

Ethereum-WhitePaper Summary :

The Ethereum-Whitepaper was written by Vitalik Buterin in 2014.

It was in 2009, that Satoshi Nakamoto introduced “bitcoin” to the world; most probably the first ever asset that simultaneously was not controlled by a central authority/body, that had no backing and didn’t possess any intrinsic value (perceived value of an asset). Also, **bitcoin** works on **blockchain** technology that is based on “Proof of Work” (a distributed consensus mechanism). There are several other applications of the technology as well like – namecoins (cryptocurrency used in dns registry based on first to file paradigm), coloured coins (allows people to create their own currency, can be used to represent non-monetary assets), meta-coins e.t.c. However the scripting language used in bitcoin has certain limitations like – (Lack of Turing completeness, value blindness, Lack of state e.t.c) .

Any interaction on the **Ethereum** network occurs via “**Accounts**”; they are of two types – EOAs and Contract accounts. EOAs are controlled by a private key whereas contract accounts don’t need one since they are just run by the code present on these accounts. Each account possesses a **state** and cumulatively they constitute the global state of Ethereum that is maintained by all the nodes on the network (in a synchronized manner).

Ethereum **transactions** are data packets containing vital information: the recipient’s address, the value, the gas limit and gas price, a nonce, and the sender’s signature. Each transaction is digitally signed, utilizing the private key associated with the initiator’s account. They can trigger contract executions, resulting in a new state influenced by the transaction’s data. Once validated and recorded on the blockchain, transactions and their state transitions are irreversible. “**Gas**” in Ethereum refers to the unit that measures the amount of computational effort required to execute operations like transactions or smart contracts. Miners, responsible for transaction validation, prioritize transactions offering higher gas prices, influencing transaction processing speed. This mechanism encourages fair bidding for network resources. In the Ethereum network, **messages** refer to virtual objects exchanged between contracts, triggering function executions, sharing data and outputs seamlessly, akin to integrated software modules in traditional programming.

Ethereum is not just a typical cryptocurrency but emerges as a sophisticated platform for executing programmable contracts, or **smart contracts**. The

Ethereum Virtual Machine (EVM) powers this functionality. Each operation consumes a certain amount of gas, and these costs ensure the network isn't clogged with computationally intensive or infinite-loop contracts. During execution, the EVM uses a stack for quick, temporary data storage, memory for storing data temporarily during execution, and storage for keeping data long-term across all Ethereum nodes.