies with much faster block times than bitcoin

- <https://themerple.com/4-cryptocurrencies-with-much-faster-block-times-than-bitcoin/>

Monero

- <https://www.monero.how/how-does-monero-privacy-work>
- <https://www.monero.how/how-does-monero-work-details-in-plain-english>

Dash - Proof of Stake

- <https://coinsutra.com/dash-cryptocurrency/>

Grin Coin

- <https://grin-tech.org/>
- <https://blockonomi.com/grin-mimblewimble/>

Another Mimblewimble based coin: <https://www.coinbureau.com/review/beam-coin/>

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

Further Reading

Stablecoins Trend

- <https://www.forbes.com/sites/yoavvilner/2019/03/02/stablecoin-101-all-there-is-to-know-about-the-trend/#26a614131c37>
- Consensus Algorithms
- <https://hackernoon.com/a-hitchhikers-guide-to-consensus-algorithms-d81aae3eb0e3>

Zcash: Decentralized Anonymous Payments from Bitcoin

- <http://zerocash-project.org/paper>
- <https://blockonomi.com/zcash-guide/>

Digital assets trading platforms:

- <https://www.coindesk.com/fidelity-reveals-cryptocurrency-and-digital-asset-trading-platform>
- <https://www.coinspeaker.com/tzero-security-trading/>

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



UNIVERSITY *of* NICOSIA

Questions?

Contact Us:

Twitter: **@mscdigital**

Course Support: **digitalcurrency@unic.ac.cy**

IT & Live Session Support: **dl.it@unic.ac.cy**