Overview and Etherium Network

Introduction to Etherium

- **Vitalik Buterin** conceptualized Ethereum in November 2013, introducing a Turing-complete language to enable smart contracts and decentralized applications on the blockchain.
- Designed for smart contracts and decentralized applications (DApps).
- Unlike Bitcoin, Ethereum supports a Turing-complete scripting language.
- The **first version of Ethereum**, called Olympic, was released in May, 2015

The Etherium Yellow Paper

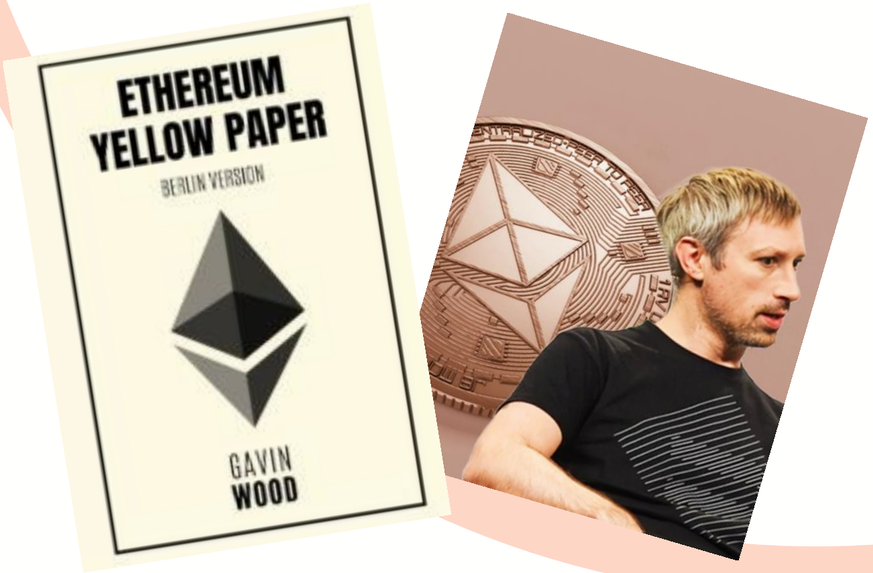
- Written by **Dr. Gavin Wood**, co-founder of Ethereum & Parity.
- It provides a formal definition of the Ethereum protocol and serves as a guide for implementing Ethereum clients.
- Developers can follow its rules to build compliant clients.
- It is a highly technical document requiring expertise.
- Understanding mathematical notations is necessary.
- [Ethereum Yellow Paper]

s we may define a world-state collapse functi

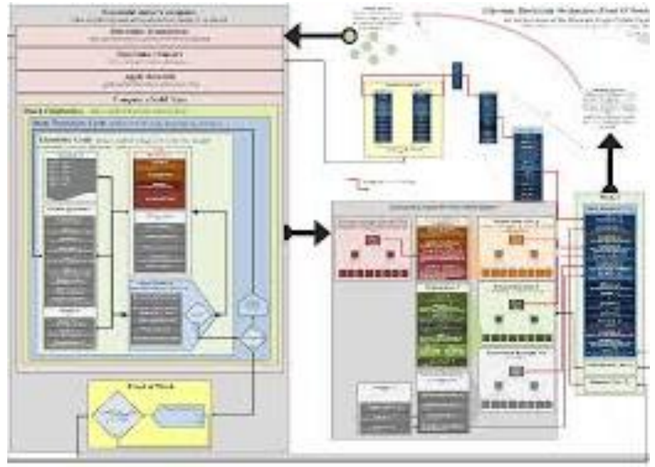
$$L_S(\boldsymbol{\sigma}) \equiv \{p(a) : \boldsymbol{\sigma}[a] \neq \varnothing\}$$

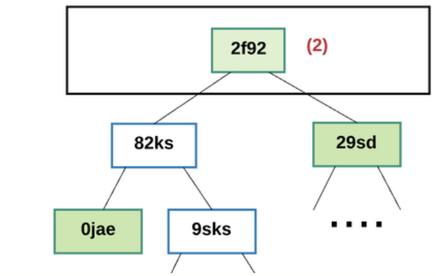
$p(a) \equiv \left(\text{KEC}(a), \text{RLP}\left((\boldsymbol{\sigma}[a]_{\text{n}}, \boldsymbol{\sigma}[a]_{\text{b}}, \boldsymbol{\sigma}[a]_{\text{s}}, \boldsymbol{\sigma}[a]_{\text{c}}\right.\right.$

s function, L_S, is used alongside the trie fu
ide a short identity (hash) of the world stat
:



- The Yellow Paper can be difficult to read.It requires knowledge of algebra and mathematical notations.
- It provides a complete formal specification.Developers can use it to create fully compliant Ethereum clients.
- Understanding symbols makes reading easier.Knowing their meanings helps in grasping key concepts.
- The paper defines Ethereum’s core logic.It explains how transactions and state changes work.
- It serves as a technical guide for developers.





Whitepapers vs Yellowpapers

Useful Mathematical symbols

Symbol	Meaning	Symbol	Meaning
≡	Is defined as	≤	Less than or equal to
=	Is equal to	σ	Sigma, World state
≠	Is not equal to	μ	Mu, Machine state
‖ ... ‖	Length of	Υ	Upsilon, Ethereum state transition function
∈	Is an element of	Π	Block level state transition function
∉	Is not an element of	.	Sequence concatenation
∀	For all	∃	There exists
∪	Union	∧	Contract creation function
∧	Logical AND	Δ	Increment
:	Such that	⌊...⌋	Floor, lowest element
{}	Set	⌈...⌉	Ceiling, highest element
()	Function of tuple	|...|	No of bytes
[]	Array indexing	⊕	Exclusive OR
∨	Logical OR	(a ,b)	Real numbers >= a and < b
>	Is greater than	∅	Empty set, null
+	Addition		

- Mathematical symbols define Ethereum's logic. These symbols represent key functions, states, and operations.
- Understanding symbols helps in protocol implementation. Developers can use them to correctly interpret Ethereum’s rules.

Etherium Blockchain

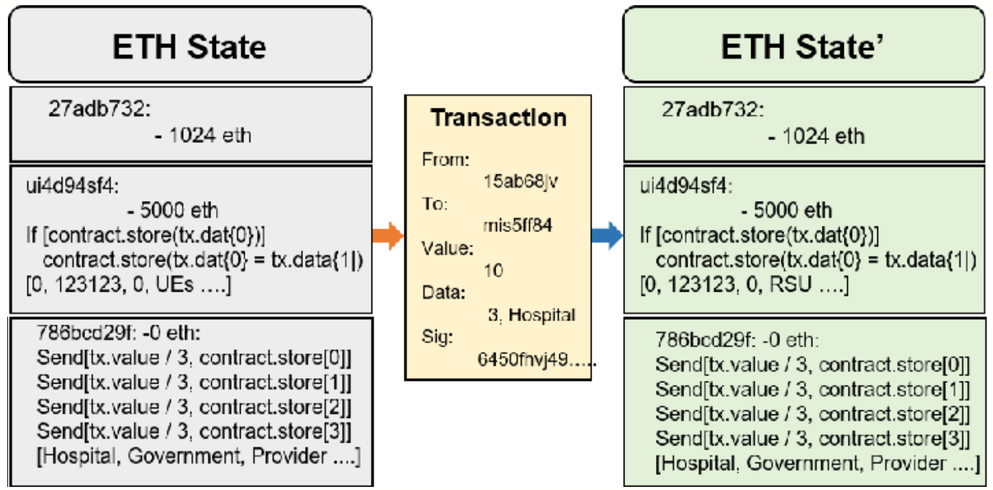
- Ethereum operates as a transaction-based state machine, as defined in the Ethereum yellow paper by
  Dr. Gavin Wood.

- A genesis state transforms into a final state by executing transactions incrementally.

- The Ethereum state transition function ensures that executed transactions lead to an undisputed final state.

- Mining plays a crucial role in validating transactions and facilitating state transitions.

- The Ethereum world state stores the global blockchain state, ensuring consistency across the network.



State transition function

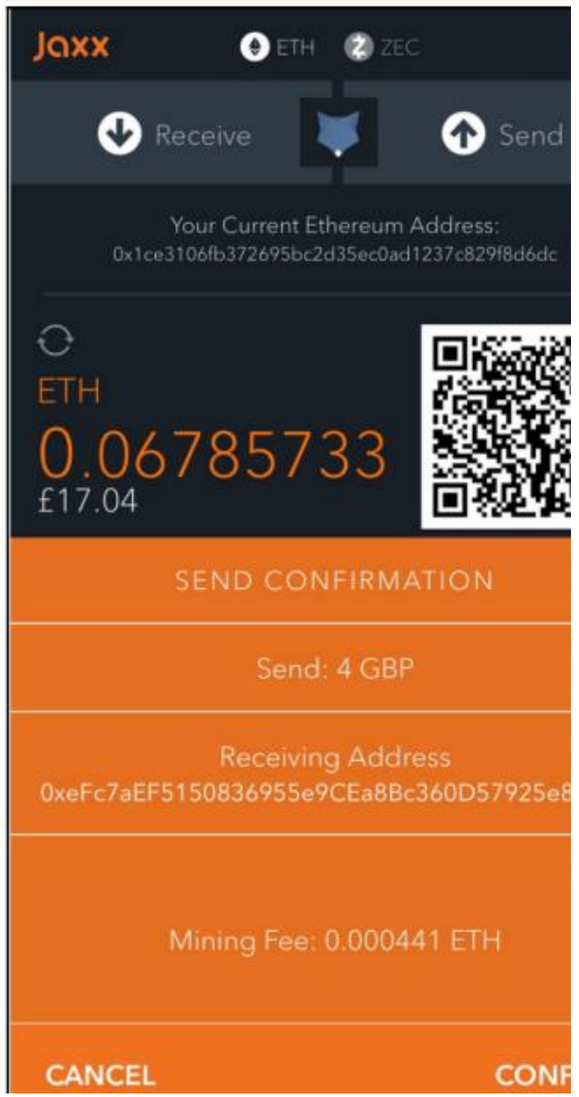
Bird’s eye view

Ethereum Transactions – User Perspective

- Ethereum transactions involve sending and receiving funds between users using Ethereum clients.
- A user can request funds by sharing their Ethereum address, often via a QR code.
- The sender can scan the QR code or manually enter the recipient's address to transfer Ether.
- Transactions can be initiated through wallets like Jaxx Wallet (https://jaxx.io) for seamless transfers.
- Requests and transactions can be shared via email, text, or other communication methods.

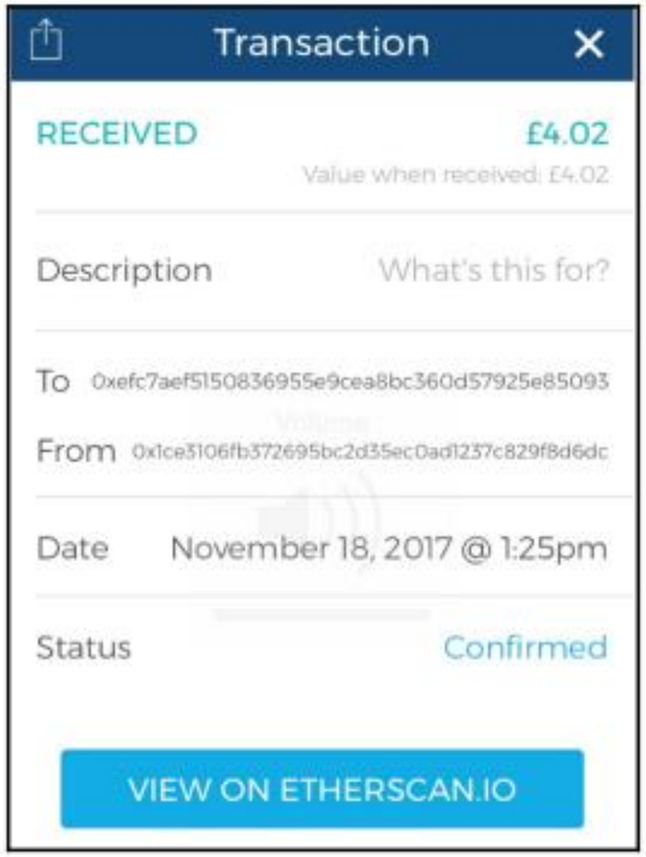
Bird’s eye view

- The sender scans the QR code or copies the recipient’s Ethereum address into their wallet software.
- The sender enters the amount and the destination address before confirming the transaction.
- Wallets like Jaxx (used in this example) facilitate Ethereum transactions.
- Multiple wallet applications are available on the iOS App Store, Android Play Store, and online.
- The transaction is first broadcasted to the Ethereum network and digitally signed by the sender. This signature proves ownership of the Ether and ensures transaction authenticity.



Bird’s eye view

- Miners pick up the transaction for verification and include it in a block. Until a miner confirms it, the transaction remains unconfirmed in the network.
- The Proof of Work (PoW) process begins, where miners repeatedly hash the block with a nonce. This computational process ensures security and prevents fraudulent transactions.
- Once a miner solves the PoW puzzle, the block is broadcasted to the network. Other nodes verify the block and ensure that all transactions follow Ethereum’s consensus rules.
- If the block is successfully verified, it is added to the blockchain. The recipient then receives the Ether, and the miners are rewarded for their efforts.
- A transaction hash (TxHash) is generated, which acts as a unique ID. This hash can be used to track and validate the transaction across the Ethereum blockchain.

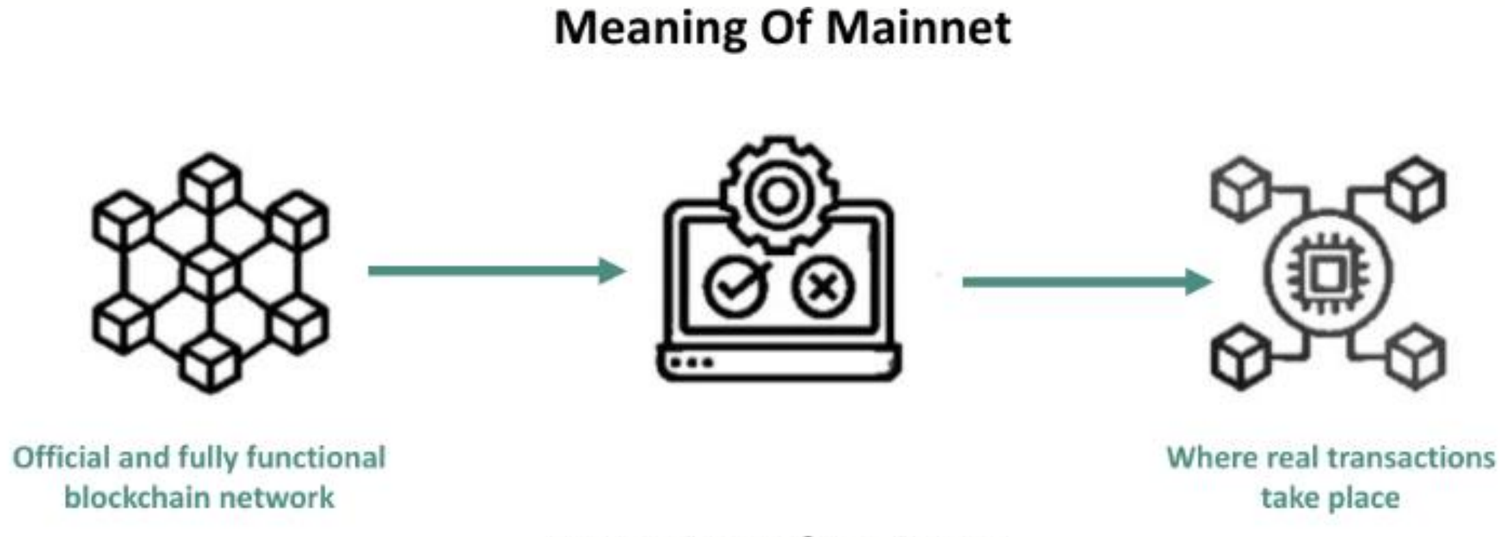


Etherium Network

- The Ethereum network is a peer-to-peer system, where nodes work together to maintain the blockchain and ensure consensus. Different networks exist based on requirements and usage.

Types of Ethereum Networks

- **Mainnet**: The live Ethereum blockchain where real transactions occur. The latest version is Byzantium (Metropolis), and its Chain ID is 1. Users can explore blocks using Etherscan (https://etherscan.io).



Etherium Network

- **Testnet (Ropsten)**: A test environment for smart contracts and DApps before deploying them on the mainnet. Other testnets like Kovan and Rinkeby were merged into Ropsten for improved testing.

- **Private Net**: A custom Ethereum network created by defining a new genesis block. It is used for private blockchains where access is restricted to selected entities.

- **Network Identification**: Each Ethereum network has a unique Chain ID (e.g., Mainnet = 1, Ropsten = 3, Kovan = 42). These IDs help Ethereum clients differentiate between networks

Open to Queries

Thank you