



# *A HASH-CASH BASED MUSIC STREAMING PAYMENT SYSTEM*

Timothy Chen  
San Jose State University  
Fall 2014

# AGENDA

- Introduction
- Background
- Features implemented
- Issues Encountered During Testing
- Conclusion

# INTRODUCTION

- There are many popular music streaming services
  - Pandora
  - Spotify
- Many of these pay using a royalty system
  - Artist paid by number of streams
- My project is to create a new payment service based on a crypto currency like set-up

# MY PROJECT DESIGN

- I built
  - A web front end
    - Upload music in MP3 format
    - Play music
    - A ranking tool
    - Verify crypto-coin tool
  - A back end
    - Uses artist's name, content of music, timestamp, music listener's IP address as seed in a hash cash SHA256 function for artist to earn the new crypto-currency
    - Mining process is run in parallel while music is playing

# BACKGROUND

- ASCAP
  - American Society of Composers, Authors, and Publishers
  - Protects its members' rights by licensing, distributing royalties, and copyright for the music publicly
- Payola
  - The illegal paying of cash or gifts in exchange for airplay
- Streaming music websites
  - Pandora
  - Spotify
- Bitcoin
- SHA256

# BACKGROUND

## ○ Distribution of Royalty System for Spotify



# ROYALTY SYSTEM ISSUES

## MUSIC STREAMING PRICE INDEX AS OF FEB 1, 2014

| Store         | Per Stream | Per Song Download |
|---------------|------------|-------------------|
| Nokia         | 0.07411    | 9                 |
| Google Play   | 0.04573    | 15                |
| Xbox Music    | 0.03212    | 22                |
| simfy         | 0.01626    | 43                |
| Napster       | 0.01578    | 44                |
| MediaNet      | 0.01140    | 61                |
| Rhapsody      | 0.01122    | 62                |
| Muve Music    | 0.00875    | 80                |
| Deezer        | 0.00754    | 93                |
| Rdio          | 0.00692    | 101               |
| Spotify       | 0.00521    | 134               |
| MySpace Music | 0.00094    | 745               |
| Amazon Cloud  | 0.00012    | 5,862             |

- \* Indie Label Catalog of 1,500 Songs
- \* Sales for Calendar Years 2012-2013
- \* These Streaming Rates before Dist Fee's
- \* Per Song Download Ratio @ .70

# MY SYSTEM VS SPOTIFY'S

|           | 100 user listen for 5 minutes  | Artist earns |
|-----------|--|--------------|
| My System | $\$1000 * (500 \text{ the artist own coins} / 1000 \text{ total coins}) * (\text{my cut } 10\%)$ | \$450        |
| Royalty   | $\$1000 * (100 \text{ streams} / 600 \text{ streams}) * (70\% \text{ website cut})$              | \$50         |



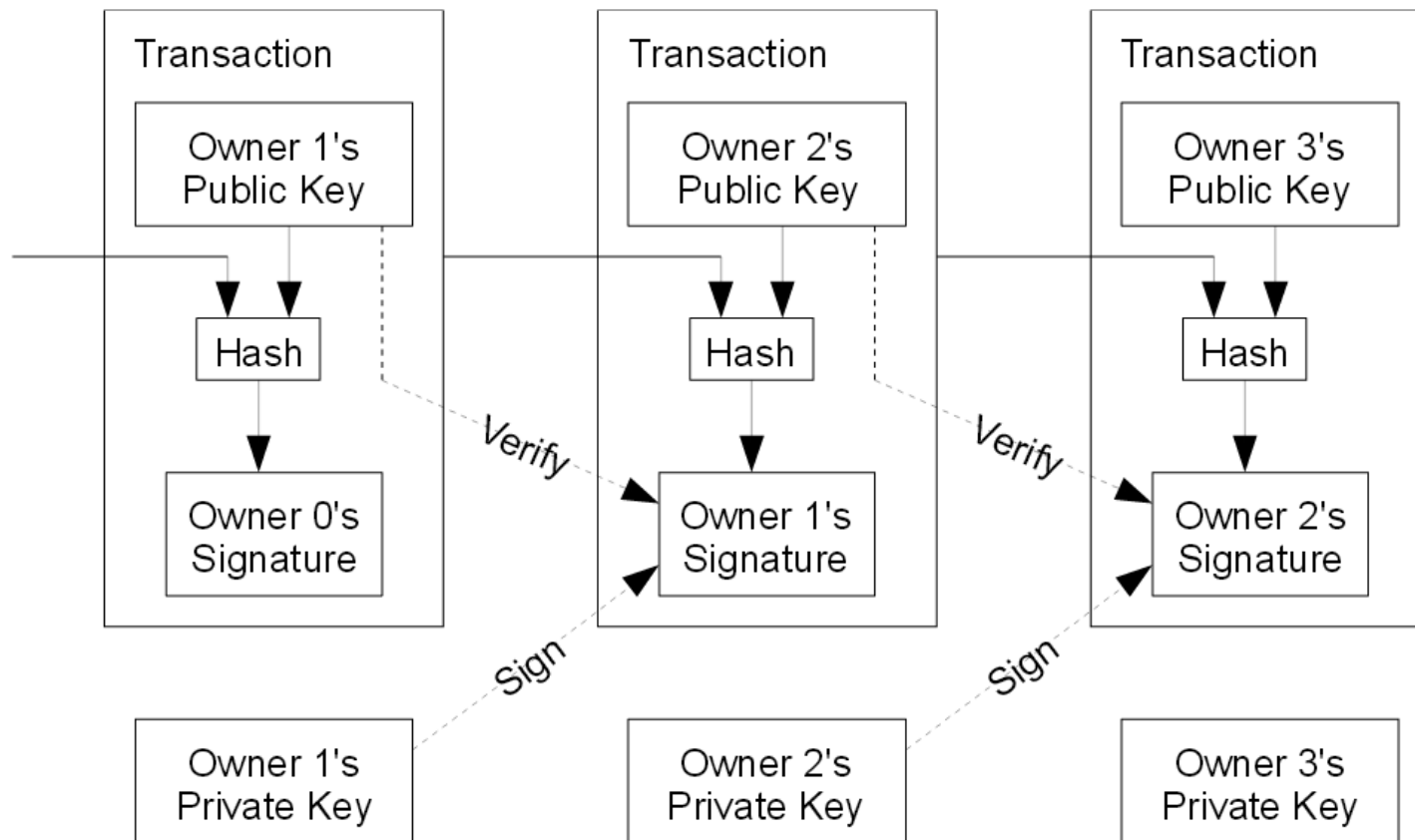
# BITCOIN

- Bitcoin uses peer-to-peer technology
- No central authority or banks
- Managing transactions and the issuing of bitcoins is carried out collectively by the network
- Bitcoin is open-source
- Its design is public
  - Nobody owns or controls Bitcoin and everyone can participate

# BITCOIN TRANSACTIONS

- Public key
  - Verify the signatures to check the chain of ownership
- Private key
  - Proves who is the owner of a bitcoin

# BITCOIN TRANSACTIONS



# TIMESTAMP SERVER

- Peer-to-peer
  - Lets everybody know a bitcoin's history
- Prevents the use of the same bitcoin twice
  - Keeps track of who is the owner of a bitcoin at a given time
- All transactions have to be public
  - Notification sent to bitcoin network when a transaction is completed

# INCENTIVE

- Earn bitcoins
  - Verify others' transactions
  - The number of leading zeros required is increasing to do verification
  - Number of people mining is increasing

# MINING REQUIREMENTS

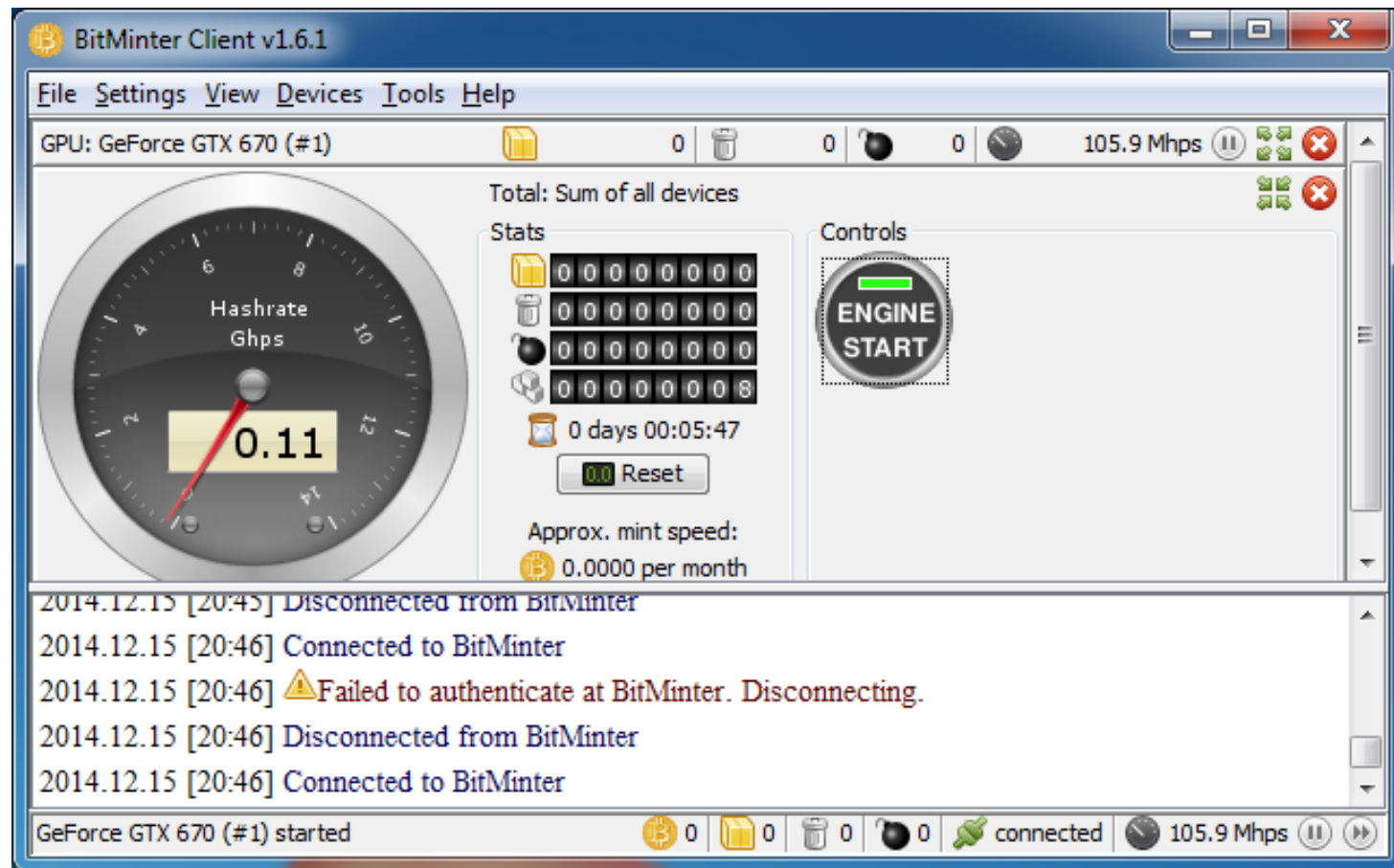
- CPU
- Graphics card
  - AMD (ATI)
  - Nvidia
- Mining Tool

^ . .

Bitcoin [double SHA256](#) ASIC mining hardware

| Product               | Advertised Mhash/s    | Mhash/J | Mhash/s/\$ | Watts              | Price                  | Currently shipping | Comm ports     | Dev-friendly  |
|-----------------------|-----------------------|---------|------------|--------------------|------------------------|--------------------|----------------|---------------|
| <b>AntMiner S1</b>    | 180,000               | 500     | 155        | 360                | \$1,160                | Yes                | Ethernet       | code, samples |
| <b>AntMiner U1</b>    | 1,600                 | 800     | 55         | 2                  | \$29                   | Yes                | USB            | code, samples |
| <b>Avalon ASIC #1</b> | 66,300 <sup>[1]</sup> | 107     | 52.34      | 620 <sup>[2]</sup> | \$1,299 <sup>[3]</sup> | Discontinued       | Ethernet, Wifi | code          |
| <b>Avalon ASIC #2</b> | 82,000 <sup>[3]</sup> | 117     | 54.70      | 700                | \$1,499 <sup>[3]</sup> | Discontinued       | Ethernet, Wifi | code          |
| <b>Avalon ASIC #3</b> | 82,000 <sup>[3]</sup> | 117     | 54.70      | 700                | \$1,499 <sup>[3]</sup> | Discontinued       | Ethernet, Wifi | code          |

# BITCOIN MINING



# MY BITCOIN ACCOUNT

- I got 0.00000875 bitcoin for one day
- Nvidia GTX 670

## Account Details for timchen623

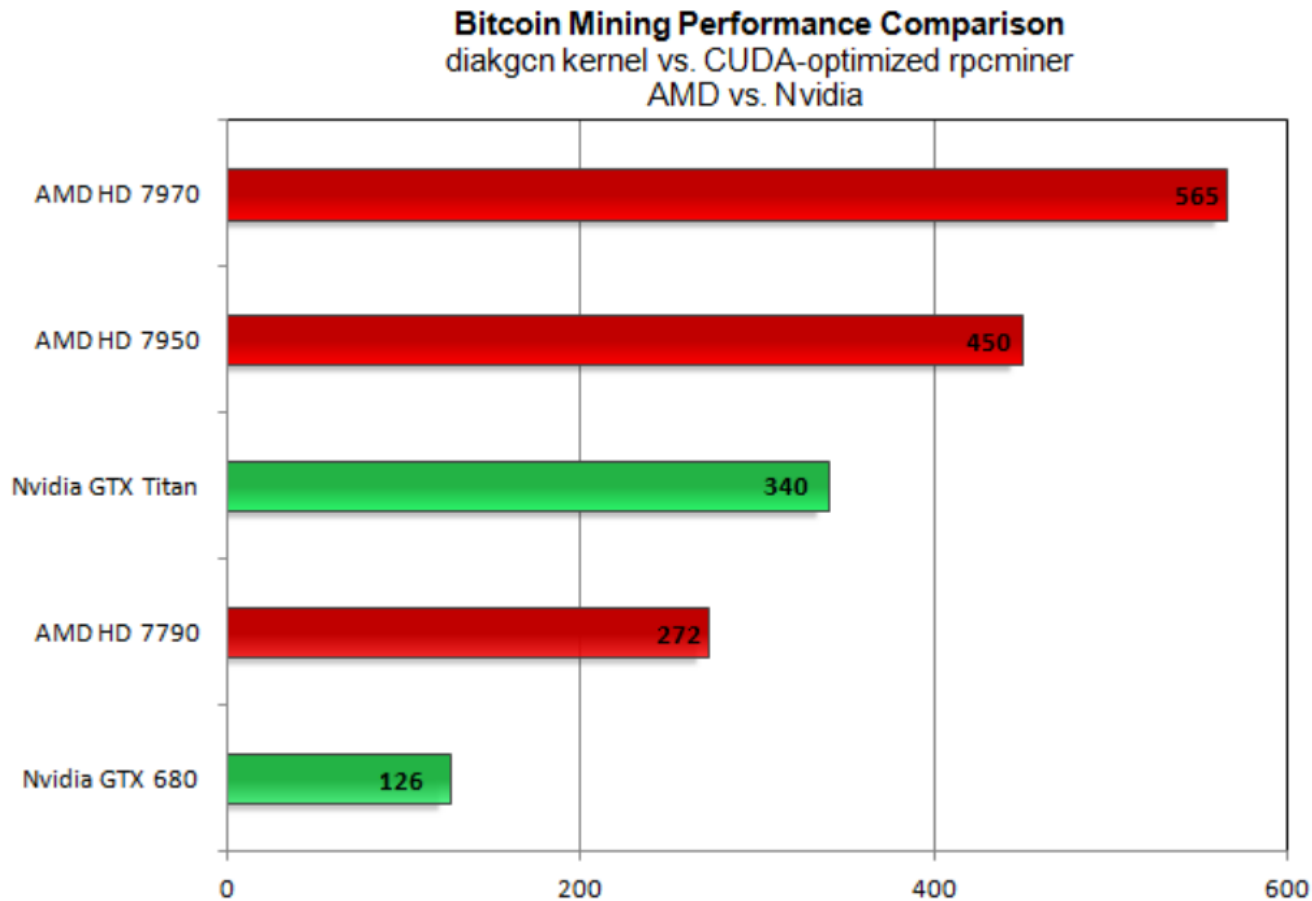
---

Unconfirmed income is added to your balance if and when [blocks](#) are confirmed. To improve your income per block, improve your score in the [shifts](#) eligible for payments by increasing your hash power.

| Personal Assets                  | Balance    | Unconfirmed | Future     | Expected per block |
|----------------------------------|------------|-------------|------------|--------------------|
| Bitcoins <a href="#">[send]</a>  | 0.00001243 | -           | 0.00001243 | 0.00000423         |
| Namecoins <a href="#">[send]</a> | 0.00002894 | -           | 0.00002894 | 0.00000846         |



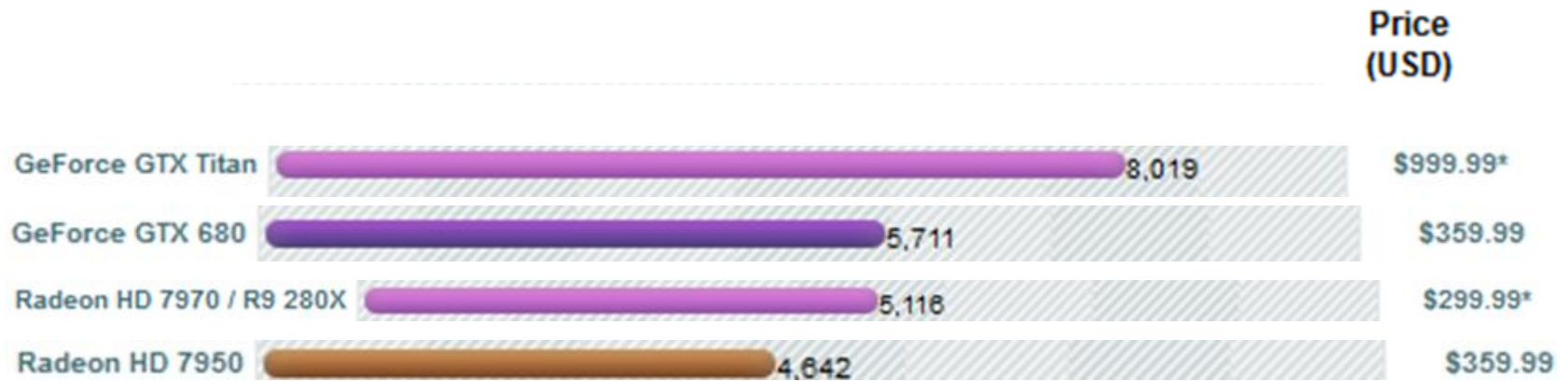
# MINING PERFORMANCE COMPARISON



Source: <http://www.ExtremeTech.com>

# PRICE COMPARSION

High End Videocards - Updated 11th of March 2014



# SHA256

- Hash function computed with 32-bit words
- One-way hashing method
  - Cannot be reversed to original value
- Implement version SHA256 both in JavaScript and WebGL

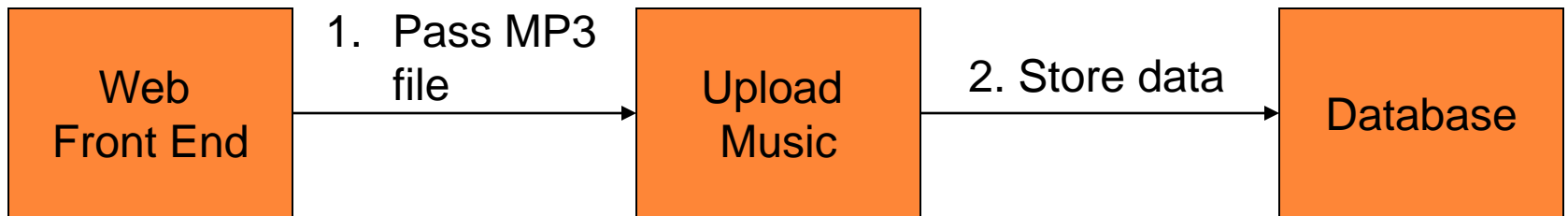
# FEATURES IMPLEMENTED IN THE MP3-BASED CURRENCY SYSTEM

- System to upload music
- Generate a hash string for each individual listening coin
- Use the SHA256 method to mine for listening coins
- System to save the coin after the artist receives it

## FEATURES IMPLEMENTED IN AN MP3-BASED CURRENCY SYSTEM

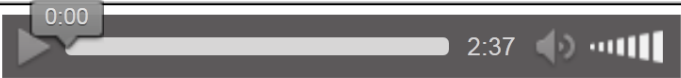







- Rank for who has the highest listening coin count for each month
- Verification check for each transaction

# UPLOAD THE MUSIC FLOWCHART



# UPLOAD THE MUSIC APPLICATION

[artist Rank verification coin tool](#)










| Music    | Player   | artist name |
|----------|--|-------------|
| 1450.mp3 |    | Tim         |
| 2537.mp3 |    | Tom         |
| 2555.mp3 |    | Larry       |
| 2558.mp3 |    | Jack        |
| 4038.mp3 |    | Tim         |
| 4040.mp3 |    | Goodman     |
| 4050.mp3 |   | Harry       |
| 4174.mp3 |  | Tommy       |

Select the music:  4158.mp3

Artist name

# UPLOAD THE MUSIC APPLICATION

[artist Rank verification coin tool](#)

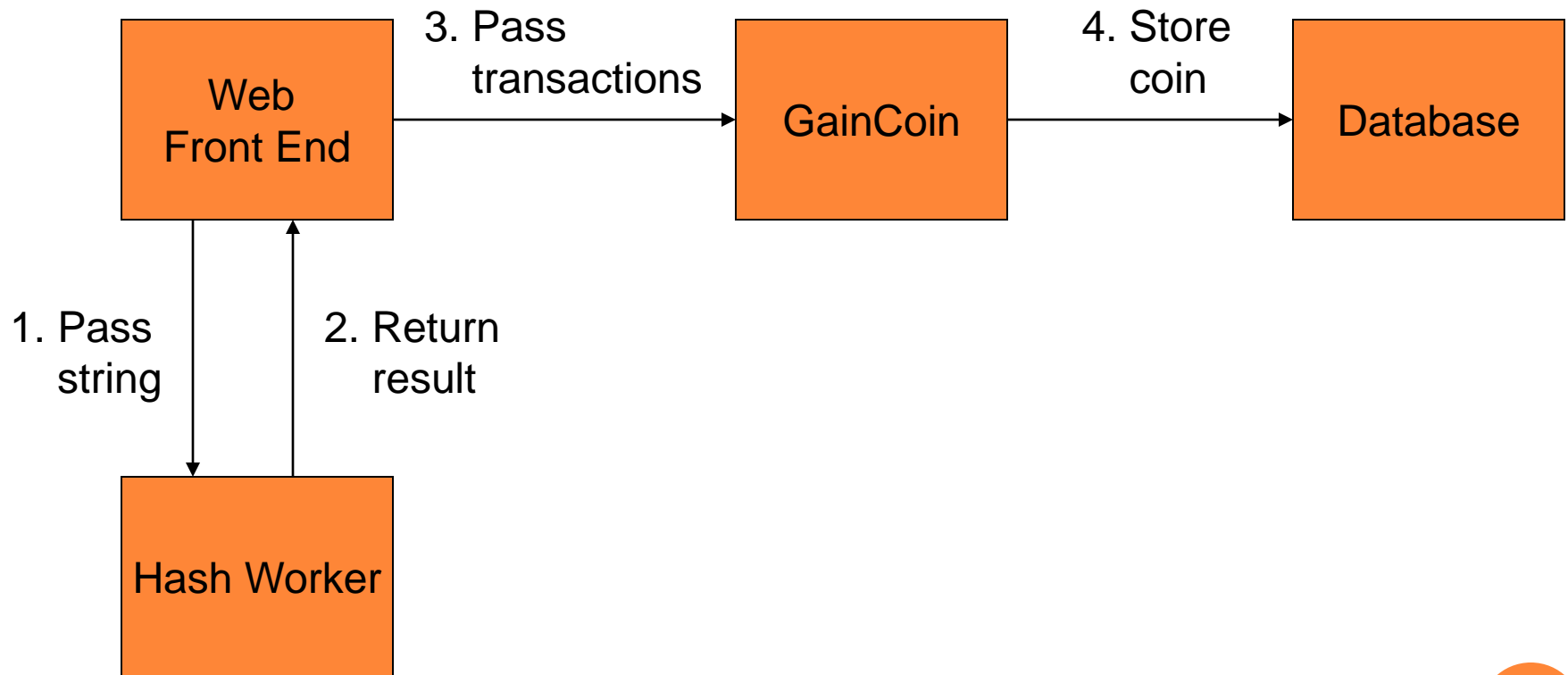
| Music    | Player   | artist name |
|----------|--|-------------|
| 1450.mp3 |    | Tim         |
| 2537.mp3 |    | Tom         |
| 2555.mp3 |    | Larry       |
| 2558.mp3 |    | Jack        |
| 4038.mp3 |    | Tim         |
| 4040.mp3 |    | Goodman     |
| 4050.mp3 |    | Harry       |
| 4174.mp3 |  | Tommy       |
| 4158.mp3 |  | Brian       |

Select the music:  No file selected.

Artist name












# GENERATE LISTENING COIN FLOWCHART



# GENERATE listening COIN APPLICATION

[artist Rank verification coin tool](#)

| Music    | Player   | artist name |
|----------|--|-------------|
| 1450.mp3 |    | Tim         |
| 2537.mp3 |    | Tom         |
| 2555.mp3 |    | Larry       |
| 2558.mp3 |    | Jack        |
| 4038.mp3 |    | Tim         |
| 4040.mp3 |    | Goodman     |
| 4050.mp3 |    | Harry       |
| 4174.mp3 |   | Tommy       |
| 4158.mp3 |  | Brian       |

Select the music:  No file selected.

Artist name

# TRANSACTION FORMAT

- (artistname)(music\_data)(timestamp)(userIPAddress)(1)(nonce)
- base64\_encode(\$string)
- Larry8eac221e13834defb2e14d636e1a2417b30009dee009a6a07dd7b862c1b579b02014-12-0915:59:1512ca17b49af2289436f303e0166030a21e525d266e209267433801a8fd4071a01 n

# WEB WORKER

- New in HTML5

Browser Support

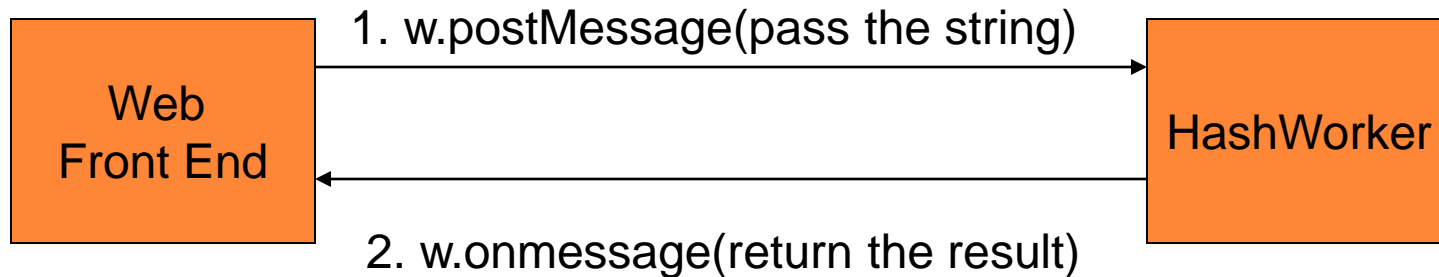


- JavaScript running in the background, without affecting the performance of the page
- Allows the browser to mine for listening coins while listening to music in parallel

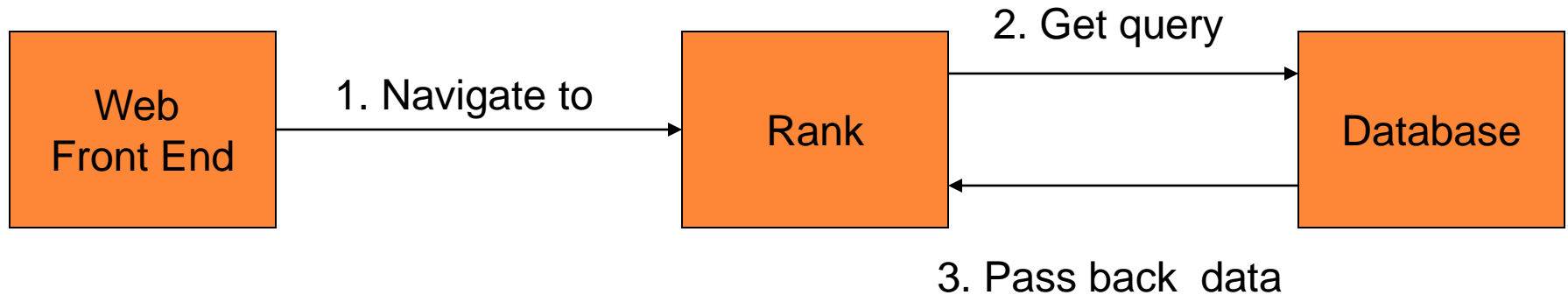
# WEB WORKER EXAMPLE CODE

```
if(typeof(Worker) !== "undefined") {  
    if(typeof(w) == "undefined") {  
        w = new Worker("hash_workers2.js");  
    }  
  
    w.onmessage = function(event) {  
        zeros = event.data;  
        var hashString = ""+event.data;  
        countNumber = event.data;  
    };  
  
    w.postMessage(a);  
}
```

# WEB WORKER DESIGN



# RANK FLOWCHART



# RANK

## Rank

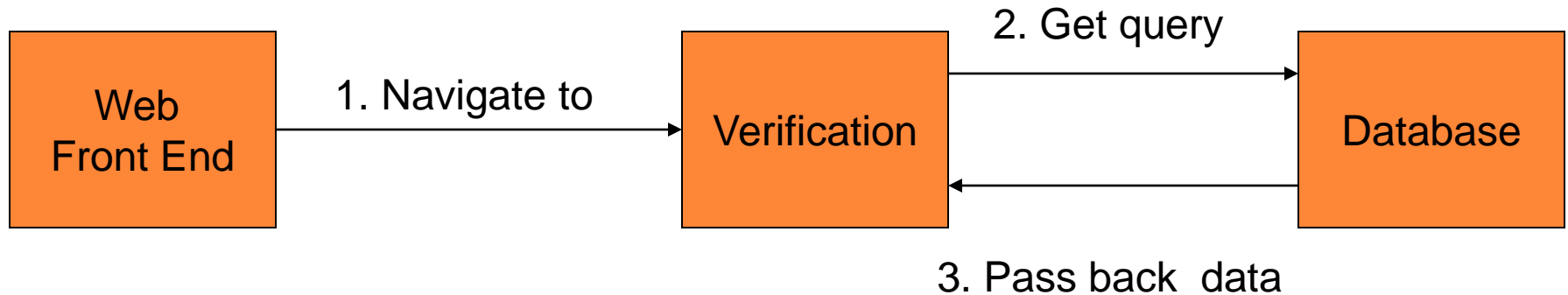
| Rank | Artist Name |
|------|-------------|
| 1    | Goodman     |
| 2    | Tim         |
| 3    | Larry       |
| 4    | Tom         |
| 5    | Jack        |

**Coin:**

| Artist Name | Coin  | Base64                                      |
|-------------|---|---|
| Larry       | Larry8eac221e13834defb2e14d636e1a2417b30009dee009a6a07dd7b862c1b579b02014-12-03 04:00:5712ca17b49af2289436f303e0166030a21e525d266e209267433801a8fd4071a01 | TGFycnk4ZWJjMjIxZTEzODM0ZGVmYjJlMTRkNjE1a01 |
| Larry       | Larry8eac221e13834defb2e14d636e1a2417b30009dee009a6a07dd7b862c1b579b02014-12-03 04:00:5712ca17b49af2289436f303e0166030a21e525d266e209267433801a8fd4071a02 | TGFycnk4ZWJjMjIxZTEzODM0ZGVmYjJlMTRkNjE1a02 |
| Larry       | Larry8eac221e13834defb2e14d636e1a2417b30009dee009a6a07dd7b862c1b579b02014-12-03 04:00:5712ca17b49af2289436f303e0166030a21e525d266e209267433801a8fd4071a03 | TGFycnk4ZWJjMjIxZTEzODM0ZGVmYjJlMTRkNjE1a03 |



# VERIFICATION TOOL FLOWCHART



# VERIFICATION TOOL APPLICATION

[back to music menu](#)

## Input Your Hashcoin Value

Text to hash

Calculate

MY-SHA256

Result:

## Input Your Base64 Value

Text to hash

Calculate

MY-SHA256

Result:

To verify all the coins artist has please enter his name :

Search

# VERIFICATION TOOL

## Input Your Base64 Value

**Text to hash** R29vZG1hbjYzM2RIYTJiNGUwMjBmNDlh

**Calculate**

MY-SHA256

Result: 000054f5e8501e85a8922c5f6f7802ea7b1084de6b42110e245d1832e53cad39

# VERIFICATION TOOL

To verify all the coins artist has please enter his name :

[back to music menu](#)

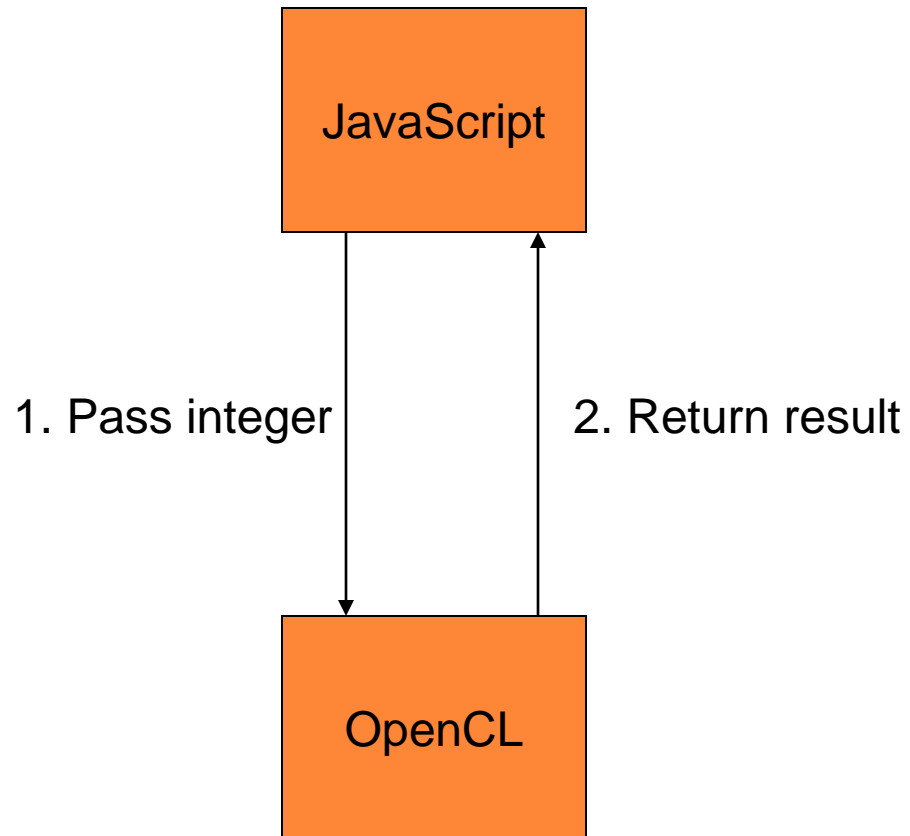
| Artist Name | Coin  | verify   |
|-------------|---|--|
| Jack        | Jack0e2371b4fd4ec412c868762c583cc5e4888bbf3f40404dd4a08686d98458cc032014-12-03 04:36:5812ca17b49af2289436f303e0166030a21e525d266e209267433801a8fd4071a01◆   | 000058f01b231b972e338616239c1923b9ba24c126fcb3a3b3f30e86ebf7dcf5 |
| Jack        | Jack0e2371b4fd4ec412c868762c583cc5e4888bbf3f40404dd4a08686d98458cc032014-12-03 13:36:3112ca17b49af2289436f303e0166030a21e525d266e209267433801a8fd4071a01Z◆  | 0000bc1426119089888a86fa6f2cb91b41fc6f1f95bf43bac2c5e4690359e214 |
| Jack        | Jack0e2371b4fd4ec412c868762c583cc5e4888bbf3f40404dd4a08686d98458cc032014-12-03 13:36:3112ca17b49af2289436f303e0166030a21e525d266e209267433801a8fd4071a02k\$ | 0000e440217e6f4869877ebf1e1bb2cb0042d69f18b7133f0585f38dc8023f4c |
| Jack        | Jack0e2371b4fd4ec412c868762c583cc5e4888bbf3f40404dd4a08686d98458cc032014-12-03 13:36:3112ca17b49af2289436f303e0166030a21e525d266e209267433801a8fd4071a03+   | 0000236e52c3512b419d007697bf5aca3aa7bc6f8e20111c8038e61e0fd6c9ec |

# ISSUES ENCOUNTERED DURING TESTING

## ○ WebCL

- Interface that allows JavaScript to run code on the GPU
- Utilize the GPU for processing instead of the CPU
- Multi-core CPU parallel processing from within a Web browser
- Out of memory
- No cross-platform compatibility

# WEBCL DESIGN



# IN OPENCL

- Execute SHA256
- Return result
  - 3 leading zero if less then decimal 1048576
  - 4 leading zero if less then decimal 65536
  - 5 leading zero if less then decimal 4096
  - 6 leading zero if less then decimal 256

## ISSUES ENCOUNTERED DURING TESTING

# Browser

- Some ASCII characters not supported
  - Base64 used as solution

# Input Your Hashcoin Value

**Text to hash** 5d266e209267433801a8fd4071a0100020004\$N

## Calculate

MY-SHA256

Result: 4de667d3717f76f61057dc34c3ec545540e1e09917d2b49844aca32458462b37



## CONCLUSION

- Generates listening coins to the artists while one of their songs is being streamed
- The longer a song is played, the more listening coins are paid out to the artist of the song
- Allows artists to verify other artists' listening coins