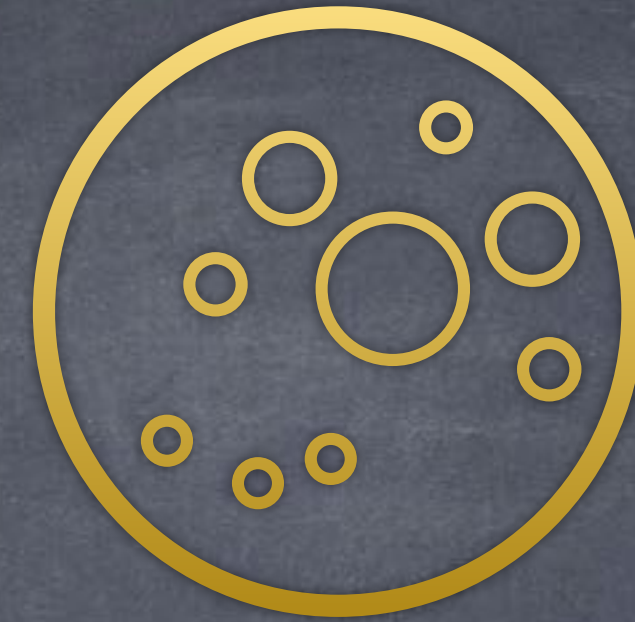
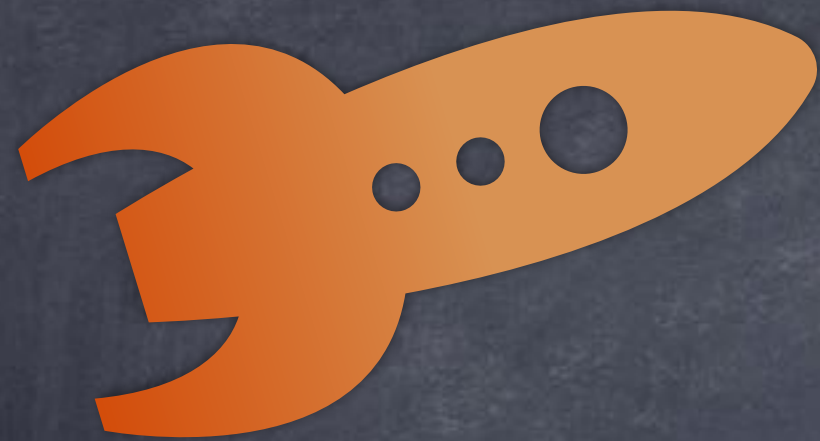
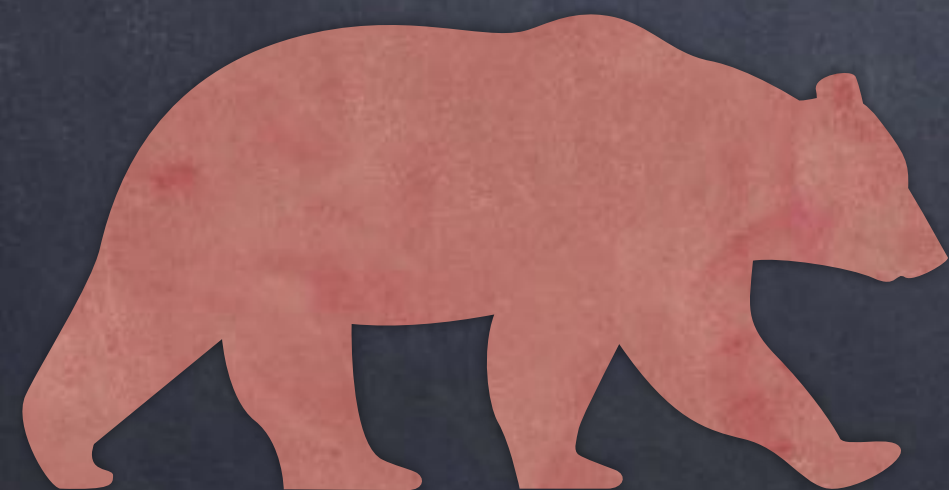
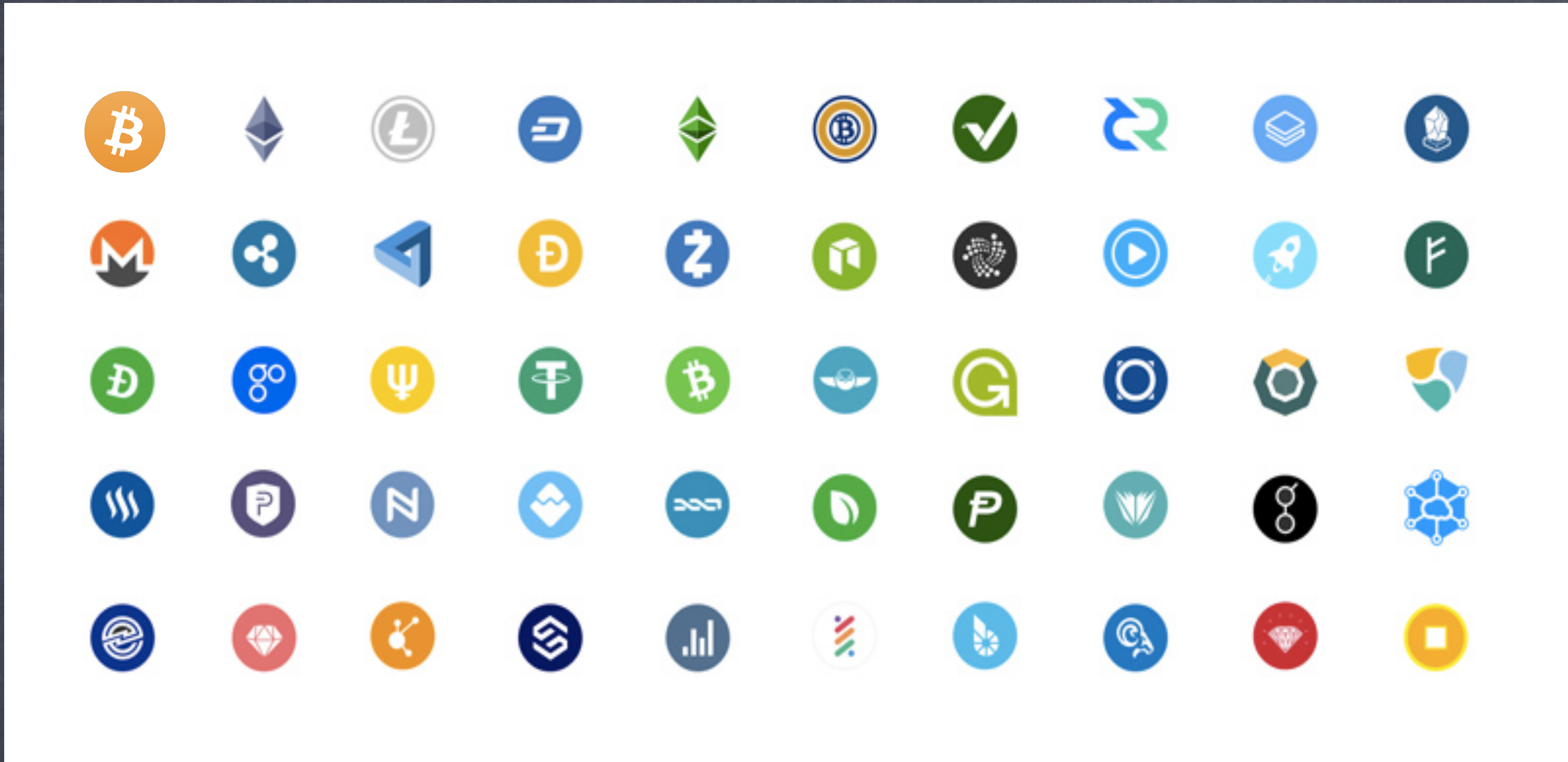




Hacking Deterministic Bitcoin Addresses

Michael McKinnon - @bigmac





This talk is ONLY about Bitcoin

Bro, wanna buy some #sheepcoin?



I won't be outing Satoshi

#whoissatoshi



I'm not a Lawyer,
This is not legal advice.

Just because something is technically
possible doesn't mean it isn't stealing...

...even in a decentralised world.

Secure https://docs.google.com/spreadsheets/d/1xTRCekDerP1TPOB3SOD_1bbQr580BPqohF3YHd096pw/edit#gid=189298223

Dormant Bitcoin Addresses with a balance of 25btc or more

File Edit View Insert Format Data Tools Add-ons Help

100% View only

BlockChain Statistics Report generated by: <https://code.google.com/p/blockchain/>

Written by John W. Ratcliff <mailto:jratcliffscarab@gmail.com>
 Website: <http://codesuppository.blogspot.com/>
 TipJar Address: 1NY8SuaXfh8h5WHd4QnYwpgL1mNu9hHVBT

This Spreadsheet lists all dormant bitcoin addresses with a balance of 25 bitcoins or more.

Days	Value	FirstUsed	LastReceived	LastSpent	TotalSent	TotalReceived	Transaction	Public Key Address	ZombieScore
1,425	79,957.11	3/1/11 10:26	1/20/15 11:21	NEVER	0.00	79,957.11	65	1FeexV6bAHb8ybZjqQMjJreCrHGw9sb6uF	162362905225
1,754	25,150.05	4/5/10 22:47	9/23/14 21:03	NEVER	0.00	25,150.05	27	12ikqA9xSuowkzuERHMWNkSTey55YEBqkv	86604081629
1,644	31,000.05	5/13/10 8:22	1/20/15 11:21	7/24/10 23:35	21,700.00	52,700.05	34	12ib7dApVfyg82TXKyeWBNpN8kfyiANr	83784953248
1,645	19,414.42	7/24/10 12:16	9/7/14 0:31	NEVER	0.00	19,414.42	25	1PeizMg76CF96nUQrYg8xuoZWLQozU5zGW	52335916240
2,162	8,000.00	2/22/09 10:50	9/7/14 0:31	NEVER	0.00	8,000.00	24	195aMu6ZYAczwrESNvNTUMyJ5qkfy4g3Hi	37393954282
1,773	9,260.00	3/18/10 13:37	9/7/14 0:31	NEVER	0.00	9,260.00	48	1H1vaT3zR3oev9ys7Pzp3GH9Cqfg6XYJT	29109078540
986	26,167.05	5/12/12 21:45	10/5/14 19:01	NEVER	0.00	26,167.05	20	1Kf33BbrJDnAVC91w9ACtRgf6KJrLWSkHV	25439502101
1,628	8,999.00	5/9/10 21:35	9/7/14 0:31	NEVER	0.00	8,999.00	6	167ZWTT8n6s4ya8cGjqnNQjDwDOY31vmHg	23850815969
1,497	10,000.01	12/19/10 2:21	9/7/14 0:31	NEVER	0.00	10,000.01	12	12aUjgmXPYsPVHaHrIDnW516hb6gvh4yZq	22410109696
1,497	10,000.01	12/19/10 3:27	9/7/14 0:31	NEVER	0.00	10,000.01	11	1JpggCf3S5eCeYWEDJkYFH7Ruhv4Vp1	22410109696
1,497	10,000.01	12/19/10 1:53	9/7/14 0:31	NEVER	0.00	10,000.01	11	1Du2jAQsBQnkVZkN4ouC46tS78k7WMkVq	22410109696
1,470	10,000.01	1/14/11 18:53	9/7/14 0:31	NEVER	0.00	10,000.01	11	1Le6MkiTvkoeyC1JwYXzQUSfqA3chzGW7N	21609018992
1,392	10,000.01	4/2/11 22:18	9/7/14 0:31	NEVER	0.00	10,000.01	12	1KbrSKrT3GeEruTuuYYUSQ35JwKbrAWJYm	19376657030
1,392	10,000.01	4/2/11 21:08	9/7/14 0:31	NEVER	0.00	10,000.01	11	12L9c9RsAL4ockxa1hB4TCTSmxj2me	19376657030
1,562	7,941.06	4/10/10 16:02	9/7/14 0:31	10/15/10 6:22	6,347.12	14,288.18	72	15Z5YIaaNSxcynvr6uW6jQZ1wq3n1Hn6RX	19374948929
1,361	10,009.26	5/4/11 2:10	1/17/15 9:52	NEVER	0.00	10,009.26	17	1f1mlYFQWTzdLiCBxtHHnNiW7WAWPUccr	18540363867
1,361	10,000.01	5/4/11 1:14	9/7/14 0:31	NEVER	0.00	10,000.01	12	1P11ThxBH542Gmk1kZNXyji4E4wpsSbrt	18523226280
1,361	10,000.01	5/4/11 1:28	9/7/14 0:31	NEVER	0.00	10,000.01	11	1CPaziTqcFixPnSFTdxu74nDGbpFAotZom	18523226280
1,361	10,000.01	5/4/11 2:01	9/7/14 0:31	NEVER	0.00	10,000.01	10	1ucXXZQSEf4zny2HRwAQKvPkLPTUKRtt	18523226280
1,361	10,000.01	5/4/11 1:40	9/7/14 0:31	NEVER	0.00	10,000.01	10	14YK4mzJGo5NKkNmcVJeuEAQhL1795Gcc	18523226280
1,361	10,000.01	5/4/11 2:01	9/7/14 0:31	NEVER	0.00	10,000.01	9	1BAFWQhH9pNkz3mZDQ1tWrtKkSHVCkc3FV	18523226280
1,274	10,689.04	7/30/11 14:06	9/7/14 0:31	NEVER	0.00	10,689.04	10	1FpqQnKQCgDkFMC94JL8FpRyHTZ3uRVZ1	17349129106

TopZombies

<https://bit.ly/2HjT7a9>



Bitcoin Addresses 101

16ga2uqnF1NqpAuQeeg7sTCAdtDUwDyJav

~~3J98t1WpEZ73CNmQvieecnyijwMnqRhWNLY~~

~~bc1qar0srrr7xfkvy516431ydnw9re59gtzzwf5mdq~~

Bitcoin Addresses 101

16ga2uqnF1NqpAuQeeg7sTCAdtDUwDyJav

Generated offline.

An address is something you can prove you created when it comes time to spend.

Bitcoin Addresses 101

Never includes 0, O, I, l

16ga2uqnF1NqpAuQeeg7sTCAdtDUwDyJav

Base58Check decode...

3e546d0acc0de5aa3d66d7a920900ecbc66c20314648aa13

Which consists of...

3e546d0acc0de5aa3d66d7a920900ecbc66c2031 + 4648aa13

(Hash160 + Checksum)

Blockchain Luxembourg S.A.R.L [LU] | https://blockchain.info/address/1EQSPgH9RsNneA1DAUxeVefnGvFQpTtbkE

BLOCKCHAIN

WALLET

DATA

API

ABOUT

Q

BLOCK, HASH, TRANSACTION, ETC...

GET A FREE WALLET

Bitcoin Address

Addresses are identifiers which you use to send bitcoins to another person.

Summary

Address

1EQSPgH9RsNneA1DAUxeVefnGvFQpTtbkE

Hash 160

930865cba078ad34b426bb516790f9e966b42643

Tools

Related Tags - Unspent Outputs

Transactions

No. Transactions

212

Total Received

\$ 599,231.04

Final Balance

\$ 52,783.48

Request Payment

Donation Button



Address =
RIPEMD160(SHA256(Public Key))

Bitcoin
Address

3e546d0acc0de5aa3d6
6d7a920900ecbc66c2031

Public Key

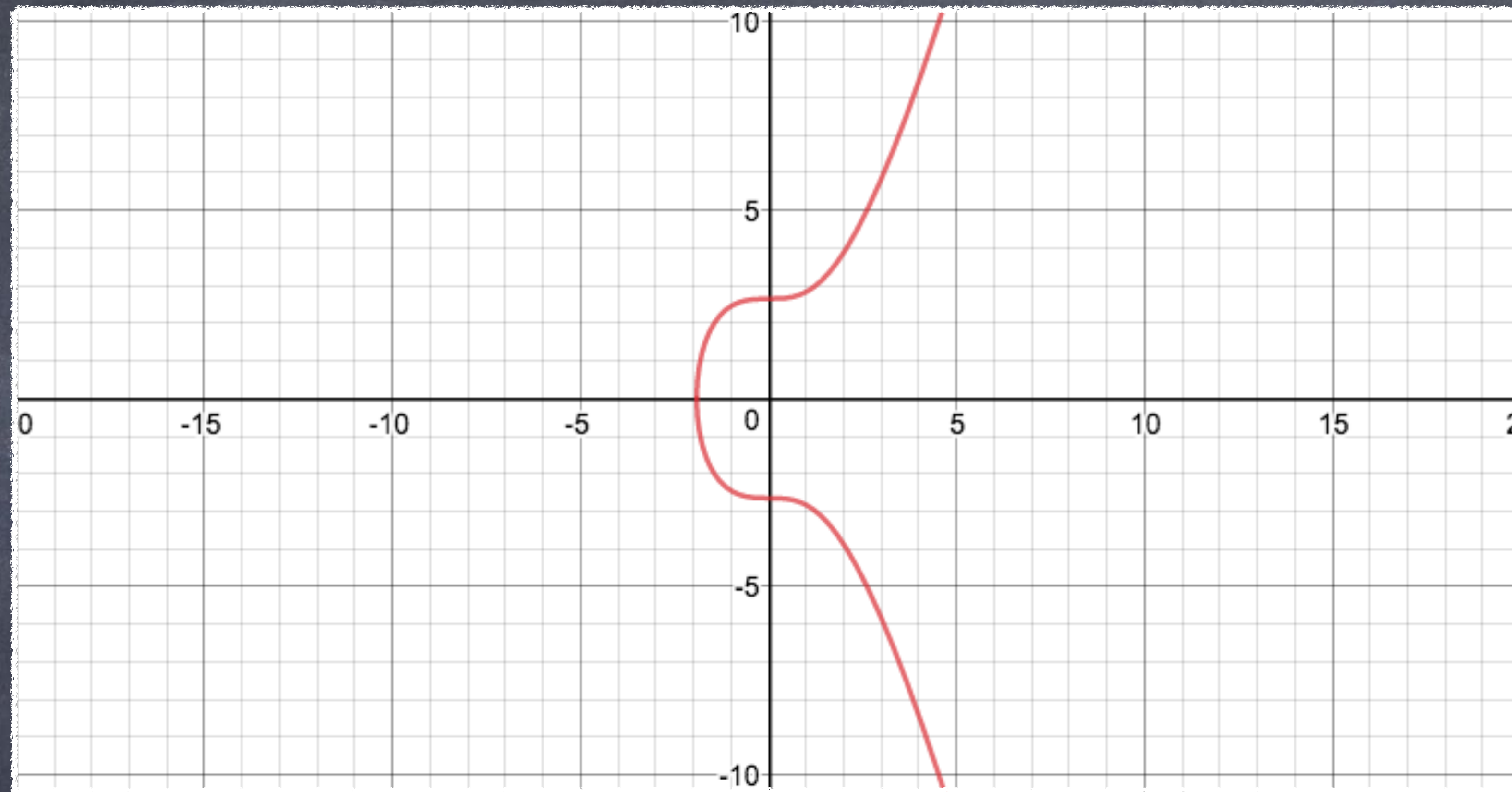
04B568858A407A8721923B89DF
9963D30013639AC690CCE5F555
529B77B83CBFC76950F90BE717
E38A3ECE1F5558F40179F8C950
2DECA11183BB3A3AEA797736A6

Elliptic
Curve
Function



Private
Key





$$y^2 = x^3 + 7$$

Magic stuff happens!

Standards for Efficient Cryptog x

Michael

www.secg.org

Standards for Efficient Cryptography Group

Purpose

The Standards for Efficient Cryptography Group (SECG), an industry consortium, was founded in 1998 to develop commercial standards that facilitate the adoption of efficient cryptography and interoperability across a wide range of computing platforms. SECG members include leading technology companies and key industry players in the information security industry.

Apologies for Site Shut Down

The SECG web site was shut down for repairs in July 2014. The site is being restored.

Documents

Standards for Efficient Cryptography

The main output of SECG are Standards for Efficient Cryptography (SEC) specifications.

The finalized SEC specifications are:

- [SEC 1: Elliptic Curve Cryptography, Version 2.0](#)
- [SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0](#)
- [SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificates](#)

secp256k1

$$y^2 = x^3 + 7$$

"G"

"h"

2.4.1 Recommended Parameters secp256k1

The elliptic curve domain parameters over $\mathbb{F}_p$ associated with a Koblitz curve secp256k1 are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

$$\begin{aligned} p &= \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE} \\ &\quad \text{FFFFFFFF} \\ &= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 \end{aligned}$$

The curve $E: y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ is defined by:

$$\begin{aligned} a &= \text{00000000 00000000 00000000 00000000 00000000 00000000 00000000} \\ &\quad \text{00000000} \\ b &= \text{00000000 00000000 00000000 00000000 00000000 00000000 00000000} \\ &\quad \text{00000007} \end{aligned}$$

The base point G in compressed form is:

$$\begin{aligned} G &= \quad \text{02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9} \\ &\quad \text{59F2815B 16F81798} \end{aligned}$$

and in uncompressed form is:

$$\begin{aligned} G &= \quad \text{04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9} \\ &\quad \text{59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448} \\ &\quad \text{A6855419 9C47D08F FB10D4B8} \end{aligned}$$

Finally the order n of G and the cofactor are:

$$\begin{aligned} n &= \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C} \\ &\quad \text{D0364141} \\ h &= \quad \text{01} \end{aligned}$$

Just pick a number
between 1 and ...

115,792,089,237,316,195,423,570,985,008,687,907,852,
837,564,279,074,904,382,605,163,141,518,161,494,337.

78 digits long.

115 quattuorvigintillion!

So, it's "just" 256-bits...

- So the only thing protecting anybody's Bitcoin is 256 bits of random data?
- That's actually pretty awesomely secure.
- Impossible vs. Improbable.
- Challenge Accepted!





Pool Trophies

Result of Hard FWork.

Below you will find events of significance (newest first) when the pool actually found something.

2017-11-15 01:25:58 UTC

The pool found a private key to `cb66763cf7fde659869ae7f06884d9a0f879a092` (`1KYUv7nSvXx4642TKeuC2SNdTk326uUpFy`) as `0x236fb6d5ad1f43`. At the time of the find, there were **0.54 BTC** on that address. This is #54 of the puzzle transaction.

2017-09-04 16:54:48 UTC

The pool found a private key to `2f4870ef54fa4b048c1365d42594cc7d3d269551` (`15K1YKJMij4fpesTVUcByoz334rHmknxmT`) as `0x180788e47e326c`. At the time of the find, there were **0.53 BTC** on that address. This is #53 of the puzzle transaction.

2017-04-21 12:50:55 UTC

The pool found a private key to `36af659edbe94453f6344e920d143f1778653ae7` (`15z9c9sVpu6fwNiK7dMAFgMYSK4GqsGZim`) as `0xefae164cb9e3c`. At the time of the find, there were **0.052 BTC** on that address. This is #52 of the puzzle transaction.

2017-04-05 02:23:00 UTC

The pool found a private key to `ef6419cffd7fad7027994354eb8efae223c2dbe7` (`1NpnQyZ7x24ud82b7WiRNvPm6N8bqGQnaS`) as `0x75070a1a009d4`. At the time of the find, there were **0.051 BTC** on that address. This is #51 of the puzzle transaction.

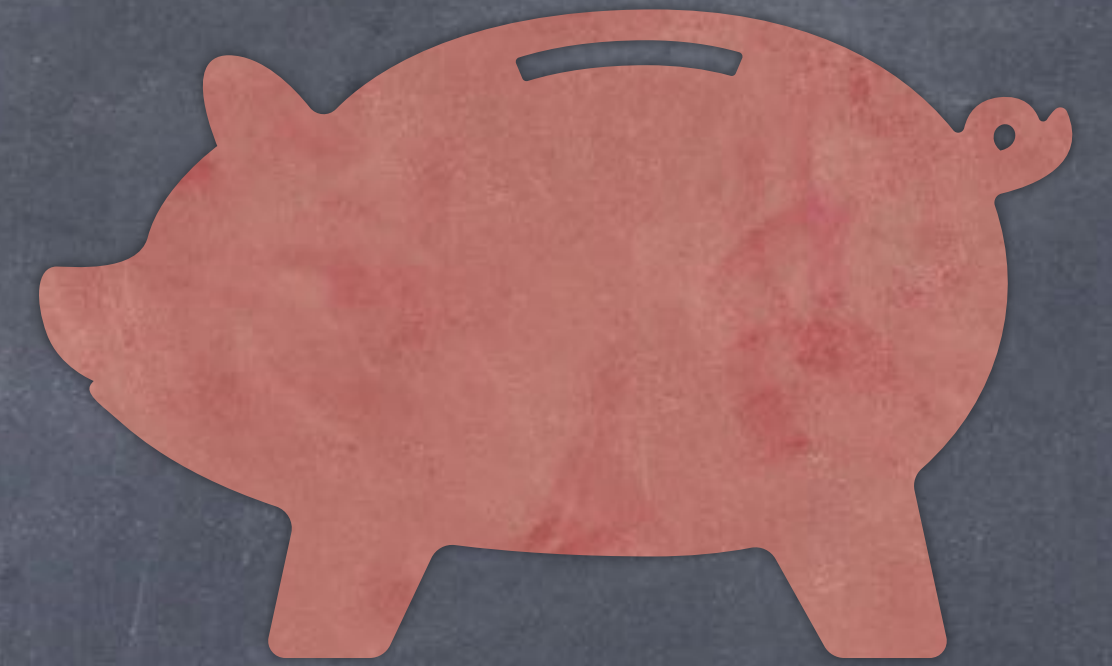
ass



Other than brute-forcing the
key space, what else?



Introducing "Brain Wallets"



Why remember 256-bits of stuff,
when you can just remember a password!

What could possibly go wrong?

"password"

- SHA256("password")

5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

- As a Bitcoin address?

16ga2uqnF1NqpAuQeeg7sTCAdtDUwDyJav

The address for "password" has been used 45,010 times!

Brainwallet - password Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	16ga2uqnF1NqpAuQeeg7sTCAdtDUwDyJav
Hash 160	3e546d0acc0de5aa3d66d7a920900ecbc66c2031
Tools	Related Tags - Unspent Outputs

Transactions		
No. Transactions	45010	
Total Received	\$ 2,418.13	
Final Balance	\$ 0.00	

[Request Payment](#) [Donation Button](#)



Okay, time to build.
a.k.a Designing the Bitcoin Death-ray.

Bitcoin
Server
(bitcoin core)

Passwords
Lists

Other
stuff?

parse blk*.dat files
(rusty-blockparser)

generate deterministic
addresses
(btcthumper, file2addr)

sort | uniq bitcoin "1*" addresses
(340,086,675)

Match?

Lists of sorted
generated addresses





Password Lists?

Get a big password dump list...

Results

193,230,656 addresses, found = 12,421 (0.0064%)

"Passwords" Found

kkkkkkkkkkkkkkkkkkkk - 0.005 BTC

12EMX7CANb7iGu4SMb3MTEg3oZ6Trz1gUF

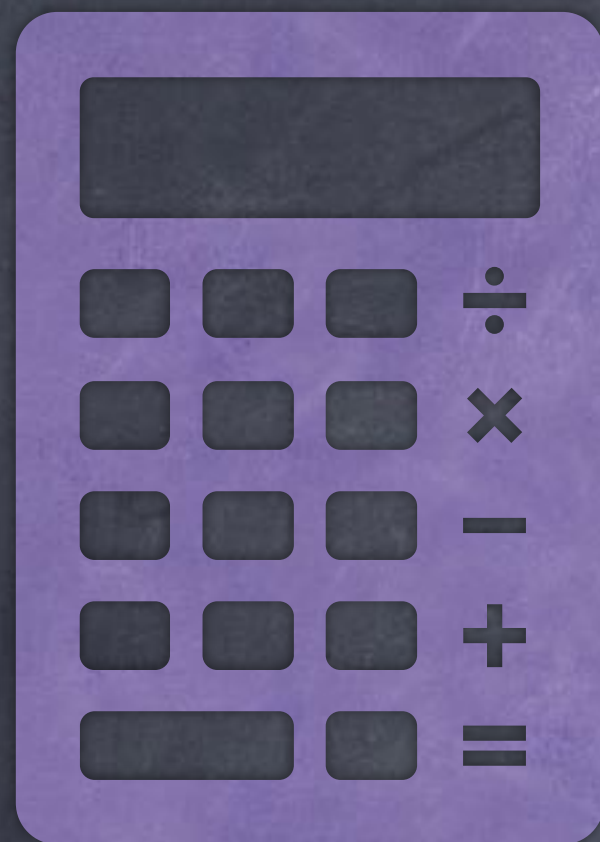
deadsheep - 14.299101 BTC

12P5JTb5kWF5h8kRCwTjTYXbwQ7RKoo5kb

asdfghjklouiutrewq - 18.24654206 BTC

19jcvAMdZvFJcrDzzvox6pjQK9fHSqfhMw





Numbers?

Generate lots of numbers... i.e. PIN, Passcode

0 ... n

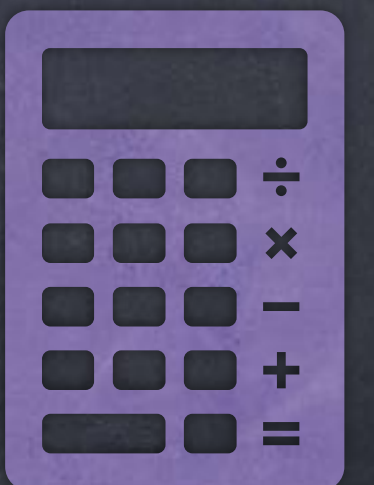
Results

0 to 15,000,000 addresses, found 37 (0.00025%)



Number Results!

0, 1, 2, 6, 39, 42, 52, 66, 83, 111, 123, 398,
420, 666, 1234, 1324, 1337, 1728, 2007, 2539,
5000, 8419, 12345, 30000, 31337, 123123,
123456, 123654, 198921, 324855, 345644, 424242,
491278, 1234567, 12345678, 8964009, 9017002





Birthdates?

Generate birthdates from 1/1/1900 – 19/6/2020

19000101, 01011900, 1900-01-01, 01/Jan/1900

Results

70,400 addresses, found 3 == 0.0043%

Birthdaydates Found

28081967 – 0.005 BTC

1DEihioBnxj9EMG8A97vDTXZurzQusCQw

02011980 – 0.001 BTC

1Bosy3yuTPiT3MMEAk9RSn3iLkZA9mvGGm

20051981 – 0.01 BTC

1Mt2sKNWhYiDZ7wBh4guZJur44acV3Pr4s





Epoch?

Generate epoch timestamps...

i.e. 1415319076 = Friday, 7 November 2014 12:11:16AM

Results

9,095,889 addresses, found 0

What else?

```
0011
1000
101
PASTEBIN + new paste trends API tools faq search...

25. Experiment 1
26. -----
27.
28. My first experiment was to see if anyone used a block hash as a private key. That would actually be a nifty way to 'compress' 32
    bytes in your head. You would only have to remember the block height (which is only maybe 6 digits) and the corresponding larger
    32 byte number would be saved for all time in the chain itself!
29.
30. Results: Success! I found 46 addresses that had some amount of bitcoin sent to them between 2009 and 2016. As expected, these all
    had 0 balances either because the owner had taken them back or they were discovered by someone else.
31.
32. Here are two examples. You can use blockchain.info to see these hex values are actually block hashes from early in the chain. This
    happened on/off up until mid-2016.
33.
34. 1Buc1aRXCqdh6r7PRYWPAy3EtVFw5Ue5dk 000000006a625f06636b8bb6ac7b960a8d03705d1ace08b1a19da3fdcc99ddbd
35. 1KLZnkqU94ZKpgtcWCRs1mhqtF23jTLMgr 000000004ebadb55ee9096c9a2f8880e09da59c0d68b1c228da88e48844a1485
36.
37. Nothing really alarming so far.
```

<https://pastebin.com/jCDFcESz>



Block hashes?

Oh no, he's about to mention "blockchain"...

```
00000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
```

Results

500,000 addresses

Method 1 "String": found 0

Method 2 "Binary": found 0

Method 3 "Double SHA256": found 0

(Not sure why my results didn't match the Pastebin post)

Other Experiments...

- Different encoding - what other deterministic things could produce 256 bit output? i.e. 1/2 of a SHA512
- Multiple iterations of encoding - SHA256("password") x 1,975 times.
- Previous transaction ID's
- Consider dev mistakes that might get made...



Oops...?

BLOCKCHAIN**WALLET****DATA****API****ABOUT**

Q BLOCK, HASH, TRANSACTION.

Jeff was here

Addresses are identifiers which you use to send bitcoins to and receive

Summary		Transactions	
Address	1HZwkjkeaoZfTSaJxDw6aKkxp45agDiEzN	No. Transactions	309 
Hash 160	b5bd079c4d57cc7fc28ecf8213a6b791625b8183	Total Received	\$ 465,123.79 
Tools	Related Tags - Unspent Outputs	Final Balance	\$ 0.00 

[Request Payment](#)[Donation Button](#)

```
echo -n "" | shasum -a 256
```

Other Weaknesses?

(time permitting)

Public Key Collision?

- The HASH160 value is only 160 bits long, but it's derived from a 256 bit input.
- Theoretically, more than one public key could result in the same HASH160 value.
- Who knows what the future may hold.



Much Randomness

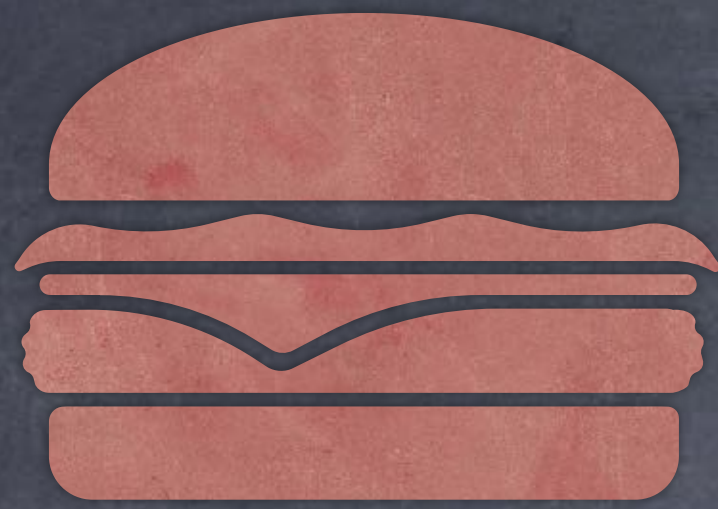
- `java.util.Random()`
- Opportunities to look for any weaknesses in generating private keys.



ECDSA Exposure

- Bitcoin addresses rely on ECDSA to verify transactions.
- ECDSA uses a random value to generate the signature.
- <http://www.nilsschneider.net/2013/01/28/recovering-bitcoin-private-keys.html>





Take Aways



- Problem applies to many other cryptocurrencies
- Managing keys is hard (i.e. PGP), Hardware Wallets?
- Which path to take?

Massive Rainbow-Like table,
monitor P2P transactions,
and MONEY GRAB.

White-Hat Services to warn
people about lame arse
addresses? Bridge the gap.

Such a waste...

BLOCKCHAIN**WALLET****DATA****API****ABOUT**

Q BLOCK, HASH, TRANSACTION

Bitcoin Address

Addresses are identifiers which you use to send bitcoins to

Summary

Address

1111111111111111111111114oLvT2

Hash 160

00

Tools

Related Tags - Unspent Outputs

Transactions

No. Transactions

52436



Total Received

\$ 503,177.08



Final Balance

\$ 503,177.08



Request Payment

Donation Button

Thank You!

