

DECENTRALIZED TEST OF LIVENESS

September 9, 2022

INTRODUCTION

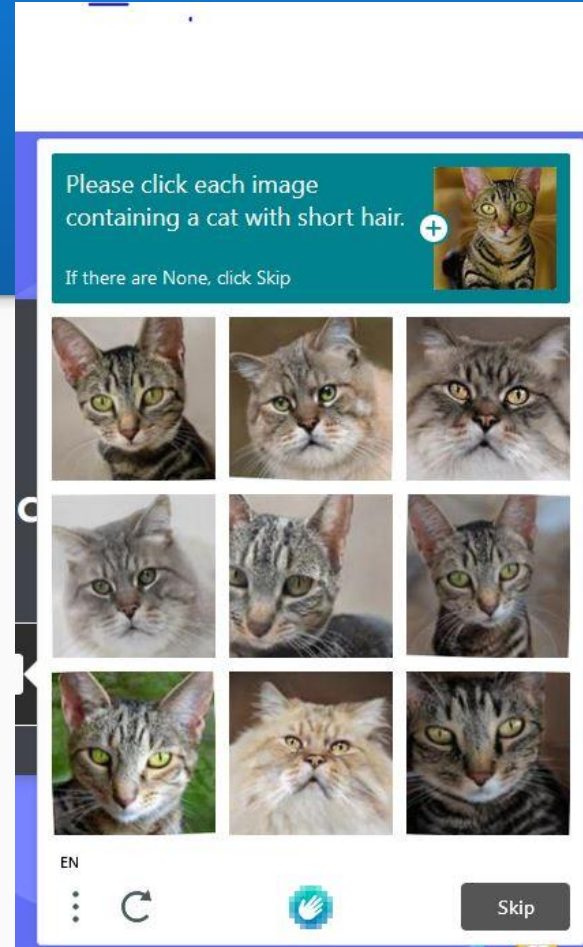
[LEDGER]

- French Unicorn founded in 2014
- The Nano S/X
- A general misconception that the tokens are on the device itself



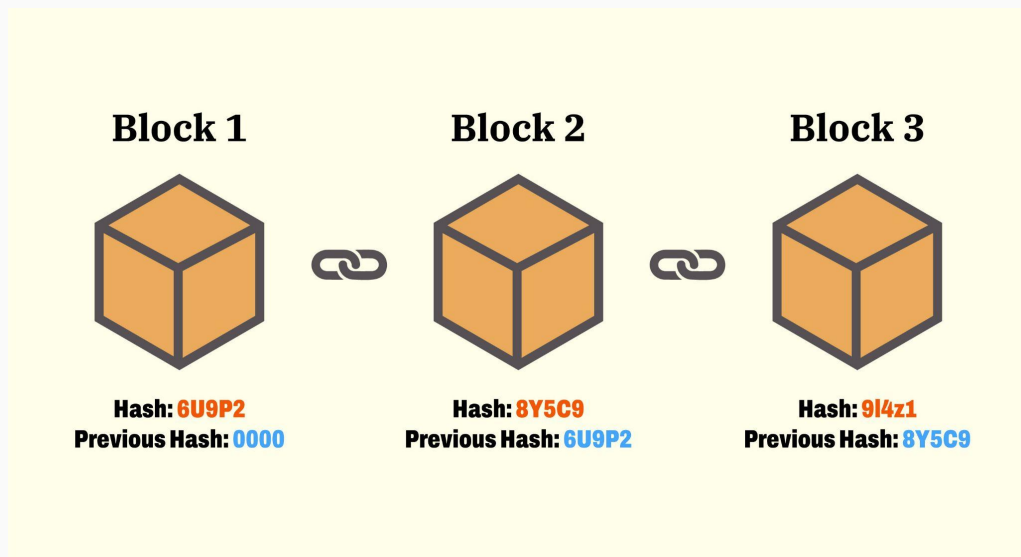
BOT DETECTION

- Know Your Customer(KYC)
- Bot detection
- Use Case: User authentication, Anti spam...
- Exemple : hCAPTCHA



DECENTRALIZATION

- Blockchain, hash functions, Digital signatures
- Bitcoin, Ethereum
- Smart Contracts
- L2's, STARKNET, Cairo language



STATE OF THE ART

WEB2

- Google's reCAPTCHA v2, v3, hCAPTCHA...
- Advantages, Disadvantages
- Human captcha solving farms

WEB3

- Proof Of Humanity protocol
- Advantages, Disadvantages
- AI on chain: Guilty Gyoza

CONTRIBUTIONS

OBJECTIVES

- **Open Sourcedness:** The algorithm and the test by its nature must be able to not rely on its secrecy as means for security. Even at the cost of some potential vulnerabilities.
- **Decentralization:** Use the features of the blockchain to make the test more robust(No point of failure), and personalized (Save the address that passed the test)
- Learn the **Cairo** language and to deploy smart contracts on **STARKNET**, as it has a lot of potential in the future.
- Make research in the field of **Human Machine Interactions** and ML in order to make a test that is more friendly to the human and less to the machine.

CENTRALIZED VERSION

4	9	9	0	7
8	3	1	6	8
4	1	5	9	7
6	2	5	4	5
4	6	4	2	7

4	5	7	3	9
7	2	5	5	0
3	3	9	5	0
7	1	4	0	6
3	8	9	1	9

Test of Liveness: Steps

Activities Google Chrome août 29 15:28

cairofication_CNN.ipynb Manual_CNN.ipynb - Colab Honest Test of Humanity x +


http://127.0.0.1:5000

Apps ledger.fr bookmarks pcalic-ledger Google Docs Welcome To C... Learn web dev... 5. Testing con... Introduction t... Solidity — Soli... The Art of Ro...

Test of Liveness

You have X seconds to select a picture of:

- The Number: 3



Press the button to confirm your choice:

Click Coordinates:

Test of Liveness: Steps

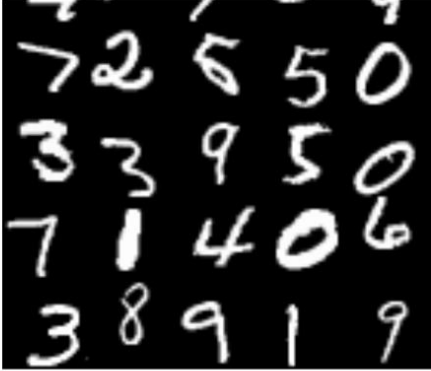
Activities Google Chrome aout 29 15:30

cairofication_CNN.ipynb - x Manual_CNN.ipynb - Colab x Honest Test of Humanity x +

http://127.0.0.1:5000


Apps ledger.fr bookmarks pcalic-ledger Google Docs Welcome To C... Learn web dev... 5. Testing con... Introduction t... Solidity—Soli... The Art of Ro...

Update



Press the button to confirm your choice:

Click Coordinates: (214.5, 292)



Upload answer

Answer:

The code of this test is open source, it's in this [Repository](#).

Test of Liveness: Steps

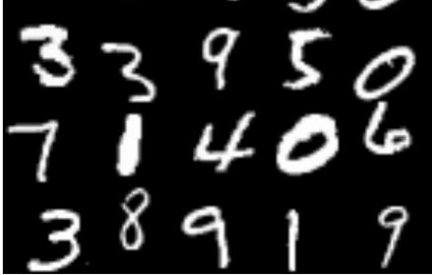
Activities Google Chrome août 29 15:33

cairofication_CNN.ipynb x Manual_CNN.ipynb - Colab x Honest Test of Humanity x +

http://127.0.0.1:5000


Apps ledger.fr bookmarks pcalic-ledger Google Docs Welcome To C... Learn web dev... 5. Testing con... Introduction t... Solidity — Soli... The Art of Ro...

Update



Press the button to confirm your choice:

Click Coordinates: (57.5, 378)



Upload answer

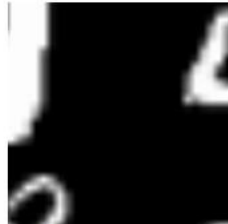
Answer: true

The code of this test is open source, it's in this [Repository](#).

Test of Liveness: Steps

Press the button to confirm your choice:

Click Coordinates: (162.5, 313.5)

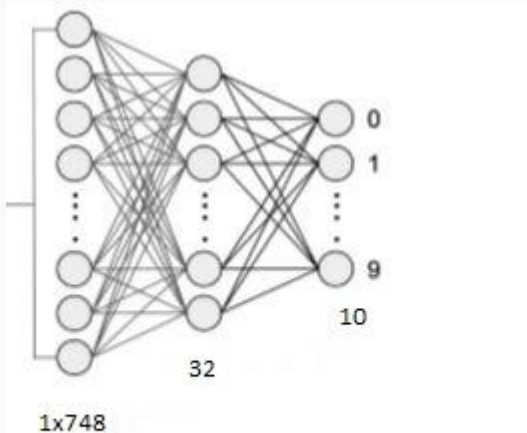


Upload answer

Answer: false

DECENTRALIZATION

- The simple neural network used by Gyoza won't suffice.

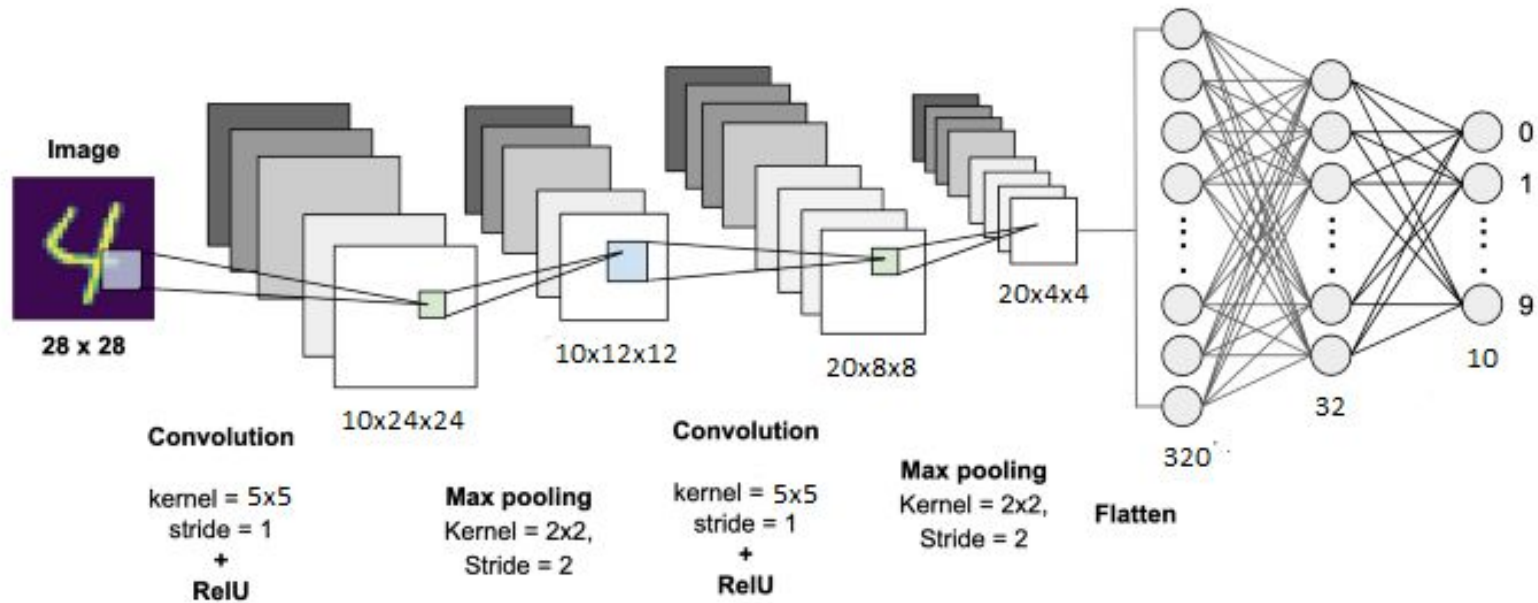


- We have to implement a CNN from scratch (Without the backpropagation)

Translation during training	Translation during test	Classification on test sample
0	0.3	22%
0.2	0	96%
0.1	0.3	40%
0.2	0.3	70%
0.2	0.2	83%

Table 5.1: MLP classification results in function of the translation amount

CNN vs MLP



CNN Architecture Implemented in python: 98% classification performance.

Conv. layers	filters	filter size	fully connected layers	epochs	classif.	parameters
2	8	5	1 fc 128 neurons	7	95%	3106
2	6	5	1 fc 96 neurons	14	94%	2032
1	6	5	1 fc 864 neurons	14	93%	8806
1	6	5	2 fc 864+50 neurons	10	95%	43916
1	7	5	1 fc 1008 neurons	20	94%	10272
2	5	5	1 fc 80 neurons	14	93%	1570
2	6	7	1 fc 24 neurons	13	91%	2320

Table 5.2: CNN architecture and number of parameters

- On Starknet, computation is cheap and memory is expensive

Conclusion

ROADMAP:

