Pigeon

If you are using a computer, you are dumb, I'm dumb too so I am now proposing a decentralized payment system with pigeons.

How does it work?

P2P Networking

In a p2p network, as the name suggests, peers connect and communicate with each other directly, not through a third-party provider.

With pigeons, we can send messages by sticking a letter to a pigeon, sending that pigeon to another person and they can send it/another pigeon back.

This is our base for a decentralized, p2p network, now let's add some spicy spiced spice to make it a payment system.

Transactions

Transactions will be hand-written on the paper, it will contain:

- Sender's address.
- Recipient's address.
- Amount to be sent.
- Some random nonce value.
- A cryptographic signature.

Note that "signature" is probably a random, nonsense sequence of characters, not a human signature.

To prevent people from using others' accounts, Bitcoin had this system implemented: You will generate a cryptographic key pair with one key called "private key" used for creating a cryptographic signature and one called "public key", which is used as your address and also to verify the signature.

To prevent people from basically copying and pasting transaction letters, you would want to add in a nonce, which can help generate randomized signatures. Used nonces will not be used in the future.

The main difference with other network's transactions is that it is written by hand, yes.

Blocks

Blocks are stuff that is written as a list containing:

- Block creation timestamp.
- A list of transactions.
- Cryptographic hash of the previous block.

- Cryptographic hash generated from the provided information.

Blocks help keep the data immutable throughout history because one slight change to one block makes the next block's hash change, it is easy to recognize the difference.

Timestamps also record the history of the network which is neat.

Just like transactions, blocks should also be hand-written.

Consensus

We would need a way to keep all individuals agreed on a single blockchain, because there should only be one correct list of balances.

Just like Bitcoin, Pigeon also uses proof-of-work to handle this.

Basically, in a block, you add another property which is a nonce. You increment that nonce until the hash starts with an amount of zeros.

To make this a bit fairer and less computer-involved, you are not just going to provide nonce as proof, but also write down all steps to achieve this nonce, plus a picture of a pigeon. If the proof is not hand-written, the block is discarded.

A guy who got the proof first will receive a large amount of coins as a reward. This should make participants in the network want to be good guys rather than dirty attackers. (Unless they just catch your pigeon and sell it, which is unlikely if your currency worth more, yes).

The network

People can broadcast transactions using pigeons to others, they will then take the received letter, verify the transactions, add it to the block once they are all verified, write down the proof, pack it into the pigeons and send them away to other peeps.

Gas fee

Unlike Bitcoin, you simply don't need gas fees, nada, not at all, because a pigeon already costs like, 300 dollars?

Conclusion

Pigeons are cute.