Accounts, Addresses and Transaction in Ethereum.

An Ethereum account is an entity with an ether (ETH) balance that can send transactions on Ethereum. Accounts can be user-controlled or deployed as smart contract (Program on ethereum blockchain).

Account types

- Externally-owned (EOA) - controlled by anyone with the private key.
- Contract - a smart contract deployed to the network, controlled by code.

Both account types have the ability to:

Both account types have ability to:

- Receive, hold and send ETH
- Interact with deployed smart contracts.

Key differences

EOA:

- Creating an account costs nothing
- Can initiate transaction
- Transaction between EOA accounts can only be assets transfers

Contract account:

- Creating contract has a cost
- Can only send transaction in response to receiving a transaction
- Transaction from an EOA account to a contract account can trigger code which can execute many different actions

An account examined

Ethereum accounts have four fields:

- nonce - A counter that indicates the number of transactions sent from the account

- balance - The number of wei owned by this address. Wei is a denomination of ETH and there are 1e+18 (10^18) wei per ETH

- codeHash - This hash refers to the code (contract code) of an account on the Ethereum virtual machine. For EOA accounts this field is zero

- storageRoot - Talk about it later

EOA and key pairs

An account is made up of a cryptographic pair of keys: public and private. They help prove that a transaction was actually signed by sender and prevent forgeries. Your private key is what you use to sign transactions, so it grants you custody over the funds associated with your account.

Account creation (EOA)

When you want to create an account most libraries will generate you a random private key.

A private key is made up of 64 hex characters and can be encrypted with a password.

Example: `fffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd036415f`

The public key was generated from the private key using the Elliptic Curve Digital Signature Algorithm. You get a public address for your account by taking the last 20 bytes of the Keccak-256(Hash function) hash of the public key and adding 0x to the beginning.

Account creation (EOA)

It is possible to derive new public keys from your private key but you cannot derive a private key from public key. This means it’s vital to keep private key safe and, as the name suggests PRIVATE.

You need a private key to sign messages and transactions which output a signature. Others can then take the signature to derive your public key, providing the author message.

Account creating (contract)

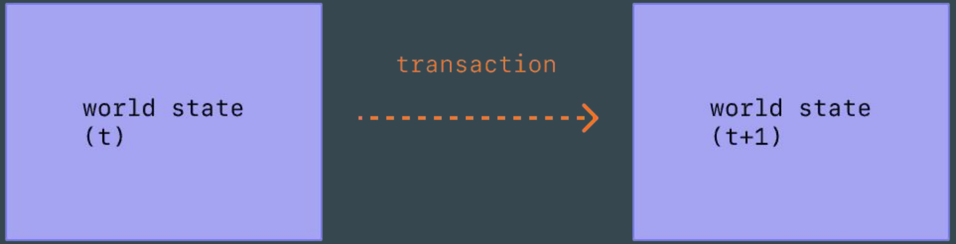
Contract account also have a 42 character hexadecimal address:

Example: `0x06012c8cf97bead5deae237070f9587f8e7a266d`

The contract address is usually given when a contract is deployed to the Ethereum Blockchain. The address comes from the creator’s address and the number of transactions sent from that address (the “nonce”).

Transaction

An Ethereum transaction refers to an action initiated by an EOA. in other words an account managed by human. not contract. Transaction, which change the state of the Ethereum. need to be broadcast a request for a transaction to be executed.



Gas

Gas refers to the unit that measures the amount of computational effort required to execute specific operations on the Ethereum network. Since each Ethereum transaction requires computational resources to execute, each transaction require a fee. Gas refers to the fee required to conduct a transaction on Ethereum successfully.

Gas price are denoted in gwei, which itself is a denomination of ETH - each gwei is equal 10^-9 ETH.

Mining and Miners

Mining is the process of creating a block of transactions to be added to the Ethereum blockchain.

Why do Miners exist ?

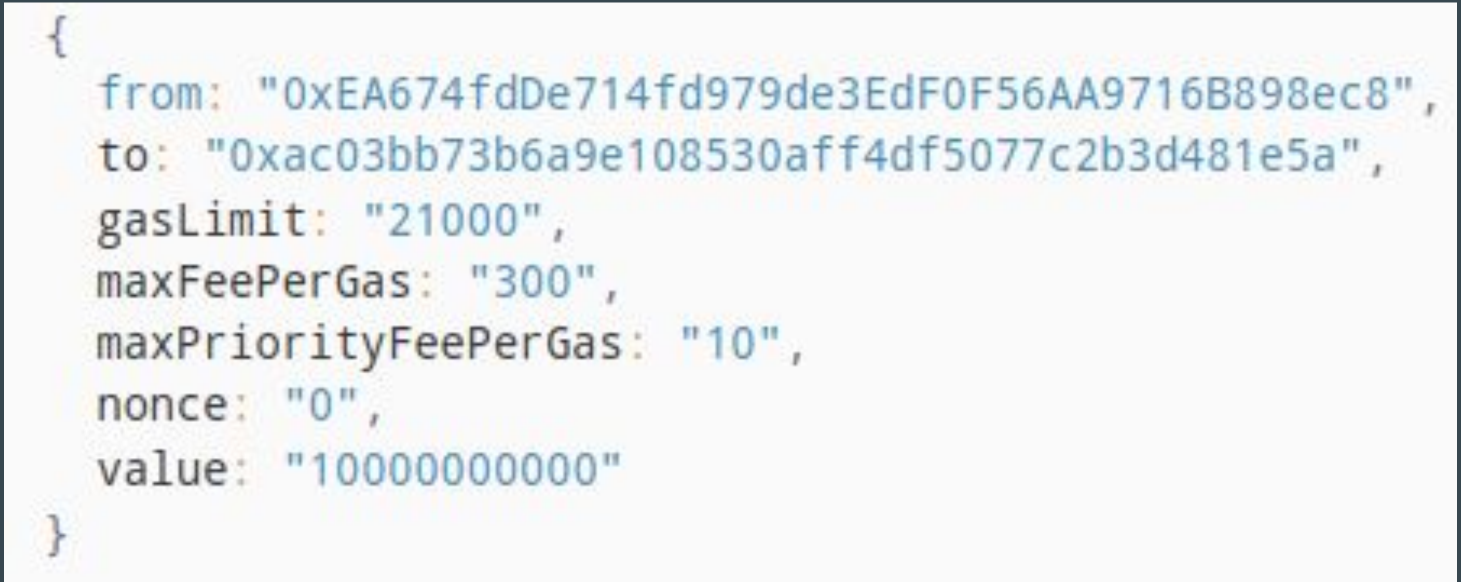
In decentralized systems like Ethereum, we need to make sure everyone agrees on the order of transactions. Miners help with this by solving computationally complex puzzles to create blocks. protecting network from attacks, and earning some rewards.

Transaction

A submitted transaction includes the following information:

- recipient - the receiving address
- signature - the identifier of the sender.
- value - amount of ETH to transfer
- data - optional field to include arbitrary data
- gasLitim - the maximum amount of gas units that can be consumed by the transaction
- maxPriorityFeePerGas - the maximum amount of gas to be included as tip to the miner
- maxFeePerGas - the maximum amount of gas willing to be paid for the transaction inclusive of baseFeePerGas and maxPriorityFeePerGas)

Transaction example



```
{
  from: "0xEA674fdDe714fd979de3EdF0F56AA9716B898ec8",
  to: "0xac03bb73b6a9e108530aff4df5077c2b3d481e5a",
  gasLimit: "21000",
  maxFeePerGas: "300",
  maxPriorityFeePerGas: "10",
  nonce: "0",
  value: "10000000000"
}
```

Types of Transactions

On Ethereum there are a few different types of transaction:

- Regular transaction: a transaction from one wallet to another

- Contract deployment transaction: a transaction without a “to” address, where the data field is used for the contract code

- Execution of a contract: a transaction that interacts with a deployed smart contract. In this case, “to” address is the smart contract address.

Useful links

- Transaction: https://ethereum.org/en/developers/docs/transactions/
- Ethereum accounts: Ethereum accounts
- Gas: Gas and fees | ethereum.org
- Miners and Minign: Mining | ethereum.org
- Article in Russian, some information given in that article hasn’t yet learned at our classes:

Как работает Эфириум (Ethereum)?