BUILDING A BLOCKCHAIN

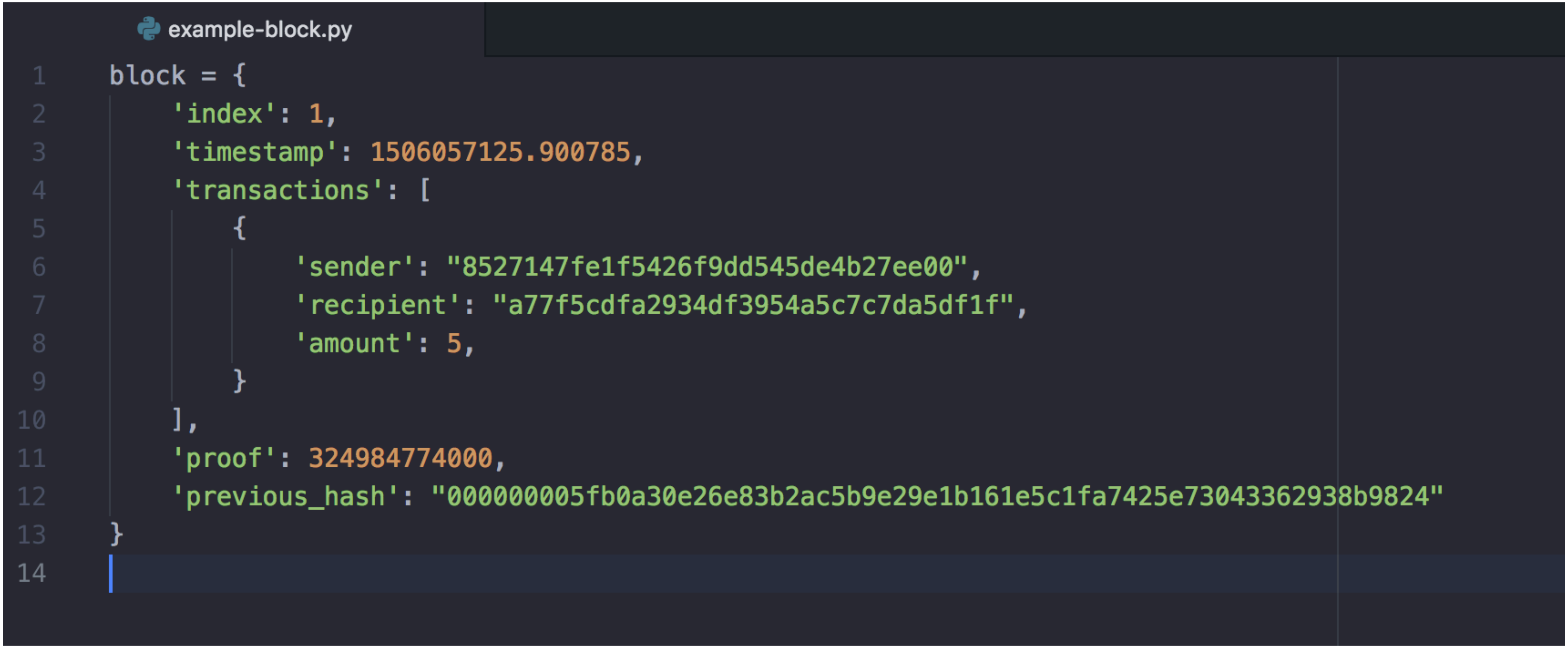
Jamie LeMercier, Suzanne Huldt,
Majdeddine Jebri, Robert Clayton

WHAT IS A BLOCKCHAIN?

A CHAIN OF BLOCKS?

WHAT IS A BLOCK?

- A block is a JSON file

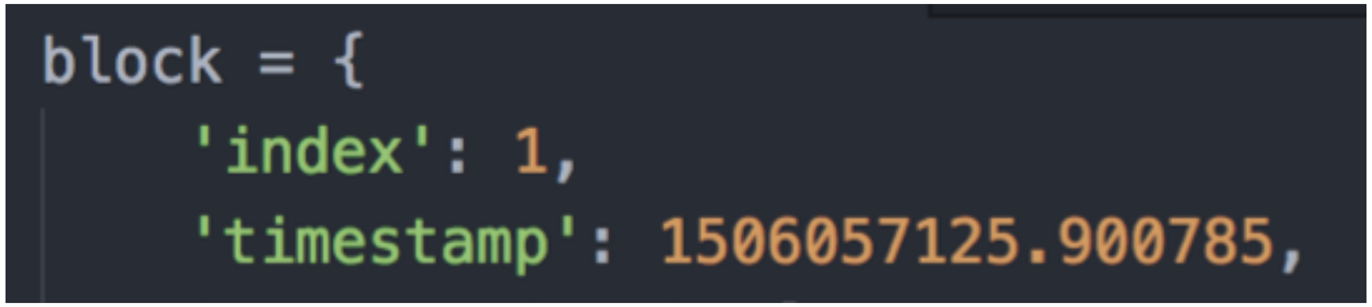


```python
block = {
    'index': 1,
    'timestamp': 1506057125.900785,
    'transactions': [
        {
            'sender': "8527147fe1f5426f9dd545de4b27ee00",
            'recipient': "a77f5cdfa2934df3954a5c7c7da5df1f",
            'amount': 5,
        }
    ],
    'proof': 324984774000,
    'previous_hash': "000000005fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824"
}
```

WHAT IS A BLOCK?

INDEX TIMESTAMP TRANSACTIONS PROOF PREV-HASH

- Index
  - The position of the block within the chain
- Timestamp
  - The timestamp is in Unix time, which is the amount of time that has elapsed since 00:00:00 UTC, Thursday 1st January 1970.

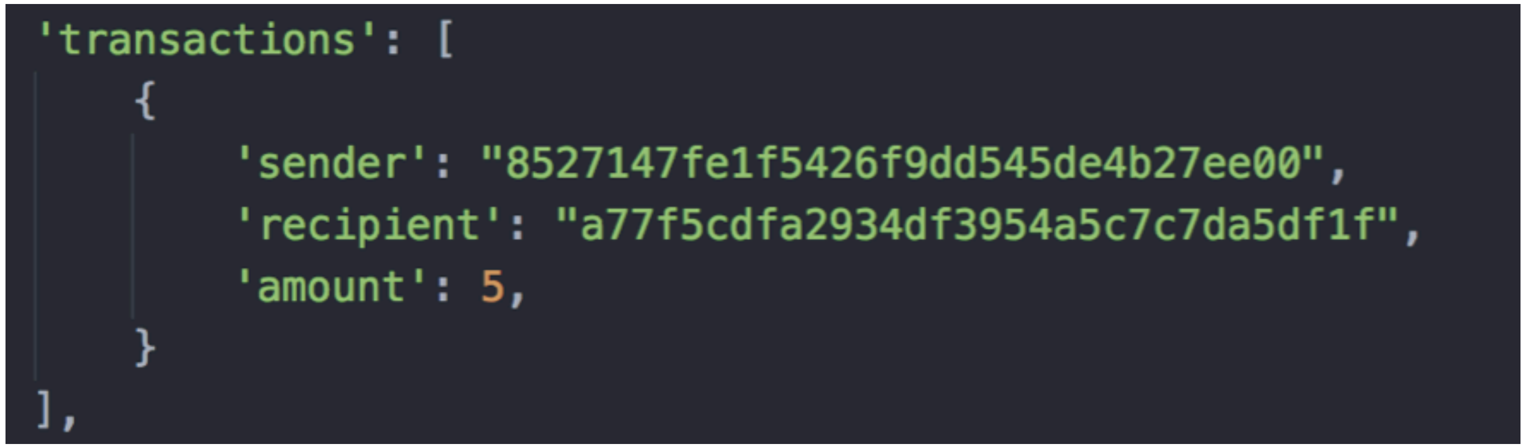


```
block = {
    'index': 1,
    'timestamp': 1506057125.900785,
```

WHAT IS A BLOCK?

INDEX TIMESTAMP TRANSACTIONS PROOF PREV-HASH

- Transactions require three parameters
    - Sender & Recipient are just simple strings. These could be ID’s for anonymity (see example), or something simpler like a name.
    - The third parameter is for Data. This could be a contract, a vote (in a voting application), or anything which creativity will allow. In our case its an amount.

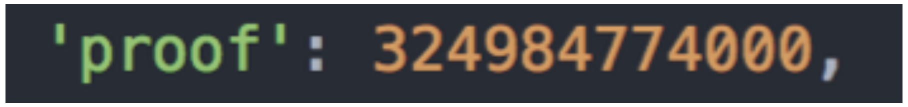


```
'transactions': [
    {
        'sender': "8527147fe1f5426f9dd545de4b27ee00",
        'recipient': "a77f5cdfa2934df3954a5c7c7da5df1f",
        'amount': 5,
    }
],
```

WHAT IS A BLOCK?

INDEX TIMESTAMP TRANSACTIONS PROOF PREV-HASH

- The Proof / Proof-of-Work also often called the Nonce, is simply a counter.
  - This number is the amount of times(loops performed) the computer has attempted to find the correct hash (more on what hashes are later).

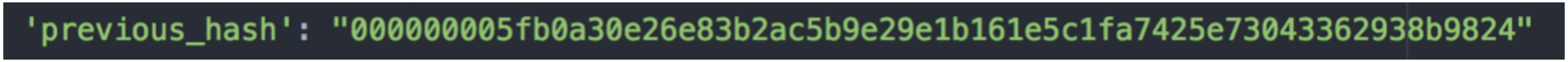


```
'proof': 324984774000,
```

WHAT IS A BLOCK?

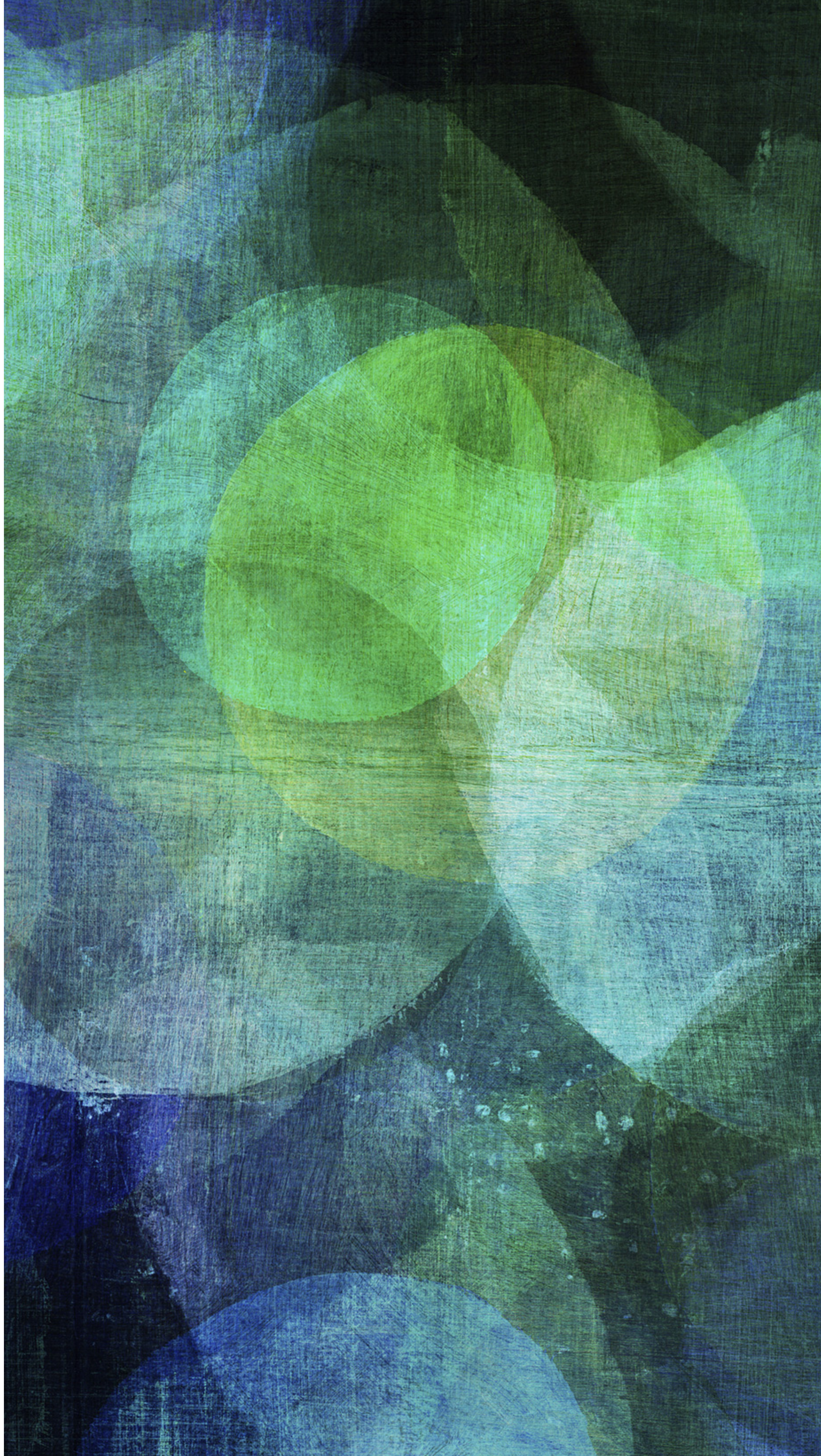
INDEX TIMESTAMP TRANSACTIONS PROOF PREV-HASH

- A block will always need to carry over the hash from the previous block.
  - This is for verification purposes and means the chain can be verified by checking all of the previous hashes in the chain (more on this process later).



```
'previous_hash': "000000005fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824"
```

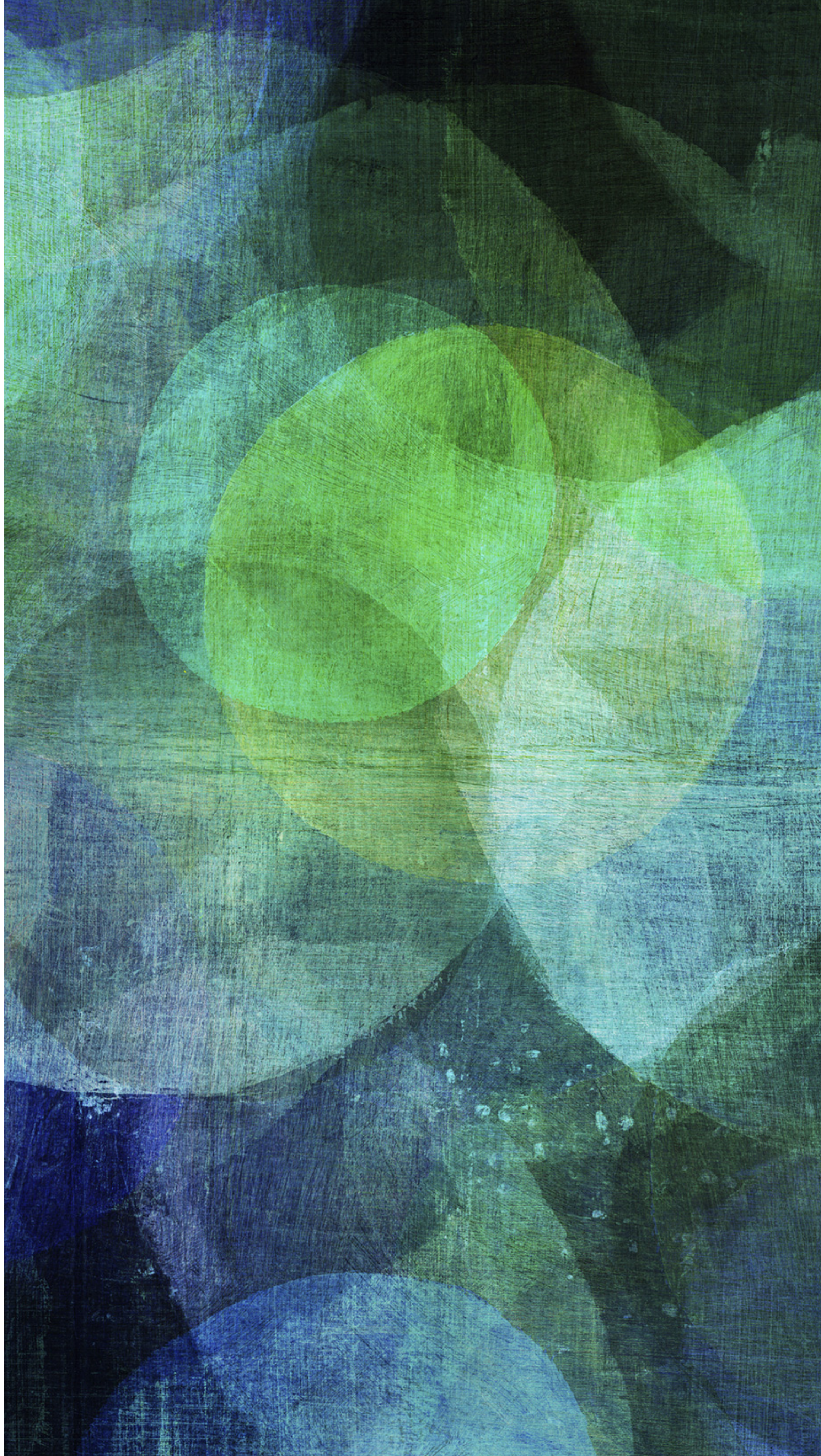
WHAT ARE THESE HASH THINGS YOU KEEP TALKING ABOUT?



WHAT IS A HASH

- A Hash is the value returned after using a hashing algorithm on a string. A hashing algorithm takes a string of any size and maps it to a string of a fixed length.
  - It is a way to encrypt data, and is only one way. Meaning that you cannot determine the input from the outputted hash.
  - Each time the same string is entered you will get the same outputted hash.
  - To check if the hash is correct you would need to pass in the same string as before, to get the same hashed result.
  - String in => String out
    - e.g. "Password" => 009bc8d6ef86eb3ad2800c715c0….

SO HOW DOES A BLOCK-CHAIN WORK?



WHAT IS A BLOCKCHAIN?

CREATING A NEW TRANSACTION

- To create a new transaction the Sender, Recipient and Data must be submitted to the Blockchain.
- This requested is stored as a pending transaction.
- A Miner will take a collection of pending transactions and check their validity.
- If a block passes the validation checks it will be added as a new block in the chain.

WHAT IS A BLOCKCHAIN?

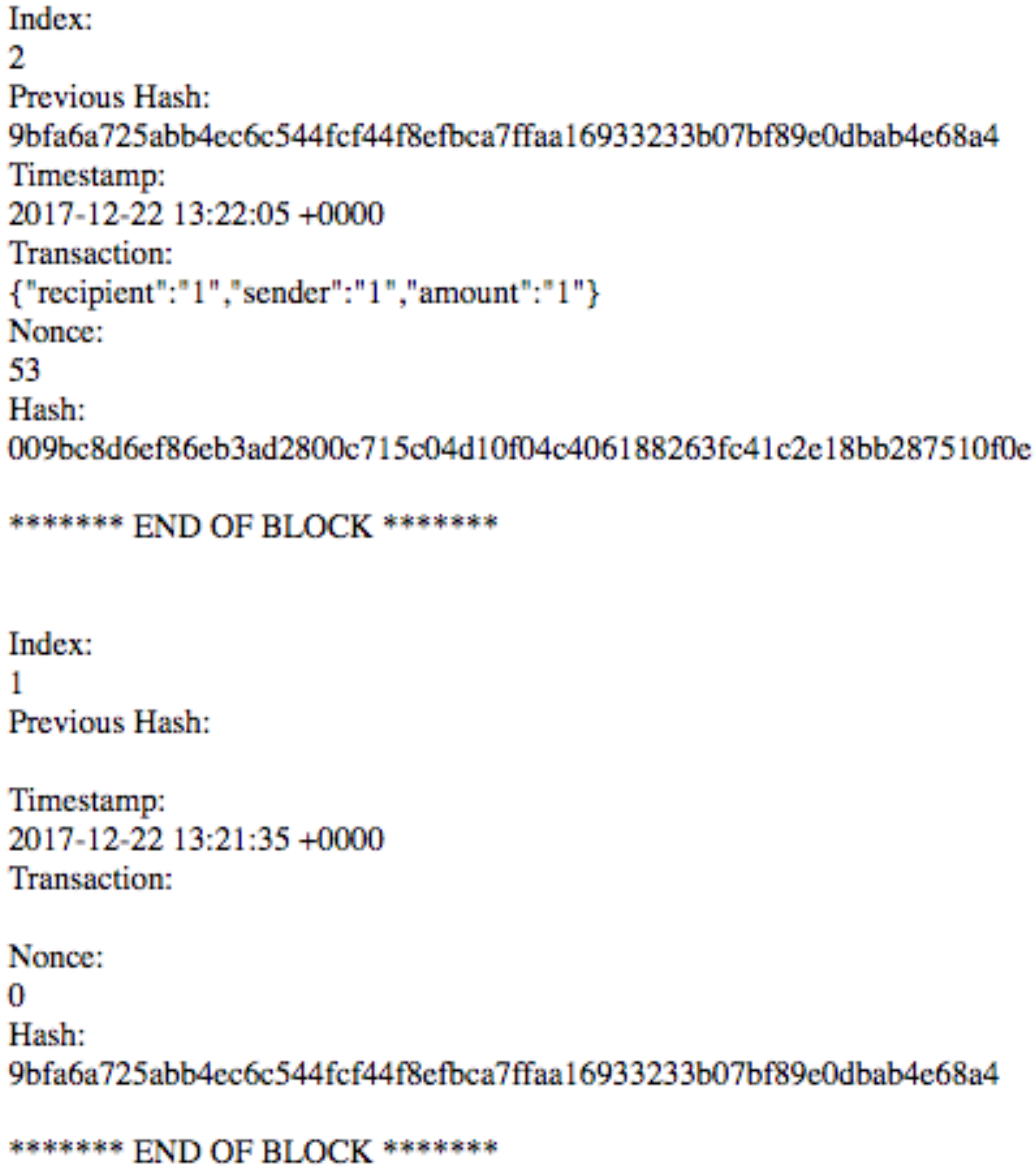
MINING - PERFORMING VALIDATION CHECKS

- A Miner is a single CPU on the network, who volunteers to perform all the validation checks. They will usually be rewarded for this.
- How does the miner determine if a block is valid?
  - There is an inbuilt difficulty level in the blockchain. This determines how many 0's need to be at the beginning of the hash.
  - One of the miner's roles is to find this hash.

WHAT IS A BLOCKCHAIN?

MINING – PERFORMING VALIDATION CHECKS

- This is done by finding the new Proof-of-Work. As mentioned before this is a counter, and is found by adding (through string interpolation) the previous hash to the Proof-of-Work and hashing the result.
- If this result does not have the required number of 0’s. The POW is incremented by 1



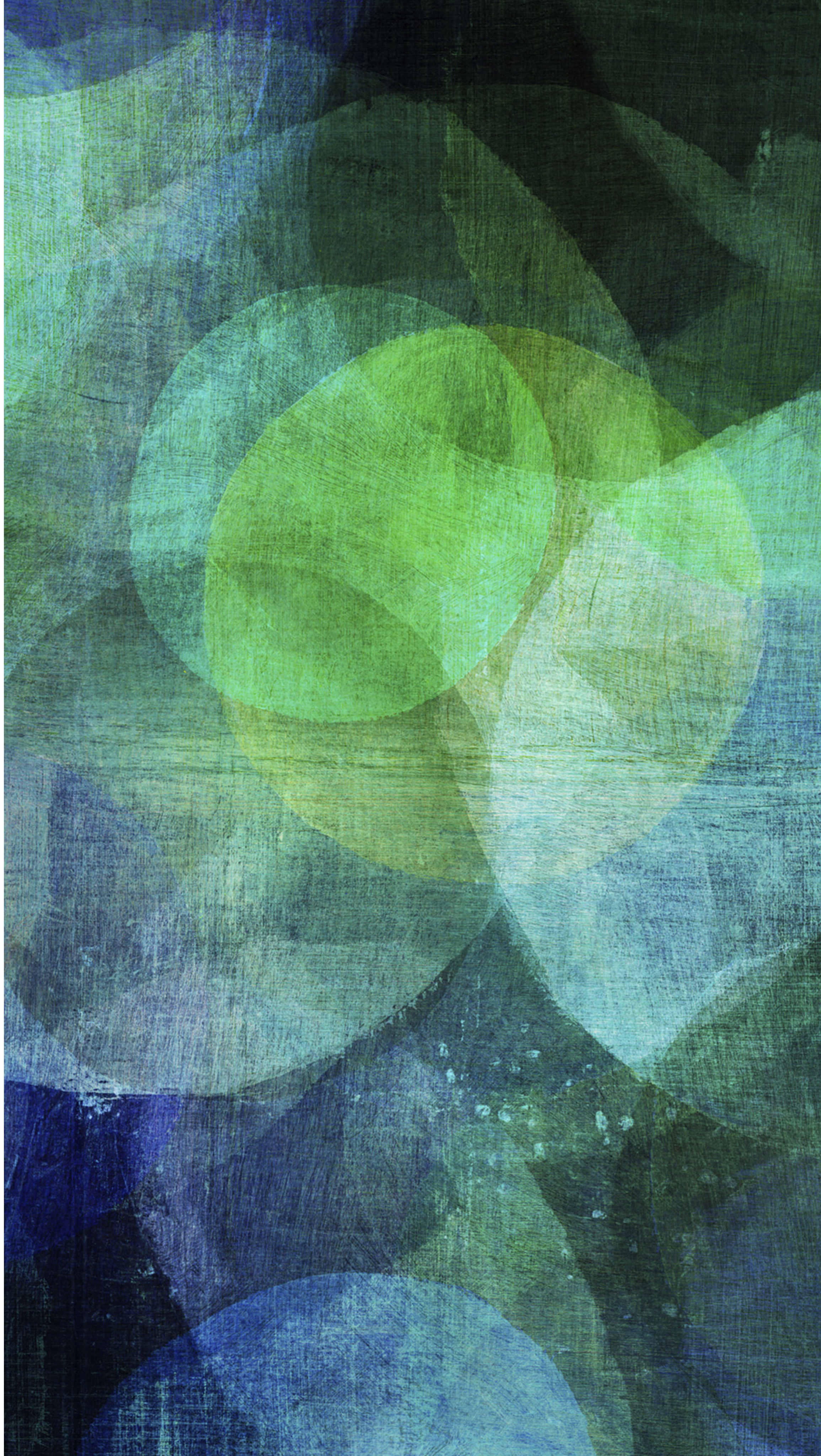
```
Index:
2
Previous Hash:
9bfa6a725abb4ec6c544fcf44f8efbca7ffaa16933233b07bf89e0dbab4e68a4
Timestamp:
2017-12-22 13:22:05 +0000
Transaction:
{"recipient":"1","sender":"1","amount":"1"}
Nonce:
53
Hash:
009bc8d6ef86eb3ad2800c715c04d10f04c406188263fc41c2e18bb287510f0e

******* END OF BLOCK *******


Index:
1
Previous Hash:

Timestamp:
2017-12-22 13:21:35 +0000
Transaction:

Nonce:
0
Hash:
9bfa6a725abb4ec6c544fcf44f8efbca7ffaa16933233b07bf89e0dbab4e68a4

******* END OF BLOCK *******
```

WHAT IS A BLOCKCHAIN?

MINING - PERFORMING VALIDATION CHECKS

- Other validations:
  - Checking the all previous blocks in the chain and making sure the hash is correct when hashing the previous hash and proof of work.
  - Checking that they have the latest version of the chain. This is done by searching all the connected nodes and checking if they have a longer blockchain.

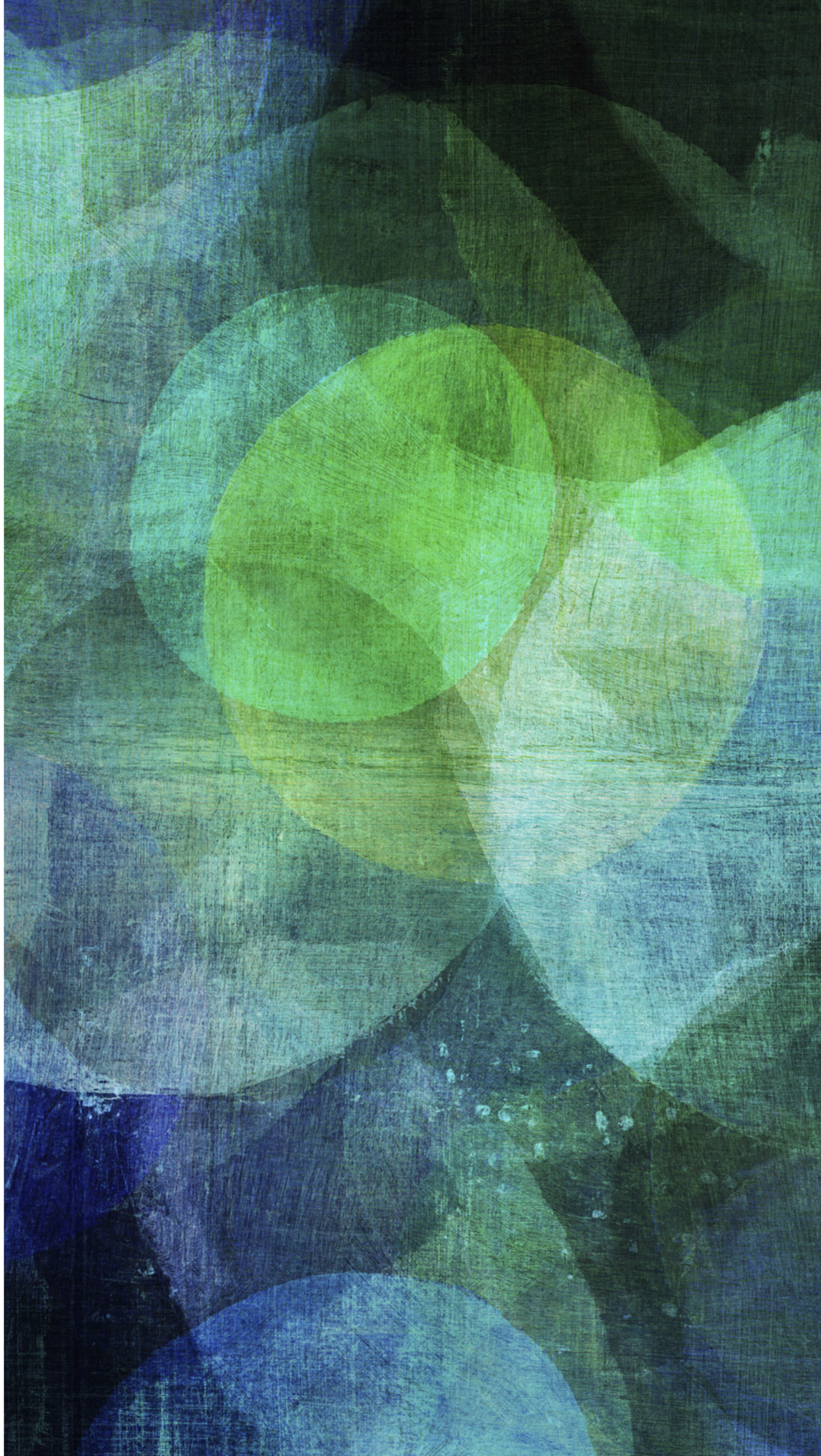
WHAT MAKES A BLOCKCHAIN SECURE



WHAT MAKES A BLOCKCHAIN SECURE

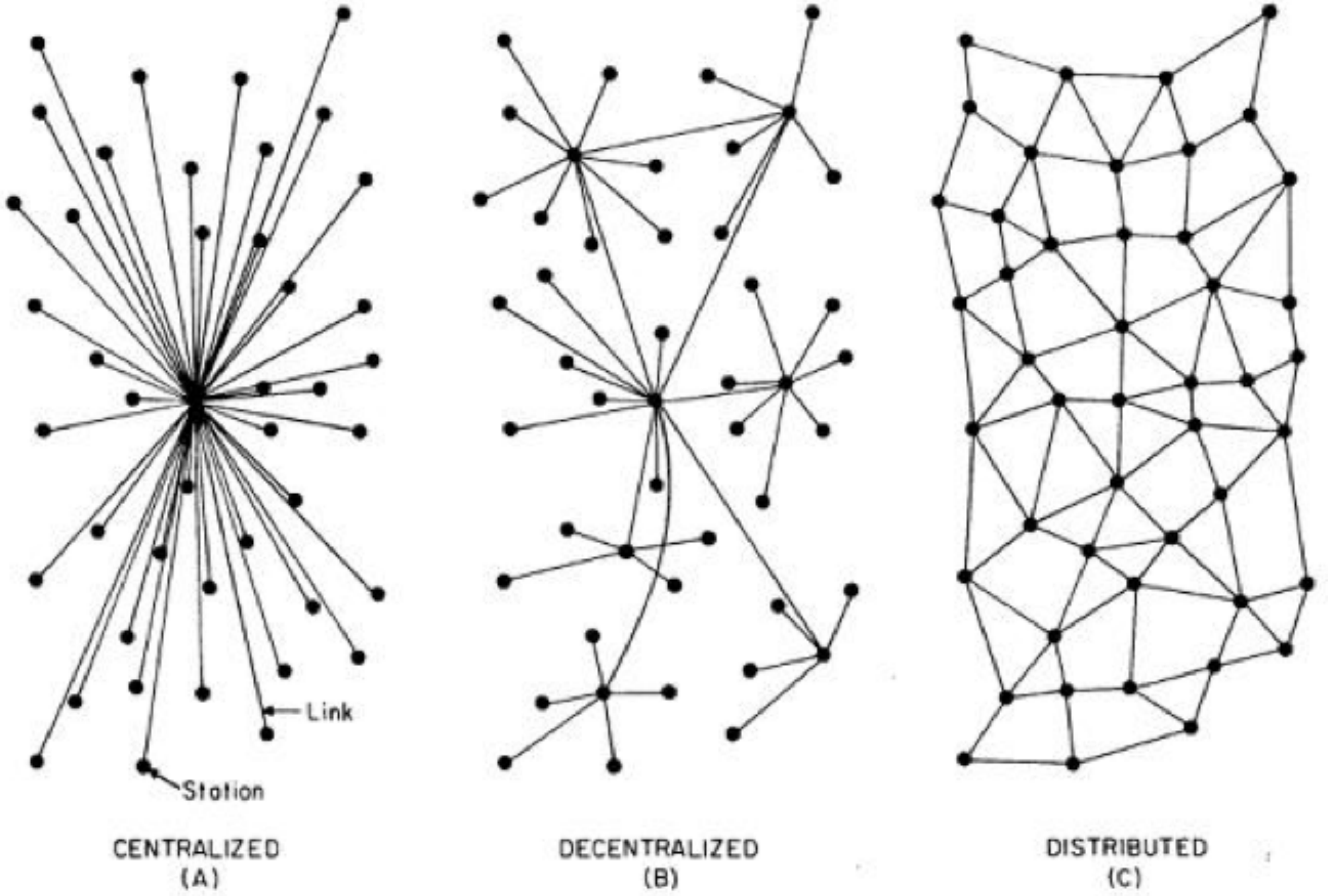
- The validation checks performed by the miners.
- To edit or corrupt the chain you would need 50% of the CPU of the entire network. The majority of the network has to agree on the current longest chain (longest in terms of Proof, not blocks).
- To manipulate the chain, you would have to redo all the previous proofs from the point on manipulation. The playing catchup with the current chain, trying to surpass it.
- The CPU cost of the above process is very high. A miner benefits more from being an honest node, then trying to manipulate the system.

NEXT STEPS?



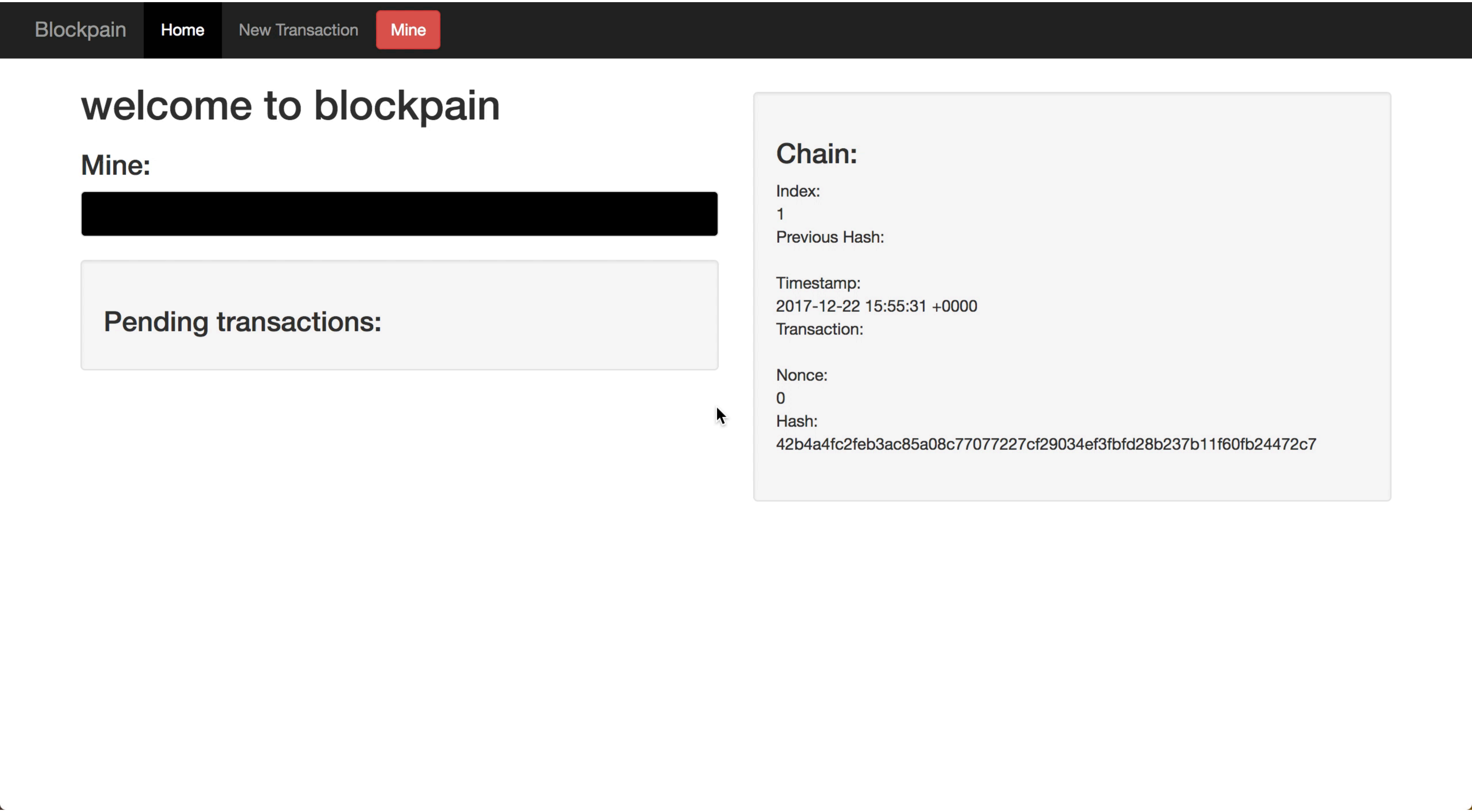
WHAT'S NEXT?

- Distributed Networks



WHAT'S NEXT?

- Voting application?
- Payment system?
- Mine racers?



welcome to blockpain

Mine:

Pending transactions:

Chain:

Index:
1
Previous Hash:

Timestamp:
2017-12-22 15:55:31 +0000
Transaction:

Nonce:
0
Hash:
42b4a4fc2feb3ac85a08c77077227cf29034ef3fbfd28b237b11f60fb24472c7