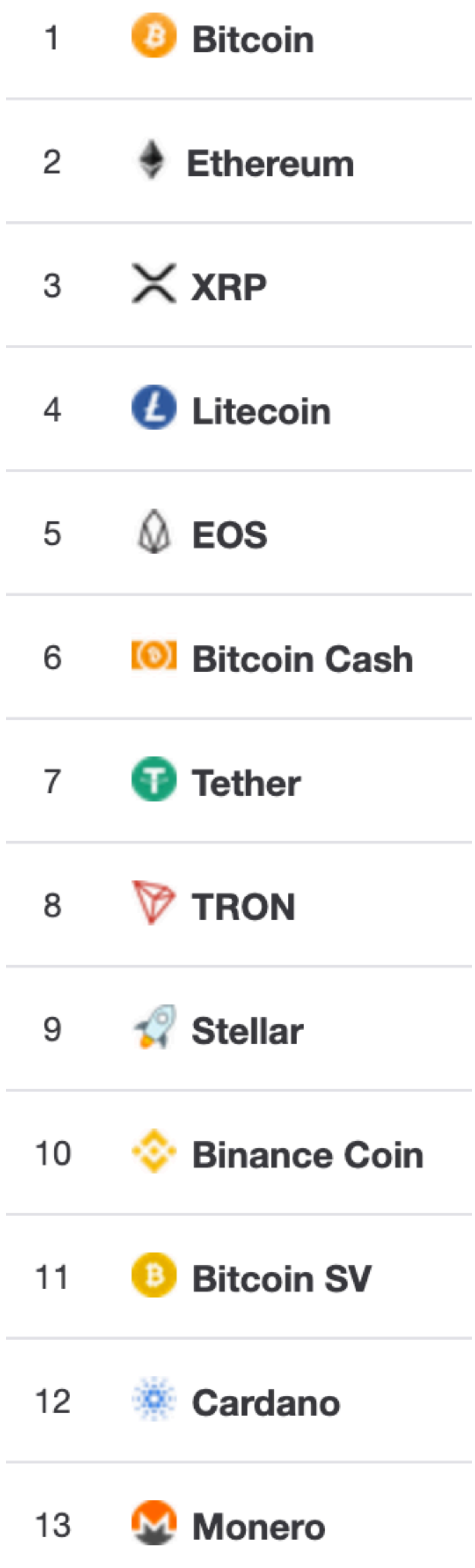
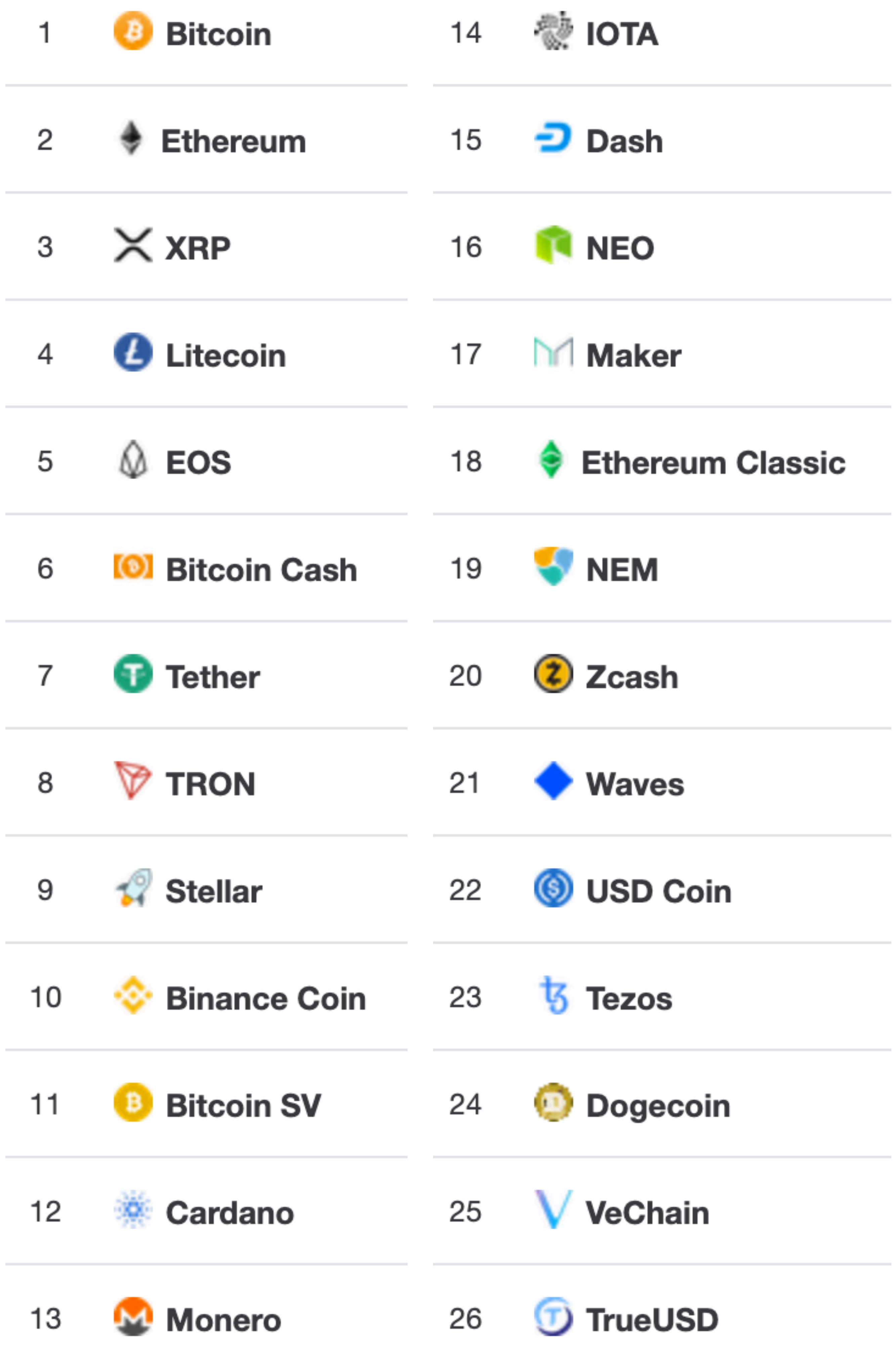
# AN EXPLORATION OF CODE DIVERSITY IN THE CRYPTOCURRENCY LANDSCAPE

SARAH MEIKLEJOHN (UCL)

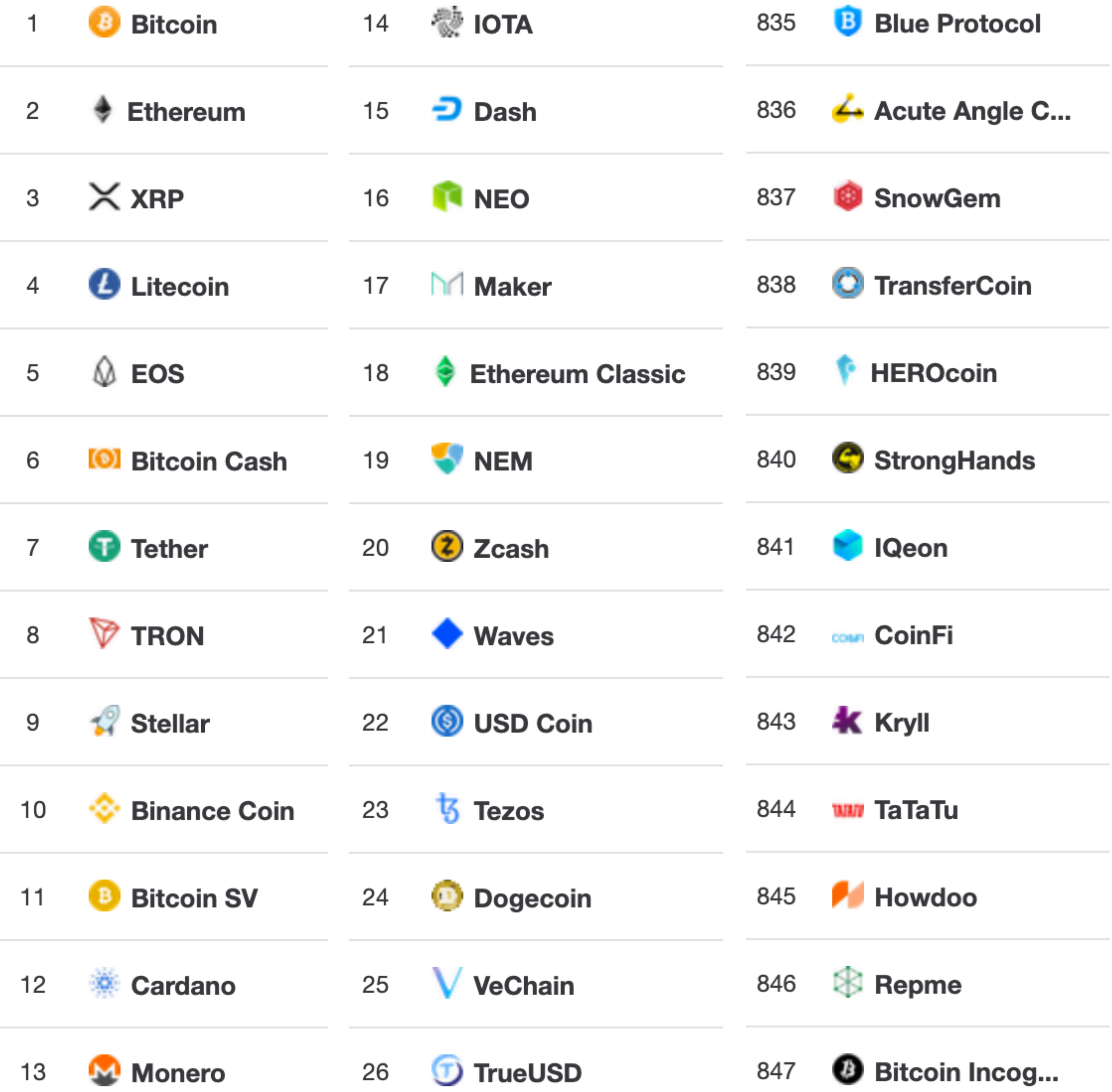
JOINT WORK WITH
PIERRE REIBEL
HAAROON YOUSAF



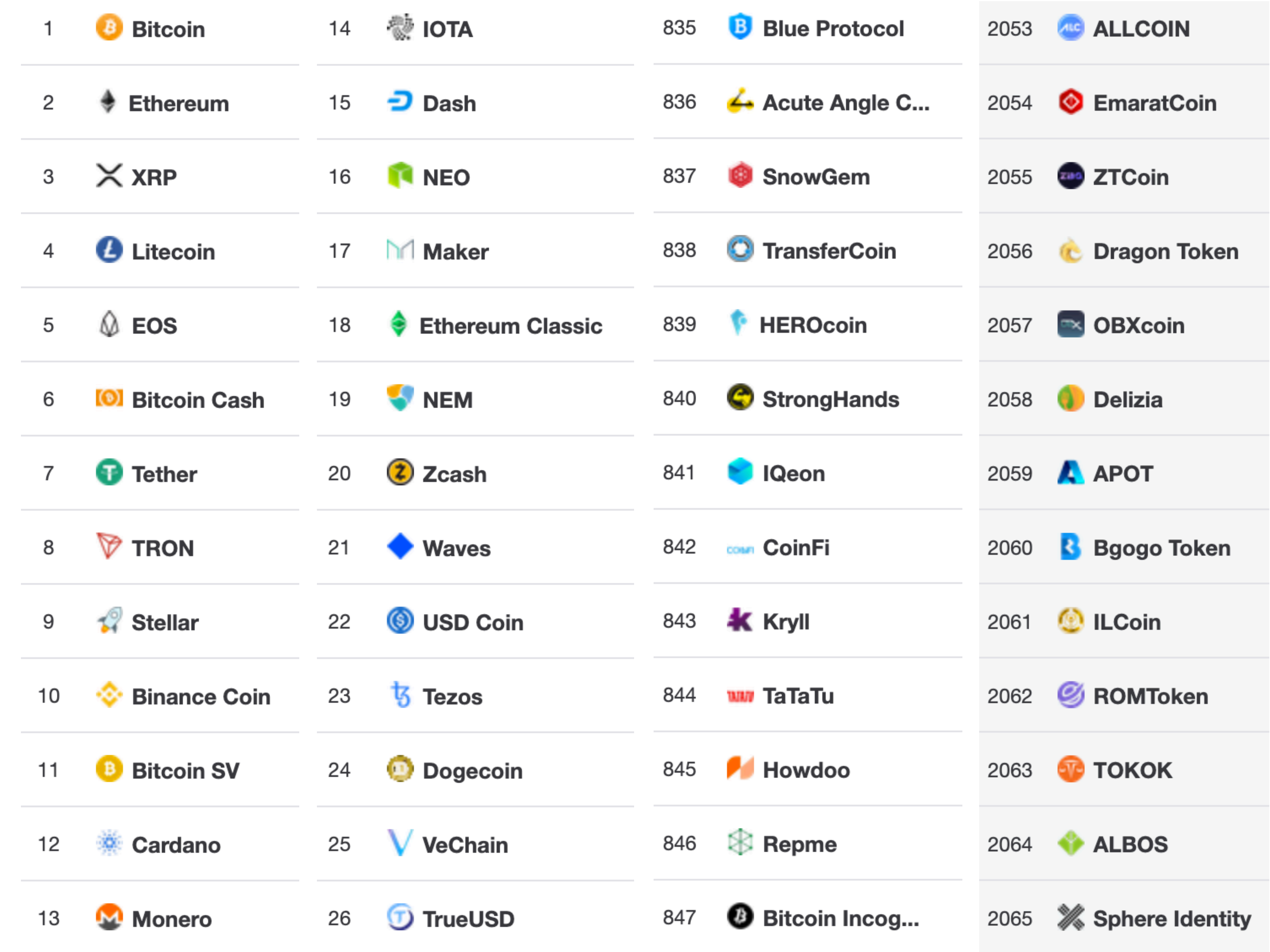
| | |
|---|---|
| 1 | **Bitcoin** |
| 2 | **Ethereum** |
| 3 | **XRP** |
| 4 | **Litecoin** |
| 5 | **EOS** |
| 6 | **Bitcoin Cash** |
| 7 | **Tether** |
| 8 | **TRON** |
| 9 | **Stellar** |
| 10 | **Binance Coin** |
| 11 | **Bitcoin SV** |
| 12 | **Cardano** |
| 13 | **Monero** |



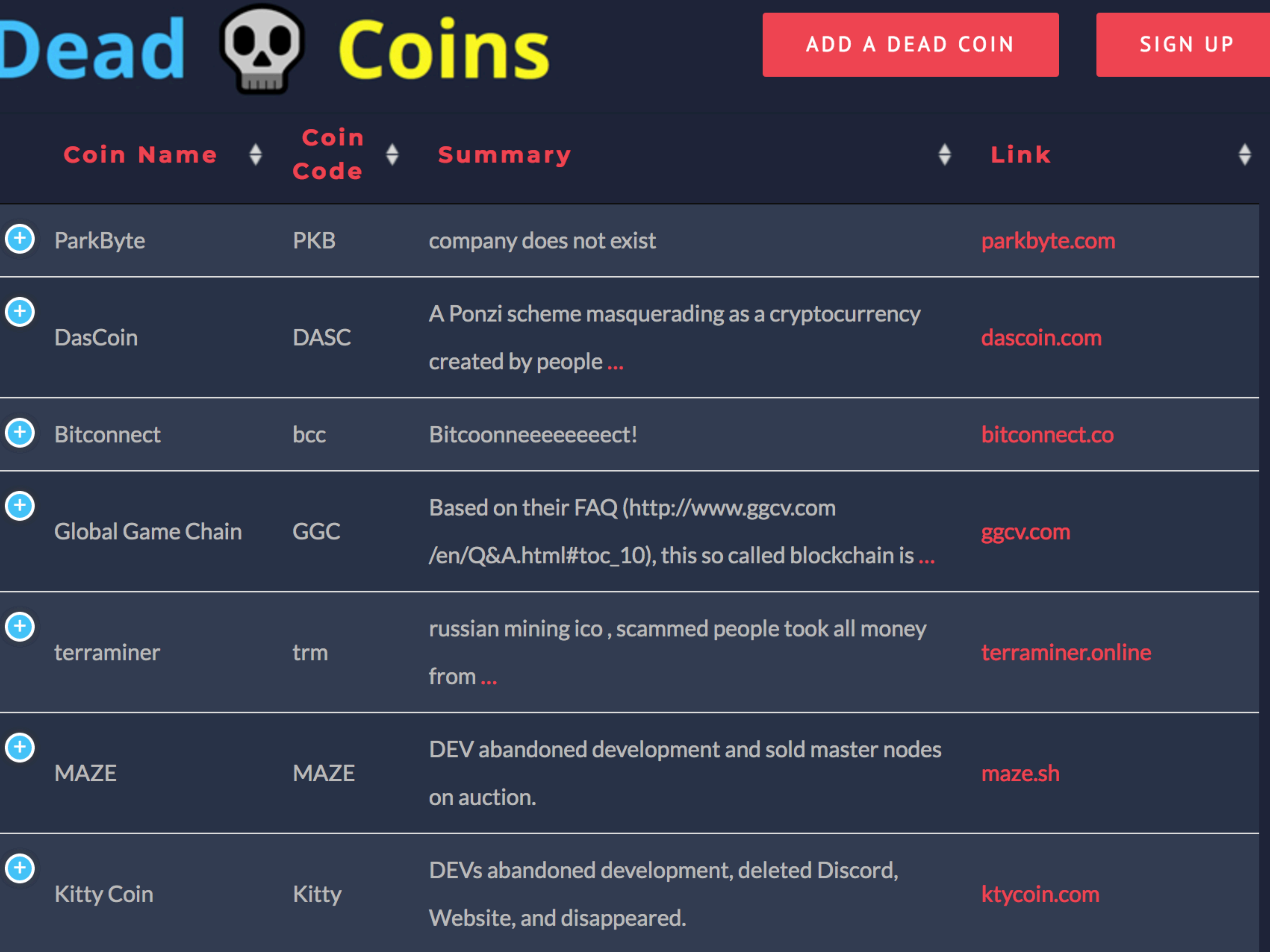
| | |
|---|---|
| 1 | Bitcoin |
| 2 | Ethereum |
| 3 | XRP |
| 4 | Litecoin |
| 5 | EOS |
| 6 | Bitcoin Cash |
| 7 | Tether |
| 8 | TRON |
| 9 | Stellar |
| 10 | Binance Coin |
| 11 | Bitcoin SV |
| 12 | Cardano |
| 13 | Monero |
| 14 | IOTA |
| 15 | Dash |
| 16 | NEO |
| 17 | Maker |
| 18 | Ethereum Classic |
| 19 | NEM |
| 20 | Zcash |
| 21 | Waves |
| 22 | USD Coin |
| 23 | Tezos |
| 24 | Dogecoin |
| 25 | VeChain |
| 26 | TrueUSD |



| | | | | | |
|---|---|---|---|---|---|
| 1 | Bitcoin | 14 | IOTA | 835 | Blue Protocol |
| 2 | Ethereum | 15 | Dash | 836 | Acute Angle C... |
| 3 | XRP | 16 | NEO | 837 | SnowGem |
| 4 | Litecoin | 17 | Maker | 838 | TransferCoin |
| 5 | EOS | 18 | Ethereum Classic | 839 | HEROcoin |
| 6 | Bitcoin Cash | 19 | NEM | 840 | StrongHands |
| 7 | Tether | 20 | Zcash | 841 | IQeon |
| 8 | TRON | 21 | Waves | 842 | CoinFi |
| 9 | Stellar | 22 | USD Coin | 843 | Kryll |
| 10 | Binance Coin | 23 | Tezos | 844 | TaTaTu |
| 11 | Bitcoin SV | 24 | Dogecoin | 845 | Howdoo |
| 12 | Cardano | 25 | VeChain | 846 | Repme |
| 13 | Monero | 26 | TrueUSD | 847 | Bitcoin Incog... |



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | Bitcoin | 14 | IOTA | 835 | Blue Protocol | 2053 | ALLCOIN |
| 2 | Ethereum | 15 | Dash | 836 | Acute Angle C... | 2054 | EmaratCoin |
| 3 | XRP | 16 | NEO | 837 | SnowGem | 2055 | ZTCoin |
| 4 | Litecoin | 17 | Maker | 838 | TransferCoin | 2056 | Dragon Token |
| 5 | EOS | 18 | Ethereum Classic | 839 | HEROcoin | 2057 | OBXcoin |
| 6 | Bitcoin Cash | 19 | NEM | 840 | StrongHands | 2058 | Delizia |
| 7 | Tether | 20 | Zcash | 841 | IQeon | 2059 | APOT |
| 8 | TRON | 21 | Waves | 842 | CoinFi | 2060 | Bgogo Token |
| 9 | Stellar | 22 | USD Coin | 843 | Kryll | 2061 | ILCoin |
| 10 | Binance Coin | 23 | Tezos | 844 | TaTaTu | 2062 | ROMToken |
| 11 | Bitcoin SV | 24 | Dogecoin | 845 | Howdoo | 2063 | TOKOK |
| 12 | Cardano | 25 | VeChain | 846 | Repme | 2064 | ALBOS |
| 13 | Monero | 26 | TrueUSD | 847 | Bitcoin Incog... | 2065 | Sphere Identity |

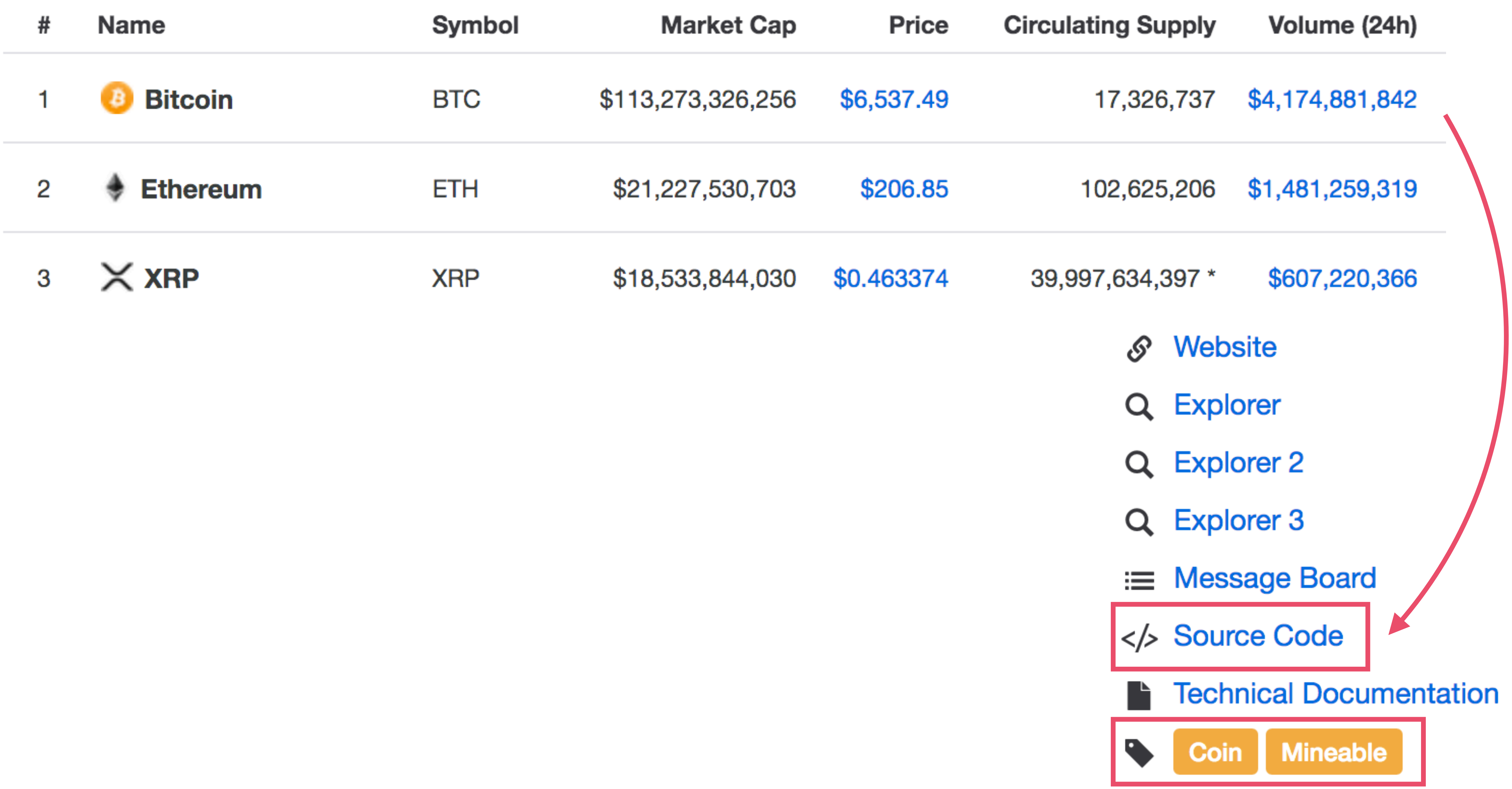


# Dead 💀 Coins

| Coin Name | Coin Code | Summary | Link |
|---|---|---|---|
| ParkByte | PKB | company does not exist | parkbyte.com |
| DasCoin | DASC | A Ponzi scheme masquerading as a cryptocurrency created by people ... | dascoin.com |
| Bitconnect | bcc | Bitcoonneeeeeeeect! | bitconnect.co |
| Global Game Chain | GGC | Based on their FAQ (http://www.ggcv.com /en/Q&A.html#toc_10), this so called blockchain is ... | ggcv.com |
| terraminer | trm | russian mining ico , scammed people took all money from ... | terraminer.online |
| MAZE | MAZE | DEV abandoned development and sold master nodes on auction. | maze.sh |
| Kitty Coin | Kitty | DEVs abandoned development, deleted Discord, Website, and disappeared. | ktycoin.com |

# CRYPTOCURRENCY LANDSCAPE

As of July 2018, there were 1664 cryptocurrencies listed on coinmarketcap.com

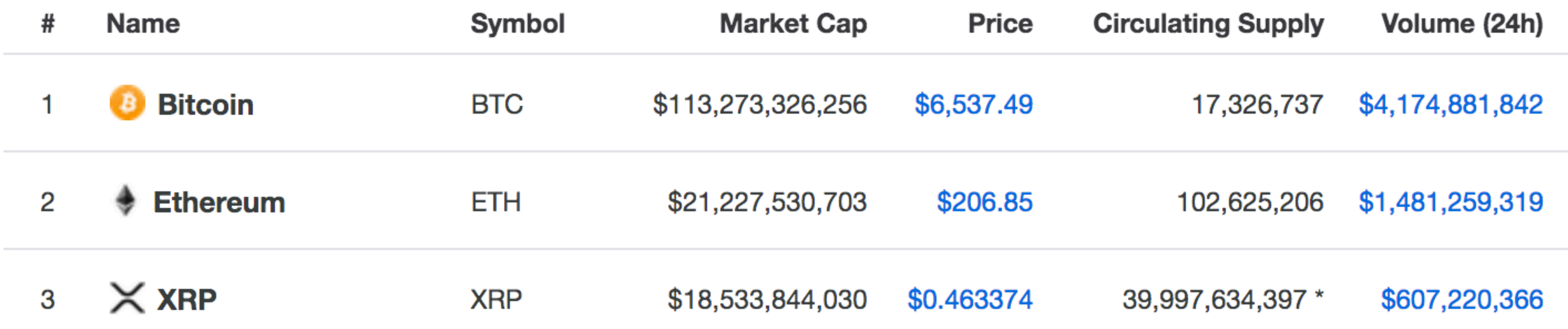


| # | Name | Symbol | Market Cap | Price | Circulating Supply | Volume (24h) |
|---|---|---|---|---|---|---|
| 1 | Bitcoin | BTC | $113,273,326,256 | $6,537.49 | 17,326,737 | $4,174,881,842 |
| 2 | Ethereum | ETH | $21,227,530,703 | $206.85 | 102,625,206 | $1,481,259,319 |
| 3 | XRP | XRP | $18,533,844,030 | $0.463374 | 39,997,634,397 * | $607,220,366 |

- Website
- Explorer
- Explorer 2
- Explorer 3
- Message Board
- </> Source Code
- Technical Documentation
- Coin Mineable

# CRYPTOCURRENCY LANDSCAPE

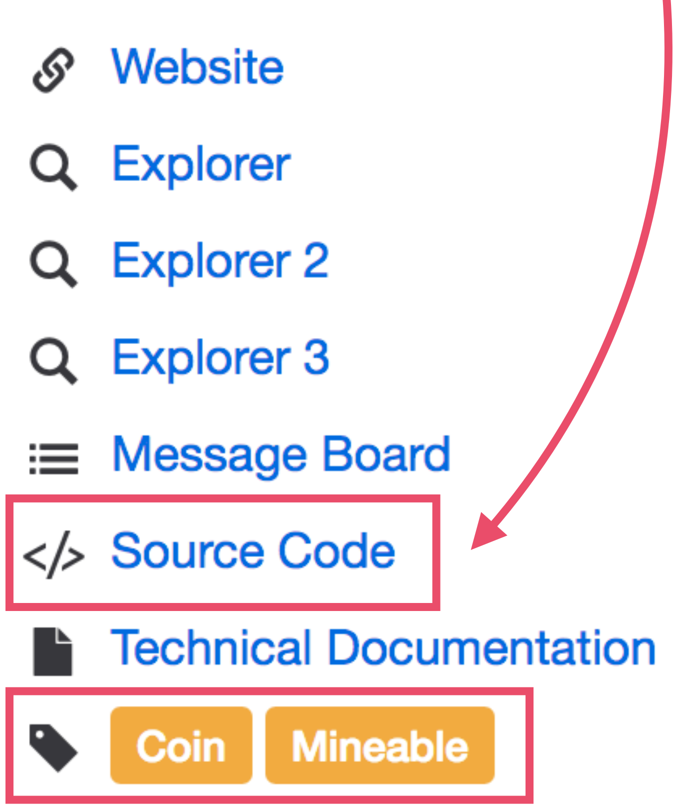
As of July 2018, there were 1664 cryptocurrencies listed on coinmarketcap.com



| # | Name | Symbol | Market Cap | Price | Circulating Supply | Volume (24h) |
|---|---|---|---|---|---|---|
| 1 | Bitcoin | BTC | $113,273,326,256 | $6,537.49 | 17,326,737 | $4,174,881,842 |
| 2 | Ethereum | ETH | $21,227,530,703 | $206.85 | 102,625,206 | $1,481,259,319 |
| 3 | XRP | XRP | $18,533,844,030 | $0.463374 | 39,997,634,397 * | $607,220,366 |

We scraped all this data on July 24 2018

Scraped 2354 repositories out of a total 13,694, roughly 100 GB of data (see paper to see how we selected repositories)



Website

Explorer

Explorer 2

Explorer 3

Message Board

</> Source Code

Technical Documentation

Coin Mineable

# MAKING A SCAMCOIN

What makes a currency a scamcoin?

One definition (of scamcoin): no meaningful codebase, code is missing or just copied from that of another cryptocurrency

This means: we can identify scamcoins by looking at their codebases, seeing if they're "meaningful"

One definition (of meaningful): code or currency has some unique properties

# UNIQUE PROPERTIES

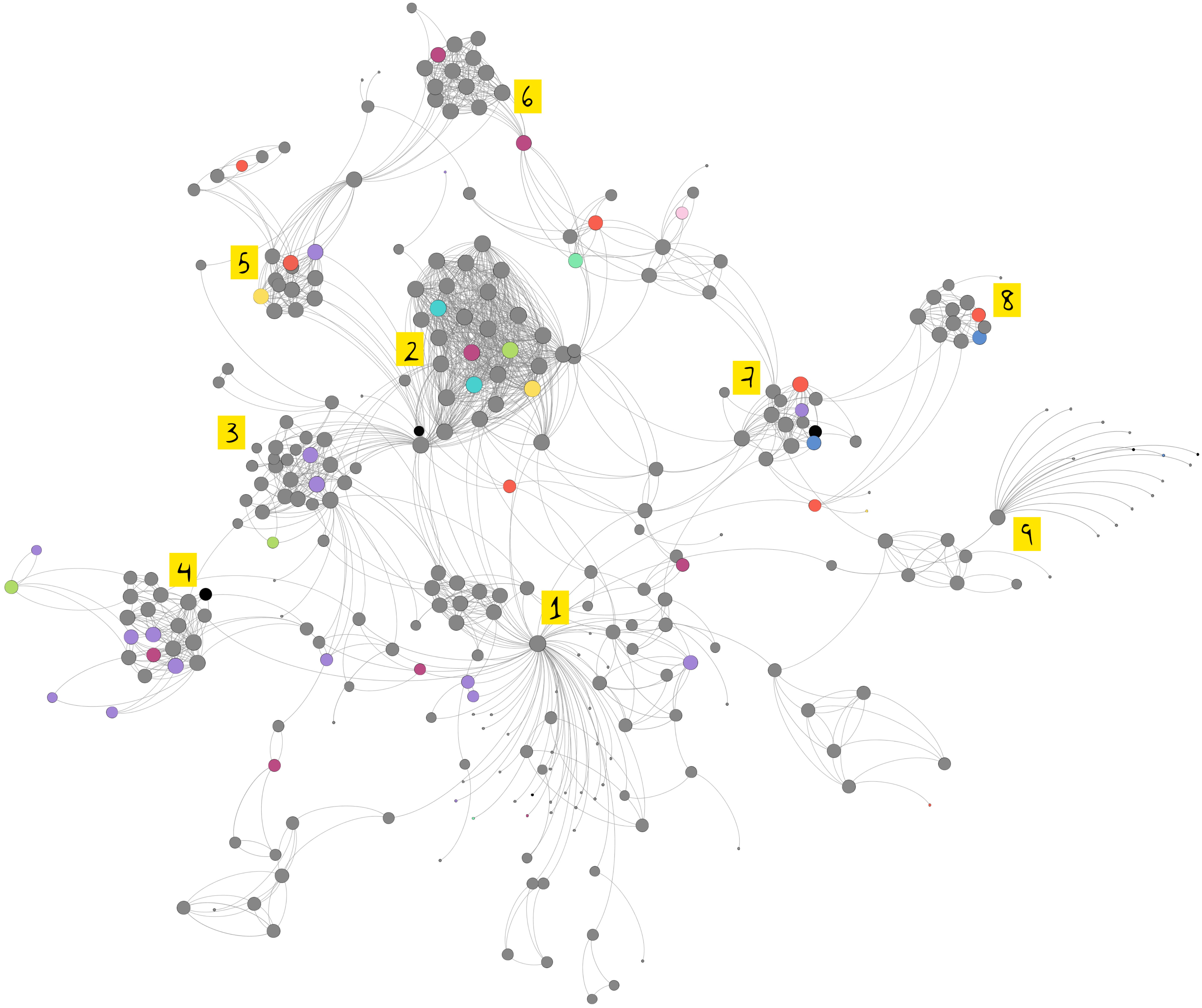
Name: borrowed from another?

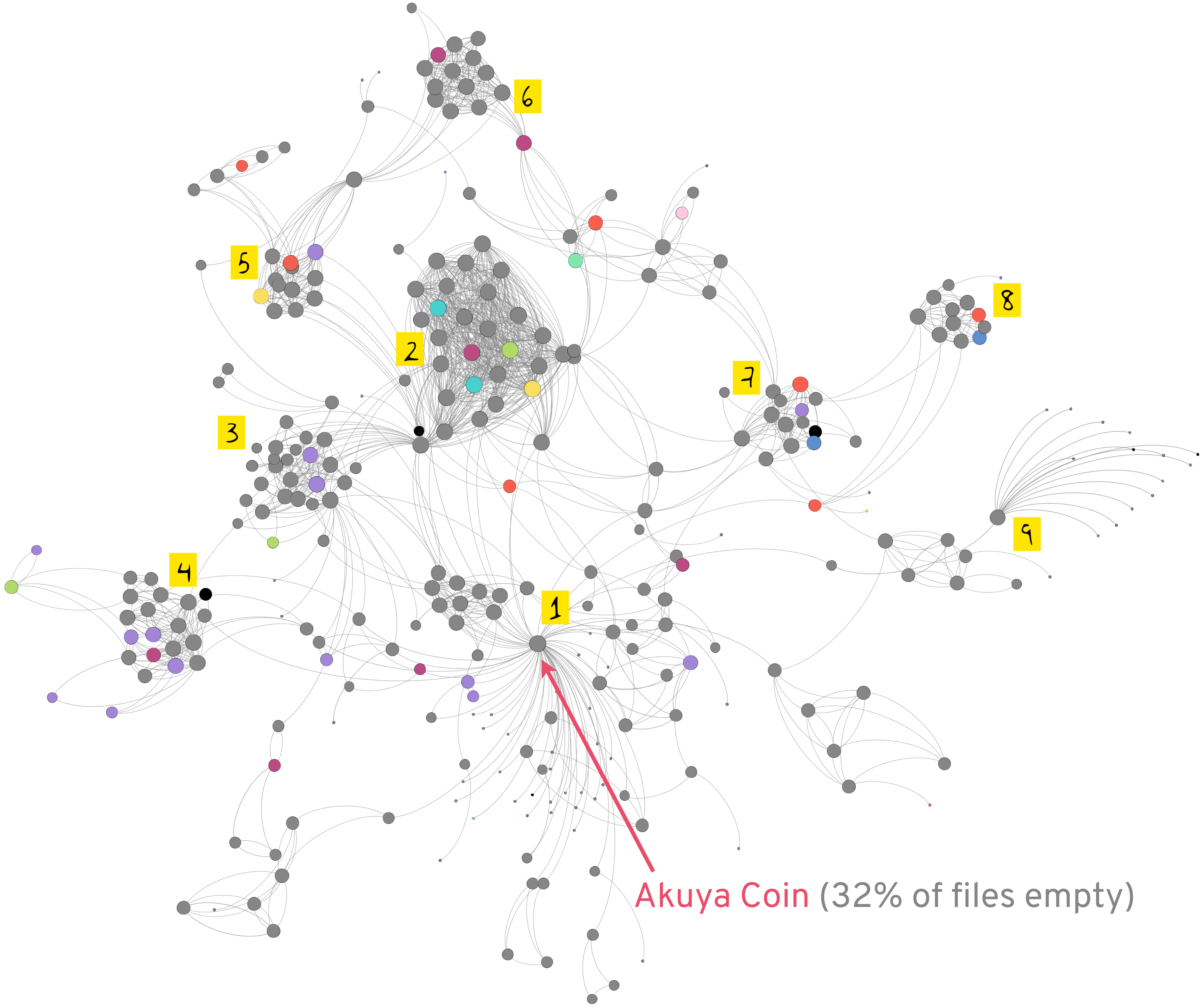
Git commits: forked from another?

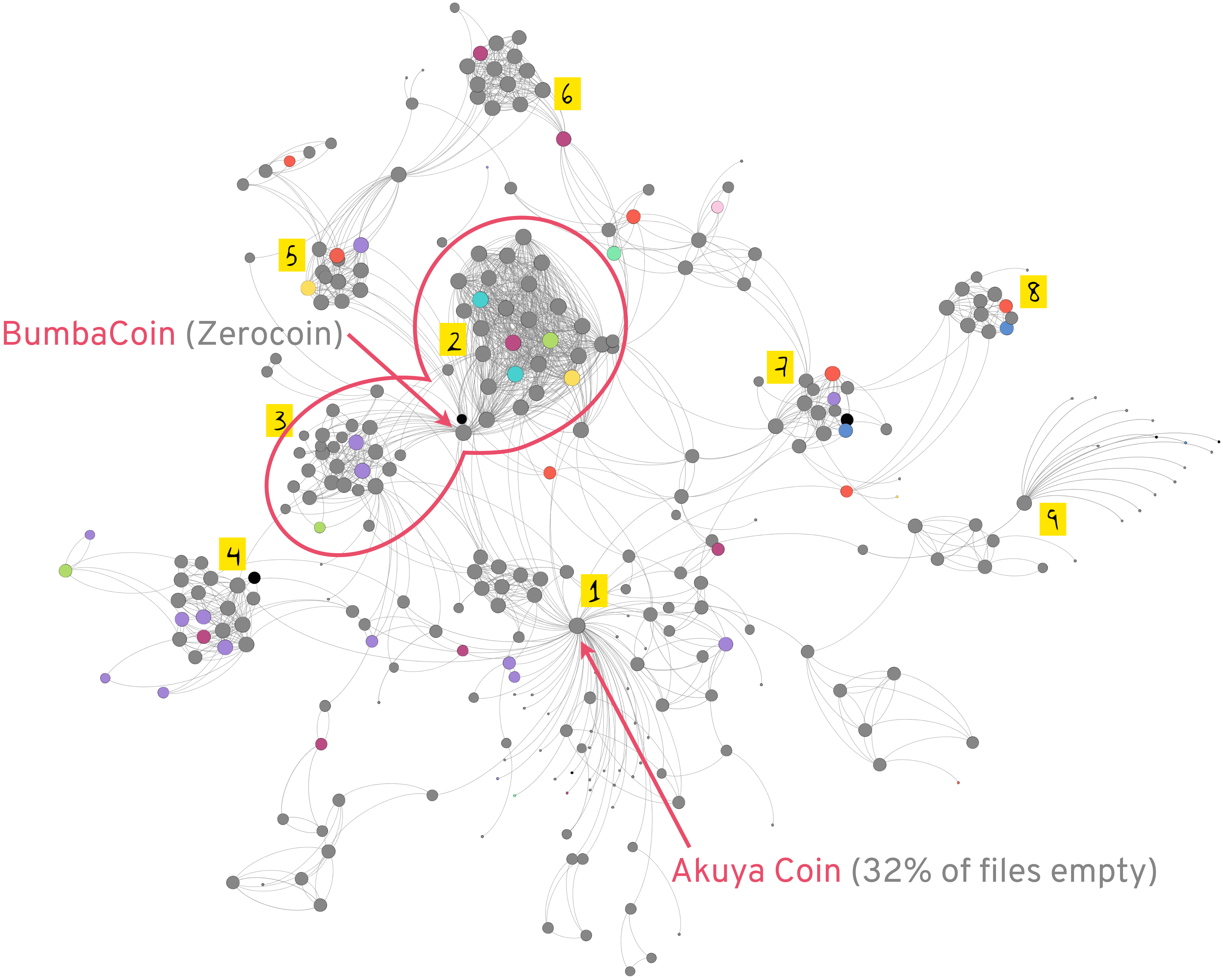
Copyrights: using code from another?

**Files: using (unchanged) files from another?**

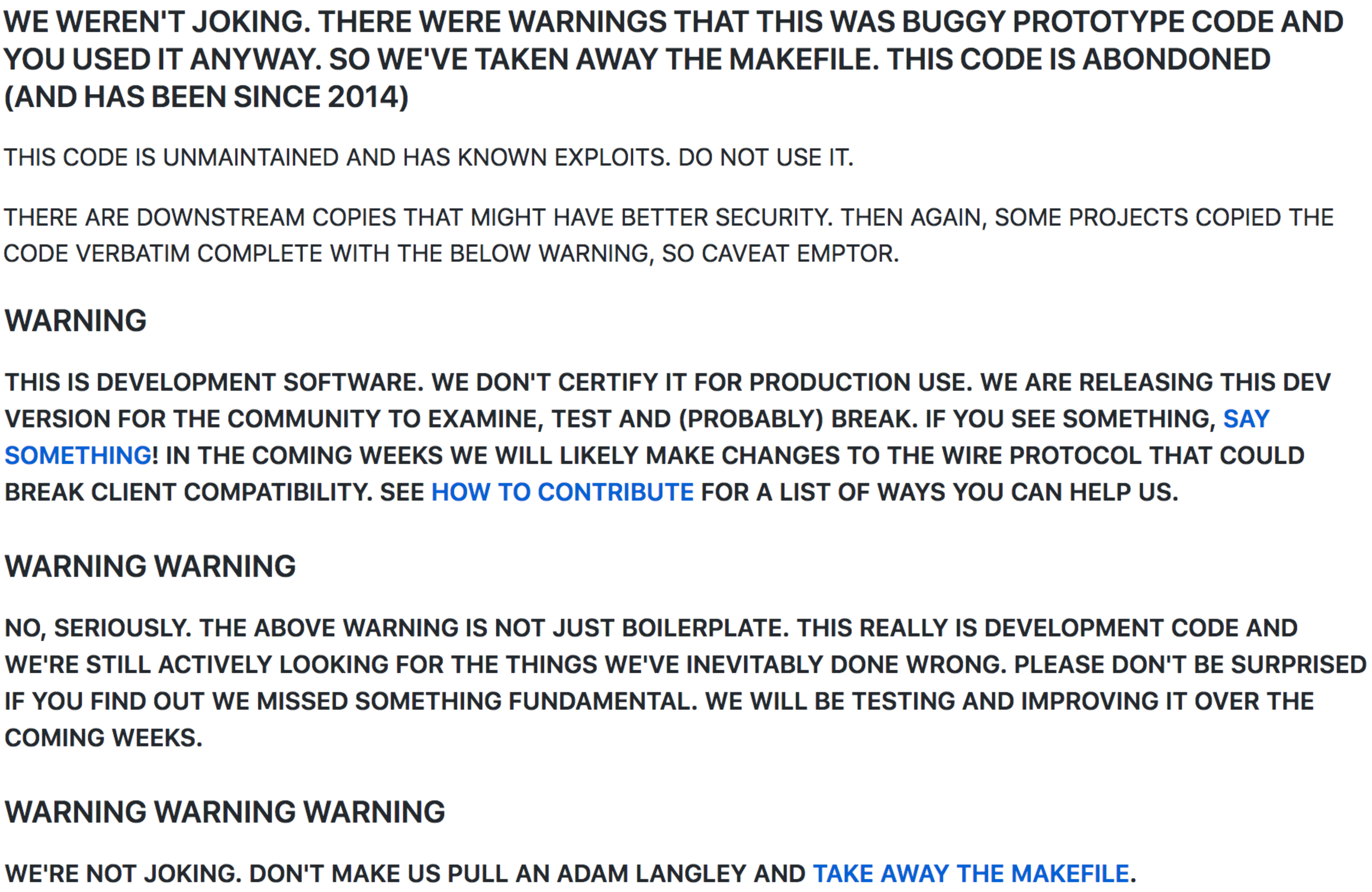
Which currencies have a significant fraction of files identical to those of other currencies?


6
5
2
3
4
1
7
8
9


6
5
2
3
7
8
4
1
9
Akuya Coin (32% of files empty)


6
5
2
BumbaCoin (Zerocoin)
3
7
8
4
1
9
Akuya Coin (32% of files empty)

# ZEROCOIN (CLUSTERS #2 AND #3)



## WE WEREN'T JOKING. THERE WERE WARNINGS THAT THIS WAS BUGGY PROTOTYPE CODE AND YOU USED IT ANYWAY. SO WE'VE TAKEN AWAY THE MAKEFILE. THIS CODE IS ABONDONED (AND HAS BEEN SINCE 2014)

THIS CODE IS UNMAINTAINED AND HAS KNOWN EXPLOITS. DO NOT USE IT.

THERE ARE DOWNSTREAM COPIES THAT MIGHT HAVE BETTER SECURITY. THEN AGAIN, SOME PROJECTS COPIED THE CODE VERBATIM COMPLETE WITH THE BELOW WARNING, SO CAVEAT EMPTOR.

### WARNING

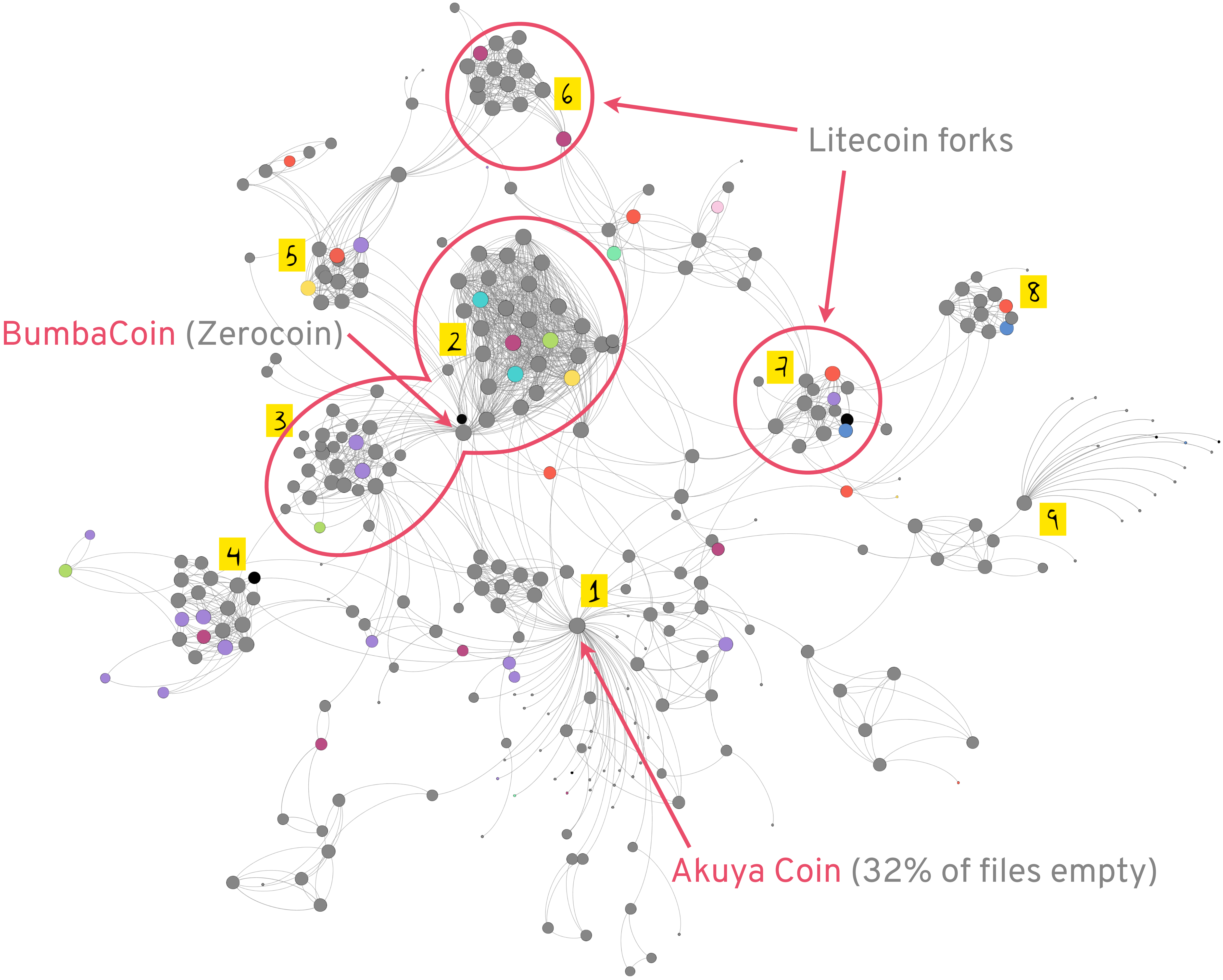
**THIS IS DEVELOPMENT SOFTWARE. WE DON'T CERTIFY IT FOR PRODUCTION USE. WE ARE RELEASING THIS DEV VERSION FOR THE COMMUNITY TO EXAMINE, TEST AND (PROBABLY) BREAK. IF YOU SEE SOMETHING, SAY SOMETHING! IN THE COMING WEEKS WE WILL LIKELY MAKE CHANGES TO THE WIRE PROTOCOL THAT COULD BREAK CLIENT COMPATIBILITY. SEE HOW TO CONTRIBUTE FOR A LIST OF WAYS YOU CAN HELP US.**

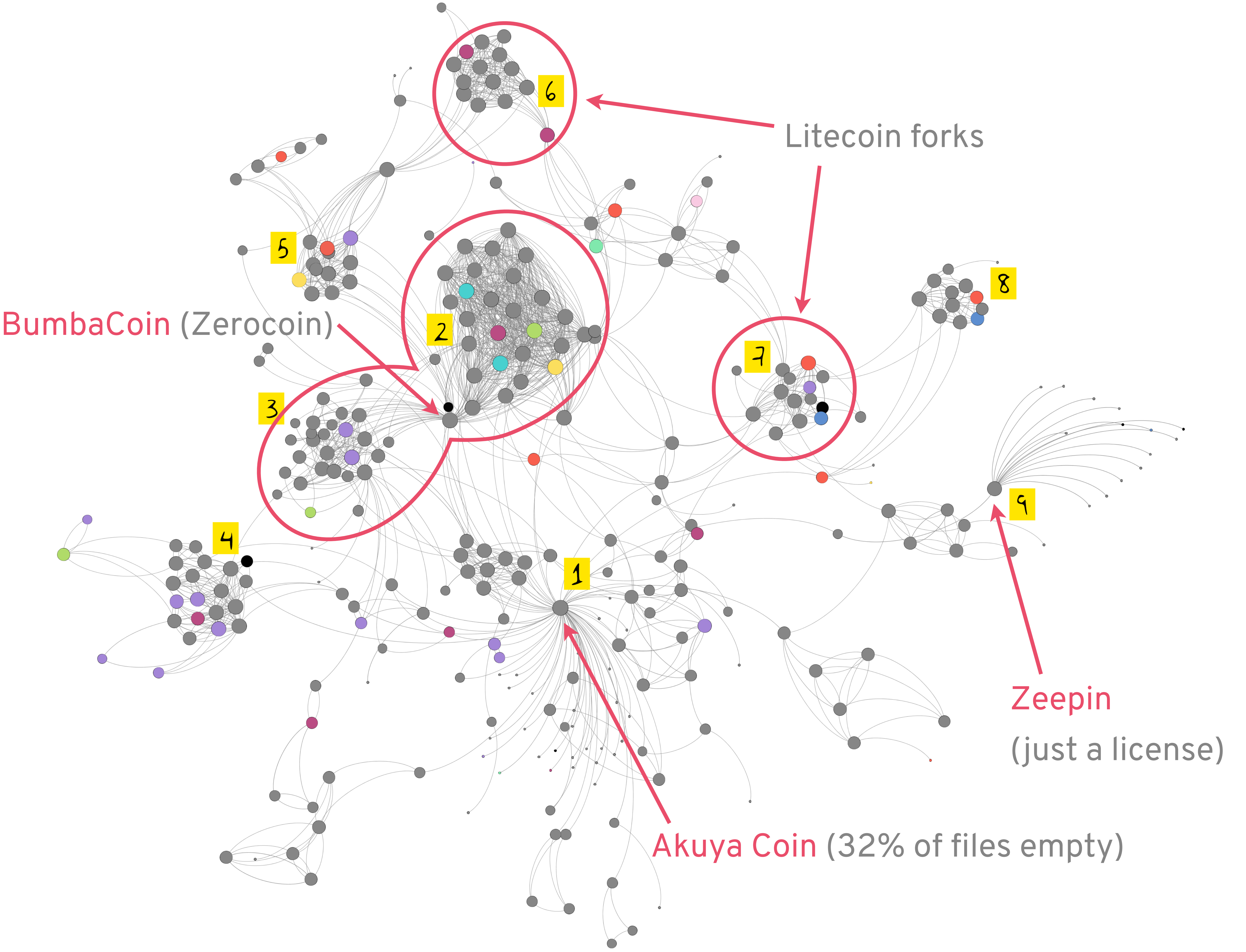
### WARNING WARNING

**NO, SERIOUSLY. THE ABOVE WARNING IS NOT JUST BOILERPLATE. THIS REALLY IS DEVELOPMENT CODE AND WE'RE STILL ACTIVELY LOOKING FOR THE THINGS WE'VE INEVITABLY DONE WRONG. PLEASE DON'T BE SURPRISED IF YOU FIND OUT WE MISSED SOMETHING FUNDAMENTAL. WE WILL BE TESTING AND IMPROVING IT OVER THE COMING WEEKS.**

### WARNING WARNING WARNING

**WE'RE NOT JOKING. DON'T MAKE US PULL AN ADAM LANGLEY AND TAKE AWAY THE MAKEFILE.**


Litecoin forks
BumbaCoin (Zerocoin)
Akuya Coin (32% of files empty)
1
2
3
4
5
6
7
8
9



Litecoin forks

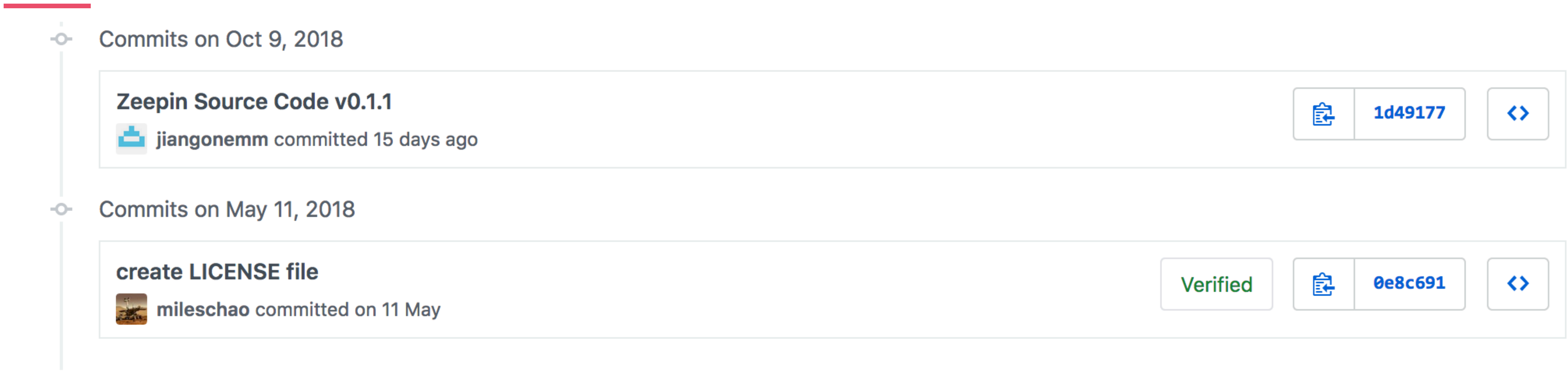
BumbaCoin (Zerocoin)

Zeepin

(just a license)

Akuya Coin (32% of files empty)

# ZEEPIN

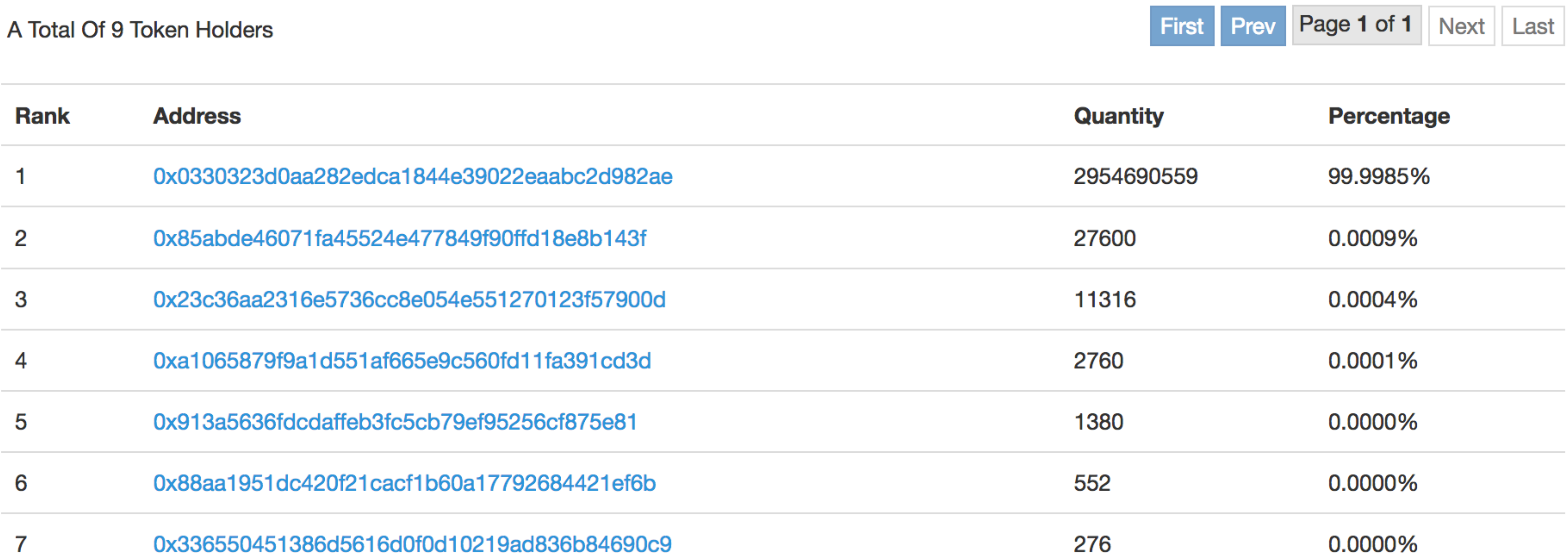


Commits on Oct 9, 2018

**Zeepin Source Code v0.1.1**
**jiangonemm** committed 15 days ago

Commits on May 11, 2018

**create LICENSE file**
**mileschao** committed on 11 May

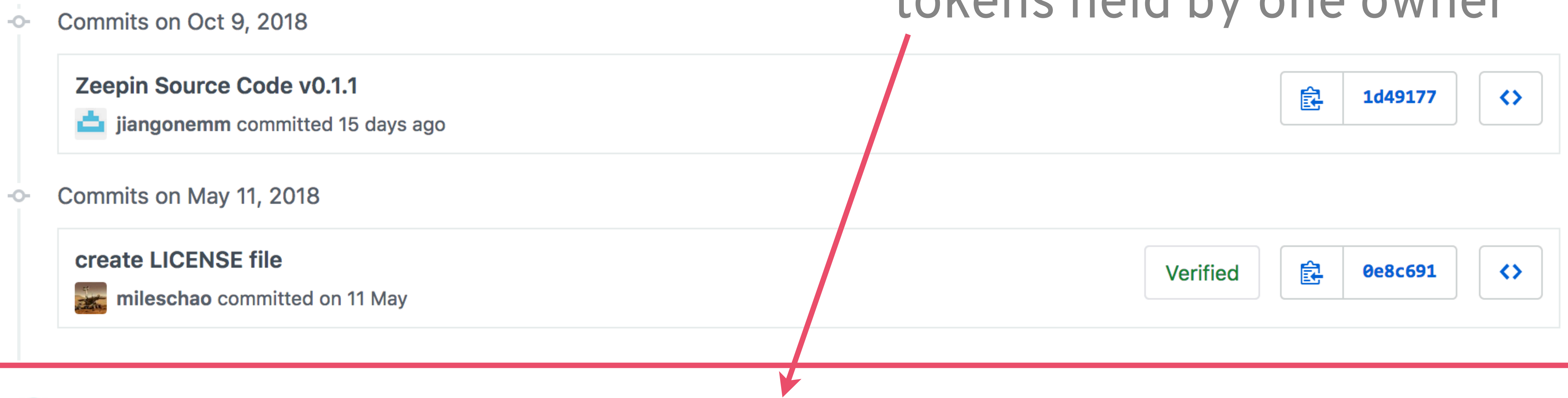


A Total Of 9 Token Holders

| Rank | Address | Quantity | Percentage |
|---|---|---|---|
| 1 | 0x0330323d0aa282edca1844e39022eaabc2d982ae | 2954690559 | 99.9985% |
| 2 | 0x85abde46071fa45524e477849f90ffd18e8b143f | 27600 | 0.0009% |
| 3 | 0x23c36aa2316e5736cc8e054e551270123f57900d | 11316 | 0.0004% |
| 4 | 0xa1065879f9a1d551af665e9c560fd11fa391cd3d | 2760 | 0.0001% |
| 5 | 0x913a5636fdcdaffeb3fc5cb79ef95256cf875e81 | 1380 | 0.0000% |
| 6 | 0x88aa1951dc420f21cacf1b60a17792684421ef6b | 552 | 0.0000% |
| 7 | 0x336550451386d5616d0f0d10219ad836b84690c9 | 276 | 0.0000% |

# ZEEPIN

market capitalization of $22.8M with only a license and 99.99% of tokens held by one owner

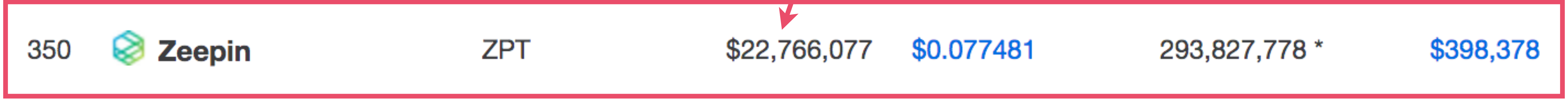


Commits on Oct 9, 2018

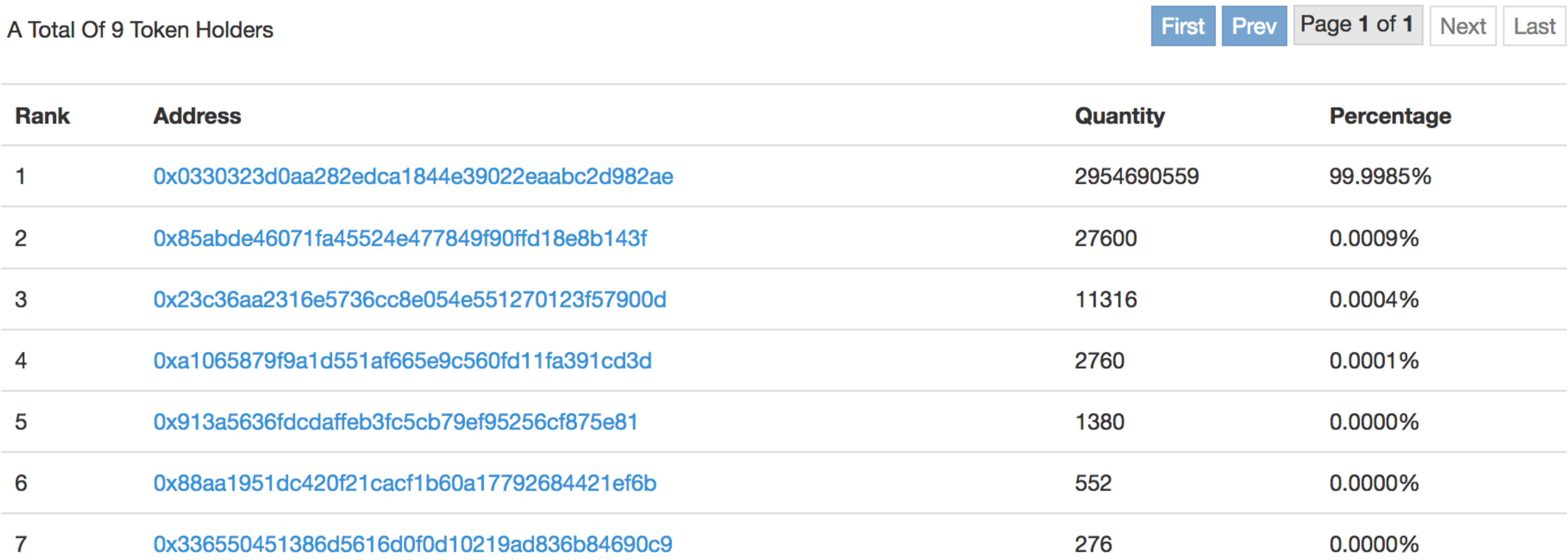
**Zeepin Source Code v0.1.1**
**jiangonemm** committed 15 days ago

Commits on May 11, 2018

**create LICENSE file**
**mileschao** committed on 11 May



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 350 | **Zeepin** | ZPT | $22,766,077 | $0.077481 | 293,827,778 * | $398,378 |



A Total Of 9 Token Holders

| Rank | Address | Quantity | Percentage |
|---|---|---|---|
| 1 | 0x0330323d0aa282edca1844e39022eaabc2d982ae | 2954690559 | 99.9985% |
| 2 | 0x85abde46071fa45524e477849f90ffd18e8b143f | 27600 | 0.0009% |
| 3 | 0x23c36aa2316e5736cc8e054e551270123f57900d | 11316 | 0.0004% |
| 4 | 0xa1065879f9a1d551af665e9c560fd11fa391cd3d | 2760 | 0.0001% |
| 5 | 0x913a5636fdcdaffeb3fc5cb79ef95256cf875e81 | 1380 | 0.0000% |
| 6 | 0x88aa1951dc420f21cacf1b60a17792684421ef6b | 552 | 0.0000% |
| 7 | 0x336550451386d5616d0f0d10219ad836b84690c9 | 276 | 0.0000% |

# UNIQUE PROPERTIES

Name: borrowed from another?

Git commits: forked from another?

Copyrights: using code from another?

**Files: using (unchanged) files from another?**

Many currencies seem to borrow (heavily) from others, and in particular from Bitcoin

# ERC20 TOKENS

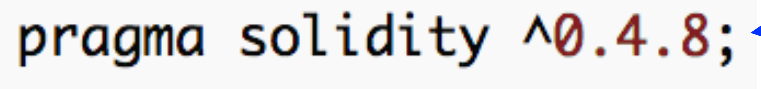
One definition (of meaningful): code or currency has some unique properties

One resource we’ve overlooked so far: Ethereum smart contracts

These are the main source code for ERC20 tokens, which comprise 52% of the listed currencies (866 in total)

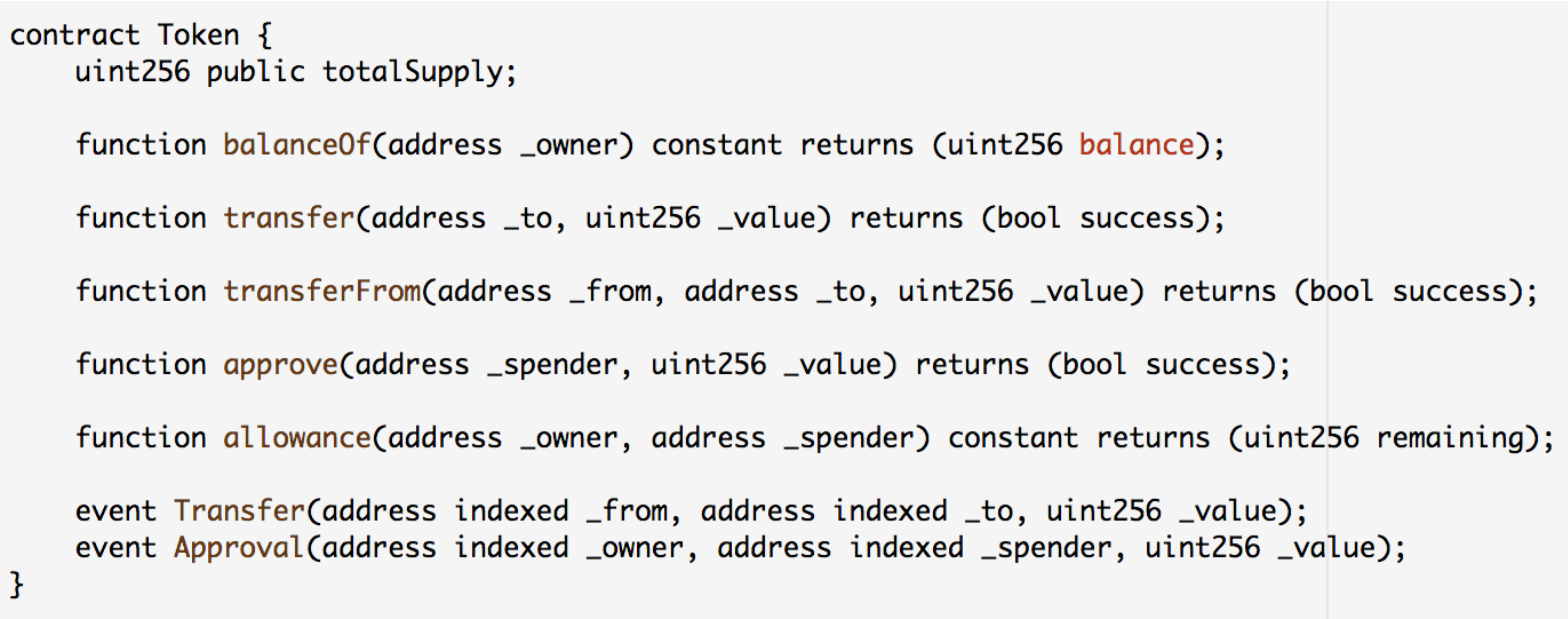
Scraped Solidity code from etherscan.io, found contract code for 438 currencies

# ERC20 TOKEN CONTRACT

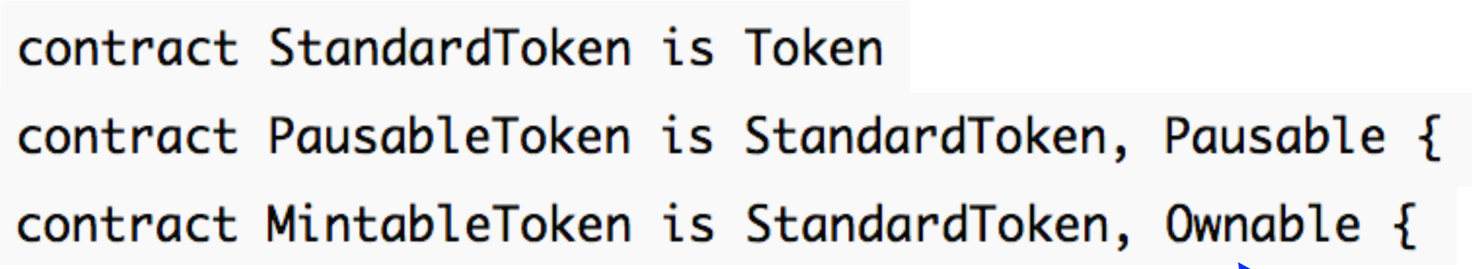


```
pragma solidity ^0.4.8;
```

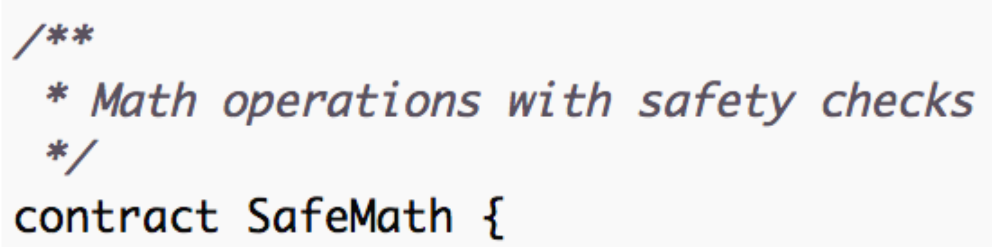
extracted version number



```
contract Token {
    uint256 public totalSupply;

    function balanceOf(address _owner) constant returns (uint256 balance);

    function transfer(address _to, uint256 _value) returns (bool success);

    function transferFrom(address _from, address _to, uint256 _value) returns (bool success);

    function approve(address _spender, uint256 _value) returns (bool success);

    function allowance(address _owner, address _spender) constant returns (uint256 remaining);

    event Transfer(address indexed _from, address indexed _to, uint256 _value);
    event Approval(address indexed _owner, address indexed _spender, uint256 _value);
}
```

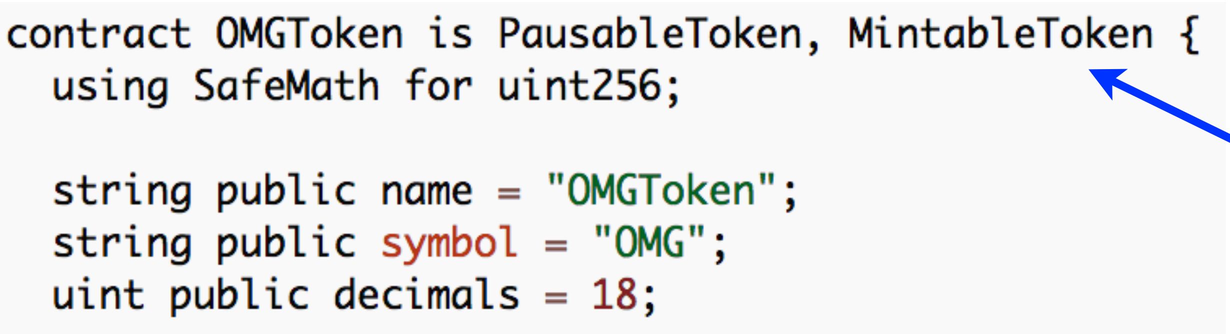


```
contract StandardToken is Token
contract PausableToken is StandardToken, Pausable {
contract MintableToken is StandardToken, Ownable {
```



```
/**
 * Math operations with safety checks
 */
contract SafeMath {
```

extracted SafeMath version

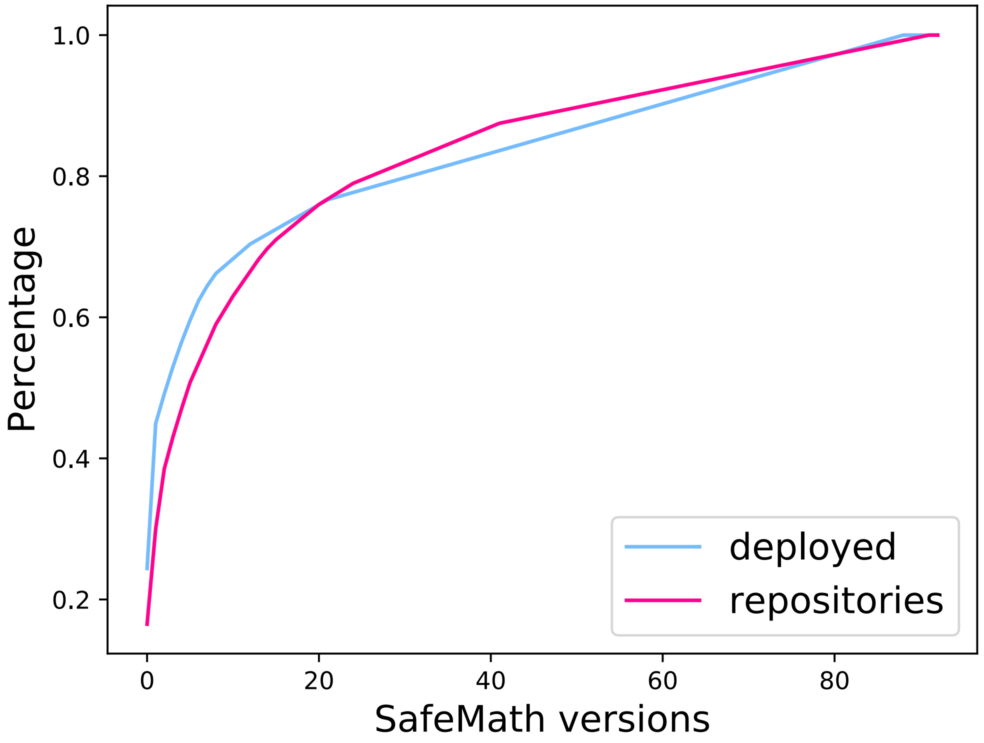


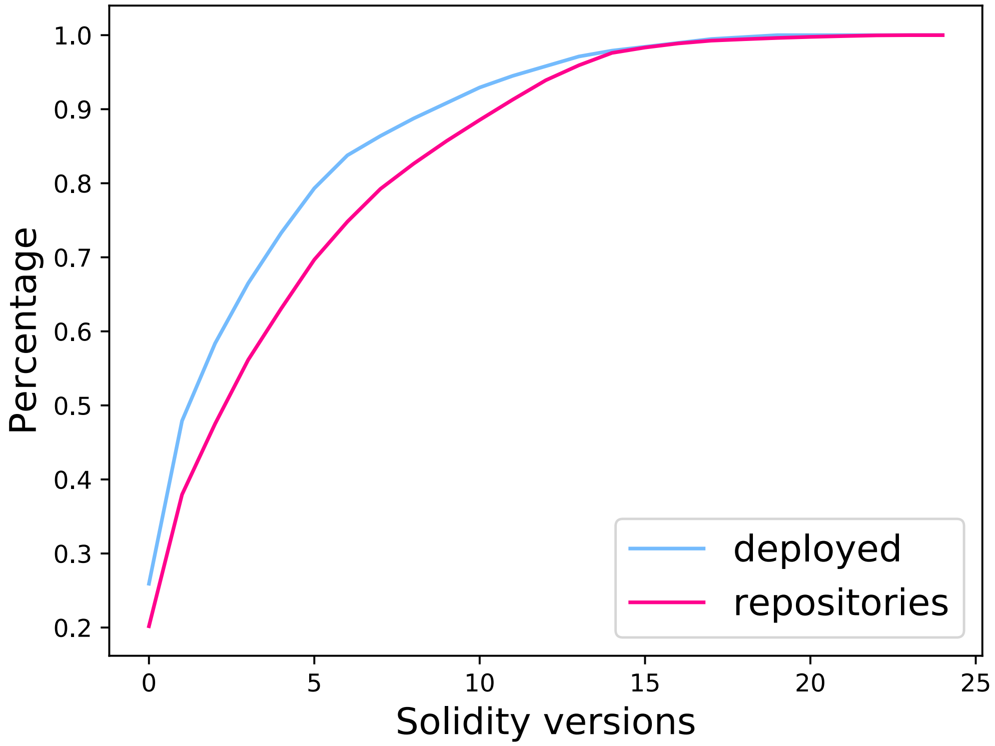
```
contract OMGToken is PausableToken, MintableToken {
  using SafeMath for uint256;

  string public name = "OMGToken";
  string public symbol = "OMG";
  uint public decimals = 18;
```

extracted all types

# DIVERSITY IN ERC20 TOKENS

Found SafeMath in 65.9% of deployed contracts, only 5.2% of contracts in repositories, but many different versions





Same was true for Solidity version and other features

Found 246 distinct types in deployed contracts, 1002 in ones in repositories

# CONCLUSIONS

Scamcoins seem common and are harmful to legitimate projects, clear motivation to find them and weed them out

Much easier to innovate when implementing a simpler functionality (using Ethereum) than when creating an entire platform (like Bitcoin)

Paper is available at https://arxiv.org/pdf/1810.08420.pdf

EPSRC

European Commission
HORIZON 2020

# THANKS!
# ANY QUESTIONS?