

Tuňákium

Aneb Bitcoin je moc mainstream





What is the Blockchain?



Tuñ

- Ne
- Ne
- Ale

```
import rsa

Transaction = namedtuple("Transaction", ["sender", "recipient", "signature", "amount"])

class Block(namedtuple("Block", ["prev_hash", "data", "proof"])):
    @property
    def hash(self):
        return sha256(self.serialize().encode()).hexdigest()

    def serialize(self):
        return json.dumps({
            "prev_hash": self.prev_hash,
            "data": self.data,
            "proof": self.proof,
        }, sort_keys=True)

class Client:
    def __init__(self):
        self.chain = [Block(0, [], 42)]
        self.ongoing_transactions = []
        self.address = str(uuid4())
        self.privkey, self.pubkey = rsa.newkeys(1024)
        self.app = tornado.web.Application([
            (r"/", self.get_handler()),
        ])

    def run(self):
        self.app.listen(4242)
        tornado.ioloop.IOLoop.current().start()

    def new_block(self, proof):
        self.chain.append(Block(self.chain[-1].hash, self.ongoing_transactions, proof))
        self.ongoing_transactions = []

    def send_transaction(self, recipient, amount):
        self._transaction(self.address, recipient, amount)

    def _transaction(self, sender, recipient, amount):
        sig = rsa.encrypt(struct.pack("!36s36sd", sender.encode(), recipient.encode(), amount), self.privkey)
```

42

#42