RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: BAC-R03

Raiding Lost BTC and Other Cryptocurrencies

Konstantinos Karagiannis

CTO, Security Consulting
BT
@KonstantHacker

Is Bitcoin dead?

Opinion: Bitcoin is close to becoming worthless

By Atulya Sarin
Published: Dec 4, 2018 5:05 p.m. ET

304

Bitcoin is now entering a death spiral

Just one year has passed since bitcoin enthusiasts forecasted that the cryptocurrency would hit a price of $1 million.

Is Bitcoin Dead?

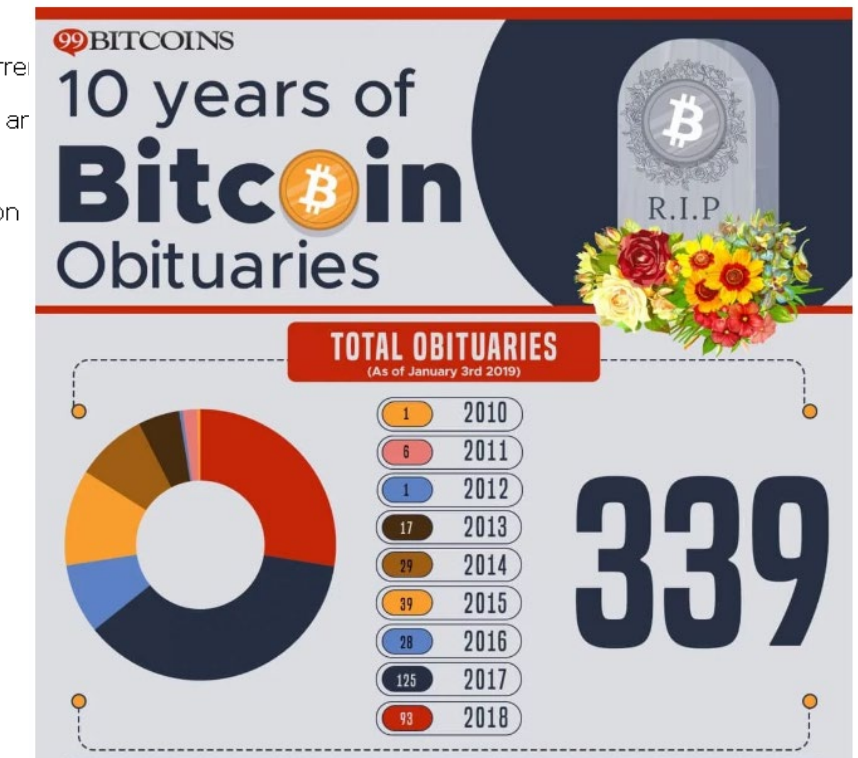
Dec. 8, 2018 2:35 PM ET | 5 Likes | Includes: BTC-USD

Katusa Research
Commodities, energy, dividend growth investing, gold & precious metals
Katusa Research

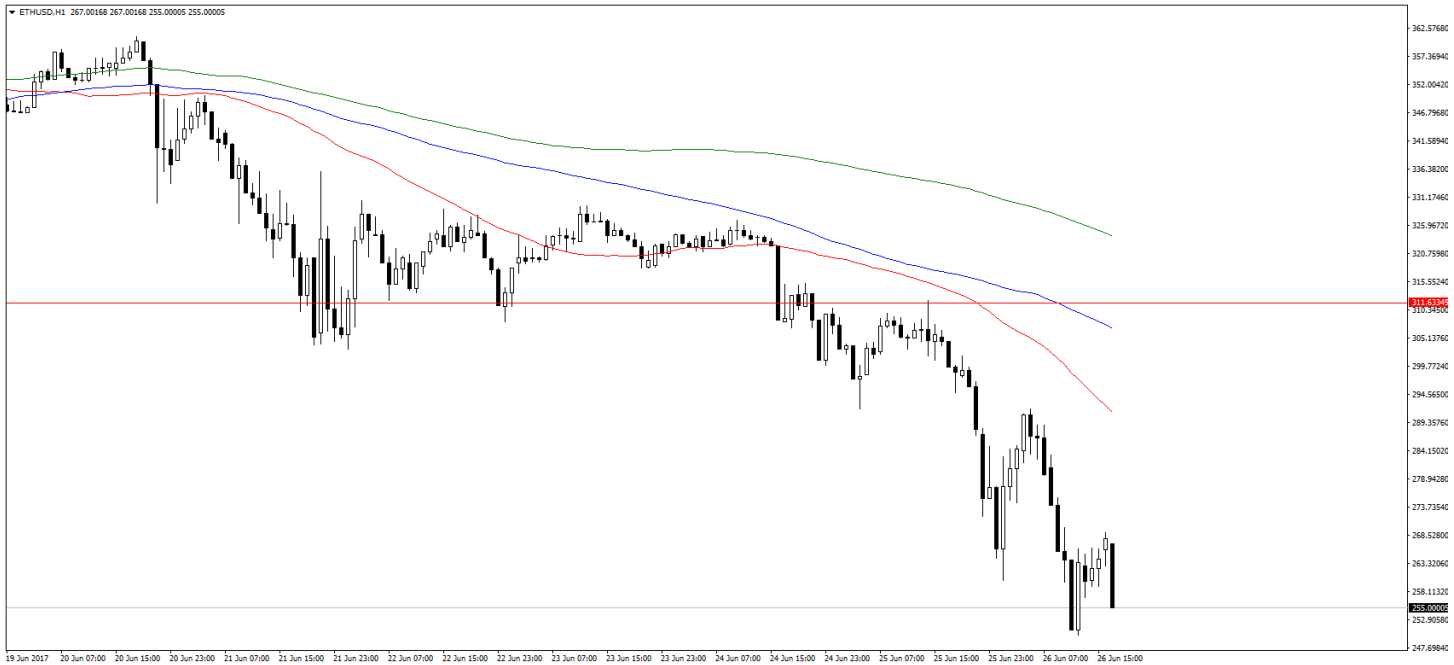
Follow
(758 followers)

Summary

- What will happen to Bitcoin and cryptocurre
- The Bitcoin aftermath - will there be new ar emerge from crypto ashes?
- Here's where the Blockchain 2.0 Revolution



It's still a lot of money, folks…

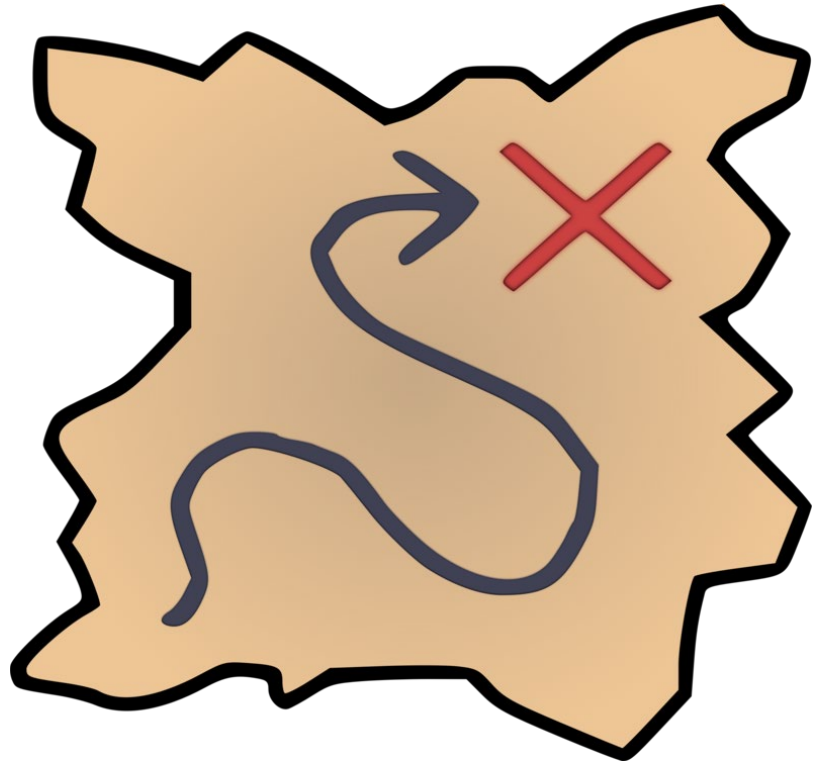


- 4 million BTC
- Only 21 million can be mined by 2140
- Almost 20%, plus other crypto

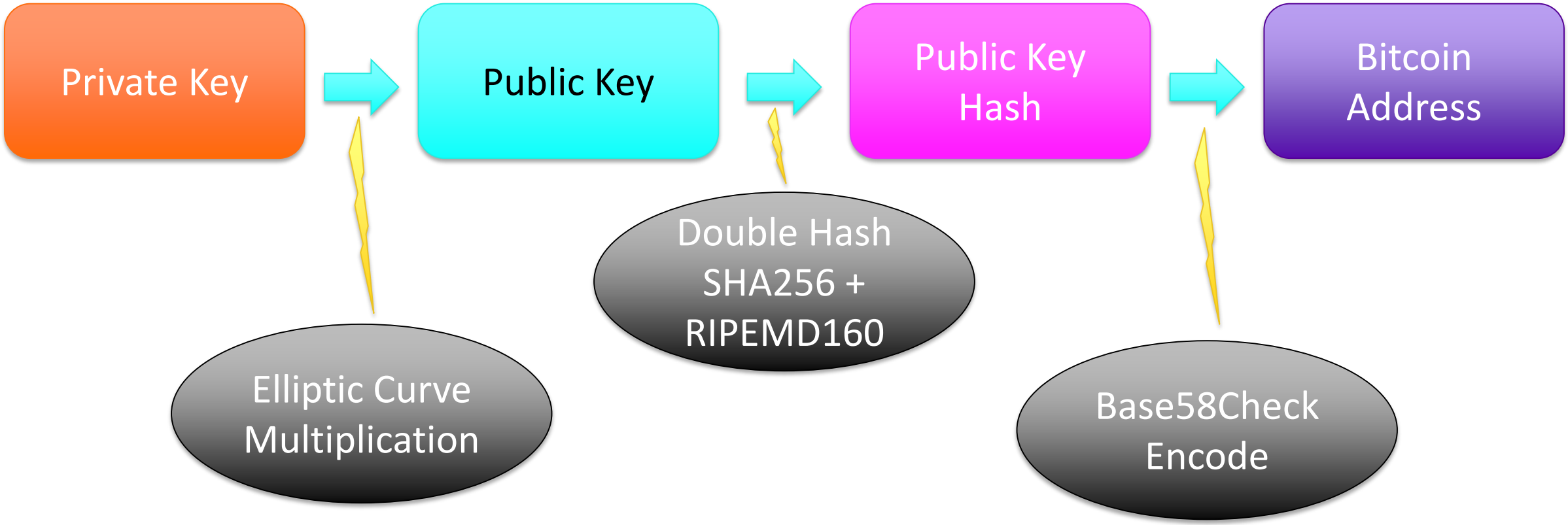
Why so many BTC and other coins are lost

- Failed hard drives
- Forgotten passphrases
- “Suicidal” hacks (Parity)
- Death

A word before we proceed



How Bitcoin private keys work



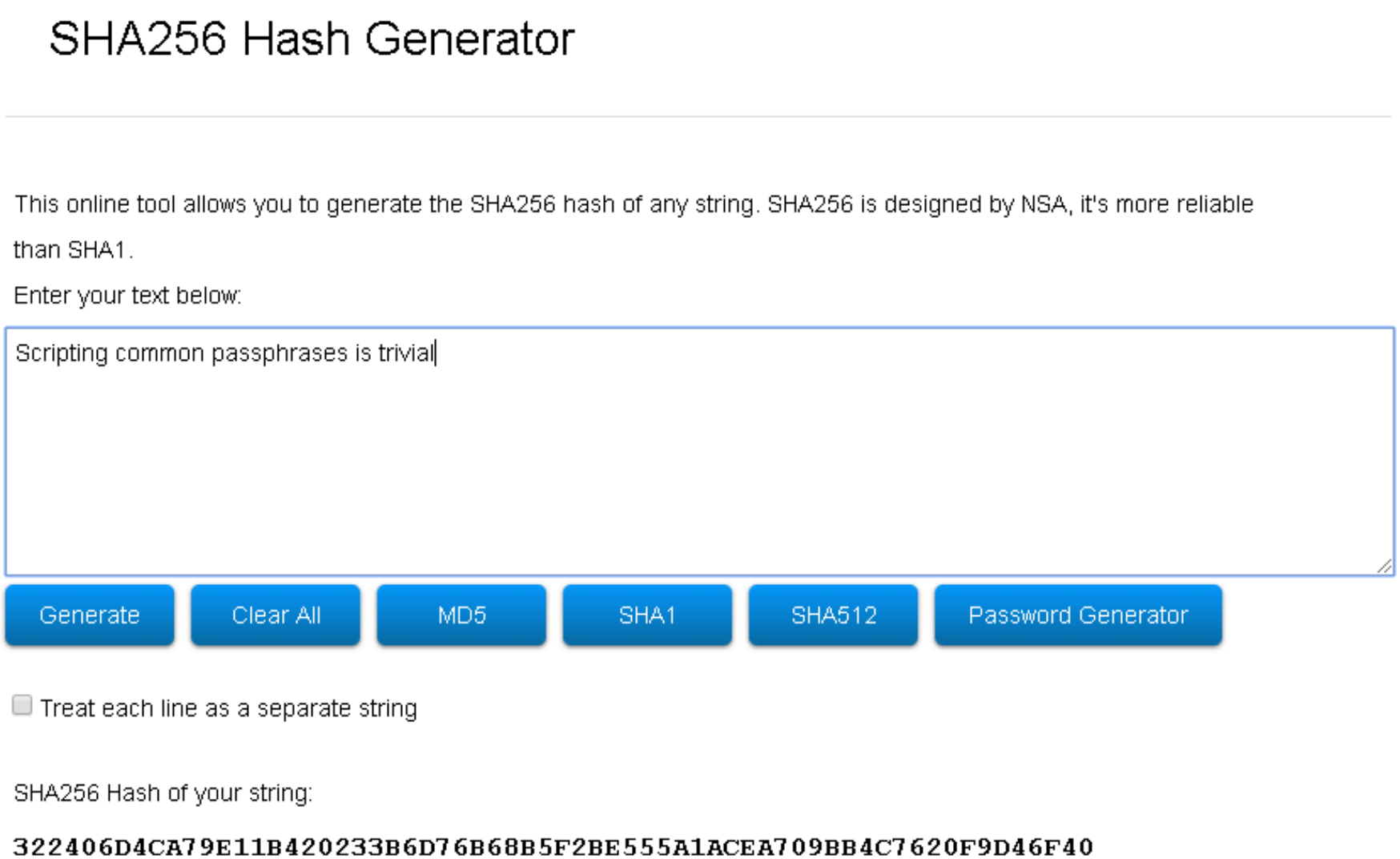
Finding the right strings

"The Legend of Satoshi Nakamoto" art puzzle

Passphrases and other insecure ways to generate keys

- “These are not the droids you’re looking for”
- Block hashes
- Merkle root
- Repeated SHA256
- SHA256 of another public address (over 100 found)

Not a way to go



Large Bitcoin Collider

Pool Trophies

Result of Hard ~~F~~Work.

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.

Finding keys by address collision

- Given a bitcoin address from a random(unknown) private key of numeric value between 2^{160} and 2^{256}, find another private key in the interval between 0 and 2^{159} which will evaluate to the same bitcoin address.
- Too much for one machine

Using forensics on abandoned hard drives

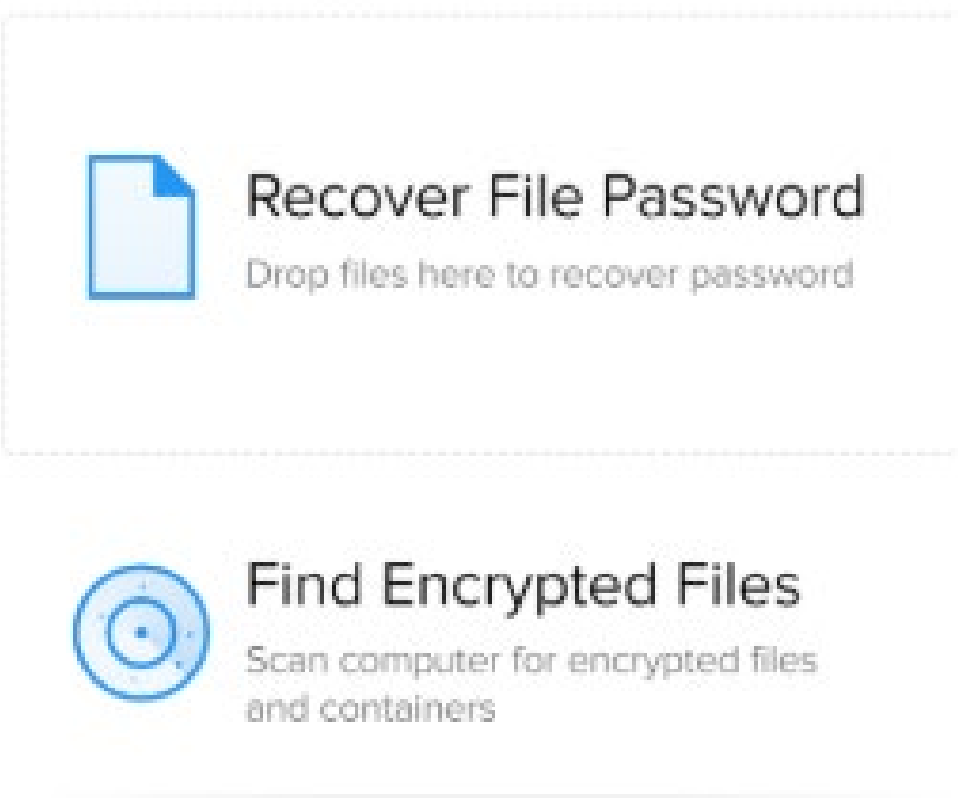
Maybe use a live Linux distro and risk it?

Forensic search terms

- Wallet.dat
- debug.log
- Db.log
- peers.dat
- Blocks
- Chainstate
- database

Tools

- Open Source like CAINE
- Passware Kit Forensic ($1000, bruteforces wallet passwords)
- Magnet Internet Evidence Finder
- Forensic Toolkit (FTK)
- EnCase



Corrupt wallet recovery

- pywallet

```
python pywallet.py –
dumpwallet > wallet.text
```

- bitcoinj and mvn

```
wallet-tool dump –dump-
privkeys –wallet=~/wallet-
decrypt.dat > wallet.txt
```

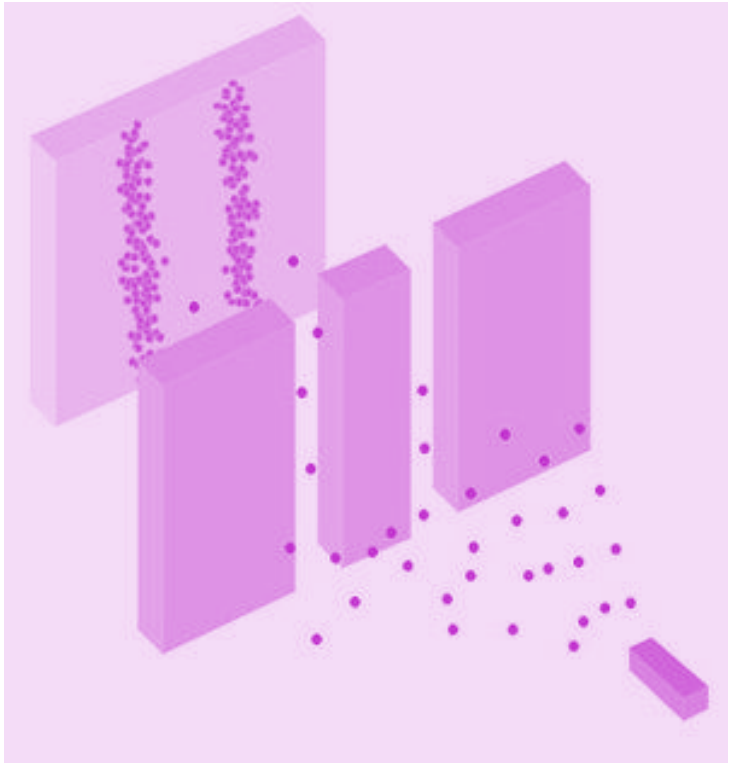
- Hex editor search for 0201010420

Key backups exposed online

```
0xDUDE@DESKTOP-1O1F032:~$
0xDUDE@DESKTOP-1O1F032:~$ grep wallet.dat AWS-S3-bucket-scan-15-01-2018
<Public> http://s3.amazonaws.com/[redacted]/btc/3012/wallet.dat
<Public> http://s3.amazonaws.com/[redacted]/btc/4314/wallet.dat
<Public> http://s3.amazonaws.com/[redacted]/btc/4783/wallet.dat
<Public> http://s3.amazonaws.com/[redacted]/btc/4811/wallet.dat
<Public> http://s3.amazonaws.com/[redacted]/btc/4839/wallet.dat
0xDUDE@DESKTOP-1O1F032:~$
0xDUDE@DESKTOP-1O1F032:~$
```

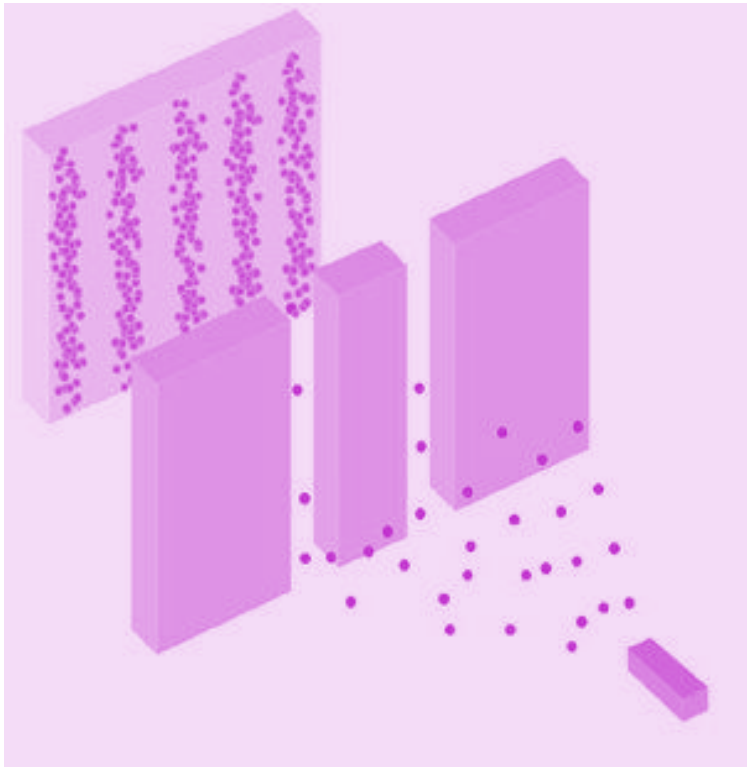
Quantum threats—from room size to tabletop

Quantum primer on particle-wave duality



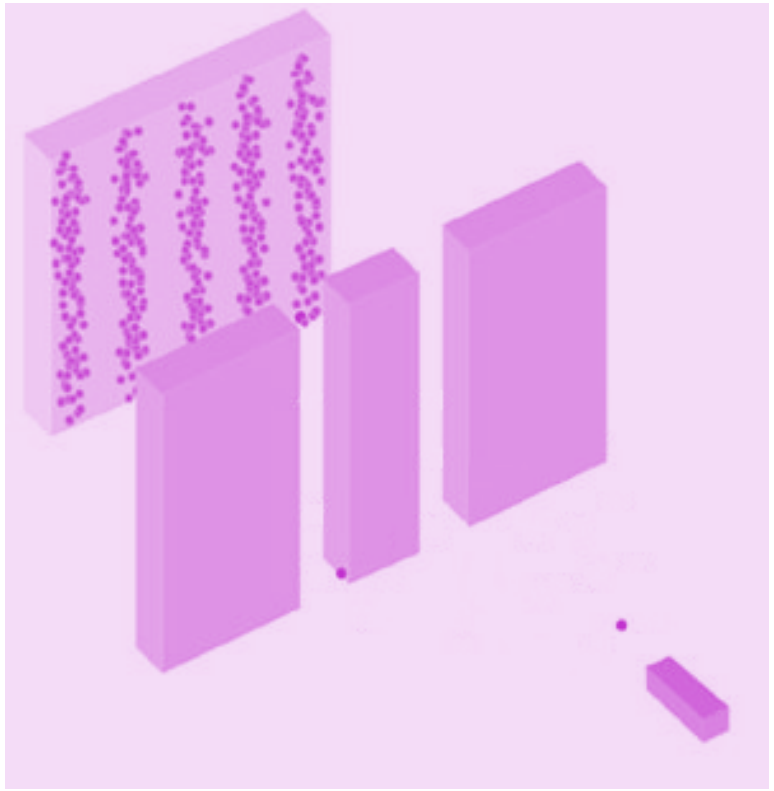
Expected particle behavior (“pooling”)

Quantum primer on particle-wave duality



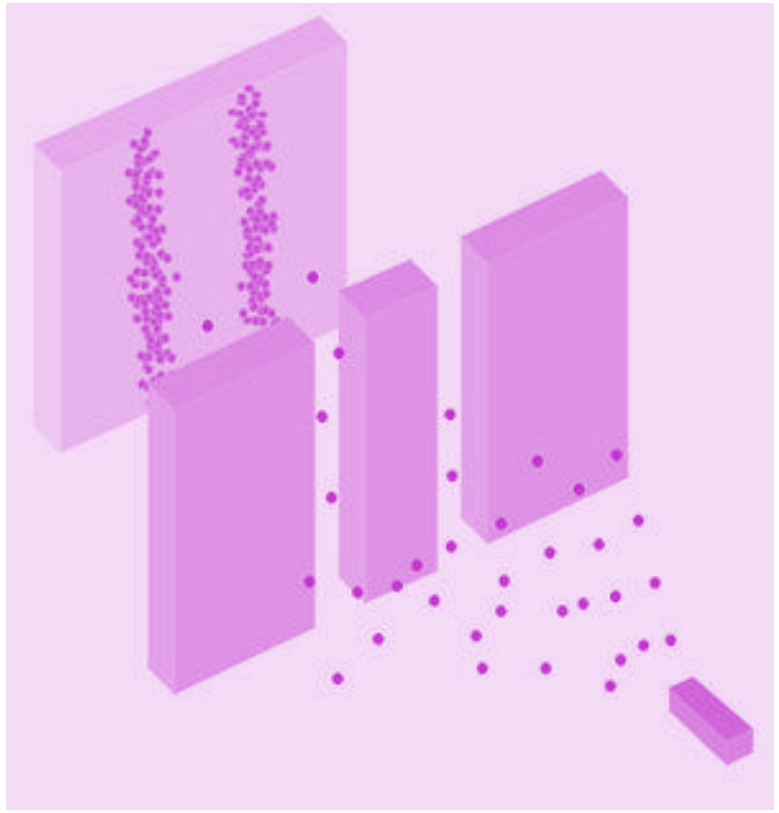
Wave pattern without observation of which slit particle goes through

Quantum primer on particle-wave duality



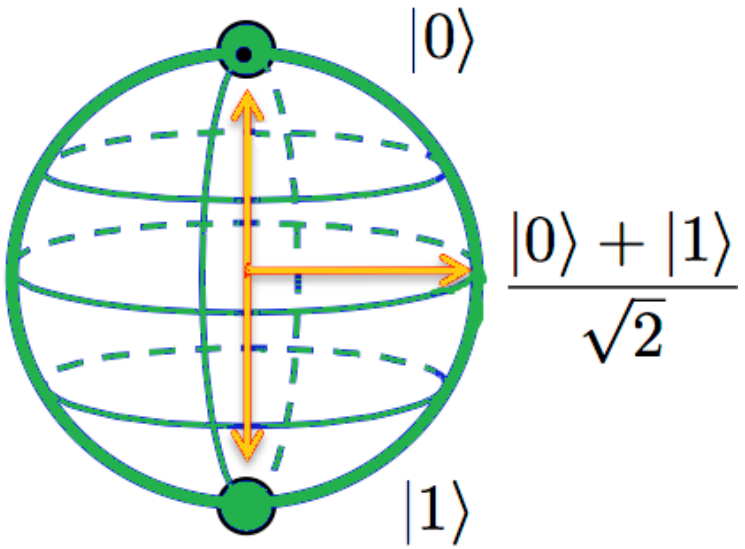
Even one particle at a time creates wave pattern

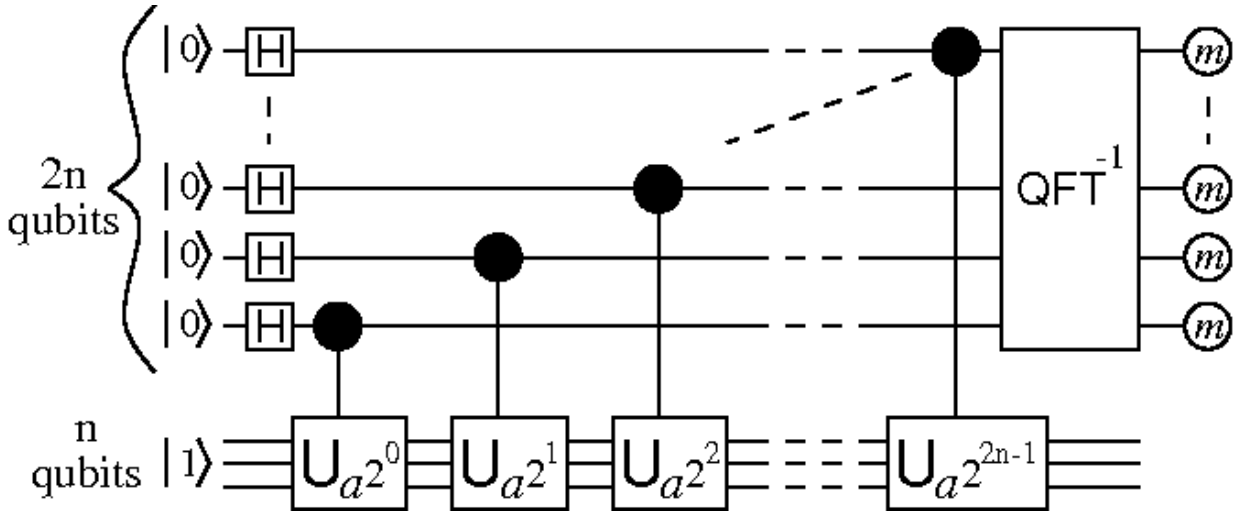
Quantum primer on particle-wave duality



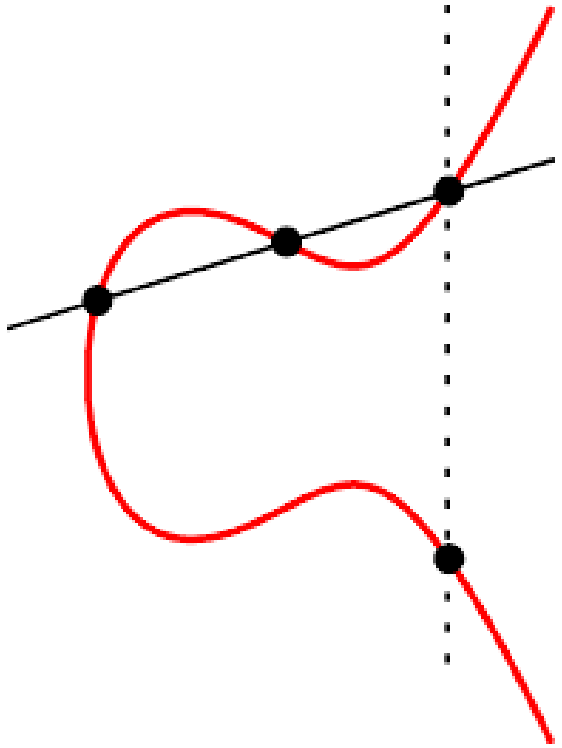
Use a detector on either slit, and pooling appears: particle-wave duality

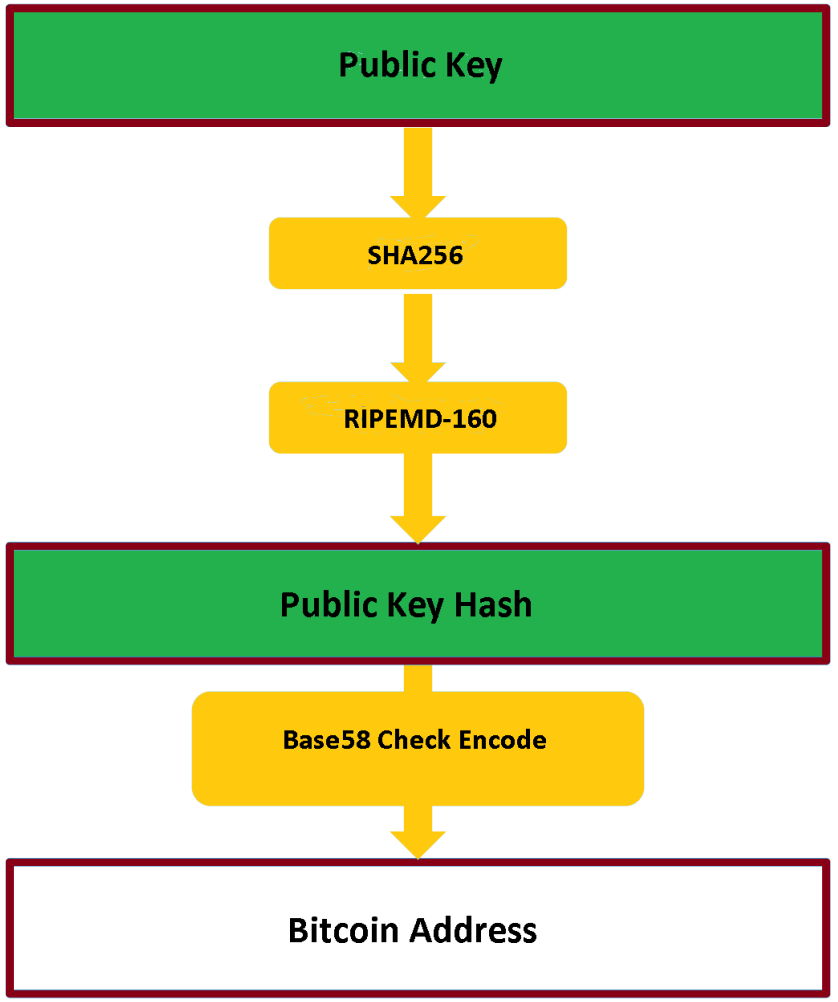
Qubits and quantum algorithms





Cracking ECC encryption





Mining with quantum algorithms?

1: **procedure** QUANTUM MINING STRATEGY
2: $B \leftarrow$ the tip of the unique longest block-chain, and $k \leftarrow$ the current target
3: **loop**
4: Propagate B to all neighbors
5: Create a candidate template for a block B_{mine} without a nonce, with the parent B
6: Define $f(x) = \begin{cases} 1, & \text{if } H(B_{mine}, x) \leq k \\ 0, & \text{otherwise.} \end{cases}$
7: Sample Q according to some distribution
8: **for** $i = 1, \ldots, Q$ **do**
9: Apply 1 Grover iteration, with respect to the function f
10: **if** a new block B_{other}, which is the tip of the unique longest block-chain, is received **then**
11: set $B \leftarrow B_{other}$
12: **if** *agressive* **then**
13: **goto** line 19
14: **else if** *peaceful* **then**
15: **goto** line 4
16: **end if**
17: **end if**
18: **end for**
19: Terminate Grover's algorithm. If it terminated with a succesful output x (i.e., an output x for which $f(x) = 1$, or alternatively, $H(B_{mine}, x) \leq k$ then set $B \leftarrow (B_{mine}, x)$
20: **end loop**
21: **end procedure**

Be safe … and keep it legal!

- This is crypto research in both uses of the term. Up to you to use it legally.
- Protect your own cryptocurrencies from accidental loss or theft:
  - Keep wallets backed up and encrypted
  - Only keep as much crypto on your phone as you'd keep cash in your pocket. Store majority in cold storage or a hardware wallet
  - Use password managers
  - Use two-factor auth on any accounts
  - Speak with estate lawyer about how to handle your crypto after…
- Keep an ear to the quantum grapevine. Not kidding.