



UNIVERSITY *of* **NICOSIA**

MSc in Digital Currency

Introduction to Digital Currencies

Session 7

Alternative Uses of the Blockchain II

DFIN-511: Introduction to Digital Currencies

Session Objectives

- ▼ Provide an overview of some popular alternative currencies and DLT networks
- ▼ Devise categorization criteria for most popular alt-coins
- ▼ Summarize Key Performance Indicators (KPIs) to keep in mind when assessing alternative digital currencies
- ▼ *As mentioned in Session 6, boundaries between concepts are not always 100% clear in an area of constant innovation. Bitcoin might be the “king” (with about 50% of the total space market capitalization) but there are alternative digital currencies that represent various functionalities and advancements. There are also alternative blockchain infrastructures with the aim to innovate procedures in terms of efficiency, cost, scalability and speed.*
- ▼ *In the following pages, we aim to build a framework for the reader to better understand the notions behind networks that are being developed, other than Bitcoin. This session is devoted to them since they certainly deserve our attention.*
- ▼ *We will examine the nature of Initial Coin Offerings in Session 11 which is dedicated to innovation*

Agenda

1. Why alternative currencies?
2. Indicative alternatives
3. Common characteristics
4. Criteria for categorization
5. KPIs for assessing digital currencies
6. Permissioned Ledgers and Private Blockchains
7. Conclusions
8. Further Reading

A decorative border on the left side of the slide, composed of various sizes and orientations of triangles. Some triangles are solid dark red, while others are outlined in dark red. The pattern is dense and abstract.

1. Why alternative currencies?

Why alternative currencies?

- ▼ **Bitcoin is the first application of a technology that paves the way forward, revealing an opportunity for innovation that was not apparent before.**
- ▼ Bitcoin is wholly open source, so every element of it can be tweaked, modified, altered and tested for potentially improved iterations, just like evolution.
- ▼ Bitcoin's blockchain has grown large (approximately 206GB by March 2019) – and will only become larger, as Bitcoin use becomes more widespread.
- ▼ The process of mining is power intensive, which may be argued is with a disproportionate benefit towards the network, unless this is mutualized to many more transactions.
- ▼ The nature of a predetermined, and eventually deflating monetary base as coins are irrecoverably lost, may also be among the dissuading factors of some using it.

Why alternative currencies?

- ▼ The freedom to try out every possible solution has driven many to spawn their own “alt – coins”, with their own rules and their own networks. Other concepts like Ripple have also flourished and are being tested for transaction efficiency among governmental and corporate institutions.
- ▼ While some are merely small modifications of the Bitcoin protocol and have limited audiences, others are interesting sources of innovation. The differences derive from changes in the basis of blockchain/DLT philosophy which are achieved in a variety of ways, such as:
 - ▼ Altering the issuance method to less energy intensive processes
 - ▼ Adding more functions like smart contracts
 - ▼ Improving fungibility and privacy characteristics of the currency itself
 - ▼ Altering the monetary supply and issuance rate
 - ▼ Altering the hashing algorithms or other parameters
 - ▼ Introducing other concepts such as demurrage to increase the velocity of money

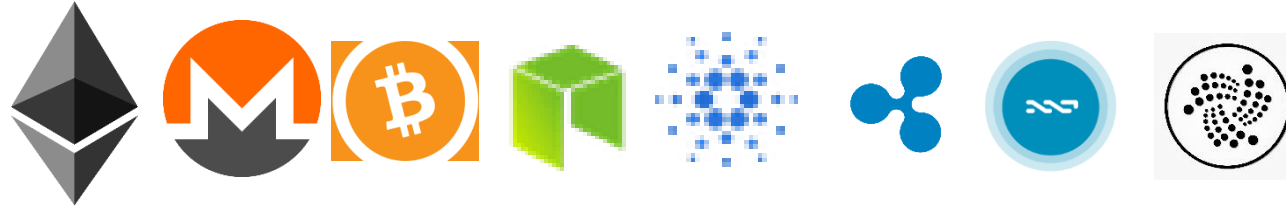
A decorative border on the left side of the slide, composed of various triangles in different shades of red and pink, arranged in a complex, overlapping geometric pattern.

2. Indicative alternatives

A decorative border on the right side of the slide, featuring a few scattered triangles in red and pink, including one solid red triangle at the top right.

Indicative alternatives























Bitcoin may be the king, but several alt-coins have seen plenty of attention :



Cryptocurrencies: 2093 • Markets: 16097 • Market Cap: \$130,522,321,810 • 24h Vol: \$27,762,315,509 • BTC Dominance: 52.1%

- ▼ The so called “market cap” (available supply*current exchange rate) for each coin, is at best a vague indicator of each coins’ adoption. Several other important factors are harder to quantify and are not usually considered in tandem (user base, merchants accepting, exchanges trading each coin, active development taking place, availability of coins in the market, etc.)
- ▼ Even if we assume, that these elements are already “embedded” in the exchange rate of each coin, there is still a degree of subjectivity surrounding valuation and the final exchange rates

Indicative alternatives

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)	
1	 Bitcoin	\$68,044,479,980	\$3,874.39	\$8,304,059,618	17,562,625 BTC	0.15%		...
2	 Ethereum	\$14,482,101,523	\$137.87	\$4,566,434,164	105,040,796 ETH	-1.31%		...
3	 XRP	\$13,014,130,902	\$0.314612	\$680,490,100	41,365,634,610 XRP *	-1.52%		...
4	 EOS	\$3,253,093,867	\$3.59	\$1,354,871,403	906,245,118 EOS *	1.83%		...
5	 Litecoin	\$2,801,839,376	\$46.18	\$1,095,506,536	60,668,186 LTC	0.81%		...
6	 Bitcoin Cash	\$2,360,440,152	\$133.76	\$289,319,049	17,646,375 BCH	-0.68%		...
7	 Tether	\$2,041,331,749	\$1.01	\$7,820,158,377	2,021,459,017 USDT *	-0.14%		...
8	 Stellar	\$1,641,514,504	\$0.085471	\$108,755,506	19,205,488,369 XLM *	-0.99%		...
9	 TRON	\$1,607,648,471	\$0.024109	\$145,079,379	66,682,072,191 TRX	-0.84%		...
10	 Binance Coin	\$1,414,725,131	\$10.02	\$93,425,671	141,175,490 BNB *	2.51%		...
11	 Bitcoin SV	\$1,196,230,358	\$67.79	\$110,451,651	17,644,911 BSV	-5.63%		...

source:
coinmarketcap.com,
as of February 28,
2018

The * indicates
cryptocurrencies
which are not
mineable

A coin by any other name

- ▼ Any means of exchange that is based on the design concepts of Bitcoin, yet with differences or enhancements in its implementation, could be considered an “alt-coin”.
- ▼ An alt-coin is in some cases considered a software “fork” of the Bitcoin code, with minor alterations to its characteristics. Using the original open source software with a number of modifications, these new coins have different properties and create their own blockchains, which are unrelated to the Bitcoin blockchain. Some designs start from the ground up, with new code and additionally confer other characteristics to the functionality of the coins themselves (like Ethereum, Monero, NXT or Ripple).
- ▼ Their market cap is only one possible indicator of their prowess in the market, and is usually not meant to be directly comparable between different coins.

Ethereum

- ▼ **Ethereum** is a hybrid meta/alt-coin (briefly discussed in Session 6) that attempts to build, in their own words, “a revolutionary new platform for applications”, targeting anything from voting to financial exchanges, to smart property, and most importantly, **decentralized applications**. Even though the currency used in the network is an alt-coin (ether), it is used more as computational fuel than a scarce currency. Ethereum features:

- ▼ A standardized foundation platform (i.e. the enhanced Ethereum programming abstractions, protocol and network)
- ▼ A programming language to facilitate the creation of distributed applications by anyone. Besides validation and distributed storage enhanced by Bitcoin, Ethereum also enhances processing of data and logic
- ▼ Its own currency or cryptofuel – the “Ether” which can be tracked on the blockchain
- ▼ Ethereum nodes can validate and process more information rather than just payments
- ▼ Ethereum block time is approximately 14 seconds but can vary.
- ▼ Ethereum block size ranges between 20kb-25kb and is based on the smart contracts’ complexity

One of the very important concepts that Ethereum attempts to achieve is a level of being “**Turing Complete**”. (Definition) The explanation given by the Ethereum team is that they are attempting to make a quasi-Turing-complete system. The cost of each step of these recursive processes or loops is the fuel of the system (ether) as a fee.

- ▼ Ethereum is based on the concept of self-executing smart contracts (Session 6), software contracts that execute specific instructions upon interacting with them through transactions.



Source: ethereum.org

Ethereum

- ▼ **Ethereum is a decentralized open-source platform developed to host smart contracts.** Ethereum blockchain is able to run the programming code of any decentralized application.
- ▼ Transactions create smart contracts, stored on the blockchain and nodes. Smart contracts are first uploaded on the Ethereum blockchain i.e a users sends the code to the miners who process the transaction. These smart contracts are then facilitated by sending gas to the miner to run it. Miners then compete for the Proof-of-Work and the winner broadcasts the block to the network
- ▼ All Ethereum nodes validate blocks, run the contract code and update their ledger with the result. This is done by the **Ethereum Virtual Machine** (EVM) used by the participants.
- ▼ Developers can build thousands of different applications, different to anything we have seen before, because of Ethereum's real innovation, the **EVM**.
- ▼ **EVM** enables users to run any program, no matter what the programming language is, given there is enough time and memory available. In simple words, EVM is able to perform any calculation that any other programmable computer is capable of, therefore capable of designing any type of smart contract.
- ▼ Instead of having to build a new blockchain for each new application, Ethereum enables the development of many applications all on one platform.
- ▼ See [here](#) for the equivalent clients to Bitcoin's Bitcoin Core. Upon installation, you can connect to the network, validate transactions/blocks, create new transactions and contracts, run contracts and mine.



ETHEREUM

EVM

- The EVM processes and keeps track of all transactions, blocks and smart contract results. Basically Ethereum nodes run the EVM which runs the smart contracts' code and come in agreement of its state.
- Different kinds of Ethereum transactions exist, which add to its complexity (i.e. a simple transaction to send an ETH balance which costs 21,000 gas vs a transaction to upload and run a smart contract).
- “Gas” exists to address this complexity. It is imposed to award miners for the operations they are required to perform

Operation Name	Gas Cost	Remark
step	1	default amount per execution cycle
stop	0	free
suicide	0	free
sha3	20	
sload	20	get from permanent storage
sstore	100	put into permanent storage
balance	20	
create	100	contract creation
call	20	initiating a read-only call
memory	1	every additional word when expanding memory
txdata	5	every byte of data or code for a transaction
transaction	500	base fee transaction
contract creation	53000	changed in homestead from 21000

<http://www.ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html>

Ethereum – in detail

- ▼ Ethereum approaches the existing Bitcoin infrastructure as a “state machine”, where transactions (which store messages) serve as “state transitions” between Ethereum accounts without the UTXO basis we saw in Bitcoin. There are two types of Ethereum accounts – the equivalent of addresses in Bitcoin:
- ▼ **“Externally-owned account”** – used only to facilitate payments between users, acts like Bitcoin addresses
 - ▼ *has an ether balance,*
 - ▼ *can send transactions (ether transfer or trigger contract code),*
 - ▼ *is controlled by private keys,*
 - ▼ *has no associated code.*

<http://www.ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html>
- ▼ **Contract account**
 - ▼ *has an ether balance,*
 - ▼ *has associated code,*
 - ▼ *code execution is triggered by transactions or messages (calls) received from other contracts.*
 - ▼ *when executed - perform operations of arbitrary complexity (Turing completeness) - manipulate its own persistent storage, i.e., can have its own permanent state - can call other contracts”*
- ▼ Ethereum messages serve as “functions” and have the following characteristics:
 - ▼ They can be created by an external entity or a contract
 - ▼ They can contain data
 - ▼ They can only receive responses from contract accounts

Ethereum

- ▼ **Ether**, is the token mined which fuels the network. It used by application developers to pay for transaction fees and services on the Ethereum network.
- ▼ Does a vending machine have any uncertainty whether it will deliver your chocolate? An Ethereum application is programmed without any possibility of fraud and downtime.
- ▼ When a transaction is sent with a message addressed to a specific contract, depending on the code embedded into that contract (think about the code as the terms of a legal contract), the contract may **execute transactions, modify its storage, trigger other contracts, etc.**
- ▼ List of Dapps on Ethereum with smart contract functionality:
<https://www.stateofthedapps.com/>

```
contract token {
    mapping (address => uint) public coinBalanceOf;
    event CoinTransfer(address sender, address receiver, uint amount);

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function token(uint supply) {
        if (supply == 0) supply = 10000;
        coinBalanceOf[msg.sender] = supply;
    }

    /* Very simple trade function */
    function sendCoin(address receiver, uint amount) returns(bool sufficient) {
        if (coinBalanceOf[msg.sender] < amount) return false;
        coinBalanceOf[msg.sender] -= amount;
        coinBalanceOf[receiver] += amount;
        CoinTransfer(msg.sender, receiver, amount);
        return true;
    }
}
```

Example of a smart contract on Ethereum

Ethereum – in detail

- ▼ **Transactions** in Ethereum are viewed as “signed data packages” and contain:
 - ▼ **A message** to be sent from an externally-owned account
 - ▼ **A Sender signature** – which indicates the sender of the message
 - ▼ **A Receiver address** – which indicates the receiver of the message
 - ▼ **An Ether amount** – which indicates the amount of Ether to send
 - ▼ **Data** – which encapsulates the data to be sent
 - ▼ **A Start Gas field or sometimes referred to as Gas limit** – which specifies how much gas a user is willing to spend and represents the maximum number of computational steps over which a contract code will execute. This protects a user from paying high fees for a complex transaction, which he/she this is a simpler transaction. If more gas is required from the imposed gas limit, the transaction will fail and mining fee is not reimbursed
 - ▼ **A Gas Price field** – it can be specified when you submit a transaction. The fee which the user is willing to pay the miner at each computational step (Eth to be paid per gas used)
- ▼ To achieve its goals, Ethereum defines its own logic for state transitions processing and code execution, whose details are beyond the scope of this Session.

Mining Fee = Gas Price (amount of ETH per unit of gas to be paid) * Actual Gas Consumed

Ethereum Benefits & Challenges

Benefits:

- ▼ **Security** – Being decentralized and using advanced cryptography, apps are protected against hackers
- ▼ **Immutability** – A third party cannot make any changes to data. Because of the consensus mechanism, corruption and attempts to change the state of the apps is impossible.
- ▼ **Longevity – Zero downtime** – An app never goes down even if someone loses interest in maintaining it

Challenges: (see also next slide)

- ▼ Do not forget that code is written by humans. Therefore smart contracts are as good and reliable as their creators
- ▼ Smart Contracts are still difficult to understand and to be implemented by a non-programmer. Perhaps we should expect that creating a smart contract may become simpler and possible for an average person in the future. OpenLaw is an initiative working towards that idea. <http://openlaw.io/>

Still a long way to mature

- ▼ The concept is still in an early phase. That's why we cannot see a decentralized application which has gone mainstream and disrupted an industry
- ▼ Questionable if it is ideal beyond the finance/business sector even though the concept of ERC-20 tokens aims to boost adoption via a universal standard.
- ▼ Many sectors still require human judgment, i.e. how about a car accident?
- ▼ Oracles are able to link events from the outside world and combine information while the contract code is executed. Oracles can include business logic, laws and other agreed terms within a contract. However, this concept is still in an early stage. Oraclize is a promising project. <http://www.oraclize.it/>
 - ▼ E.g. my insurance company is compensating me in case of flood according to the amount of water entered into my field – How is this going to be recorded reliably? What kind of oracle is going to be used?
- ▼ Legality of smart contracts is questionable
- ▼ Privacy? Current implementations are mostly public
- ▼ Difficult to understand for non-programmers
- ▼ Scalability issues – every transaction needs to be processed by every node



Ethereum, progress so far and roadmap

- ▼ Ethereum is so far, one of the most highly crowdfunded project globally, gathering a staggering 31,529.49449551 BTC by September 3rd 2014 (address). Total amount of Bitcoins received as of March 2019 is approximately 31,550.50.
- ▼ To perform everything the team is poised for, in a scalable and secure manner is a very tall order in itself. Several implementations of the Ethereum VM already exist, including C++, Go, Java, Python, JavaScript, Node, NET
- ▼ Homestead is the second release of the Ethereum project, moving beyond developers and to the mainstream, after the successful hard fork towards it. This is not to be confused with the DAO sustained hard fork which happened later, and resulted in two version of the protocol and two chains (ETH and ETC).
- ▼ "Metropolis" is the third release with the aim to reduce complexity of the EVM and provide flexibility for smart contract developers. zk-SNARKs and ring signatures support is added. It is divided into 2 steps: Byzantium and Constantinople which was implemented on February 28th at block number 7,280,000.
- ▼ The last phase is Serenity – the conversion of the Ethereum Network from Proof-of-Work to Proof-of-Stake

The world computer?

- ▼ While Frontier allowed only for command line, the production release of Ethereum called [Homestead](#) was released via a hard fork of the blockchain, and it allows users to build more on the platform. More information on the improvements of Homestead can be found [here](#)
- ▼ More resources and use cases are springing daily, making the Ethereum blockchain grow far faster than Bitcoin's ever has.
- ▼ A consortium of large companies including JPMorgan, Intel, Microsoft And Others formed the [Enterprise Ethereum Alliance \(EEA\)](#), which aims at creating a standard version of the Ethereum software that businesses around the world can use to track data and financial contracts.
- ▼ The most recent update came in October 3, where the EEA and Hyperledger [announced](#) that they are joining each other's organizations to enable *“more active and mutual cross-community collaboration through event participation, connecting with other members, and finding ways for our respective efforts to be complementary and compatible”*. The goal is to accelerate the evolvement of blockchain technology for businesses.

The DAO hack and the ensuing fallout

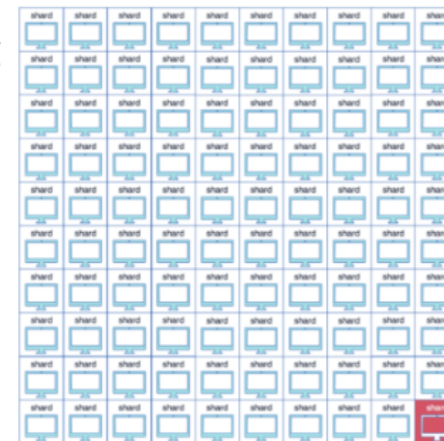
- ▼ “The DAO” (Decentralized Autonomous Organization) had a formidable calling, to create the first decentralized crowdfunding platform, a place where investors would have proportional decision making ability on the investment of funds which a decentralized organization held. At its height it gathered about \$160 million (at that time), and became the largest crowdfunded project ever by then.
- ▼ Despite criticism on the “too much, too fast, too early” nature of the project while it was starting, it went on, and on Friday June 17th 2016, an attacker syphoned about \$50 million worth of the native tokens away. The exploit used was suggested as an attack vector before, and was even, reportedly, fixed.
- ▼ The proposed solution by the ETH community was a hard fork to remove the funds from the attacker. This caused a split in the community as not everyone was in favor of “bailing out” the DAO since it was a construct on ETH and not an ETH vulnerability itself. This led to a hard fork and the creation of two Ethereum blockchains. The majority one (retained the Ethereum name) and the minority one was named Ethereum Classic.
- ▼ Some further reading :
- ▼ <https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/>
- ▼ <http://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/>

Ethereum switch to Proof of Stake (PoS)

- ▼ Several very novel approaches are being implemented in Ethereum, including an improved version of the GHOST protocol to decrease block times, and the transition to Proof of Stake, called Casper.
- ▼ As Ethereum is growing, more miners want to enter the game
- ▼ One reason for this switch from Proof of Work (PoW) to PoS is environmental friendliness as PoW is very wasteful in terms of electricity usage
- ▼ It was also taken into consideration that if PoW remained in place, people with money and resources to mine the most ETH would be the majority of miners, therefore creating an unbalanced distribution of wealth and mining power. The average person can not afford to set up and maintain a mining rig and this is directly opposite to the ideals of a decentralized economy
- ▼ PoS addresses this issue by making the mining process affordable to the average person. This allows the mining environment to continue to grow and attract more participants, supporting the essence of a decentralized economy
- ▼ This is because under PoS, in order to mine ETH a miner needs to own a certain amount of ETH staked for the mining operation. The amount of ETH mined would be based on the amount staked
- ▼ The calculations processed in POS are simpler to solve than PoW. As a result no wasteful miners are needed.
- ▼ The obvious drawback is that miners owning a considerable amount of ETH have a distinct advantage over new miners entering the game, but in any case it is a step towards the right direction

Scaling Ethereum

- ▼ Layer 1 Solution: What if each node does not have to process each transaction
 - ▼ Aim: Increase Ethereum network transaction capacity
 - ▼ Notable Proposal: **Sharding**
- ▼ In Sharding, the idea is to split the network into many shards each one containing their own dependent piece of blockchain history. Someone can see this system as many small blockchains running with their own validating nodes which would increase the throughput of transactions processed.
- ▼ To avoid a single-shard attack the idea is a random sampling of validators on each shard. Validators will not know which shard they will get. Many validators will work on each shard and the ones that will actually be validating will be randomly selected from this set.



1% Attack

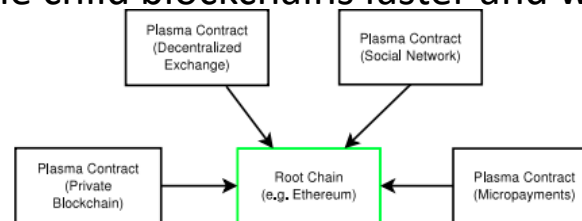
“ In 100 shards system, it takes only 1% of network hash rate to dominate the shard. ”

Credits Hsiao-Wei Wang

For further explanation of Sharding click [here](#)

Scaling Ethereum

- ▼ Layer 2 Solutions – built on top of the Ethereum main-chain: Can we do more thing with the current capacity capabilities?
 - ▼ Aim: Operate more useful transactions and decentralized applications with the current capacity
 - ▼ Notable Proposals: Smart contracts interacting with off-chain software - **State Channels, Plasma and Truebit**. No changes to the base level protocol are needed
- ▼ **State channels**: The equivalent of payment channels in blockchain – can be used for payments and blockchain state updates such as modifications in a smart contract
- ▼ **Plasma**: Creation of “child blockchains” attached to the main-chain. Child blockchains can create their own “child blockchains” and so on. The interaction with the main-chain is very limited, while thousands of decentralized applications can run on the child blockchains faster and with lower confirmation times.



plasma.io/plasma.pdf

- ▼ **Truebit**: Move heavy and complex computation off-chain. The aim is to allow dapps to run more computationally expensive operations outside the main-chain but still be verifiable by it. Example: Validation of SPV proofs from other blockchains. The computation is done off-chain with a much cheaper transaction fee for the solver. The solvers pay a deposit in a smart contract and only when they run the computation and return a result, their deposit is returned. Results are checked via a **verification game**

Augur

- ▼ An example of a Dapp is **Augur** (www.augur.net) - A decentralized prediction market which is built on the Ethereum blockchain

How it Works

- ▼ Users purchase and sell shares in the outcome of an event
- ▼ **The current market price of a share is an estimate of the probability of an event occurring** – this is a typical application of the **wisdom of the crowd** principle.

The role of Blockchain

- ▼ Augur aims to address traditional prediction market drawbacks by eliminating counterparty risks and allowing users to settle their bets in cryptocurrencies. **Funds are stored in smart contracts.**
- ▼ Augur uses the crowd to report on market outcomes. Each reporter keeps a reputation balance (REP), based on the correct outcomes s/he has provided in the past.
- ▼ Using Augur, users are able to create a prediction market on any subject and win trading fees (either as market makers or as good reporters).
- ▼ See this video for more explanation <https://www.youtube.com/watch?v=yegyih591Jo>

Augur



Other dapps developed on Ethereum

- ▼ WeiFund (<http://weifund.io/>): A decentralized, secure crowdfunding platform which allows the integration of smart contracts. It allows contributions to be turned into contractually backed digital tokens that can be stored and traded within the Ethereum ecosystem
- ▼ Provenance (<https://www.provenance.org/>): Enables businesses to use the Ethereum blockchain in order to provide supply chain transparency on their goods. By tracing the origins and the path of products from their creation until the time they are consumed by people, the project aims to help consumers select the better quality products.
 - ▼ Whitepaper: <https://www.provenance.org/whitepaper>



Monero, a short introduction

- ▼ Monero was launched on April 2014 as a fork of Bytecoin. Bytecoin was an obscure cryptocurrency that, while having pioneered a novel way to achieve privacy, was plagued with a shady history and an unfair launch. As a result, the community forked the code of Bytecoin and began a long, multi-year project of cleaning it up, documenting it, and getting the fundamental aspects of it right.
- ▼ Monero focuses on providing strong privacy by default while offering optional transparency, allowing its users to selectively disclose their transactional history to selected parties. Privacy is inherent to the protocol and requires no additional steps (interactivity) from the user. As a result, fungibility is greatly improved as well.
- ▼ Monero's architecture provides a clear separation of the node functionality and the wallet. Originally having just a command line wallet, which was deemed too difficult for non-technical users to use. The second beta of Monero's Graphical User Interface (GUI) was released in late March 2017.

Monero, Privacy and Fungibility

- ▼ In Bitcoin, transactions are traceable as the transaction graph is visible in the blockchain; sender and recipient addresses as well as transaction amounts are visible. This makes Bitcoin vulnerable to coin tainting and susceptible to blockchain analysis, thus potentially significantly reducing its fungibility and usefulness as digital cash (which should be indiscernible from any other coin). Various techniques have been proposed and utilized to improve Bitcoin's privacy, however they either suffer from having to trust centralized services (coin mixers) of dubious quality and legal status, or from requiring manual user intervention and coordination (such as CoinJoin).
- ▼ Providing privacy and fungibility by default is considered a core principle of the Monero project. Monero obscures the transaction graph and hides transaction amounts by a combination of Ring Signatures and Confidential Transactions, and hides user addresses via the use of Stealth Addresses.
- ▼ Mobile & Light Wallets proposed by members of the community
 - ▼ <https://mymonero.com/#/>
 - ▼ <https://monerujo.io/>

Monero, Ring Signatures

- ▼ Monero originally used two techniques to make blockchain analysis difficult: Ring signatures and Stealth Addresses.

"A ring signature is a type of group signature that makes use of your account keys and a number of public keys (also known as outputs) pulled from the blockchain using a triangular distribution method...In a "ring" of possible signers, all ring members are equal and valid. There is no way an outside observer can tell which of the possible signers in a signature group belongs to your account similar in function to a bank account, contains all of your sent and received transactions"

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

- ▼ Ring Signatures obfuscate the transaction graph by associating each transaction input to not just one but many possible and equiprobable outputs. This number of possible outputs is called the Ring Size of the transaction. This process is constant and no manual user intervention is needed.
- ▼ Monero also hides recipient addresses by using Stealth 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, the recipient's address never appears on the blockchain, and transactions are unlinkable, as nobody can prove that two transactions have the same recipient.
- ▼ Originally, transaction amounts were visible in Monero's blockchain. However, in January 2017 a hard fork was performed that upgraded the Monero protocol to utilise a new scheme, Ring Confidential Transactions, that combines Ring Signatures with Gregory Maxwell's "Confidential Transactions" scheme. This evolution allowed the obfuscation of the transaction amounts as well, which means that Monero's blockchain is opaque at this point.

Monero, other distinguishing features

- ▼ Monero offers a dynamic block size (one of the developers discusses their interesting approach [here](#)) and a dynamic fee system, in effect making the system more robust by automating basic parameters of the system, as well as providing a more flexible cryptocurrency protocol.
- ▼ Monero transactions are an [order of magnitude](#) larger than Bitcoin's, which makes it significantly less scalable on-chain and accelerates the need for off-chain solutions such as Lightning Network or Sharding.

Monero

- ▼ Here's an interesting early discussion on the topic with Satoshi Nakamoto discussing the potential of Ring Signatures : <https://bitcointalk.org/index.php?topic=770.msg9074#msg9074>
- ▼ We shouldn't be making the mistake of saying that we don't need increased privacy because we have nothing to hide. This is a slippery slope to saying we don't need free speech because we may have nothing to say, or the equivalent of permanently removing the shutters/blinds from our house. Fungibility and privacy are important enough topics for the cryptocurrency community. It's a tricky problem and one that involves complicated cryptographic schemes that are understood by few (so far), and are not very accessible to the average user, without a practical way to hide the complexity.
- ▼ You can read more about it, and its features in more detail here : <https://getmonero.org/home>

Bitcoin Cash

- ▼ On August 1, 2017, bitcoin went through a hard fork which gave birth to Bitcoin Cash (BCH). Records of existing transaction were kept secure
- ▼ Differences with Bitcoin:
 - ▼ The blocksize is 8 MB. More transactions in a block can generate more transaction fees for miners. Approximately 2 million transaction per day can be processed compared to 250k transactions which Bitcoin allows.
 - ▼ No segwit activation.
 - ▼ No “replace by fee” feature.
 - ▼ It will enhance replay and wipeout protection.
 - ▼ It offers a way to adjust the proof-of-work difficulty quicker than the 2016 block difficulty adjustment interval of Bitcoin.
- ▼ Anyone with the possession of Bitcoins at the time of the hard fork, got the equal amount of coins in Bitcoin Cash. This was applicable provided that users did not have their Bitcoins in exchanges and were in possession of their private keys at the time of the hard fork.
- ▼ Bitcoin Cash went into a hard fork itself, splitting into Bitcoin ABC which is widely recognized as the former Bitcoin Cash and Bitcoin SV whose supporters believe that proper scaling could result on more application being built on top of the chain

Bitcoin Cash (BCH)

- Let's focus on the metrics of the originally created BCH who is currently (March 4, 2019) traded at approximately \$125

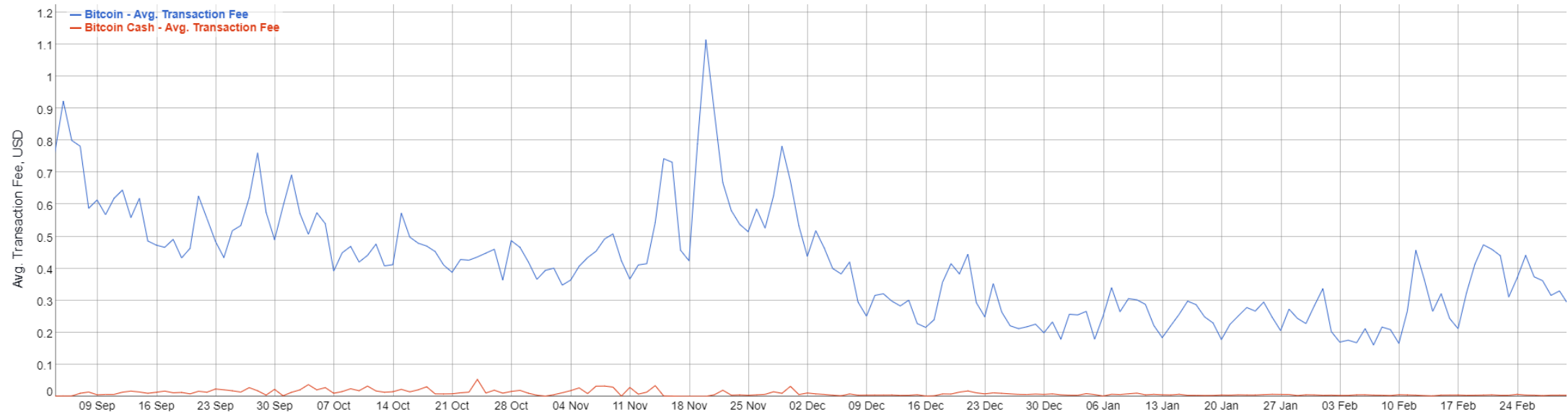


<https://coinmarketcap.com/currencies/bitcoin-cash/#charts>

How does Bitcoin Cash prevent replay attacks?

- ▼ A replay attack occurs when data are maliciously repeated or delayed in multiple locations.
- ▼ In the case of a blockchain, an example would be a transaction that happens on the Bitcoin blockchain and repeated on the Bitcoin Cash blockchain. E.g. Andreas sends 1 BTC to Antonis, as well as 1 BCH, even though this was not his intention.
- ▼ Bitcoin Cash achieves this by (Source: <https://blockgeeks.com/guides/what-is-bitcoin-cash/>):
 - ▼ Using a redefined sighash algorithm. This sighash algorithm is only used when the sighash flag has bit 6 set. These transactions would be invalid on the non-UAHF chain as the different sighashing algorithm will result in invalid transactions.
 - ▼ Using OP_RETURN output which has the string “Bitcoin: A Peer-to-Peer Electronic Cash System” as data. Any transaction which contains this string will be considered invalid by bitcoin cash nodes until the 530,000th block. Basically, before that block you can split your coins by transacting on the non-UAHF chain first with the OP_RETURN output, and then transacting on the UAHF chain second.

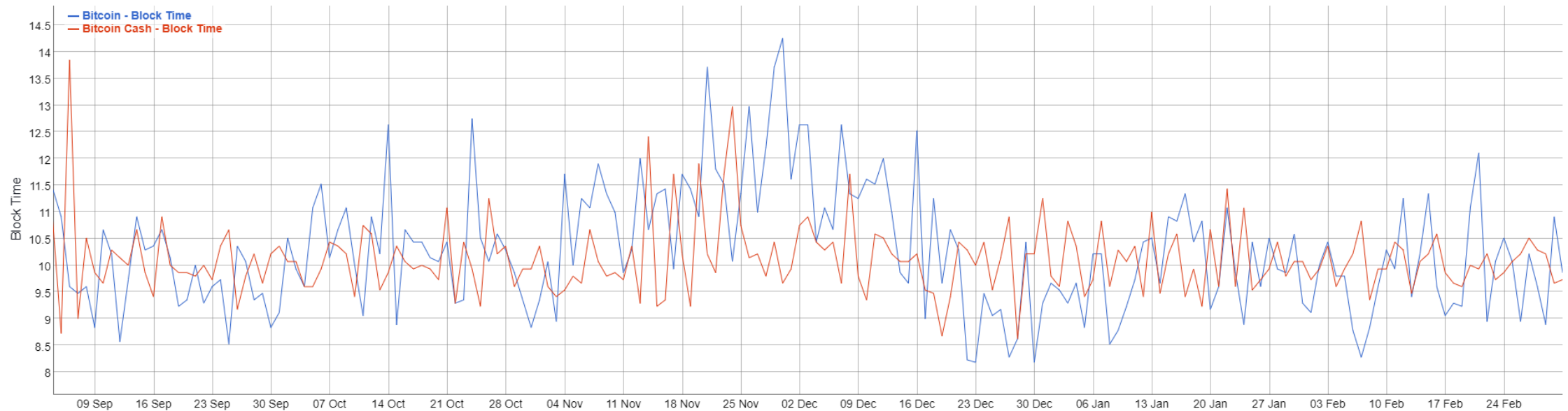
Bitcoin vs Bitcoin Cash Average Transaction Fees



Did SegWit contribute to lower fees for BTC recently?

Source: <https://bitinfocharts.com/comparison/transactionfees-btc-bch.html#6m>

Bitcoin vs Bitcoin Cash Block Time



Source: <https://bitinfocharts.com/comparison/confirmationtime-btc-bch.html#6m>



3. Common characteristics



Common characteristics

- ▼ Cryptocurrencies have some common characteristics:
 - ▼ They rely on cryptographic hash functions and asymmetric cryptography
 - ▼ Most are designed to gradually introduce new coins into circulation
 - ▼ All have a specific rate of issuance which may or may not be capped towards an ultimate number. Some are based on a pre-programmed supply, response to demand or response to their use.
- ▼ In the following pages, we will be exploring their differences, categorizing them into groups using different criteria and conclude with KPIs (Key Performance Indicators) that are important to keep in mind when assessing crypto-currencies.



4. Criteria for categorization



Criteria for categorization

Let's begin with the basic elements of the consensus and incentive method used:



Proof of work / stake / resources / ...

- ▼ There are different methods / concepts behind the process through which one can provide proof to the network of working “with the system” and not “against it”. The tradeoff between something of value (energy, time or other resource) to empower the network, aids to ascertain which participants are acting “rationally” and which are not. The incentive for this is usually earning new coins and/or transaction fees.
- ▼ **Proof of work** - mining is required to gain coins, which usually is hash or script based
- ▼ **Proof of stake** - coins are earned in an order, as a reward for displaying ownership
- ▼ **Proof of resources** – recognition of contribution of resources to the network
- ▼ **Proof of burn** – “bootstrapping one cryptocurrency off of another”

Proof of work (PoW)

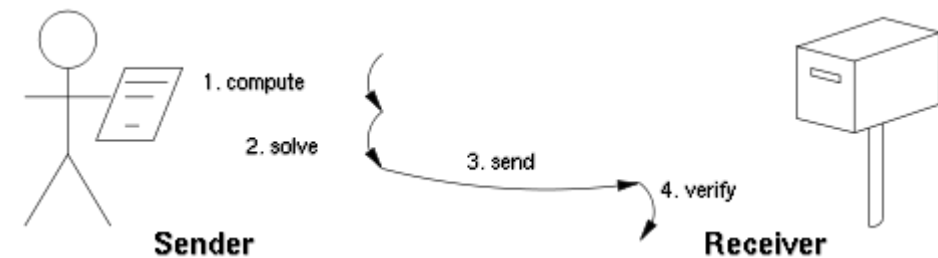
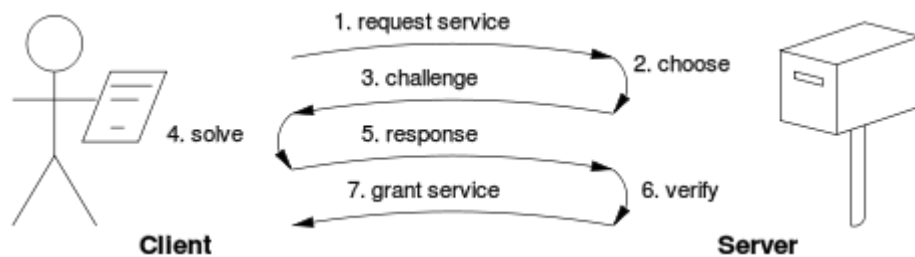
- ▼ **Proof of Work (PoW)** - One party (the **prover**) presents the result of a computation hard to **compute**, but easy to **verify** and by verifying the solution anyone else can be **sure** that the prover performed a certain amount of computational work to generate the result.

2 classes of PoW protocols:

challenge-response

VS

solution-verification



PoW - Algorithm used for verification / mining

- ▼ Secure Hash Algorithm and variations –
 - ▼ SHA-256 (Bitcoin)
 - ▼ Keccak_256 and Keccak_512 (non standard SHA3 used by Ethereum)
- ▼ scrypt algorithm (e.g. Litecoin)
- ▼ Hybrid and CPU-only algorithms (e.g. PrimeCoin)
- ▼ X11 algorithm (e.g. Dash)
- ▼ CryptoNight (e.g. Monero, other Cryptonote coins)
<https://minethecoin.com/coin/mining/algorithm/CryptoNight>

PoW - Algorithm used for verification / mining

- Examples of coins using Secure Hash Algorithm - SHA-256 besides BTC and BCH:
<https://www.multipool.us/dashboard/pools/sha256>



Namecoin – Peercoin

```
SHA256("hello") = 2cf24dba...  
SHA256("Hello") = 185f8db3...  
SHA256("Hello.") = 2d8bd7d9...
```

- SHA-256 is an asymmetric hash function for which it is easy to calculate an output given an input but impossible to do the reverse. The representation of a SHA-256 output is a series of 64 hexadecimal digits – letters and numbers in the set {0123456789abcdef}. For example, the first digits of the hashes are depicted above.

PoW - Algorithm used for verification / mining

- ▼ Examples of coins using the script algorithm: <https://www.reliablecoin.com/script-coins-list/>



Litecoin – Novacoin - Dogecoin



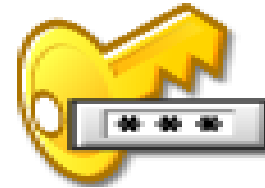
- ▼ The script algorithm uses a password-based key derivation function, designed to hinder brute-forcing by raising the demands on the algorithm in term of resources (e.g. memory). Time–memory tradeoffs need to be taken into consideration when mining for such coins. Script mining is memory intensive, which makes it harder to massively parallelize and centralize with Application Specific Integrated Circuit (ASIC) technology.

PoW - Algorithm used for verification / mining

- ▼ Examples of coins using the X11 algorithm: <https://cryptorival.com/algorithms/x11/>



Dash



- ▼ The X11 chained hashing algorithm is a PoW algorithm that uses 11 different hashing functions to calculate the block header. The X11 algorithm was intended to be ASIC resistant so as to keep mining CPU- and GPU-friendly.

Proof of Stake (PoS)

- ▼ **Proof of Stake (PoS)** – Instead of performing the task of solving difficult mathematical algorithmic problems (i.e. mining for coins), a proof of stake scheme implies that the owner of coins can earn coins by just proving that she owns a certain amount of coins.
- ▼ Some of the main approaches taken in PoS implementations also include iterations of [Casper](#) for Ethereum:

Cunicula's Implementation of Mixed Proof-of-Work and Proof-of-Stake

This suggestion is of a mixed Proof-of-Work / Proof-of-Stake system.


Meni's implementation

This proposal is for a proof-of-work (PoW) skeleton on which occasional checkpoints set by stakeholders are placed. In one variant, double-spending is prevented by waiting for a transaction to be included in a checkpoint; the variant described here uses cementing to prevent double-spending, and checkpoints to resolve cementing conflicts.

Proof of Stake (PoS)

Proof of stake - first appearance as a concept:

QuantumMechanic
Member
Activity: 110

 **Proof of stake instead of proof of work**
July 11, 2011, 04:12:45 AM

#1

I've got an idea, and I'm wondering if it's been discussed/ripped apart here yet:


I'm wondering if as bitcoins become more widely distributed, whether a transition from a proof of work based system to a proof of stake one might happen. What I mean by proof of stake is that instead of your "vote" on the accepted transaction history being weighted by the share of computing resources you bring to the network, it's weighted by the number of bitcoins you can prove you own, using your private keys.



PoS : the ..other side of the coin

Could Peercoin and “Proof-of-Stake” Turn Bitcoin Into The Myspace of Cryptocurrency?

JANUARY 19, 2014 BY SHANE DARK | FOLLOW US ON TWITTER [HERE](#)

source : www.cointrader.org/peercoin-proof-of-stake-and-bitcoin/

 **Gavin Andresen**
@gavinandresen


 

[@marioboo3](#) I think proof-of-stake is hard-coded 'the rich get richer' and is deeply unfair.

[Reply](#) [Retweet](#) [Favorite](#) [More](#)

4
RETWEETS

1
FAVORITE



5:32 AM - 10 Jan 2014

source : https://en.bitcoin.it/wiki/Proof_of_Stake/

PoS - Algorithm used for verification / mining

- ▼ Examples of coins using PoS algorithms: <https://coinsutra.com/proof-of-stake-cryptocurrencies/>



Nxt

the first 100% PoS currency.
Coins are earned solely by
charging transaction fees.



Examples of Coins using Hybrid Algorithms

▼ Examples of coins using Hybrid algorithm:



Peercoin (PPC)

Hybrid Proof of Work / Proof of Stake coin;

“The ratio of newly produced coins shifts to favor ones produced via Proof-Of-Stake minting”

Examples of Coins using Hybrid Algorithms

▼ Examples of coins using Hybrid algorithm:



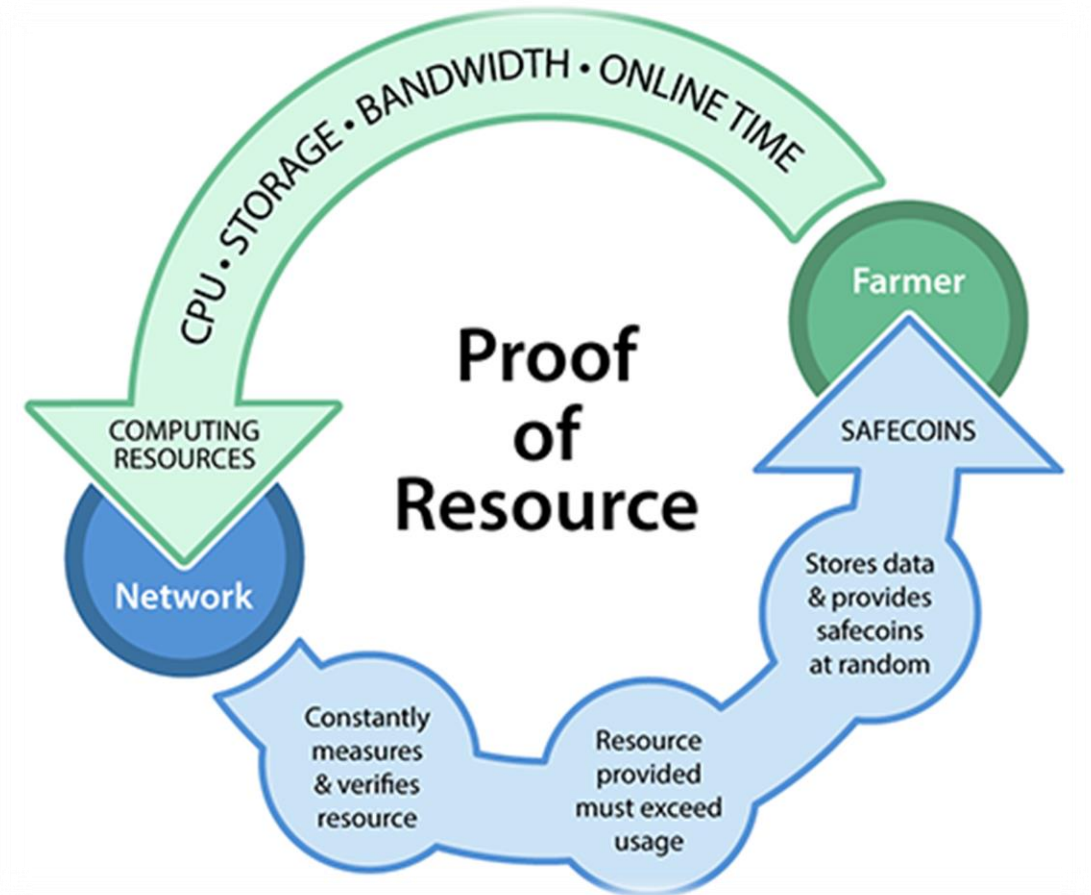
Securecoin (cap under 200BTC)

Multiple Algorithms:

Grøstl, Skein, BLAKE, BLUE MIDNIGHT WISH,
JH, SHA-3

Proof of Resources (PoR)

- ▼ This scheme is based on the notion that end users can earn coins by contributing to the network, more resources than those they use to mine coins for themselves. These users are called “farmers” and they receive this reward for maintaining / supporting the network.
- ▼ This concept has not been extensively discussed or adopted; the main idea is depicted in the diagram on the right, but it could be the spur for significant innovation.
- ▼ The main effort to apply POR is currently applied by the [MaidSAFE](#) project, in a venture to create nothing less, than a fully decentralized Internet.



PoR - Algorithm used for verification / mining

▼ Examples of coins using PoR algorithms:

safecoin

SAFE (Secure Access For Everyone)

End users can farm (or earn) safecoins by providing Proof of Resource (PoR). Resources can be bandwidth or disk space, in an attempt to further decentralize the internet.



Proof of Burn (PoB)

- ▼ The idea is that miners should show proof that they burned some coins - that is, sent them to a verifiably unspendable address. This is expensive from the miners' individual point of view, just like proof of work; but it consumes no resources other than the burned underlying asset. To date, all proof of burn cryptocurrencies work by burning proof-of-work-mined cryptocurrencies, so the ultimate source of scarcity remains the proof-of-work-mined "fuel".

https://en.bitcoin.it/wiki/Proof_of_burn

PoB - Algorithm used for verification / mining

▼ Examples of coins using PoB algorithms:



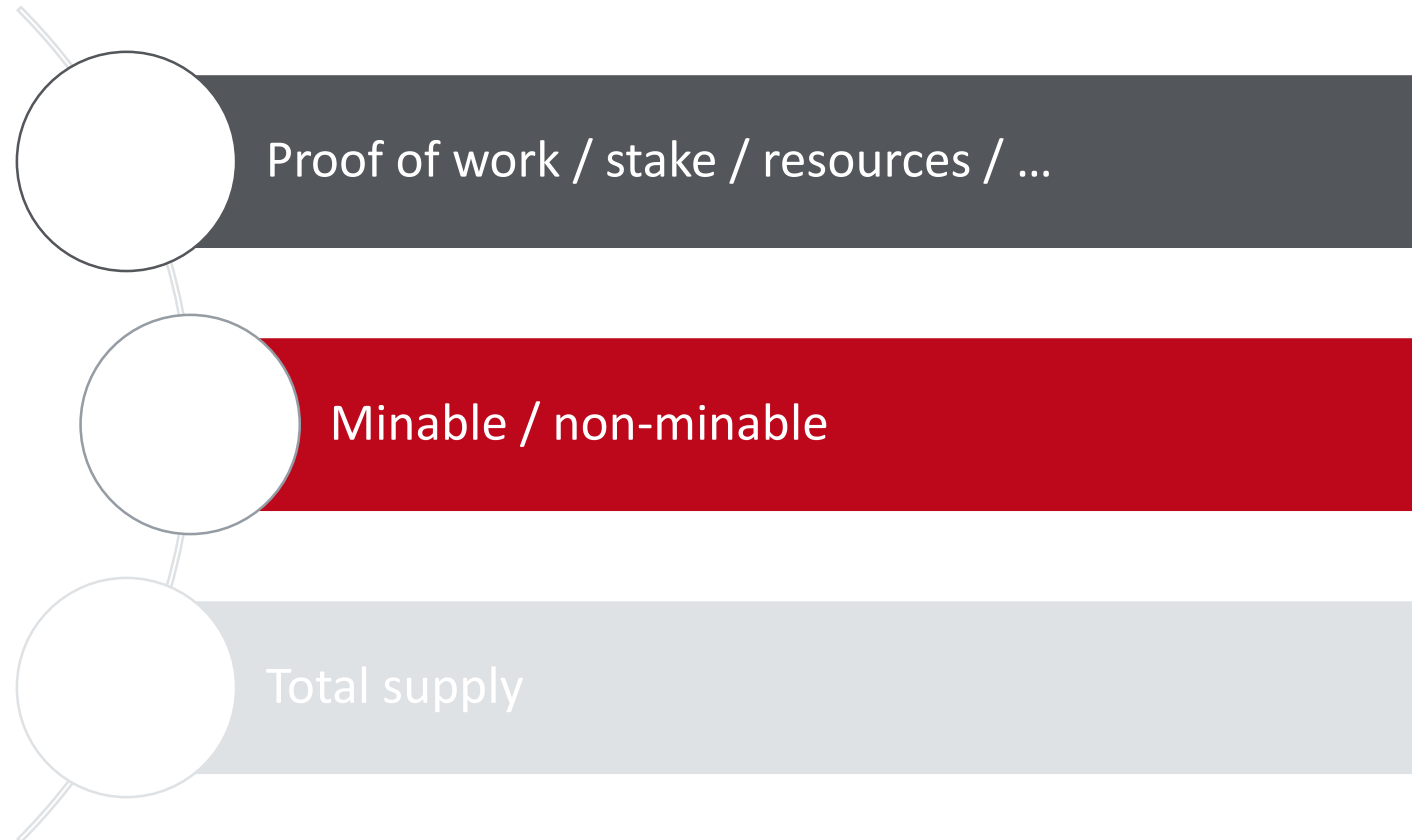
Counterparty

"Proof of burn" is also used by CounterParty, a meta-coin that sits on top of the Bitcoin blockchain (as already discussed in Session 6).



Criteria for categorization

Let us now explore
how new coins are
introduced in the
systems and how
rewards for
processors work:



Pre-mined / Merged mining

- ▼ Some currencies are **pre-mined**, which means that coins are mined from the creator of the cryptocurrency before it is actually released to the public. They can then sell them to the public, thus increase the supply of coins leading the crypto-currency to deflation.
- ▼ Joint / merged mining refers to the practice of creating hashes and submitting them to more than one blockchains, i.e. mining for Bitcoin and Namecoin at the same time (or Sidechains). No intersection of data takes place; for merged mining to take place, we only need to run two clients simultaneously and submit hashes created by your miner to both networks.
- ▼ Running more than one clients is of course resource consuming; disc space and memory are more occupied and bandwidth is also necessary. Moreover, the pair or group of currencies that we need to choose for merged mining has to be on the same difficulty level, otherwise you produce hashes that are proper for one network each time, providing you with less opportunities for synergies.

<http://bitcoin.stackexchange.com/questions/273/how-does-merged-mining-work>

Ripple

- ▼ Ripple is a case of a project that begun before Bitcoin (2004), but truly came to fruition after the technology of Bitcoin was invented.
- ▼ Ripple resembles a digital version of the ancient Hawala system, a form of social remittance mechanism based on connections of parties that trust each other. This creates a network of trusted entities (mainly financial institutions) that can transact a very large number of currencies and assets with each other at a low cost. Gateways are the interface point of users with the network and they transfer assets via issuing and transferring IOUs to each other, through the shortest trust paths of the network between sender and receiver. Transfers in Ripple usually take 2-5 seconds to make. There is no mining process involved and all internally used currency (XRP) are issued centrally. In total, 100 billion XRP were created, 80 billion of which were given to Ripple Labs to manage and distribute to users. The co-founders kept the other 20 billion.
- ▼ Testing with MoneyGram
- ▼ Adoption matters – Thai SEC gives green signal for XRP to be used as from ICO investments and as a base in trading pairs
- ▼ Differences with other cryptocurrencies
- ▼ Collaboration with Santander Bank



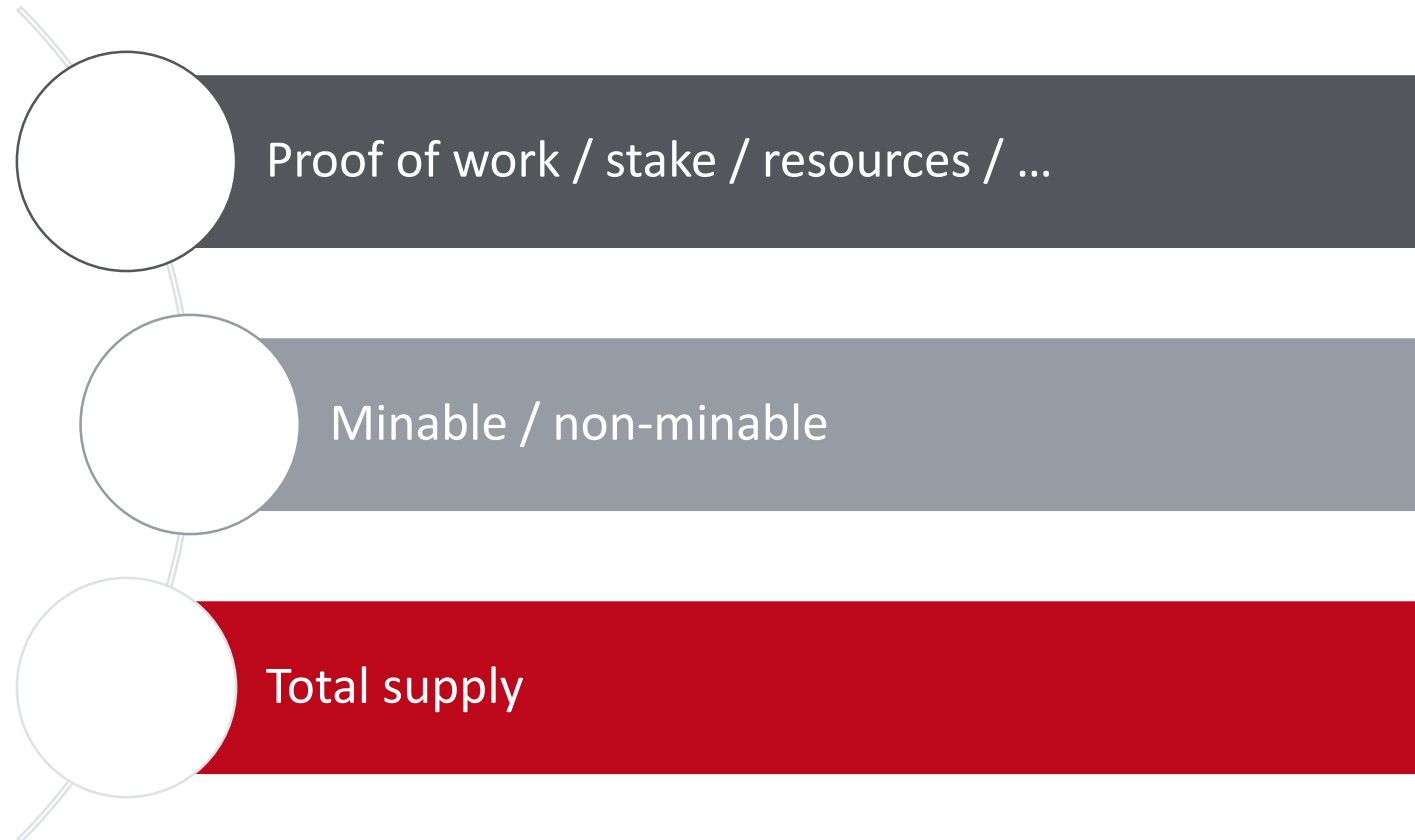
Ripple – XRP Leger Infrastructure

▼ XRP Ledger Overview from the Official Operation Guide:

- ▼ *“The XRP Ledger is a public decentralized cryptographic ledger powered by a global network of peer-to-peer servers. The XRP Ledger uses a Byzantine Fault Tolerant agreement protocol over collectively trusted subnetworks (group of validators) to prevent double-spending of funds and ensure network-wide consensus on the state of user accounts and balances*
- ▼ *The XRP Ledger is the root ledger of XRP, a native, independent digital asset designed to bridge global currencies for payments. As a software company, Ripple contributes to the open source development of the XRP Ledger, in support of the Internet of Value.*
- ▼ **Role of Validators:** *All validating nodes on the XRP Ledger determine if transactions meet protocol requirements. A subset of those validating nodes, selected by users on the network, also group transactions into ordered units to prevent double spending and can vote on protocol changes called Amendments.*
- ▼ **Role of Hubs:** *Hubs are public facing servers that help connect validator servers with other network nodes. A rippled node starting for the first time can bootstrap by peering with these hubs and more reliably receive messages from validator servers.*
- ▼ **Business Requirements:** *Only server operator will have shell access to the validator server. Server operator will run the validator independently (without any collusion with other validators) as a neutral party to act in the best interest of the users of the XRP Ledger”*

Criteria for categorization

Let us now explore the significance that total supply and new coin introduction rate may have:



Total Supply

- ▼ The total supply of bitcoins and the reason it was arbitrarily set at 21,000,000, has given fuel for much discussion in the Bitcoin community. In the true spirit of open source, this has led to a large number of coins arguing over increased scarcity (less total number of coins) or artificial abundance (many more total number of coins).
- ▼ Other characteristics are often the ground for experimentation. These include:
 - ▼ The rate of issuance until the total supply
 - ▼ The issuance rate according to issuance method (for hybrid PoS/PoW coins), and
 - ▼ Whether there will ever be a total supply, or will it be ever increasing (inflationary or tail emissions)

And...Stablecoins

- ▼ A new form of cryptocurrencies aimed to minimize risk on price volatility which have been one of the main reasons of limited cryptocurrency adoption worldwide.
- ▼ The [“State of Stablecoins” Research](#) by the Blockchain Team is a highly suggested reading which can help you explore this emerging aspect. See below for some of the most significant findings:
 - ▼ There is a total of 54 identified stablecoins, 45% of which are live, the majority of them being asset-backed.
 - ▼ US and Europe are the most popular homes for stablecoin teams
 - ▼ Off-chain asset backed stablecoins have raised \$177m, algorithmic stablecoins have raised \$41m and crypto-collateralized stablecoins have raised \$32m in funding
 - ▼ Tether has the largest [market share](#) of all stablecoins
 - ▼ Some stablecoins spark a competitive response / backlash from central banks
 - ▼ No more than 5-8 stablecoins are expected to compete on the stage in the short to medium-term

Figure 8: Stablecoins Listed on Major Cryptoasset Exchanges





5. Key Performance Indicators(KPIs) for assessing digital currencies



KPIs for assessing digital currencies












- ▼ **Market capitalization:** This metric refers to the aggregated value of a coin and its penetration “in the market” of digital currencies. This is a metric that gives us a snapshot, an indication for the present state of each coin compared to major conventional currencies. This reflects a momentarily impression and provides information for the history.

[Bitcoin Market Capitalization from blockchain.info](https://blockchain.info)



KPIs for assessing digital currencies

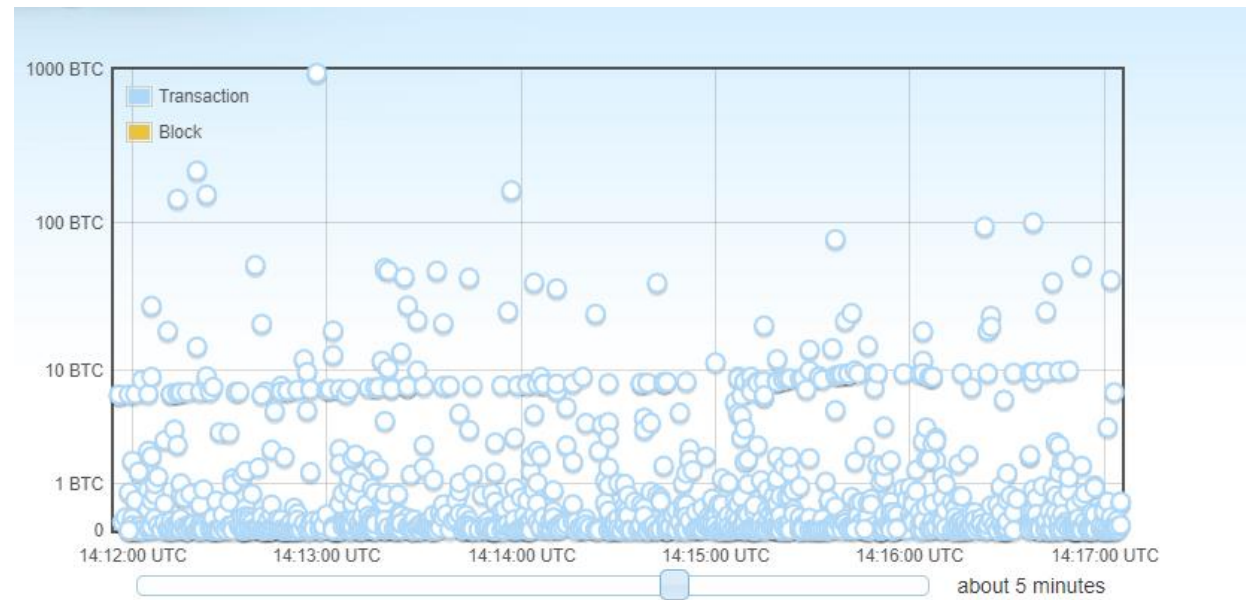
- ▼ **Volume (24h):** This metric expresses the total number of transactions taking place with the use of a particular currency over the last 24 hours.
- ▼ This metric depicts the as-is situation of a particular day and changes in time (very often in fact...)

#	Name	Market Cap	Price	Volume (24h)
1	 Bitcoin	\$66,116,322,330	\$3,762.94	\$8,434,032,449
2	 Ethereum	\$13,333,144,474	\$126.84	\$3,986,959,962
3	 XRP	\$12,638,334,384	\$0.305037	\$648,276,964
4	 EOS	\$2,942,210,934	\$3.25	\$1,473,445,540
5	 Litecoin	\$2,813,665,746	\$46.33	\$1,219,012,105
6	 Bitcoin Cash	\$2,197,015,858	\$124.45	\$295,835,705
7	 Tether	\$2,046,065,097	\$1.01	\$7,610,832,701
8	 Binance Coin	\$1,595,965,540	\$11.30	\$103,942,993
9	 Stellar	\$1,587,095,225	\$0.082608	\$145,593,211
10	 TRON	\$1,428,819,081	\$0.021427	\$157,220,618
11	 Bitcoin SV	\$1,120,035,992	\$63.45	\$87,740,423

<https://coinmarketcap.com/>

KPIs for assessing digital currencies

- Transaction volume, by number of transactions and currency amount
Another way of drawing insights from the dynamics of each network is the number of transactions happening over time, as well as the amount of coins that are involved in them.
- bitcoonitor.com is an online monitoring tool that visualizes the activity on the Bitcoin network in real time.
- In this bubble graph we can see the transactions happening in real time, correlated with their size, i.e. amount transferred – measured in a logarithmic scale.



KPIs for assessing digital currencies

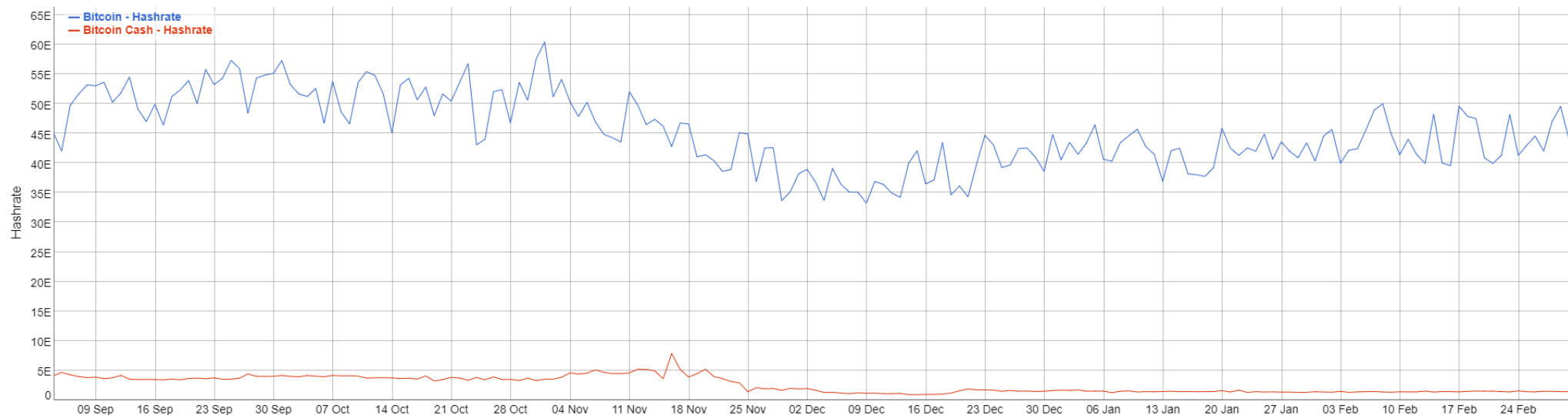
- ▼ **Exchange rate**: Another important measure to consider is the exchange rate of a coin with fiat currencies.
- ▼ The pie chart shows the exchange volume distribution of Bitcoin in the last few days.
- ▼ Moreover, we have to consider that there are multiple exchanges, each one maintaining a slightly different exchange rate.
- ▼ bitcoincharts.com can provide us with a platform with rich information, aggregated or not, about the way differences in prices of cryptocurrencies develop in time.
- ▼ Before choosing the exchange rate and volumes traded as an indication make sure to know the conditions under which said volume is produced.

KPIs for assessing digital currencies

- ▼ **Average confirmation time:** What is also important to know for a digital currency is the average time frame within which a confirmation is attained (block times).
- ▼ <https://bitinfocharts.com/comparison/confirmationtime-btc-eth-ltc-bch.html#3m>
- ▼ Litecoin came out as a faster alternative to Bitcoin, with block times in the range of 2.5 minutes. The initial choice of 10 minute blocks aimed for a full propagation of every new block and every transaction through every node. Most other altcoins have toyed with the confirmation time, as a key differentiator
- ▼ Decreasing block times has been argued to create a higher probability of orphan/stale blocks in their respective blockchains (unless something like GHOST or a variant is used like in Ethereum), and a perhaps unfair disadvantage to miners that are late to receive new blocks.

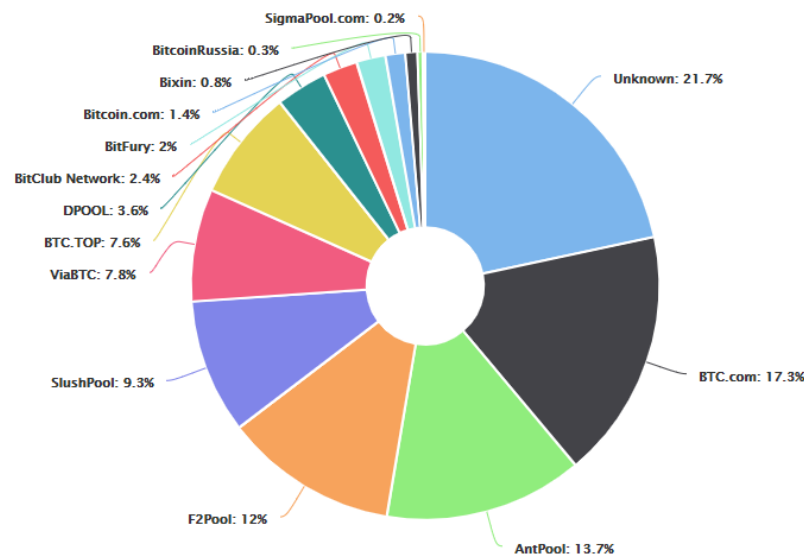
KPIs for assessing digital currencies

- ▼ **Network hash rate:** This metric refers to the measuring unit of the processing power of the network and can give us an indication of the current status of the difficulty in the mining process.
- ▼ Difficulty refers to how easy it is to generate a SHA-256 hash for a candidate block, that is in accordance with the requisites defined by the current difficulty.
- ▼ The graph on the right shows the way the hash rate of the BTC/BCH networks have performed in the last **6 months**

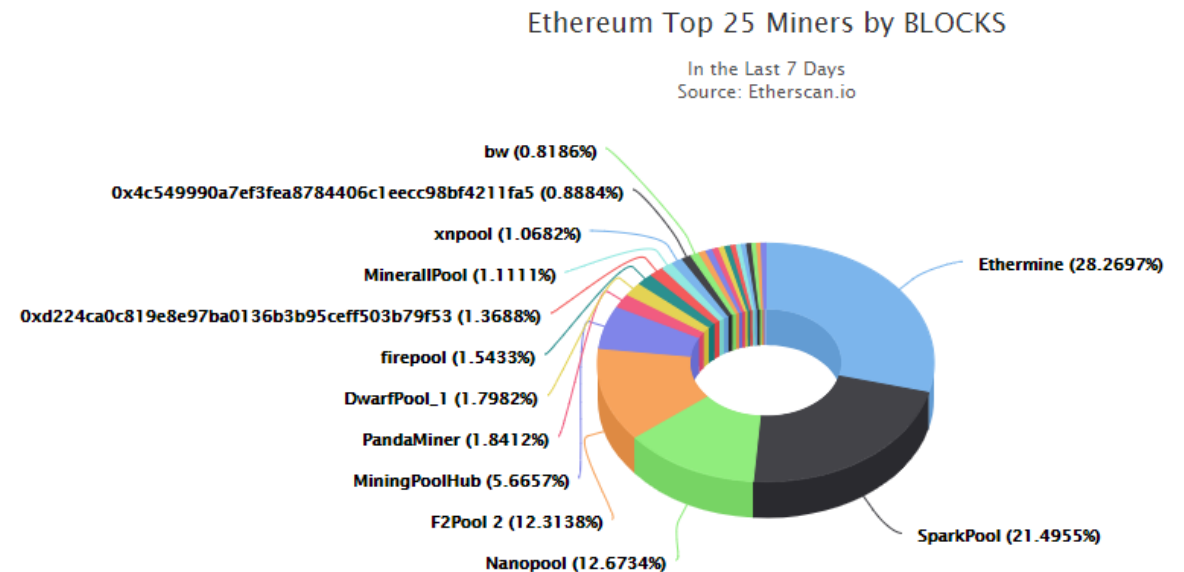


KPIs for assessing digital currencies

- ▼ **Hash rate distribution:** A pie graph like the ones below shows the most popular mining pools and their contribution to the whole network at a single point in time.
- ▼ This metric, again, is just a static picture and should be used as a quick indication of the attractiveness of different mining pools. For instance, below we can see the distribution of hash rate among different pools recently, for Bitcoin and Ethereum respectively.



Source: <https://blockchain.info/pools?timespan=4days>



Source: <https://etherscan.io/stat/miner?range=7&blocktype=blocks>



Permissioned Ledgers and Private Blockchains



Definition

- ▼ A private blockchain network is: A *permissioned network* - Restrictions are imposed on who is allowed to participate in the network and in certain transactions. Participants need to obtain an invitation/permission to join by the network starter or by a set of rules.
- ▼ Only entities granted access to the network and participating in a specific transaction have knowledge and access to relevant information.
- ▼ Examples:
 - ▼ Multichain - <https://www.multichain.com/>
 - ▼ Chain - <https://chain.com/>
 - ▼ Monax - <https://monax.io/>



Functionalities and Advantages of Private Blockchains

- ▼ Private Blockchains are suitable where only a few participants are required. As long as only the suitable people know about the database, the level of content security is satisfying.
- ▼ The access control mechanism may vary according to the wants of the organizations. E.g.
 - ▼ Existing participants decide future entrants, or
 - ▼ A regulatory authority grants access of participation
- ▼ Includes middleman functions, to a certain extent. The organization writes and verifies transactions
- ▼ Efficiency and fast execution – Few trusted nodes need to verify transactions
- ▼ Better Privacy – Company chooses who has access, data is not publicly available
- ▼ Cost saving for organizations - If an entity controls and processes all of the transactions, then there is no need to charge a transaction fee
- ▼ Useful for industries like Finance/Banking, Supply Chain, Voting etc.

Disadvantages of Private Blockchains

- Not fully “decentralized”
- Operate within an environment more suitable for attacks since the target can be few participants
- It can be argued that a Private Blockchain acts as a traditional centralized company intranet in terms of security
- As mentioned earlier, security is the first thing governments and organizations evaluate before implementing such projects
- However, it is better to rely on a private blockchain than a traditional system due to the concept behind cryptography. Data cannot be tampered and frauds/errors can be eliminated, while running such a network is also much faster and cheaper.



<https://articles.whatsn3xt.com/public-private-key-pair-sizes-in-blockchain-peers-32654b808b4>

Consortium Blockchains

- Consortium blockchain is a hybrid between the concept of fully decentralized public blockchains and the “single highly-trusted entity” model of private blockchains. These blockchains are defined as “partially decentralized” or “partially private”. Notable projects are being tested by IBM - <https://www.ibm.com/blockchain>
- People with just an internet connection cannot become nodes. One organization is not having a full control either. A number of companies form a consortium where they decide to cooperate and follow specific rules.
- The consensus process is controlled by a pre-selected number of nodes



Consortium Blockchains Functionalities and Advantages

- ▼ For example, a consortium of 50 financial institutions, each of which operates a node and of which 35 must sign every block in order for the block to be valid. Therefore, even if the transaction processing is done by multiple entities the transaction fees can still be limited as few nodes need to do the work for a transaction.
- ▼ Efficiency and Privacy without granting all the power to one single entity
- ▼ Access rights to the blockchain may be public, or restricted to the participants
- ▼ Other Notable Examples: [R3CEV](#), [Hyperledger](#) & [Digital Asset Holdings](#)
- ▼ Useful for industries like Banking/Finance, Digital identity, Supply Chain, Health Care etc.
- ▼ As this is already a heavy session in terms of material, we have included additional training material on Hyperledger and Corda (R3's network) which will not be examined on this course, but they are a great source of reading material.
- ▼ We are now constructing a new **MSc in Digital Currency Course** focusing on fundamentals and specific use cases of consortium blockchains like R3's Corda and Hyperledger.



Conclusions



Conclusions

- ▼ A large number of alt-coins exist, as alternatives to Bitcoin, which at the moment holds the leading position.
- ▼ Besides alt-coins, various other DLT networks emerge enhancing different consensus mechanisms.
- ▼ We can use several criteria to categorize alternative blockchain uses in groups, such as whether they follow the “Proof-of-work” or “Proof-of-stake” scheme (or any other from the ones described) or whether they are pre-mined, minable or not or whether they are permissionless or not. Is full decentralization the solution or do DLT networks need to be permissioned at times?
- ▼ There are some important key factors to keep in mind when assessing one digital currency over another.
- ▼ It is important to understand the technology and the concept behind each cryptocurrency as well as the potential benefits one would bring to the society if mainstream adoption occurs.
- ▼ Several businesses and banks in the finance industry are working on their own internal blockchains to replace existing functions.
- ▼ We examine in more detail, the potential benefits of using permissioned ledgers and private blockchains, and how they can tie into (and to which parts) of the existing financial and international settlement systems in the course **DFIN 513, Open Financial Systems** of the MSc in Digital Currency.

A decorative border on the left side of the slide, composed of various triangles in different shades of red and pink, arranged in a complex, overlapping geometric pattern.

Further Reading

A decorative border on the right side of the slide, featuring a few triangles in dark red and pink, arranged in a simple, vertical pattern.

Further Reading 1/3

- ▼ List of cryptocurrency market capitalizations:
 - ▼ <https://coinmarketcap.com/all/views/all/>
- ▼ On public and private blockchains :
 - ▼ <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>
 - ▼ <https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/>
- ▼ More on Ethereum and smart contract platforms:
 - ▼ <https://www.linkedin.com/pulse/why-smart-contracts-make-slow-blockchains-gideon-greenspan?forceNoSplash=true>
 - ▼ <https://support.exodus.io/article/108-what-is-an-erc20-token>
 - ▼ <https://blockgeeks.com/guides/ethereum-metropolis/>
 - ▼ <https://blog.zeppelin.solutions/the-hitchhikers-guide-to-smart-contracts-in-ethereum-848f08001f05>
 - ▼ <https://tokennews-hk.com/project/etheriums-four-major-development-phases/>
 - ▼ <https://www.gametheorygroup.co/the-blockchain-brief/2018/2/15/simplifying-the-ethereum-roadmap-byzantium-to-constantinople>
 - ▼ <https://github.com/ethereum/wiki/wiki/Sharding-FAQs>
 - ▼ <https://www.investopedia.com/terms/u/uncle-block-cryptocurrency.asp>

Further Reading 2/3

- ▼ 4 Cryptocurrencies with much faster block times than bitcoin
 - ▼ <https://themerikle.com/4-cryptocurrencies-with-much-faster-block-times-than-bitcoin/>
- ▼ Corda and the Distributed Ledger Technology
 - ▼ <https://tpbit.blogspot.gr/2017/01/corda-and-distributed-ledger-technology.html>
- ▼ Monero
 - ▼ <https://www.monero.how/how-does-monero-privacy-work>
 - ▼ <https://www.monero.how/how-does-monero-work-details-in-plain-english>
- ▼ Proof of Stake Coin – Dash
 - ▼ <https://coinsutra.com/dash-cryptocurrency/>
- ▼ Run a Ripple Validator
 - <https://developers.ripple.com/run-a-rippled-validator.html>
- ▼ EEA and Hyperledger join forces
 - <https://cointelegraph.com/news/enterprise-ethereum-alliance-and-hyperledger-enter-formal-association-agreement>

Further Reading 3/3

▼ Hyperledger & Walmart Case Study

- ▼ <https://www.hyperledger.org/resources/publications/walmart-case-study>

▼ Hyperledger Fabric Functionalities

- ▼ <https://hyperledger-fabric.readthedocs.io/en/release-1.2/functionalities.html>

▼ Four International Banks Complete Commercial Paper Transaction on R3's Corda Platform

- ▼ <https://cointelegraph.com/news/four-international-banks-complete-commercial-paper-transaction-on-r3s-corda-platform>

▼ SWIFT Integrates With R3'S Corda Settler In DLT Trial

- ▼ <https://www.investinblockchain.com/swift-integrates-r3-corda-settler-dlt-trial/>

▼ 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>



UNIVERSITY *of* NICOSIA

Twitter: @mscdigital

Course Support: digitalcurrency@unic.ac.cy

IT & live session support: dl.it@unic.ac.cy