Hashtone: Developing Novel Information Interaction and Transmission Experiences Through Sound and Color

https://github.com/ssocolow/hashtone

ENGINEERING PURPOSE

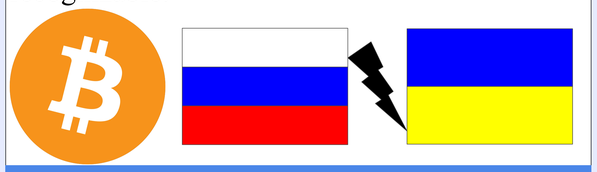
This project aims to:

- Improve cryptocurrency address verification by developing a specification to fingerprint digital information using sound and color.
- Expand on previous methods of digital information transmission by developing a specification to transmit data through sound.
- Design a mechanism to secure the state of one blockchain on another blockchain.

Constraints: the implementations will work on web browsers to increase accessibility.

RELEVANCE

This project has relevance in light of current world events such as economic sanctions imposed on Russia because of the war in Ukraine. For example, this project could help make Russia's large bitcoin addresses more recognizable.



INTRODUCTION

As more of our lives involve the internet and computers, the ways in which we interact with digital information become increasingly important.

New methods of transmitting value, including cryptocurrencies like Bitcoin [1], increase the need for alternative methods of security. Sending bitcoins to the wrong address, for example, can lose the bitcoins forever.

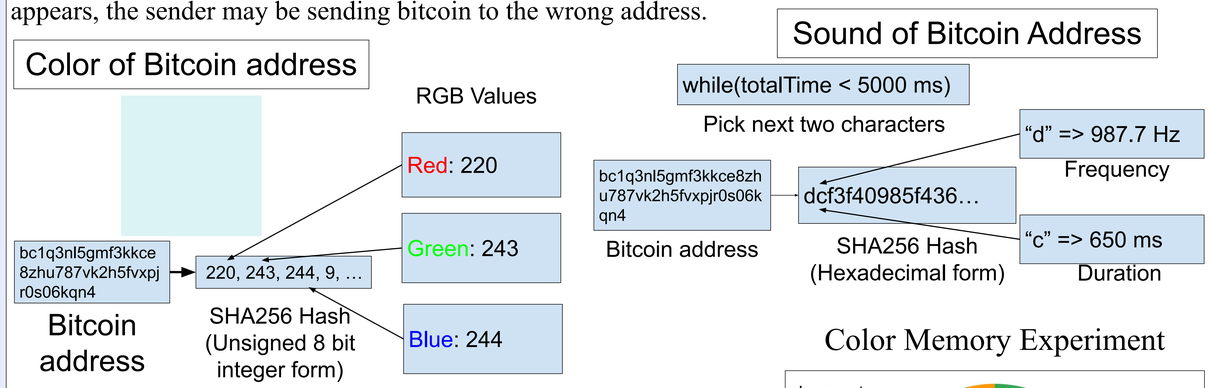
Methods of safeguarding the user exist, such as the checksum feature [2], but this is an area of research ripe for innovation.

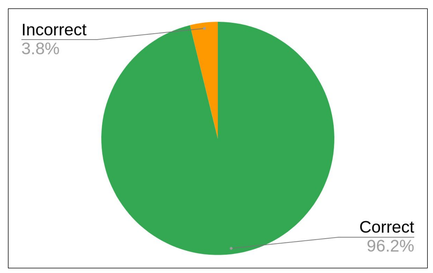
Studies have shown that color is a powerful way to improve human memory performance [4].

SPECIFICATIONS AND IMPLEMENTATIONS

Specifications were designed and implemented to address the goals of this project. These specifications lay the foundation for implementation and wider adoption of these ideas. All code is open source.

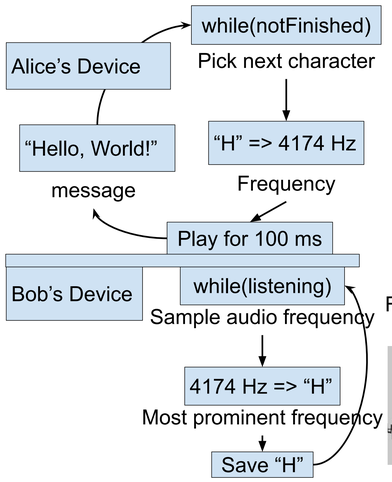
The Hashtone specification describes how to take any amount of digital information (here using a bitcoin address as an example) and deterministically assign it a color and short musical sound using the SHA-256 hash function [3,6]. A sender would remember the receiver's bitcoin address as a certain color. When the sender enters the receiver's address into their wallet software, the same color should appear. If a different color appears, the sender may be sending bitcoin to the wrong address.





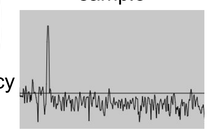
To test human color memory performance, an experiment was conducted. All participants were shown one color. Twenty minutes later the participants were shown either the original color or a different color (random assignment). Participants responded to the question: "Is this the color I originally showed you?" to simulate verifying a bitcoin address's color. This process was then repeated forty minutes later, one hour later, and four days later. With n=26, p=1.26·10^(-6), we have evidence that humans have a strong memory of colors.

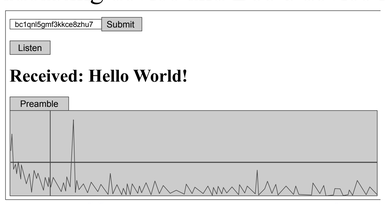
Sending Data Through Sound -- Audio QR Code -- No Need for Internet To Send Information



The Tonemap specification describes how to send and receive digital information using sound (here using the string "Hello World!" as an example). The broadcasting device encodes the message into specific frequencies over time and uses its speakers to transmit the information. The receiving device listens with its microphone and records the frequencies sent by the broadcasting device. Then it decodes those frequencies over time to recover the message. In this example Alice's device is the broadcasting device and Bob's device is the receiving device.

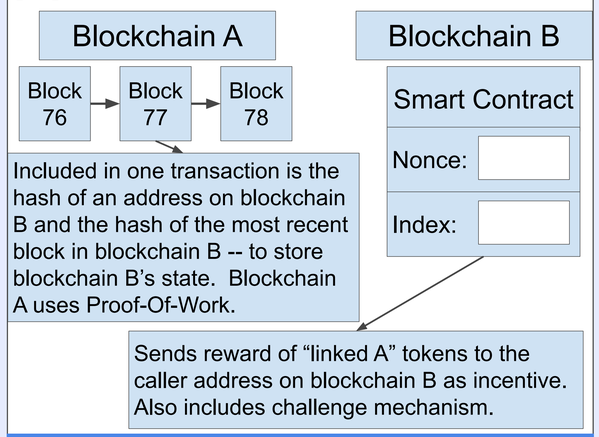
Frequency spectrum sample





https://ssocolow.github.io/hashtone/tonemap/

During this research, a method to link decentralized trustless blockchains was explored and developed. This method leverages the work of one blockchain (A) to record and protect the state of another blockchain (B). An incentive mechanism is proposed in the form of tokens on blockchain B.



CONCLUSIONS

These specifications have applications in the rising space of cryptocurrency transactions and low-infrastructure many-user digital communications. This research expands the human-computer interface and improves the verification, transmission, and protection of digital information.

FUTURE WORK

The Hashtone specification can be made into a Bitcoin Improvement Proposal (BIP) and submitted to the community for comment, improvement, and adoption.

REFERENCES

[1] Bitcoin.Org, 2022, https://bitcoin.org/bitcoin.pdf. Accessed 3 Feb 2022.

[2] "BIP 0173 - Bitcoin Wiki". En.Bitcoin.It, 2022, https://en.bitcoin.it/wiki/BIP_0173. Accessed 3 Feb 2022.

[3] "FIPS 180-4: Secure Hash Standard (SHS)". National Institute of Standards and Technology, 2015, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf. Accessed 3 Feb 2022.

[4] Mariam Adawiah Dzulkifli, Muhammad Faiz Mustafar. "The Influence Of Colour On Memory Performance: A Review". The Malaysian Journal Of Medical Sciences : MJMS, vol 20, no. 2, 2013, p. 3., https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3743993/. Accessed 3 Feb 2022.

[5] "Github - Quiet/Quiet: Transmit Data With Sound. Github, 2022, https://github.com/quiet/quiet . Accessed 3 Feb 2022.

[6] "Crypto.Subtle - Web Apis | MDN". Developer.Mozilla.Org, 2021,

[7] "Reference | P5.Js". P5js.Org, 2022, https://p5js.org/reference/#/libraries/p5.sound. Accessed 3 Feb 2022.

ALICE's Computer

while(notFinished)

Pick next character

"Hello, World!"

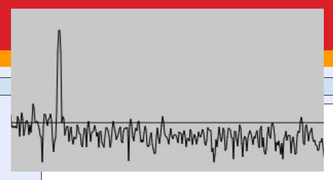
message

"H" => 4174 Hz

Frequency

Play for 300 ms

Frequency spectrum sample



Bob's Computer

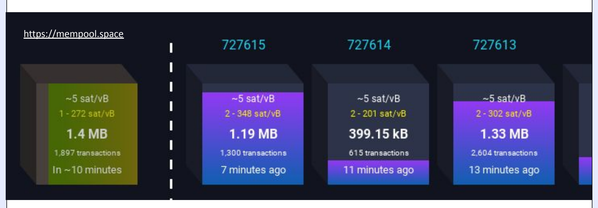
while(listening)

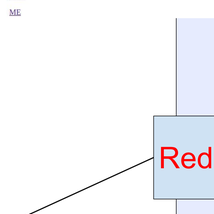
Sample audio frequency

4174 Hz => "H"

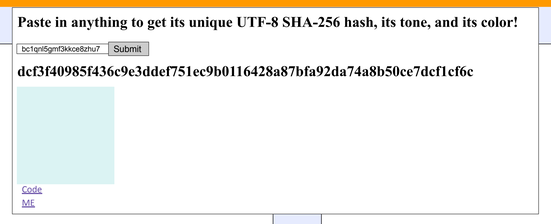
Most prominent frequency

Save "H"





https://ssocolow.github.io/hashtone/



bc1q3nl5gmf3kkce8zhu787vk2h5fvxpjr0s06kqn4

Bitcoin address

220, 243, 244, 9…

SHA256 Hash (Unsigned 8 bit integer form)

Red: 220

Green: 243

Blue: 244

RGB Values

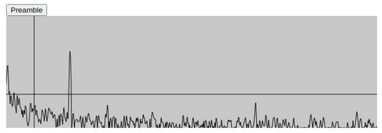
Color of Bitcoin address

Listen

Recieved:

https://ssocolow.github.io/hashtone/tonemap/

Preamble

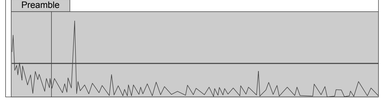


bc1qnl5gmf3kkce8zhu7 Submit

Listen

Received: Hello World!

Preamble



while(totalTime < 5000 m

Pick next two characters

bc1q3nl5gmf3kkce8zhu787vk2h5fvxpjr0s06kqn4

Bitcoin address

dcf3f40985f436…

SHA256 Hash (Hexadecimal form)

"d" => 987.7 H

Frequency

"c" => 650 ms

Duration