UNIVERSITY of NICOSIA

Session 2

DeFi Infrastructure - Ethereum

BLOC 611: Introduction to Decentralized Finance

Objectives

- Explain the foundational nature of blockchain technology for DeFi, and Ethereum's role therein.
- Give insight into Ethereum's history, characteristics, size, adoption rate and other such metrics.
- Cover the nature and role of smart contracts and decentralized applications (dApps).
- Explain how DeFi emerged out of the foundation of smart contracts and dApps.

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. Introducing the DeFi stack
2. The Ethereum Network
3. From smart contracts, to dApps, to DeFi
4. Key Ethereum concepts
5. Conclusions
6. Further Reading

Session 2: DeFi Infrastructure - Ethereum

1. Introducing the DeFi stack

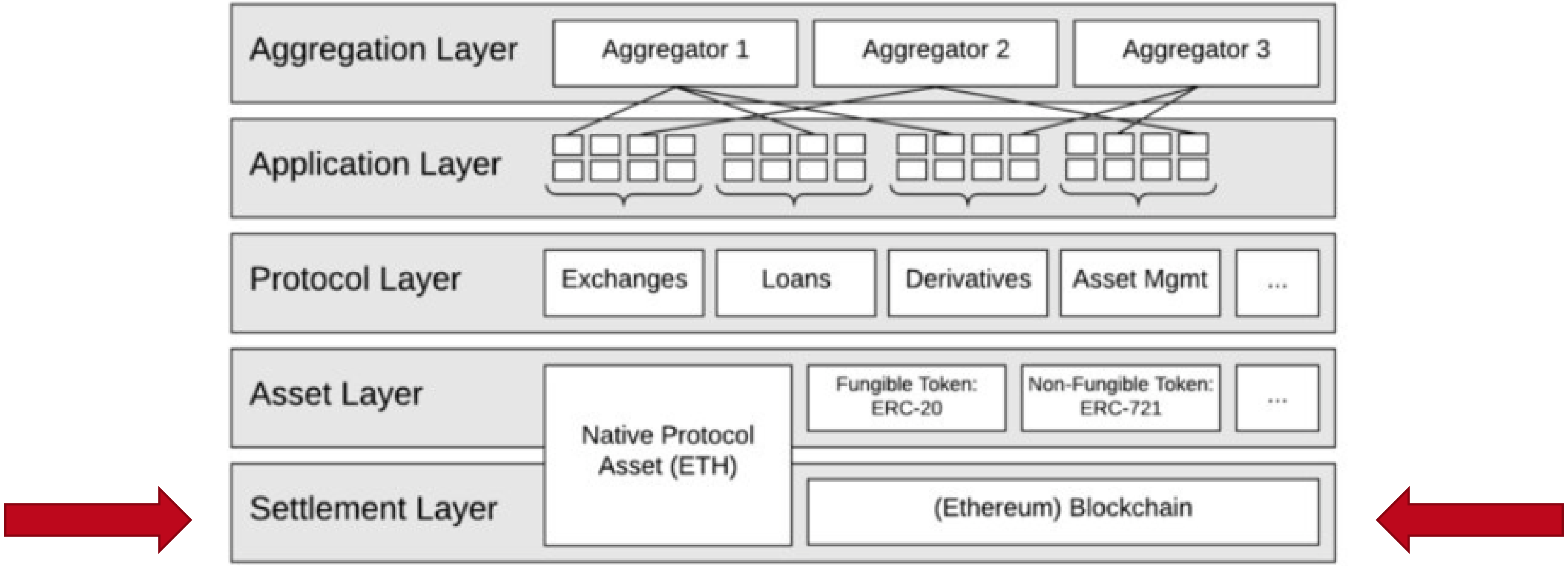
Layer 1 protocols

- Layer one protocols (often abbreviated to L1) form the **basic settlement layer** within the DeFi ecosystem.
- For those familiar with the communication stack of the Internet (the OSI model), L1 in DeFi is roughly analogous to layers 1 to 3 in the OSI reference model, or to the network layer in the TCP/IP model.
- The largest and most well known L1 protocol is the Ethereum network, which we will cover today, as well as in Week 2.
- Besides Ethereum, there is a sizable number of other competing L1 protocols too. Examples include the Cardano, Solana blockchains. More on those will come in session 3.
- Before diving into Ethereum, or any L1 protocol for that matter, it is important to understand how it relates to many other elements in the DeFi ecosystem, and how those all relate to each other. In order to do this, we review the **DeFi stack**.

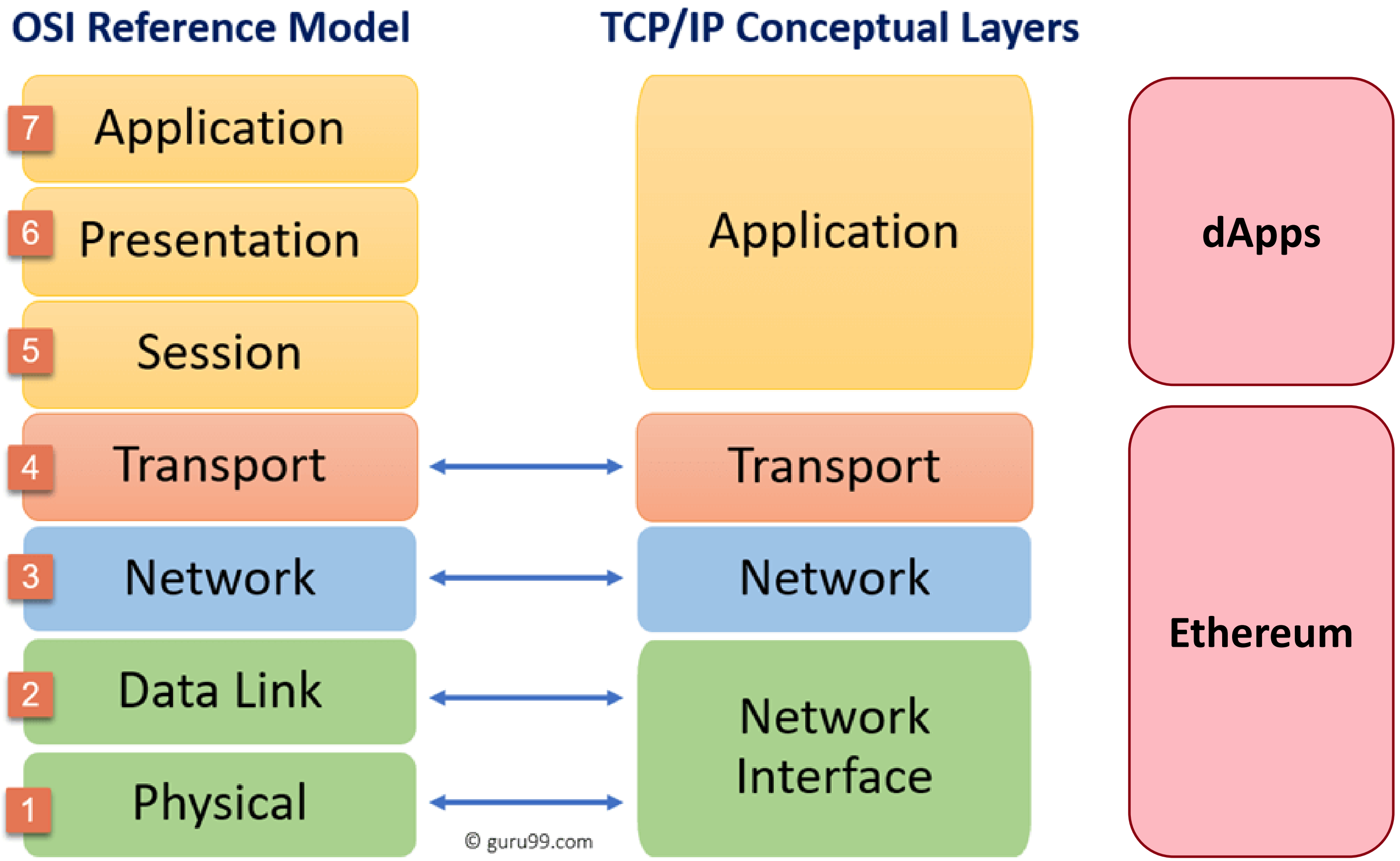
Blockchain-Comparison.com

The DeFi stack

This diagram depicts a basic version of the Ethereum DeFi stack. Note how the Ethereum blockchain sits at the bottom on the settlement layer. The ETH token itself also crosses over into the Asset layer.



Source: Researchgate



Rough mapping

Session 2: DeFi Infrastructure - Ethereum

2. The Ethereum Network

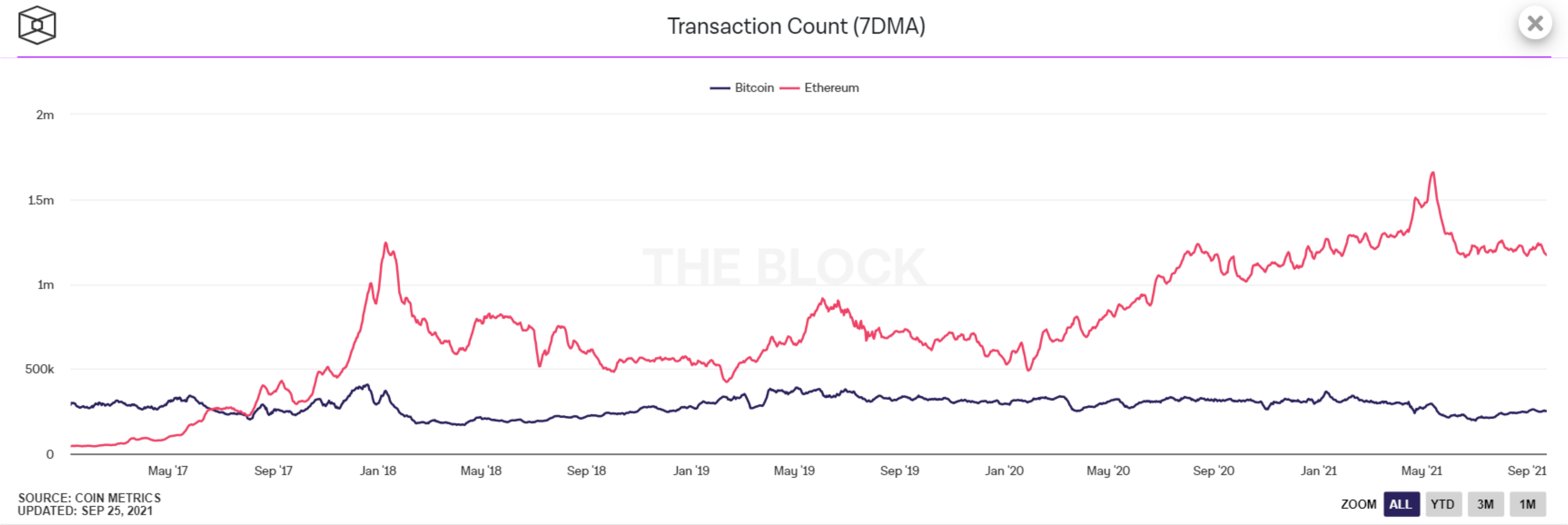
Introduction to Ethereum

- Ethereum has emerged as the most popular foundation for the building of Decentralized Applications. It currently processes more than 5x the number of daily transactions of the Bitcoin network, with Ether, the network's native token currently being the second largest cryptocurrency by market capitalization.

- Ethereum is an open, public, and permissionless infrastructure, often described as "**a world computer**" that executes computer programs. Ethereum utilizes a plethora of technologies, notably a blockchain and consensus mechanism, to store and synchronise the state of the network, along with a native cryptocurrency, called Ether, to enable and control the execution of code.

- A simpler way of thinking about Ethereum is as an **internet without intermediaries**. A big global network of private computers that combine into a single computer to run any internet application without the need for any third-party services, such as Google, Amazon, Facebook etc.

Transaction volume: Ethereum vs Bitcoin



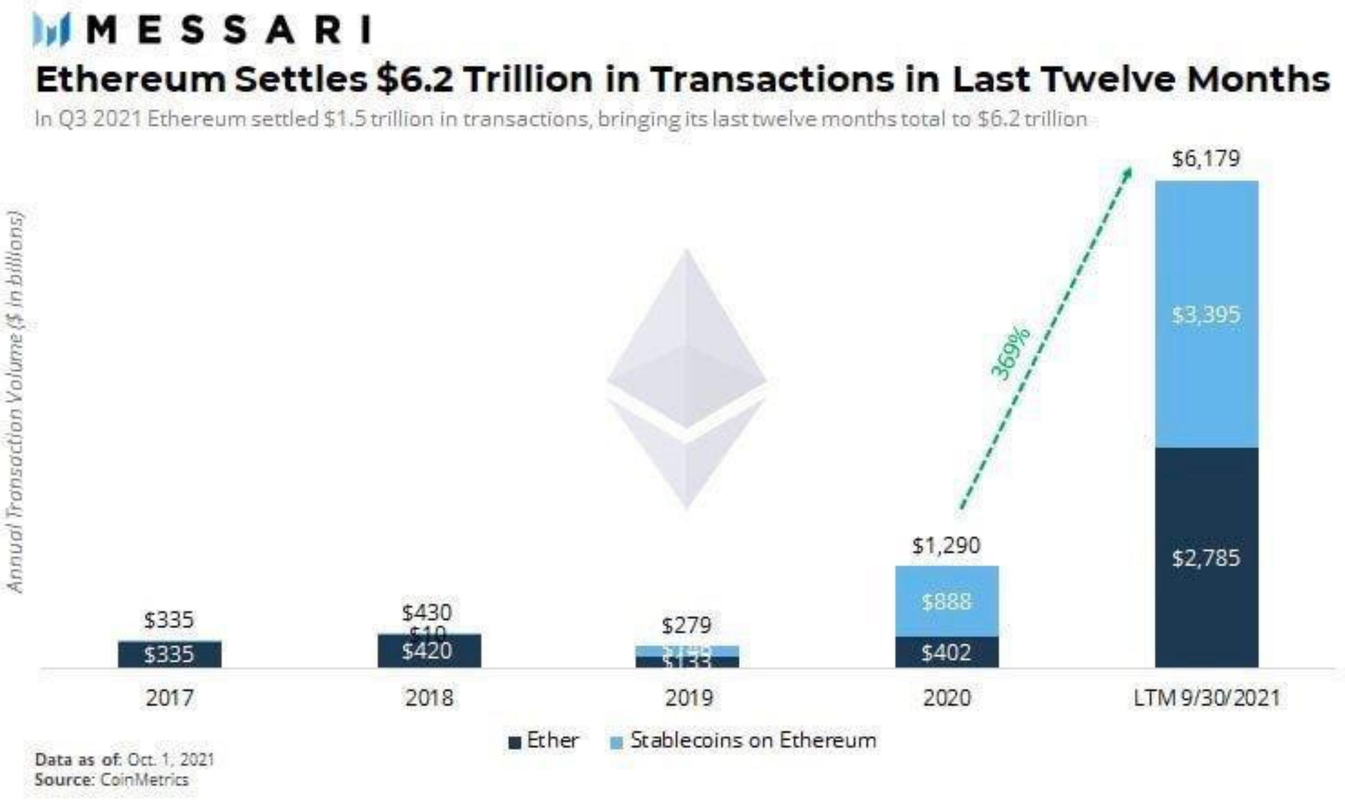
Transaction Count (7DMA)

SOURCE: COIN METRICS
UPDATED: SEP 25, 2021

Graph shows the daily volume of transactions for both Bitcoin and Ethereum, based on a 7-day moving average.

Source: theblockcrypto.com

Transaction growth: Ethereum



MESSARI

Ethereum Settles $6.2 Trillion in Transactions in Last Twelve Months

In Q3 2021 Ethereum settled $1.5 trillion in transactions, bringing its last twelve months total to $6.2 trillion

Data as of: Oct. 1, 2021
Source: CoinMetrics

Source: theblockcrypto.com

Introduction to Ethereum

As a blockchain based network that relies on cryptographic algorithms and economically incentivised participants, Ethereum (like Bitcoin, but unlike traditional finance) is:

- Open
- Borderless
- Censorship resistant
- Immutable
- Transparent
- Global
- Decentralized

A brief history of Ethereum

- Following the popularity of Bitcoin, developers started to realise that blockchains could be used for more than peer-to-peer electronic money.
- Ethereum started with a vision to **unify all possible blockchain applications** under a single network that would operate as a world computer. Allowing for the building of decentralized applications (dApps) that benefited from the unique properties of blockchain, without the need for deploying a new network.
- Ethereum started as a platform for programmable money, and thus as an iteration upon bitcoin, but eventually evolved into a general-purpose world computer. Many early Ethereum developers came from the Bitcoin space. Remember that Bitcoin was launched in January 2009, and Ethereum in July of 2015.

You can learn more about the events and history leading up to Ethereum, including anecdotes, here.

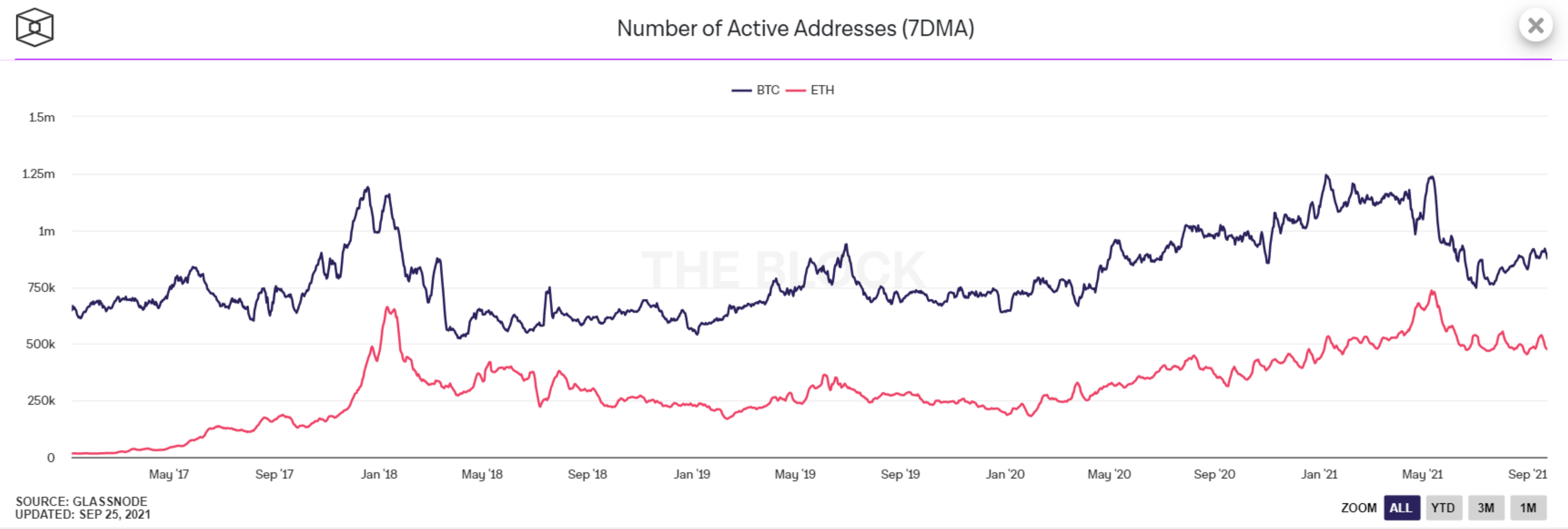
Relevant Quote

"Gavin can also be largely credited for the subtle change in vision from viewing Ethereum as a platform for building programmable money, with blockchain-based contracts that can hold digital assets and transfer them according to pre-set rules, to a general-purpose computing platform. This started with subtle changes in emphasis and terminology, and later this influence became stronger with the increasing emphasis on the "Web 3" ensemble, which saw Ethereum as being one piece of a suite of decentralized technologies, the other two being Whisper and Swarm."*

Vitalik Buterin,
Ethereum Founder

*Gavin Wood
Ethereum Co-founder, Polkadot Founder

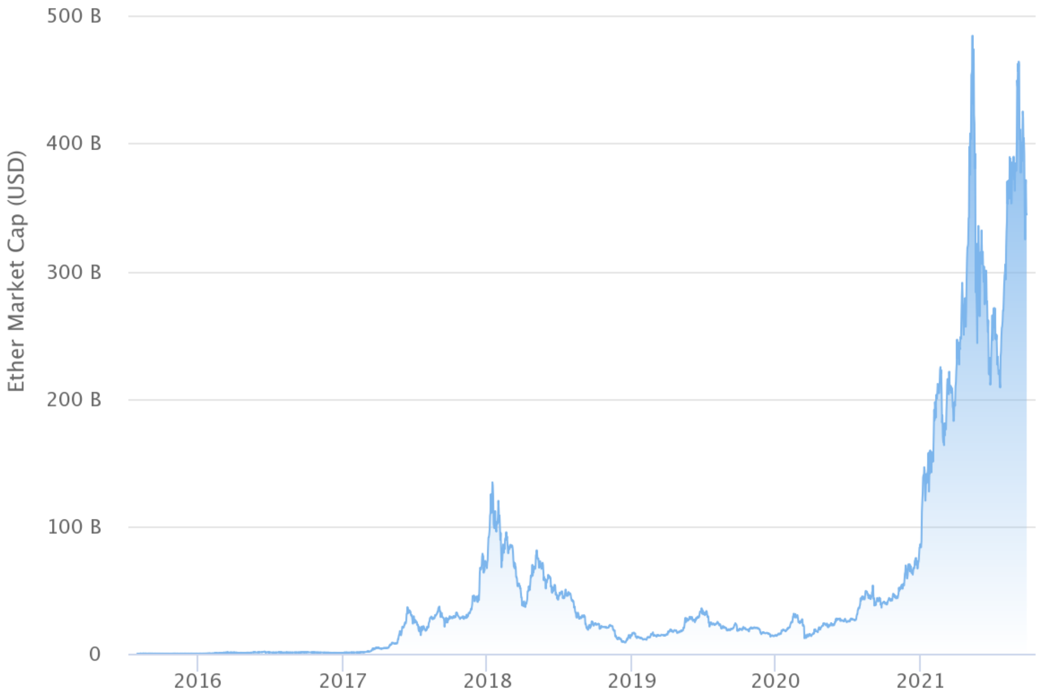
Active addresses: Ethereum vs Bitcoin

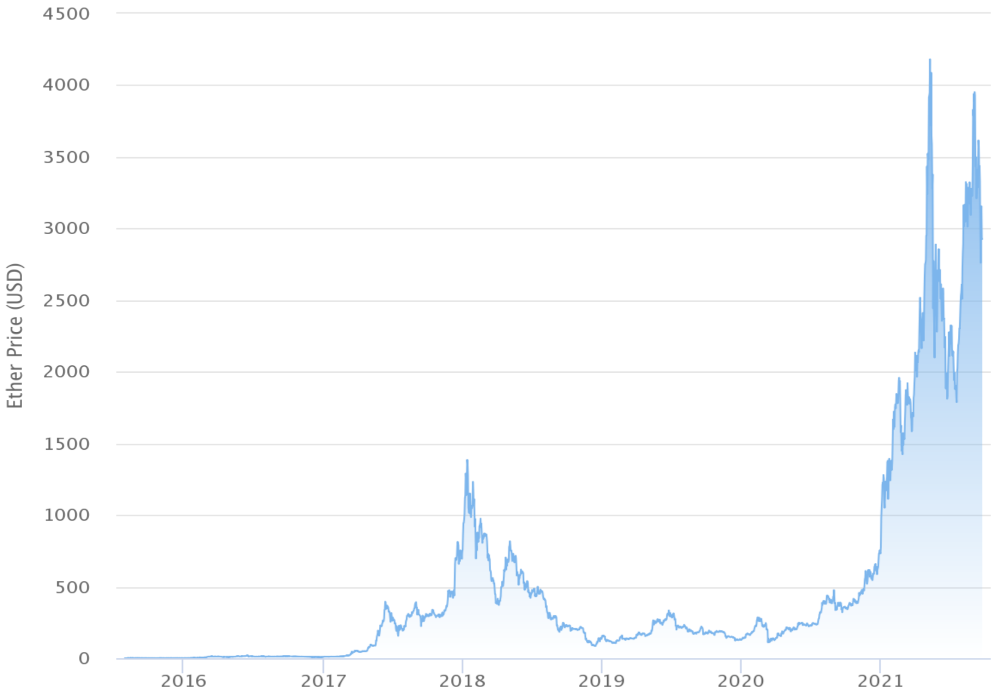


Graph shows the number of unique addresses that were active in the network either as a sender or receiver. Only addresses that were active in successful transactions are counted. Chart uses a 7-day moving average.

Source: theblockcrypto.com

Ether Market Capitalization and daily price charts

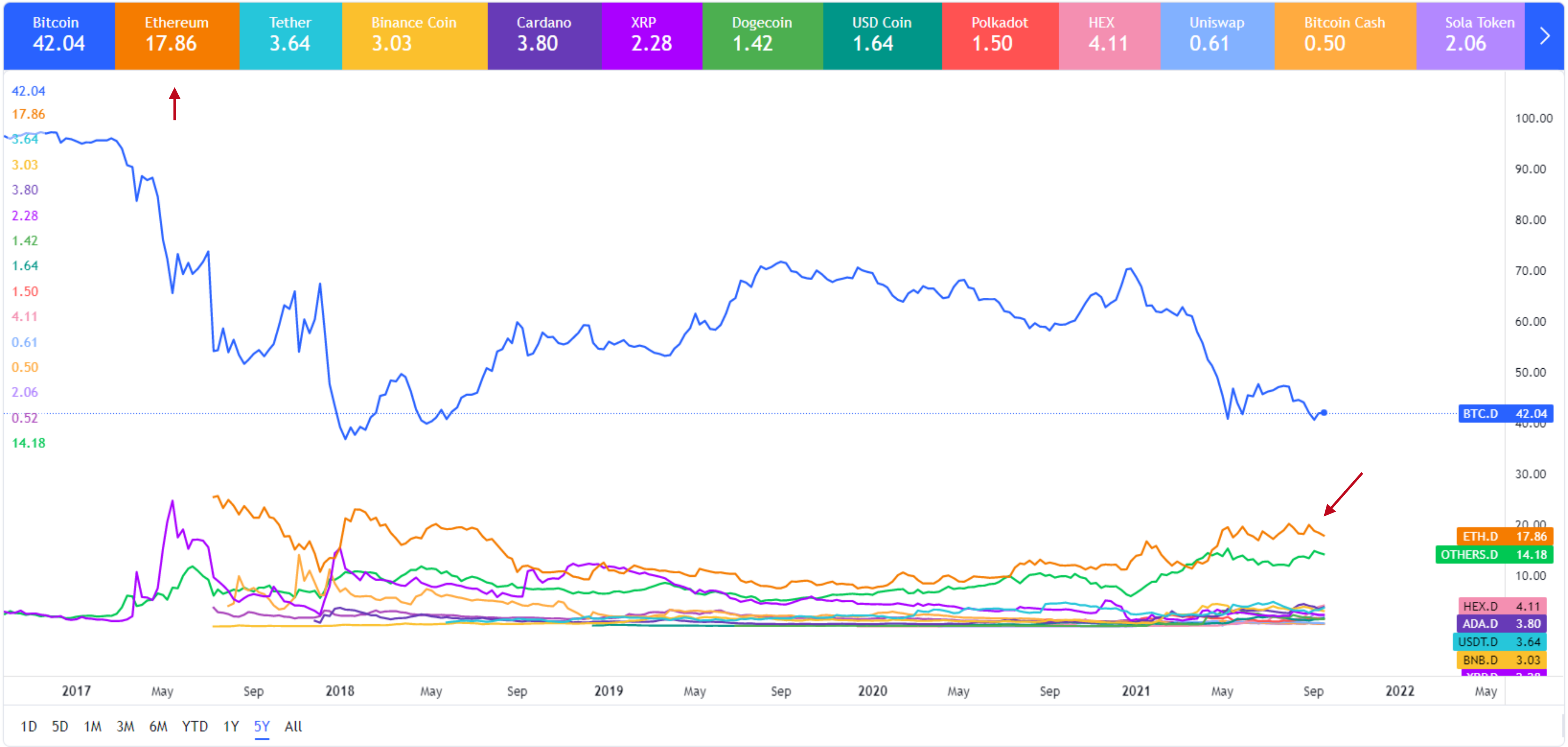




Source: Etherscan.io.

Session 2: DeFi Infrastructure - Ethereum

Total Market Capitalization Dominance



Bitcoin	Ethereum	Tether	Binance Coin	Cardano	XRP	Dogecoin	USD Coin	Polkadot	HEX	Uniswap	Bitcoin Cash	Sola Token
42.04	17.86	3.64	3.03	3.80	2.28	1.42	1.64	1.50	4.11	0.61	0.50	2.06

Source: Tradingview

Session 2: DeFi Infrastructure - Ethereum

3. Smart contracts, dApps, DeFi

Smart contracts - definition

- Let’s clear this up straight away: Smart Contracts are neither smart nor are they contracts. (source)
  A more accurate name would be ‘persistent scripts’.
- Smart contracts are essentially the basic function that powers applications (programs) built on blockchains such as Ethereum.
- They are digital agreements that **execute automatically** based on real-world inputs in data.
- It’s best to think of them is an “If-then statement.” IF condition A exists, THEN perform function B.

A more technically advanced definition would be the following:

- Smart contracts are **immutable** computer programs that run **deterministically** in the context of an Ethereum Virtual Machine (**EVM**) as part of the Ethereum network protocol—i.e., on the decentralized Ethereum world computer. (source)

On the next slide we unpack some of the core terms introduced here.

Smart contracts - definition

Unpacking the definition:

- **Computer programs**: Smart contracts are simply computer programs. The word “contract” has no legal meaning in this context.
- **Immutable**: Once deployed, the code of a smart contract cannot change. Unlike with traditional software, the only way to modify a smart contract is to deploy a new instance.
- **Deterministic**: The outcome of the execution of a smart contract is the same for everyone who runs it, given the context of the transaction that initiated its execution and the state of the Ethereum blockchain at the moment of execution.
  - A simpler way of thinking about deterministic computations is the following: they either happen in full, exactly as described, or they don’t run at all.
- **EVM context**: Smart contracts operate with a very limited execution context. They can access their own state, the context of the transaction that called them, and some information about the most recent blocks.

Smart contracts - example

Let's look at a simple example:

The King has put the castle up for rent through the blockchain, and the rental payment has been made in cryptocurrency. The renter received a receipt which is held in a smart contract with the following terms:

- The King must give the renter a digital entry key by a specified date. If the key doesn't come on time, the blockchain releases a refund. If it does, the smart contract validates and releases both the rental fee to the King and key to the renter.
- The smart contract works on the If-Then premise, so the renter can expect a faultless delivery. **If** the King gives the renter the key, **then** he is sure to be paid. **If** the renter sends a certain amount of cryptocurrency, **then** the renter receives the key from the King.
- The code cannot be interfered with by either party without the other knowing since all participants are simultaneously alerted and the code is open sourced, meaning it is publicly viewable.

Source: District0x, and castles on AirBnB

Smart contracts – the earliest example

The vending machine

The example considered to be the primitive ancestor of smart contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism).

The machine takes in coins, and via a simple mechanism, which makes it a freshman computer science problem in design with finite automata, dispenses change and product according to the displayed price. The vending machine is a **contract with bearer**: anybody with coins can participate in an exchange with the vendor. The lockbox and other security mechanisms **protect** the stored coins and contents from attackers, sufficiently to allow profitable deployment of vending machines in a wide variety of areas.

Smart contracts go beyond the vending machine in proposing to embed contracts in all sorts of property that is valuable and controlled by digital means.

Derived from "Formalizing and Securing Relationships on Public Networks" , by Nick Szabo, in 1997 (!)

Source: The idea of smart contracts

Smart contracts - implications

- Smart contracts have applications far beyond improving the reliability & efficiency of rent collection. In fact, any processes that currently involve manual interactions between two parties can now be **automated** and the **value can be moved in real time** over the blockchain rather than settling days later as with traditional banking.
- Ethereum and smart contracts are helping to build the "**smart economy**" – one in which slow, manual, error-prone processes that relies on intermediaries, is replaced with automated processes that are completely transparent, verifiable, and thus trustworthy.
- The best part is that a "middleman" or any rent seeking third party can in theory be completely eliminated.
- Plus (apart from some gas fees to power the network) there is no charge to set up and deploy.

Smart contracts are what enable developers to create decentralized applications, or 'dApps'. They are also what allows dApps to be **Turing complete**, which means given the required resources, the Dapp can perform any action.

Source: District0x

Decentralized applications - dApps

dApps is short for **decentralized** applications. They are like normal applications, and can offer similar functions, but the key difference is they are run on a peer-to-peer network, i.e., a blockchain.

That means no one person or entity has control of the network. The wide consensus in the crypto community is that the following must be true for something to be considered a dApp:

- It must be open-source and operate on its own without any one entity controlling it.
- Its data and records must be public.
- It can use a cryptographic token to help keep the network secure.

dApps can simple programms, games, financial applications and more. DeFi is **merely a popular subset** of all possible dApps

Optionally, the collection of users of a dApp can be given (and share) the governance of the Dapp’s future behavior, through so-called **governance tokens**. Essentially, those bestow voting rights.

Sources: Decrypt and District0x

Decentralized applications - benefits

No owners

Once deployed to Ethereum, dapp code can’t be taken down. And anyone can use the dapp’s features. Even if the team behind the dapp disbanded you could still use it. Once on Ethereum, it stays there.

Free from censorship

Built-in payments

Plug and play

One anonymous login

Backed by cryptography

No down time

Source: Ethereum.org

Decentralized applications - weaknesses

- **Hacks:** As many dApps are run on open-source **smart contracts**, it allows hackers the rare opportunity to probe the networks looking for weaknesses. This has led to a spate of hacks on popular dApps.

- **Usability:** A lot of dApps have poor user-interfaces, which have put a lot of users off—see for example this reviews page. It improves over time though if a dApp survives.

- **Users:** Like many apps in Web2, the more users a dApp has, the more effective the network is at delivering those services. This is often referred to as the **network effect**. Many dApps struggle from low user numbers, which can make them less interactive. It can also make them less secure, as a dApp's security can often rely on how many users it has.

Source: Decrypt

DeFi in the Web3 context

As interesting as DeFi is, ultimately it is but a subset of all the possible application in a ‘**Web3**’ context.

Web2 refers to the version of the internet most of us know today, i.e., an internet dominated by centralized companies that provide services, often times in exchange for personal data.

Web3, in the context of Ethereum, refers to decentralized apps that run on the blockchain. These are apps that allow anyone to participate without monetizing their personal data.

At the moment, it is primarily the financial services sector that is being disrupted by Web3 in the form of DeFi. But this paradigm can, and most likely will, be extended to many other sectors as well. For example, the insurance sector (see e.g. Nexus Mutual) , content creation, consumption, and ownership, etc.

Web2 example	**Web3 example**
Twitter can censor any account or tweet	Web3 tweets would be uncensorable because control is decentralized
Payment service may decide to not allow payments for certain types of work	Web3 payment apps require no personal data and can't prevent payments
Servers for gig-economy apps could go down and affect worker income	Web3 servers can't go down – they use Ethereum, a decentralized network of 1000s of computers as their backend

Source: Ethereum.org

Session 2: DeFi Infrastructure - Ethereum

4. Key Ethereum concepts

Overview of key Ethereum Concepts

1. Consensus Mechanism
2. The Ether Token
3. The Ethereum Virtual Machine (EVM)
4. Ethereum as a platform for tokens (and use cases)
5. Token standards
6. Gas and gas fees and gas limit
7. Past, present and future of Ethereum

Consensus mechanisms

Different blockchains can use different kinds of consensus mechanisms. What are those for?

- Public ledgers need an **efficient, fair, real-time, functional, reliable, and secure** mechanism to ensure that all the transactions occurring on the network are **genuine** and all participants **agree on the status of the ledger**.
- This all-important task is performed by the consensus mechanism, which is a set of rules for determining the **legitimacy of contributions** made by the various participants

Ethereum, like Bitcoin, uses a mechanism called Proof-of Work (PoW). This requires the exertion of computational power in order to **solve** a difficult but arbitrary **puzzle** in order to keep all nodes in the network **honest**. However, Ethereum is planning to upgrade to a Proof-of-Stake (PoS) consensus protocol.

- PoS has evolved as a low-cost, low-energy consuming alternative to the PoW algorithm. It involves the allocation of **responsibility** in maintaining the public ledger to a **participant node** in proportion to the **number of virtual currency tokens held** by it.
- Advantages include reduced hardware requirements, arguably stronger **immunity to centralization** and better support for shard chains. However, PoS is a plutocratic system that comes with many disadantages

The Ether token

- Ether is the **native token** of the Ethereum blockchain. Ether is referred to with is ticker name, ETH, or by the Greek letter Ξ (Xi) which resembles a stylized version of the letter “E” as in Ether. Sometimes it is also represented by the symbol ◆ which resembles Ethereum’s Octahedron logo.
- Ether can be **subdivided** into smaller units, similarly to how bitcoins are subdivided to satoshis. The smallest possible unit is named wei, with 1 ETH equal to 1 quintillion wei. (1 * 10^18 or 1,000,000,000,000,000,000) The network executes all internal transactions in wei.
- **Ether powers all applications** that run on the Ethereum blockchain, from simple transactions to complex decentralized applications. From a taxonomy standpoint, it is more akin to a **utility token**, as it serves a role similar to **gas** for cars, hence the name.
- While Ethereum’s purpose is not primarily to be a payment network, and ether’s purpose is not to serve the function of money, due to its **high utility** it is often used as a currency and as a speculative instrument.

Ethereum Virtual Machine (EVM)

There are two different types of accounts in Ethereum: externally owned accounts (EOAs) and contract accounts. EOAs are controlled by users, often via software such as a **wallet** application that is external to the Ethereum platform. In contrast, **contract accounts** are controlled by program code (also commonly referred to as "**smart contracts**") that is executed by the Ethereum Virtual Machine (EVM).

- The EVM is a computation engine which acts like a decentralized computer that has millions of executable projects. It acts as the virtual machine which is the bedrock of Ethereum's entire operating structure.
- It is considered to be the part of the Ethereum that runs execution and smart contract deployment.
- The role of the EVM is to deploy a number of extra functionalities to the Ethereum Blockchain
- Every Ethereum node runs on the EVM to maintain consensus across the blockchain.
- EVM is completely isolated meaning the code inside the EVM has no access to network, file system or other processes.
- Most of the source code for using smart contracts is done using programming language from Solidity.

Sources: Ethereumbook on github.com and Coinmarketcap

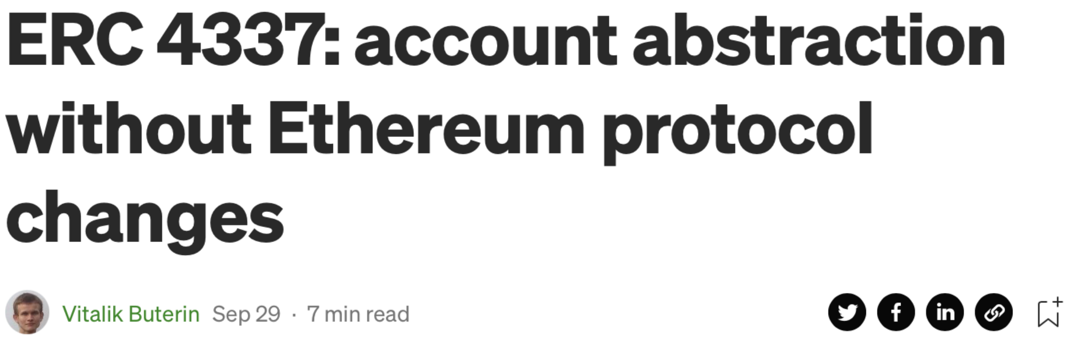
Tokens running on Ethereum

Nowadays, the word ‘token’ in a crypto context refers to blockchain-based abstractions that can be **owned** and that represent assets, currency, or access rights. Tokens on Ethereum draw their properties from specific token standards, which come in many flavors.

The most popular currently in use are

- ERC20 tokens, used for most tokens
- ERC721 tokens, predominately used for NFT

This is a fast-moving space with new token standards proposed all the time (more on that in Week 2):



ERC 4337: account abstraction without Ethereum protocol changes

Vitalik Buterin Sep 29 · 7 min read

Sources: Ethereumbook on github.com

Token use cases (non-currency)

Resource: A token can represent a resource earned or produced in a sharing economy or resource-sharing environment; for example, a storage or CPU token representing resources that can be shared over a network.

Asset: A token can represent ownership of an intrinsic or extrinsic, tangible or intangible asset; for example, gold, real estate, a car, oil, energy, MMOG items, etc.

Access: A token can represent access rights and grant access to a digital or physical property, such as a discussion forum, an exclusive website, a hotel room, or a rental car.

Equity: A token can represent shareholder equity in a digital organization (e.g., a DAO) or legal entity (e.g., a corporation).

Voting: A token can represent voting rights in a digital or legal system.

Collectible: A token can represent a digital collectible (e.g., CryptoPunks) or physical collectible (e.g., a painting).

Identity: A token can represent a digital identity (e.g., avatar) or legal identity (e.g., national ID).

Attestation: A token can represent a certification or attestation of fact by some authority or by a decentralized reputation system (e.g., marriage record, birth certificate, college degree).

Utility: A token can be used to access or pay for a service.

Gas use cases

- As the name implies gas is the fuel of the Ethereum network. A gas fee is paid for executing operations on the network. The fee is denominated in Ether or in Gwei, the latter for a better user experience. Fee levels vary from block to block, based on network congestion (supply and demand).
- The gas price paid for each transaction acts as an **incentive to miners** for your transaction to be included in a block.

Gas limits: both users and miners can use these. A user can set a gas limit in a wallet, being the maximum amount someone is willing to pay for a transaction. Miners collectively decide on adjustments to the **block gas limit** – being the maximum amount of gas contained in one block of transactions. A history of that number can be found here and on the following chart.

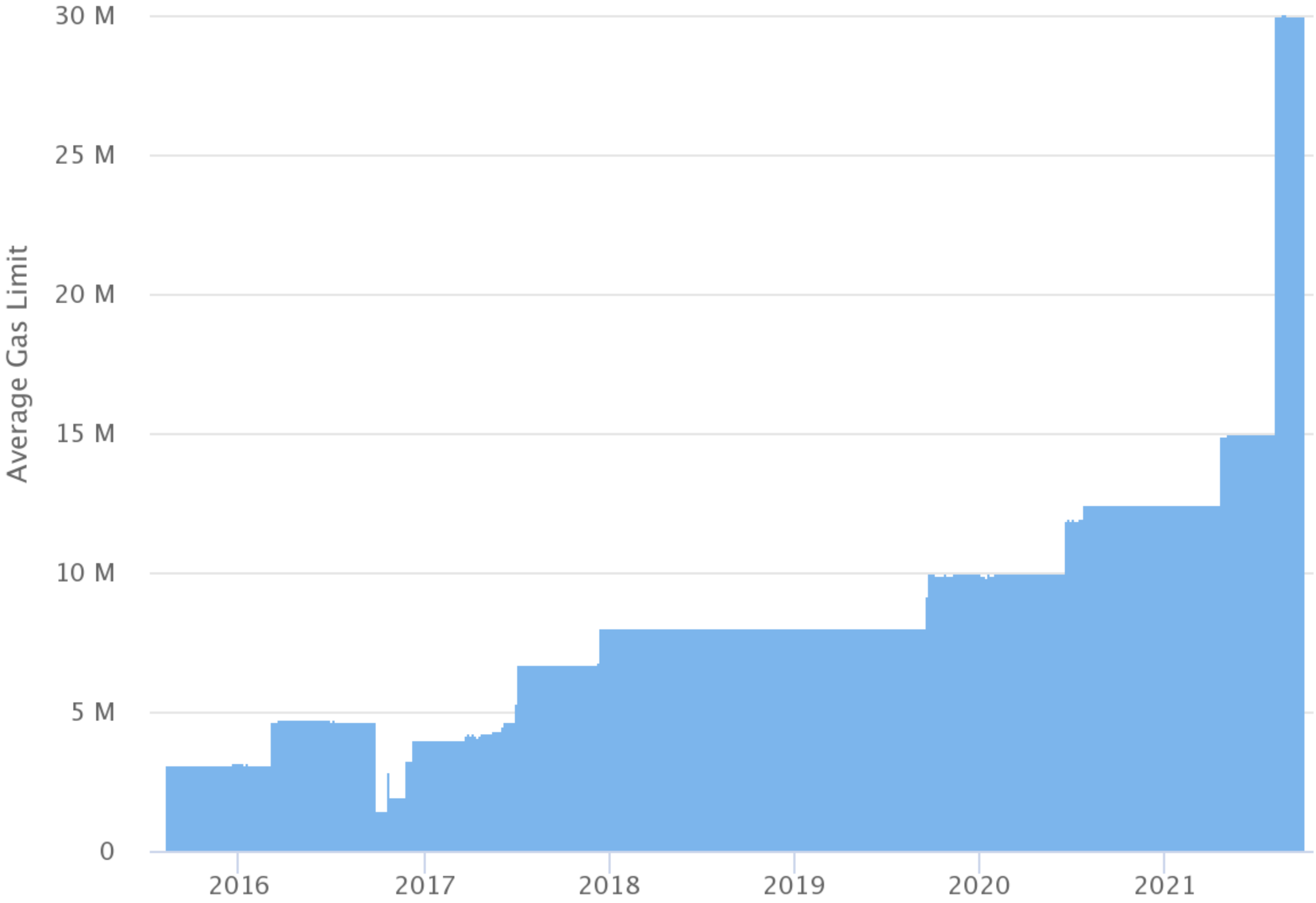
- The block gas limit is **enforced** by the consensus protocol. In each block, miners can increase or decrease the block size by a maximum of the previous block size divided by 1024. Looking to the near future of Ethereum Improvement Proposals (EIP) we see **EIP-1559**. That is a proposal to make Ethereum transactions more **efficient** by using a hybrid system of **base fees and tips** to more evenly incentivize miners in periods of high and low network congestion. If implemented, EIP-1559 could greatly reduce transaction costs and improve Ethereum's overall user experience.

Sources include Investopedia and Blocknative and Gemini.

Ethereum average gas limit chart

Ethereum **transaction fees** (gas) are based on supply and demand, a **busy network** means higher fees. The advent of DeFi sent fees skyrocketing. As a result, competing L1 chains got an impetus. However, the Ethereum development roadmap contains proposed **solutions**, expected in early 2022.

For details on gas origins and its future, see Ethereum.org.



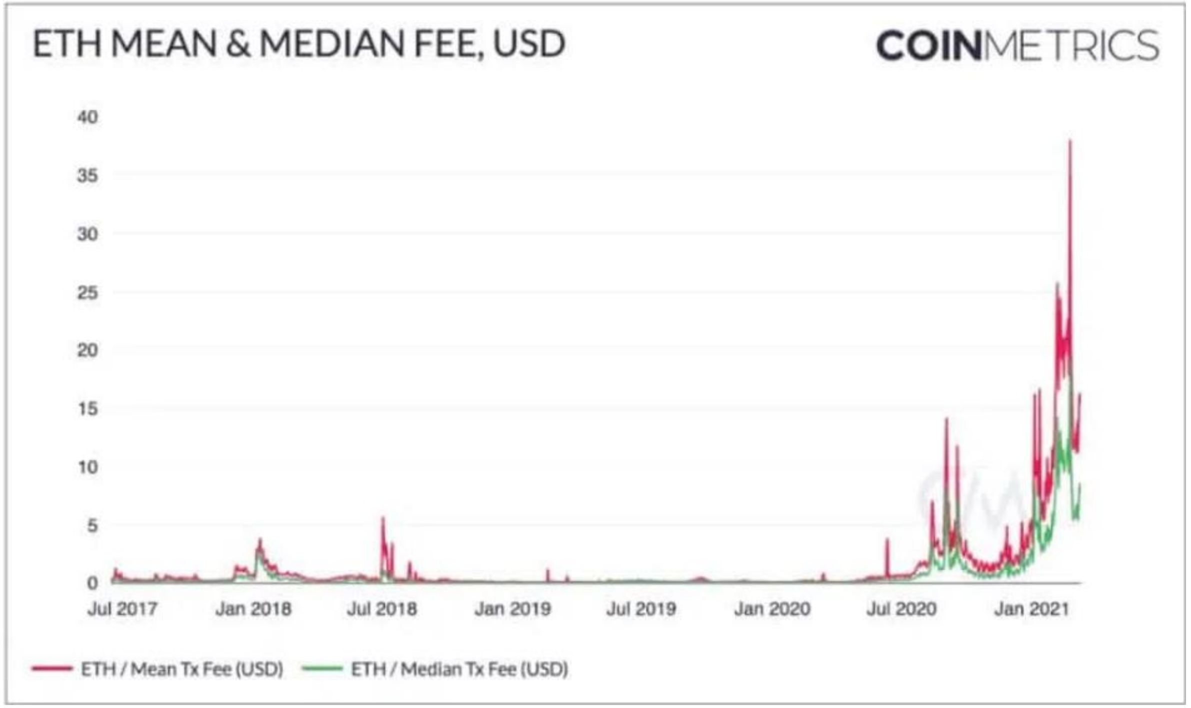
Source: Etherscan.io

Session 2: DeFi Infrastructure - Ethereum

Ethereum transaction fees reached **new highs** in early 2021.

For context, at the peak of the 2017/2018 bull run, the **average Ethereum transaction fee reached $5.70**. Ethereum average transaction fee has been more than $5.70 every day since January 18th, 2021. The median transaction fee has been above $10 for most of the year.

Part of the growth in transaction fees has been due to the sharp increase in ETH price. As ETH gets more valuable, transaction fees get more and more expensive **when measured in USD**. But it's also due to a large increase in gas prices caused by network congestion.



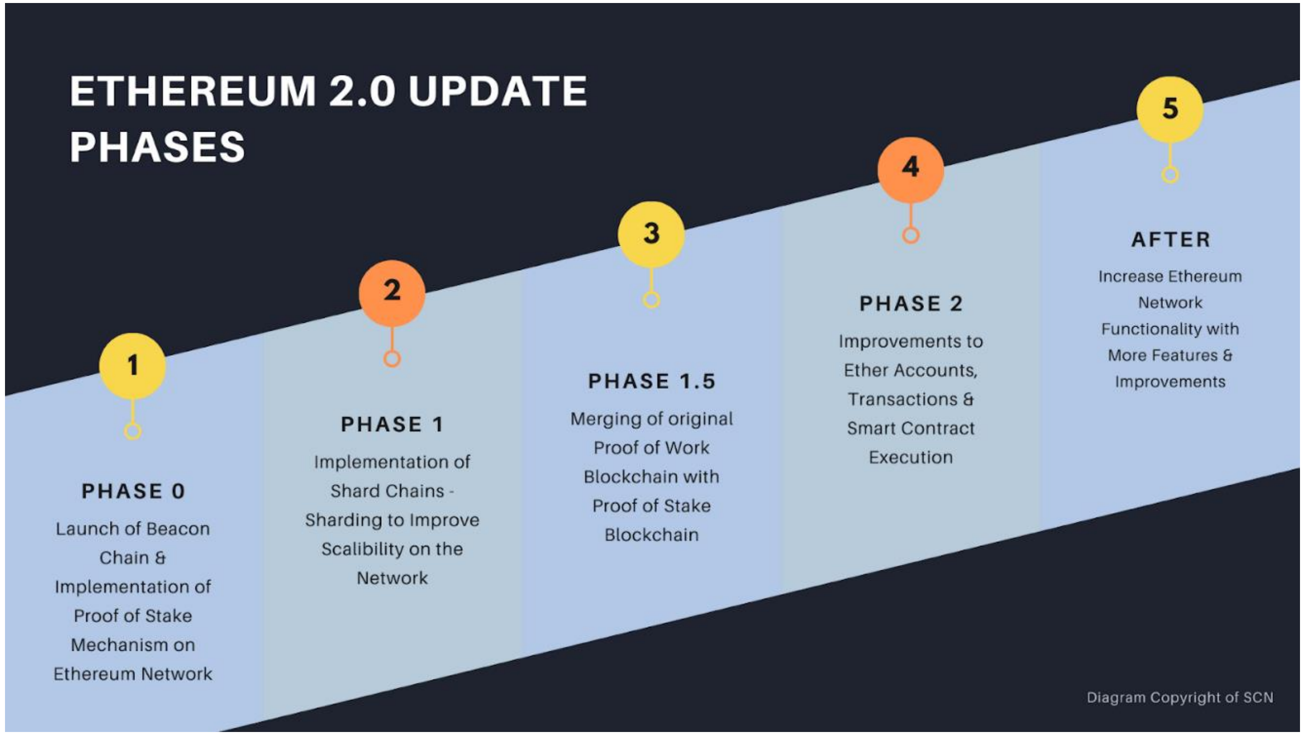
Source: Coinmetrics

Ethereum timeline and future

- Ethereum's development **deviated in culture** from other decentralized networks. In Bitcoin for example development is slow and guided by conservative principles. Changes are only implemented if they are backwards compatible.
- By contrast, Ethereum has adopted a forward-looking culture focused on **rapid innovation and evolution**, even at the expense of backwards compatibility, or community divide. This has resulted in an ever-shifting landscape, yet arguably less secure and **less decentralized** than that of Bitcoin.
- Serenity – or Eth2 is expected in the near future.
- Serenity refers to Eth2, a set of interconnected upgrades that will make Ethereum **more scalable, more secure, and more sustainable.** This will include a number of changes including transition from proof-of-work to a proof-of-stake consensus algorithm, a scaling solution called sharding, and a more efficient Ethereum Virtual Machine.

Ethereum timeline and future

Serenity will be introduced in 5 phases: a) Phase 0: Beacon Chain (officially released on Dec. 1st of 2020), b) Phase 1: Sharding, c) Phase 1.5: Merging Ethereum PoW Blockchain With New PoS Blockchain, d) Phase 2: Implementation of the new operating model, and e) Stage zero: the launch.


ETHEREUM 2.0 UPDATE PHASES
1
PHASE 0
Launch of Beacon Chain & Implementation of Proof of Stake Mechanism on Ethereum Network
2
PHASE 1
Implementation of Shard Chains - Sharding to Improve Scalibility on the Network
3
PHASE 1.5
Merging of original Proof of Work Blockchain with Proof of Stake Blockchain
4
PHASE 2
Improvements to Ether Accounts, Transactions & Smart Contract Execution
5
AFTER
Increase Ethereum Network Functionality with More Features & Improvements
Diagram Copyright of SCN

Session 2: DeFi Infrastructure - Ethereum

5. Conclusions

Conclusions

In this session, you have learned about the foundational nature of blockchain technology for DeFi, and Ethereum’s role therein. You now have insight into the DeFi stack and into Ethereum’s history, characteristics, size, adoption rate.

You should now have a grasp of the nature and role of smart contracts and decentralized applications (dApps), tokens, their benefits and weaknesses, and their relation to the Web3 concept.

Finally, you have been introduced to key Ethereum concepts such as consensus mechanisms, the EVM, the Ether token, gas, and the multitude of other tokens that exist and have become possible thanks to Ethereum.

This basis is needed as DeFi was **birthed** on Ethereum, although it is now also growing on other L1 blockchains (more on this next week). Today’s session laid a foundation in knowledge on which later sessions in this MOOC will build to explore specific applications of DeFi in greater detail.

Session 2: DeFi Infrastructure - Ethereum

6. Further Reading

Further Reading

Mapping the future of DeFi:

- https://www.realvision.com/shows/the-interview-crypto/videos/mapping-the-future-of-defi

From DeFi boom to DeFi bust?

- https://www.forbes.com/sites/kenrapoza/2021/09/12/is-ethereums-defi-boom-setting-itself-up-for-defi-bust/?sh=6e3ec7f56a57

Ethereum and DeFi

- https://ethereum.org/en/defi/

The Ethereum DeFi ecosystem:

- https://defiprime.com/ethereum

The future of DeFi: Ethereum or Bitcoin?

- https://cointelegraph.com/news/where-does-the-future-of-defi-belong-ethereum-or-bitcoin-experts-answer

UNIVERSITY *of* NICOSIA

Questions?

Contact Us:

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