Algorand

blockchain cryptocurrency protocol

ANNA SKARLATOU

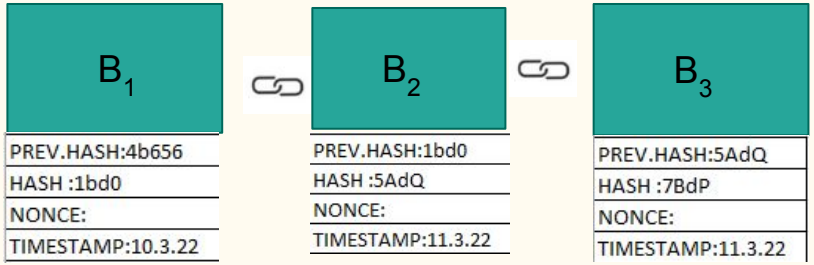
Who is Algorand creator ?

The algorand creator is Silvio Micali , a Italian computer scientist professor which is born in 1954 at Palermo, Italy and have won (in 2012) the Turing Award ,the Gödel Prize (in theoretical computer science) and the RSA prize (in cryptography). In 2017, Silvio founded Algorand.

What is a blockchain ?

Is a list of transactions , called blocks and each block is linking with others. Each block have :

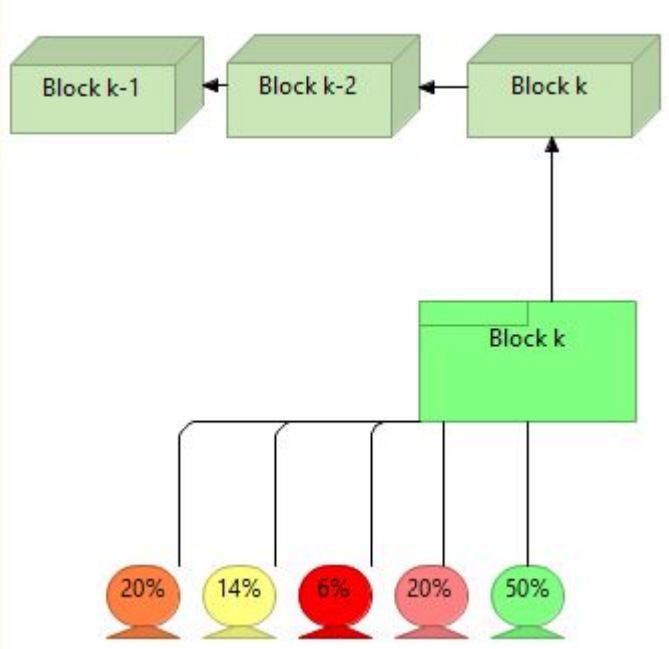
- Time Stamp
- Hash
- Previous hash
- Nonce



-One block is one coin.-

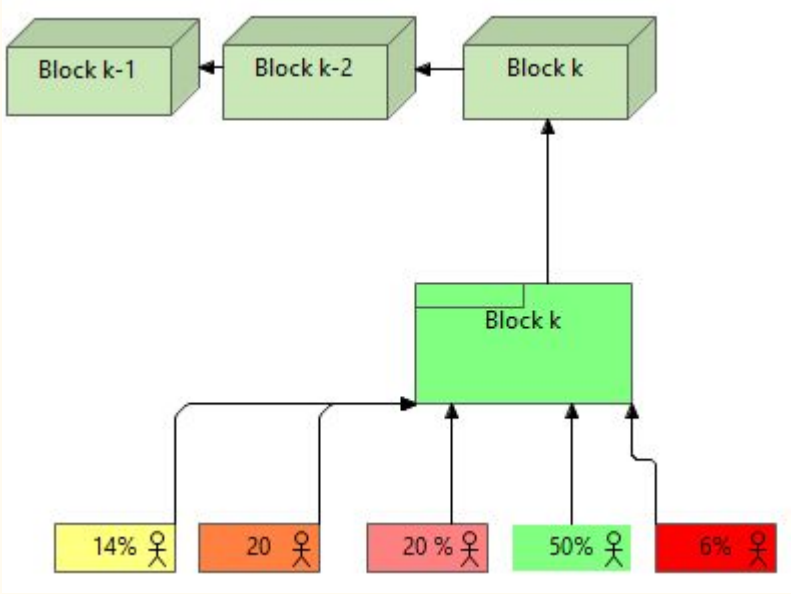
How other cryptocurrencies makes coins ?

Cryptocurrencies like Bitcoin use a Proof of Work protocol . This means that miners validate transactions by a difficult mathematical puzzle . When the puzzle is solve is produce the hash value.



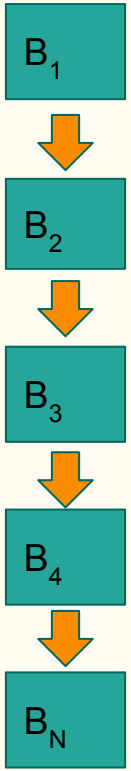
How Algorand makes coins?

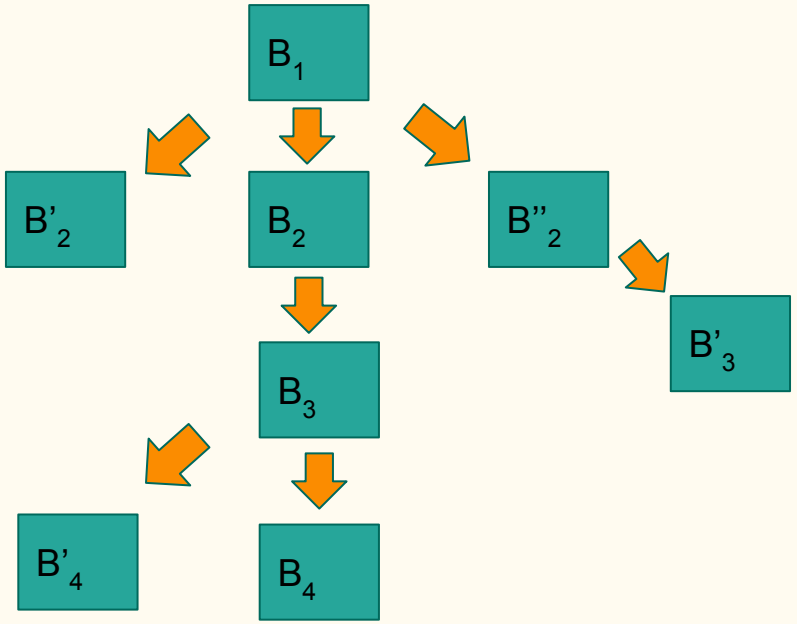
Algorand use the the Pure Proof-of-Stake (PPoS) protocol. This protocol means that each user's which hold **(at least one)** token can stake them and with a randomly* and secretly selected to propose blocks. Then vote on block proposals . The probability to choose a user, and the weight of its proposals and votes, are directly proportional to its stake.



*Cryptographic sortition

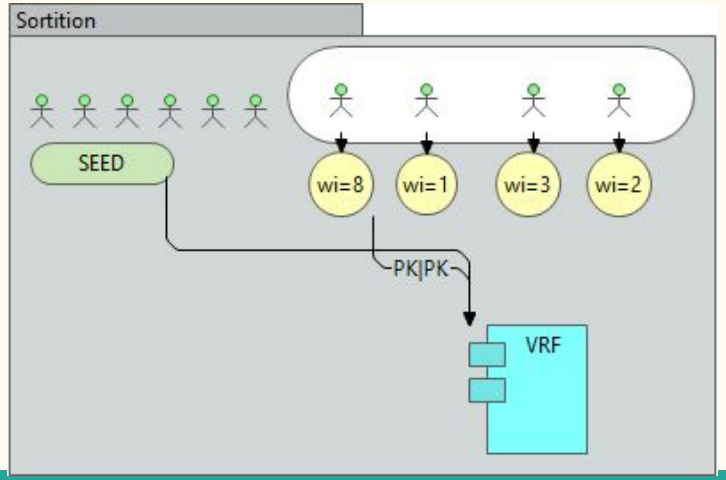
Blockchain of Bitcoin vs Blockchain Algorand





Cryptographic sortition

Cryptographic sortition is an algorithm for choosing a random subset of users with user ‘’weights’’. Weight of each user is the number of coins which is stake .So choose from ,sum of given a set of weights w_i ,$W = \Sigma_i w_i$, the probability that user i is selected is equal to w_i /W . The randomness in the sortition algorithm comes from a publicly known random seed. To allow a user to prove that they were chosen, sortition requires each user i to have a public key/private key pair, (Publick $_i$,Privatek$_i$).To verified the transactions algorand use the VRFs.

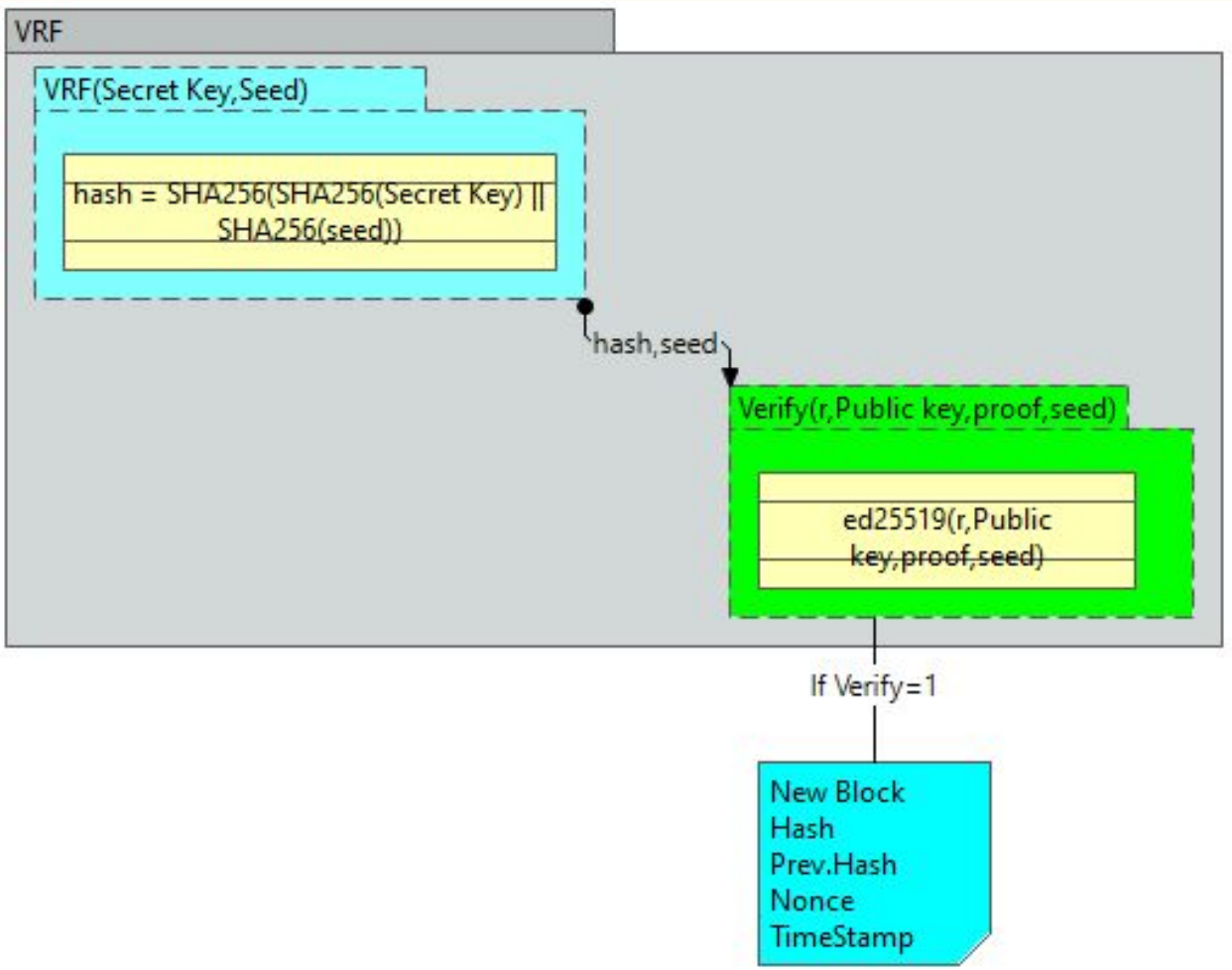


Verifiable Random Function (VRFs)

A VRF is a set of algorithms VRF and Verify.

- VRF (SK,seed) → (r,p). On a Secret key and seed input, the key generation algorithm produces a random number and a proof pair.
  hash = SHA256(SHA256(msg) || SHA256(nonce))
- Verify(r, PK, p, seed) → 0/1. The verification algorithm takes as input the random number, the public key , the proof and the seed. It outputs 1 if and only if it verifies that r is the output produced by the evaluation algorithm on inputs SK and seed
  ed25519 verify.

The seed is published and every round
is different.


VRF
VRF(Secret Key,Seed)
hash = SHA256(SHA256(Secret Key) || SHA256(seed))
hash,seed
Verify(r,Public key,proof,seed)
ed25519(r,Public key,proof,seed)
If Verify=1
New Block
Hash
Prev.Hash
Nonce
TimeStamp

Example of security tokens :

```
def create_account(fund=True):
# Change algod_token and algod_address to connect to a different client
algod_token = "2f3203f21e738a1de6110eba6984f9d03e5a95d7a577b34616854064cf2c0e7b"
algod_address = "https://academy-algod.dev.aws.algodev.network/"
algod_client = algod.AlgodClient(algod_token, algod_address)
```

https://replit.com/@Algorand/CreateSecurityTokenPython#aliceAssetMetaData.json

Conclusion

Benefits of Algorand :

- ➔ Is fast -takes only 5 seconds to ‘mining’ a Algo coin.
- ➔ Everyone can participate and make coins.
- ➔ Make coins with PPoS protocol.
- ➔ Is energy efficient than PoW.
- ➔ Can use for every day currency and all transactions -stable coin-.

References

- https://medium.com/swlh/blockchain-characteristics-and-its-suitability-as-a-technical-solution-bd65fc2c1ad1
- https://amturing.acm.org/award_winners/micali_9954407.cfm
- https://www.algorand.com/about/from-our-founder
- https://www.algorand.com/technology/pure-proof-of-stake
- https://www.researchgate.net/figure/PoW-and-PoS-consensus-mechanisms-comparison_fig2_334061880
- https://people.csail.mit.edu/nickolai/papers/gilad-algorand-eprint.pdf
- https://replit.com/@Algorand/CreateSecurityTokenPython#create_account.py
- https://www.algorand.com/resources/algorand-announcements/algorands-instant-consensus-protocol
- https://www.algorand.com/about/media-kit
- https://commons.wikimedia.org/wiki/File:Silvio_Micali.jpg