Bitcoin

Abrahim Ladha

March 13, 2019

r/bitcoin
MAGIC
Internet
Money
Join us

Motivation

- History of mining
- ASICs, design and resistance
- Bitcoin Core vs Bitcoin Cash
- Bitconnect

Recall

$$x \overset{?}{\leftarrow} X$$

$$(H(x|...) < 2^{\lambda - d})?\ \text{return } x$$

$$\text{else loop}$$

Some properties

- You have an economic incentive to speed this up.
- Supposed to be “one cpu one vote”
- Permanent arms race
- Paralizability
- Incompressibility

Parallelization

- Lots of threads are very useful
- Each thread does little work
- threads don't depend on each other

Incompressibility

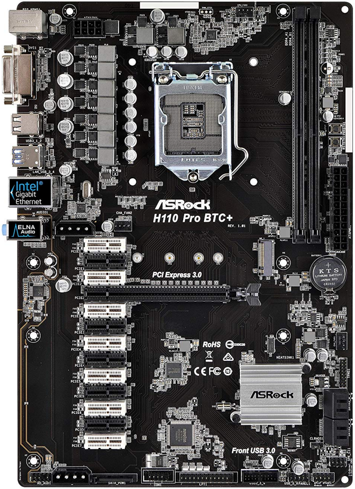
- Shouldn't exist a faster algorithm to solve
- Only way is to repeatedly guess and verify
- Only speedups you can get are from hardware, or from toy optimization
- No serious tricks allowed

2009-2009

- CPU mining exclusively
- Individuals could solve blocks easily
- This didn't last long

2010-2012

- Turns out GPUs are really good at this
- hundreds of weak cores
- each computing a single arithmetic operation.
- bitshifts require two cores but this is still okay.
- Adding more GPUs scales perfectly
- Not bottlenecked on PCIe, CPU, network, or disk.



ASRock
H110 Pro BTC+
REV. 1.01
PCI Express 3.0
Intel Gigabit Ethernet
ELNA Audio
RoHS
Front USB 3.0
KTS LITHIUM BATTERY JAPAN STD CR2032
ASRock

Recall

```
$x \overset{?}{\leftarrow} X$
$(H(x|...) < 2^{\lambda-d})$? return $x$
else loop
```

GPU wars

AMD	NVIDIA
7850	GTX TITAN
1GB/2GB	6GB
March 2012	Feb 2013
$250	$1000
411kH/s	320 kH/s

ASICs

- Application Specific Integrated Circuit
- SHA256 is really just a circuit, about 10k gates
- CPUs/GPUs can do general computation. If you know the computation task, can you optimize at the hardware level?
- Deep Blue

ASICs are bad?

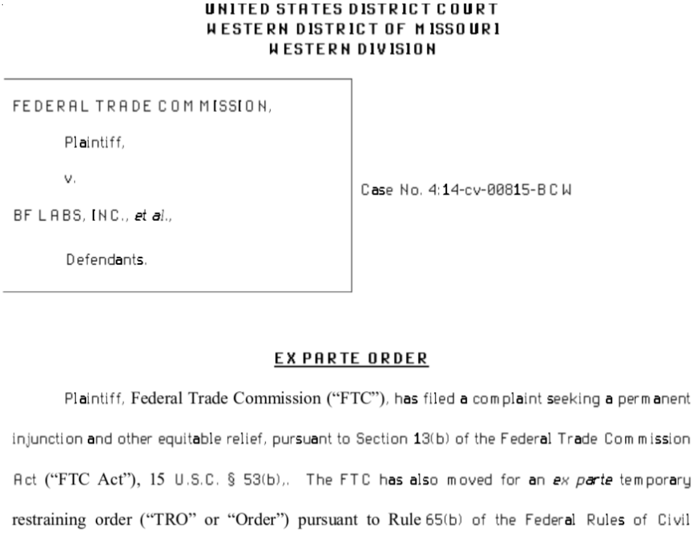
- Mining dependent on GPUs screws up the GPU market
- GPUs have other uses besides mining, so they can be repurposed.
- Once ASICs are unprofitable, they are bricks.
- Selling ASICs doesn't even make sense.
- Why would someone sell you a machine that prints money, when they could just keep it and print the money?

ASICs are bad

- Secret Mining
- You keep delaying shipment mining with a customers preorder and finally shipping it when its unprofitable
- Flooding
- You sell enough hardware to increase the difficulty to make them unprofitable

Secret Mining - Butterfly Labs

- Took preorders for the first bitcoin ASICs
- Made them, used them for 18 months, then finally gave them to customers
- By this time, the difficulty had increased to the point they were unprofitable



UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

BF LABS, INC., *et al.*,

Defendants.

Case No. 4:14-cv-00815-BCW

EX PARTE ORDER

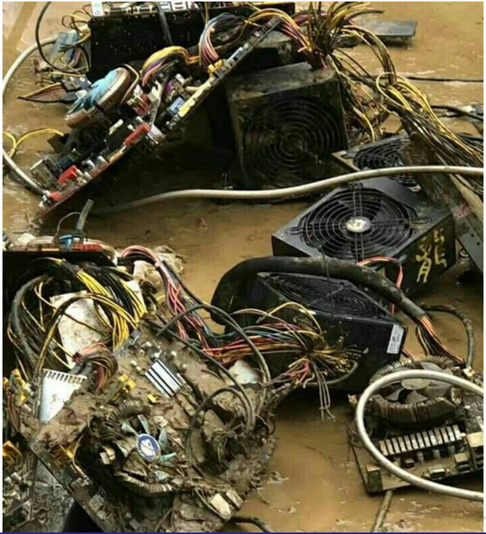
Plaintiff, Federal Trade Commission ("FTC"), has filed a complaint seeking a permanent injunction and other equitable relief, pursuant to Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b),. The FTC has also moved for an *ex parte* temporary restraining order ("TRO" or "Order") pursuant to Rule 65(b) of the Federal Rules of Civil

Flooding - Bitmain A3

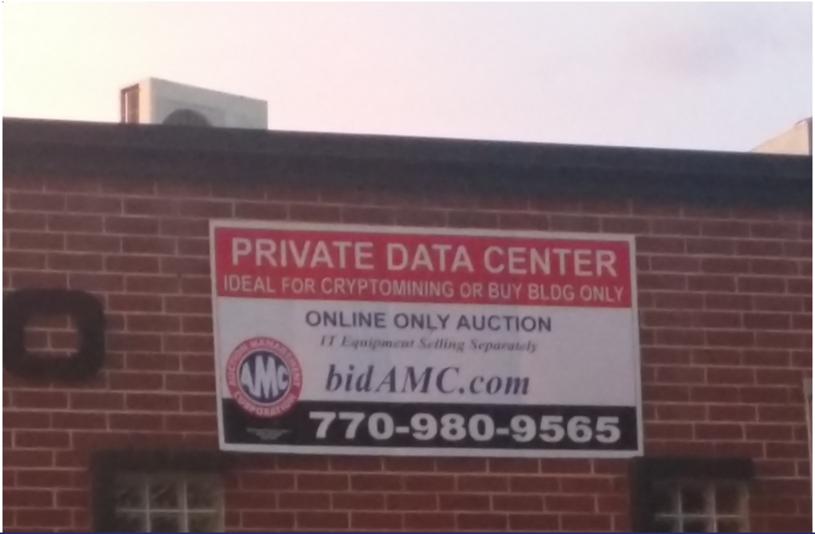
- Sell the first batch extremely fast
- People all over youtube claiming they made $800 a day
- Mania insues
- Huge orders of batch 2
- enough that it is more profitable to sell them than it is to mine with them
- The people who would buy these will never make their money back

Encourage Centralization

- You had bigshot GPU miners before
- but they didn't make up such large percentages of the hash rate
- With GPUs, you have thousands of little guys mining at home
- Big players mean big points of failure



龍


PRIVATE DATA CENTER
IDEAL FOR CRYPTOMINING OR BUY BLDG ONLY
ONLINE ONLY AUCTION
IT Equipment Selling Separately
AMC
AUCTION MANAGEMENT CORPORATION
bidAMC.com
770-980-9565

Litecoin

- Litecoin comes around 2011
- If Bitcoin is gold, Litecoin is silver
- Touted “Asic-resistance” as a feature
- Modified scrypt algorithm instead of SHA256

Recall

$$x \overset{?}{\leftarrow} X$$

$$(H(x|\ldots) < 2^{\lambda-d})\text{? return } x$$

$$\text{else loop}$$

2013-2015

- Eventually the whole cycle repeated
- People CPU mined for a day
- GPU mining dominated for a long time
- Eventually, scrypt ASICs were developed

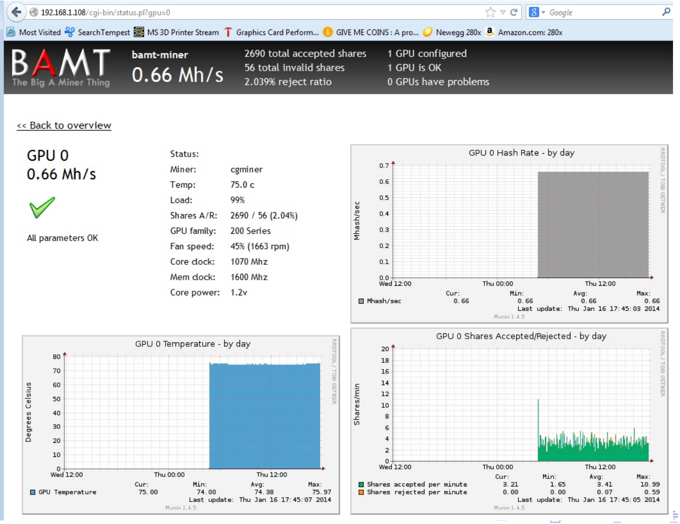
Dogecoin

- Dogecoin was a fork of Litecoin
- 100 Billion ($+\infty$) possible coins
- Community was a joke, but had the largest following

Dogecoin

- Weird implementation details on purpose.
- This is good and bad.
- Deviation from the norm invites exploits, but it can also be funny.
- Block value halfs to have the 100 billion mined in a year
- Block value no longer decreases, is now fixed, making the cap technically infinite
- ?????????

bam



bamt-miner
0.66 Mh/s

2690 total accepted shares
56 total invalid shares
2.039% reject ratio

1 GPU configured
1 GPU is OK
0 GPUs have problems

<< Back to overview

GPU 0
0.66 Mh/s

All parameters OK

Status:	
Miner:	cgminer
Temp:	75.0 c
Load:	99%
Shares A/R:	2690 / 56 (2.04%)
GPU family:	200 Series
Fan speed:	45% (1663 rpm)
Core clock:	1070 Mhz
Mem clock:	1600 Mhz
Core power:	1.2v

GPU 0 Hash Rate - by day

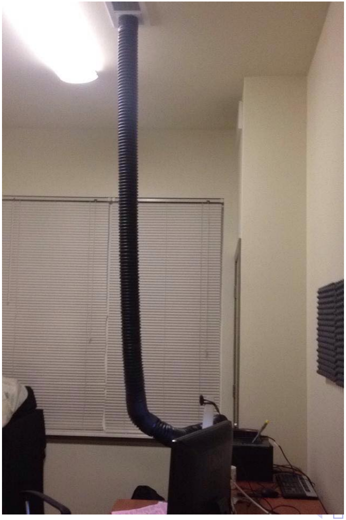
```
               Cur:      Min:       Avg:       Max:
■ Mhash/sec    0.66      0.66       0.66       0.66
                     Last update:  Thu Jan 16 17:45:03 2014
```

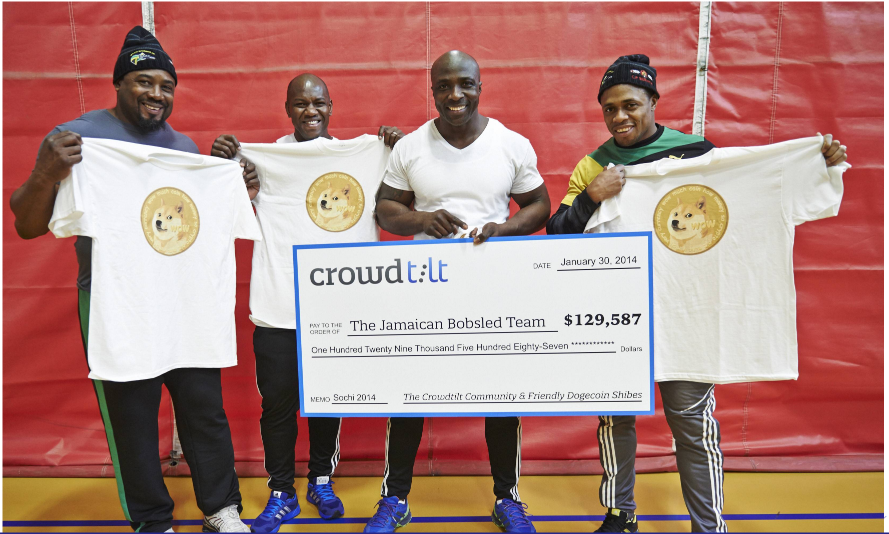
GPU 0 Temperature - by day

```
                      Cur:      Min:       Avg:       Max:
■ GPU Temperature     75.00     74.00      74.38      75.97
                     Last update:  Thu Jan 16 17:45:07 2014
```

GPU 0 Shares Accepted/Rejected - by day

```
                              Cur:      Min:       Avg:       Max:
■ Shares accepted per minute  3.21      1.65       3.41       10.99
■ Shares rejected per minute  0.00      0.00       0.07       0.59
                     Last update:  Thu Jan 16 17:45:05 2014
```





crowdtilt

DATE January 30, 2014

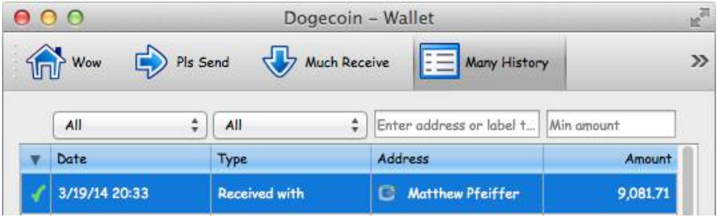
PAY TO THE ORDER OF The Jamaican Bobsled Team $129,587

One Hundred Twenty Nine Thousand Five Hundred Eighty-Seven ************ Dollars

MEMO Sochi 2014

The Crowdtilt Community & Friendly Dogecoin Shibes

Bacon
43
m&m
DOGECOIN
98
40



	Date	Type	Address	Amount
✓	3/19/14 20:33	Received with	Matthew Pfeiffer	9,081.71

Death

- When ASICs came, the community died
- Tipping became a lot less common
- The tipping bots shut down

Asic resistance

- Using scrypt was a failed attempt at ASIC resistance
- Litecoin touted asic resistance but then rolled over and let the ASICs come
- GPU mining dominated for a long time
- Are ASICs it inevitable?

Asic resistance

- Memory hard proof of work?
- Once ASICs develop, hardfork to switch hash functions.
- Deciding to hardfork is a big unstable decision that can break trust and public image

A really hard hash function?

- SHA3 was chosen by NIST contest
- The finalists aren't bad, but are all somehow weaker than SHA.
- X11(x) = Blake(BMW(Groestl(JH(Keccak(Skein(Luffa(Cubehash(Shavite(SimdEcho(x))))))))))
- The idea is the actual circuit would be so complex, converting an algorithm to a circuit would be expensive
- The ASIC itself would need more gates per hash making them less efficient

A really "hard" hash function?

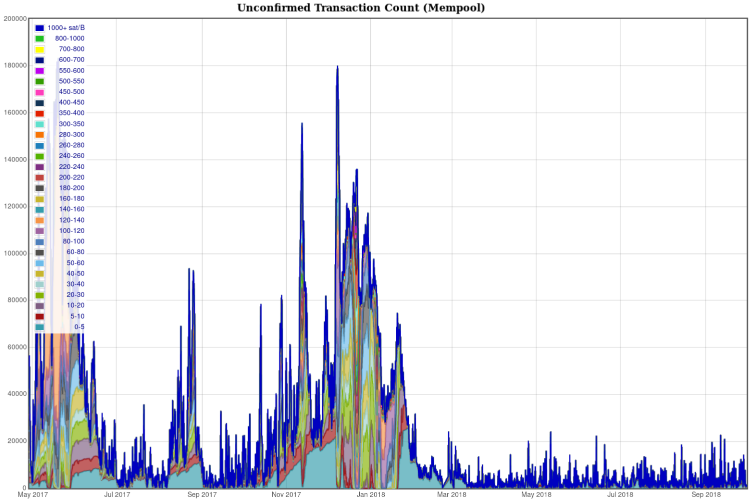
- Didn't work
- X11, X13, X14, X15, in a single ASIC
- Keep different parts in different parts of the chip, so you can reorder
- Reuse the X11 circuits into the X13,... and so on
- Its actually all secret. This is speculation.
- Nobody cares enough for the coins that use X17 to make ASICs for them

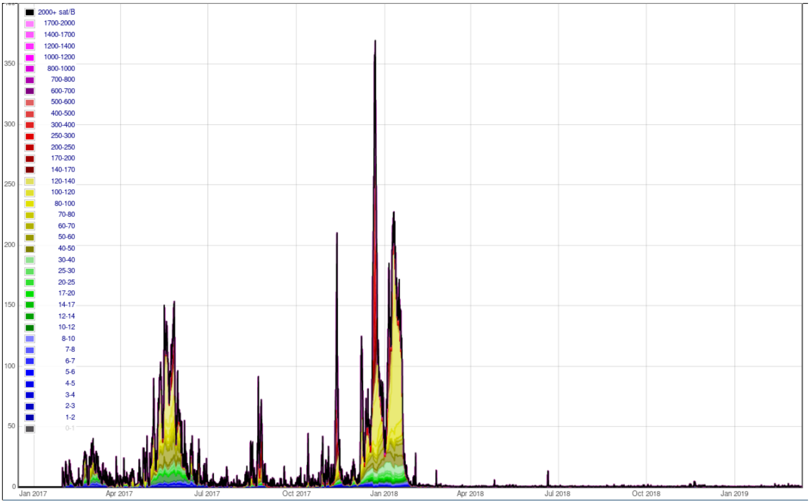
A really "hard" hash function?

- Didn't work
- X11, X13, X14, X15, in a single ASIC
- Keep different parts in different parts of the chip, so you can reorder
- Reuse the X11 circuits into the X13,... and so on
- Its actually all secret. This is speculation.
- Nobody cares enough for the coins that use X17 to make ASICs for them

End of 2017

- Bitcoin price skyrocketed to 20k
- So Bitcoin transactions skyrocketed. People were buying and selling more hoping to cash in.
- Bitcoin can only handle 7 transactions per second
- What happens if your tx doesn't get into the block? How long do you wait?


Unconfirmed Transaction Count (Mempool)
1000+ sat/B
800-1000
700-800
600-700
550-600
500-550
450-500
400-450
350-400
300-350
280-300
260-280
240-260
220-240
200-220
180-200
160-180
140-160
120-140
100-120
80-100
60-80
50-60
40-50
30-40
20-30
10-20
5-10
0-5
200000
180000
160000
140000
120000
100000
80000
60000
40000
20000
0
May 2017
Jul 2017
Sep 2017
Nov 2017
Jan 2018
Mar 2018
May 2018
Jul 2018
Sep 2018


2000+ sat/B
1700-2000
1400-1700
1200-1400
1000-1200
800-1000
700-800
600-700
500-600
400-500
300-400
250-300
200-250
170-200
140-170
120-140
100-120
80-100
70-80
60-70
50-60
40-50
30-40
25-30
20-25
17-20
14-17
12-14
10-12
8-10
7-8
6-7
5-6
4-5
3-4
2-3
1-2
0-1
350
300
250
200
150
100
50
0
Jan 2017
Apr 2017
Jul 2017
Oct 2017
Jan 2018
Apr 2018
Jul 2018
Oct 2018
Jan 2019

It doesn't scale

- 7 transactions per second, independent of:
- Nodes
- Hashpower
- Network speed, etc
- A constant function in all variables!
- Visa can do tens of thousands per second.
- What possible bottleneck does VISA have?

Lightning Protocol

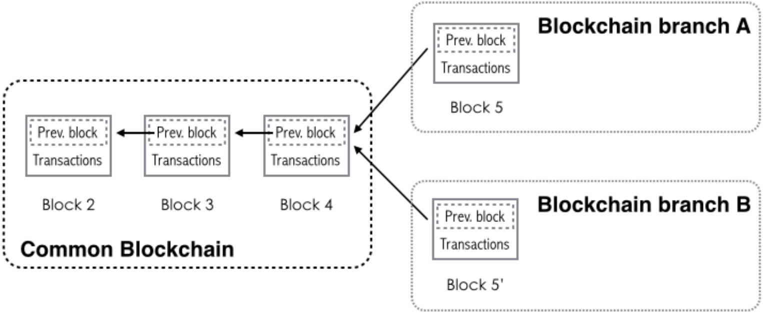
- People realized this would be a problem as early as 2015.
- Modify the blockchain protocol some, you can enable a "secondary layer" for payments.
- Replace blocksize with a variable "block limit"
- the Block limit varies between 1MB to 4MB averaging around 2.3MB
- Transactions could occur offchain, and then later be committed to
- Cheating could be detected, and cause them to forfeit some committed money

Bitcoin Cash

- Somehow this idea was controversial
- The people working on lightning were working on behalf of companies instead of being basement hackers
- Actually a general sentiment with software development in open communities

Nuclear option

- Hard fork the bitcoin
- Double the block size from 1MB to 2MB
- Rebrand everything


Blockchain branch A
Prev. block
Transactions
Block 5
Prev. block
Transactions
Block 2
Prev. block
Transactions
Block 3
Prev. block
Transactions
Block 4
Common Blockchain
Blockchain branch B
Prev. block
Transactions
Block 5'

A question for the audience

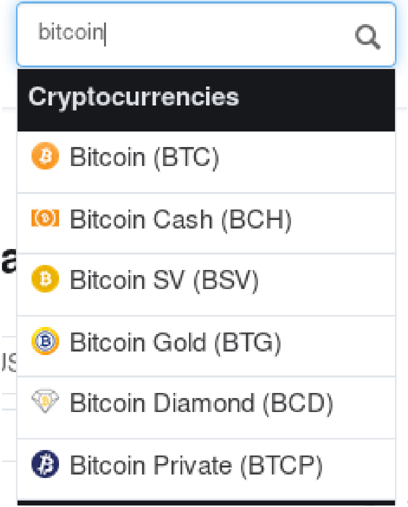
- Does this work?
- Complicated micropayment system
- vs
- Doubling the blocksize

pure ideology

- Which is the real bitcoin chain?
- "The longest chain is the true one"
- But this is more for the protocol than any sectarian fights over logos and colorschemes
- "The one with the most hashrate is the true bitcoin"
- Well, BCH doesn't have that either
- "The whitepaper determines what bitcoin is, and the design that most closely follows it while having the blockchain start with the original genesis block is the true bitcoin"
- ???????

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer



bitcoin

Cryptocurrencies
Bitcoin (BTC)
Bitcoin Cash (BCH)
Bitcoin SV (BSV)
Bitcoin Gold (BTG)
Bitcoin Diamond (BCD)
Bitcoin Private (BTCP)

Bitcoin Cash

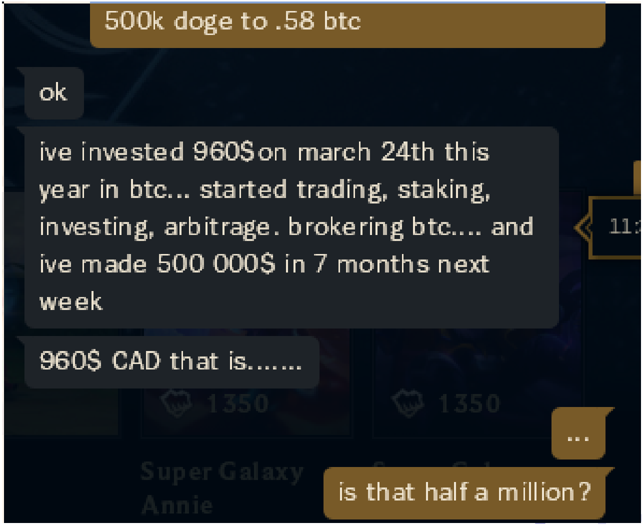
- Was this all just a huge money making scheme?
- Maybe
- The guys pushing BCH ended up profiting quite a bit
- 39 entries on coinmarketcap

Some takeaways

- Blockchain is complicated, lightning is makes it even more so
- People fear what they are too stupid to understand.
- BTC: $3900
- BCH: $130

Bitconnect

- a "proof of stake" coin that offered 1% daily returns
- I don't need to even write anything else about it
- Textbook pyramid scheme
- Suprisingly, a lot of people online didn't realize this
- There were people who did realize it was a scam
- But the dominant voice was that it was a great "investment"



500k doge to .58 btc

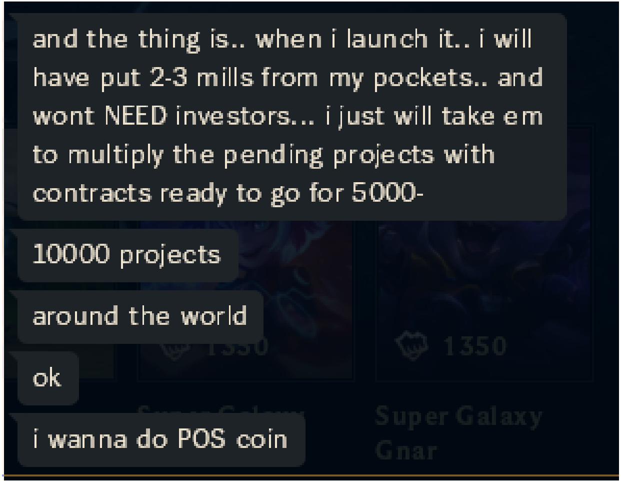
ok

ive invested 960$ on march 24th this year in btc... started trading, staking, investing, arbitrage. brokering btc.... and ive made 500 000$ in 7 months next week

960$ CAD that is.......

...

is that half a million?



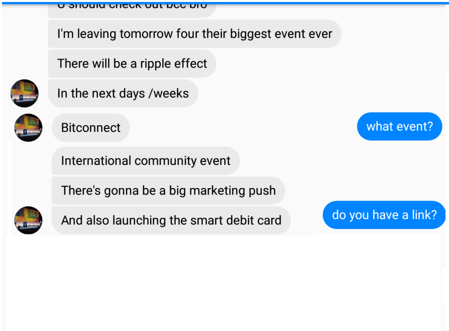
and the thing is.. when i launch it.. i will have put 2-3 mills from my pockets.. and wont NEED investors... i just will take em to multiply the pending projects with contracts ready to go for 5000-

10000 projects

around the world

ok

i wanna do POS coin



U should check out bcc bro

I'm leaving tomorrow four their biggest event ever

There will be a ripple effect

In the next days /weeks

what event?

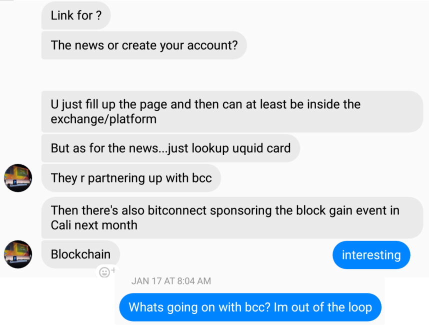
Bitconnect

International community event

There's gonna be a big marketing push

And also launching the smart debit card

do you have a link?



Link for ?

The news or create your account?

U just fill up the page and then can at least be inside the exchange/platform

But as for the news...just lookup uquid card

They r partnering up with bcc

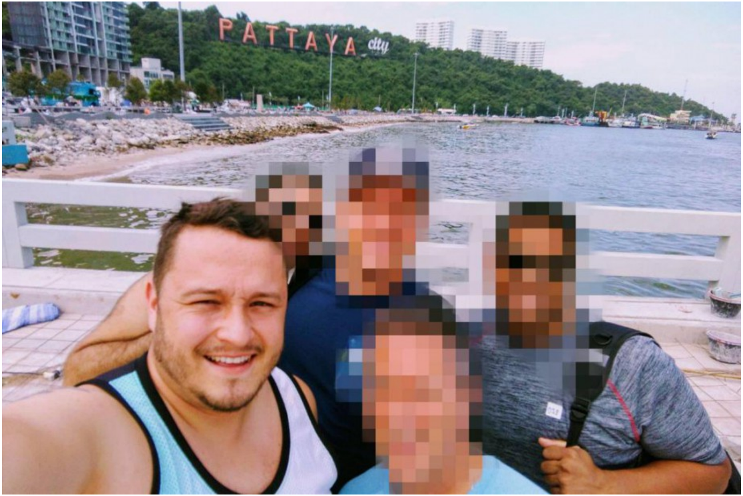
Then there's also bitconnect sponsoring the block gain event in Cali next month

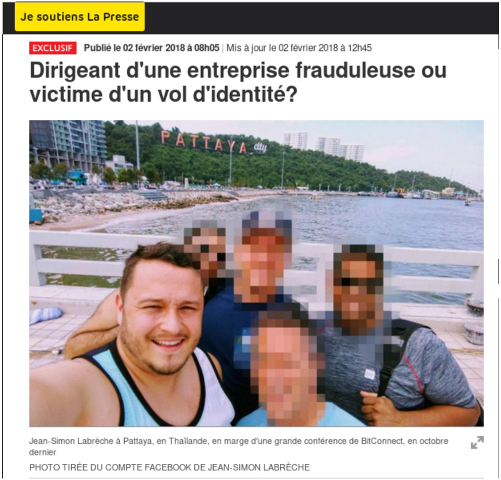
Blockchain

interesting

JAN 17 AT 8:04 AM

Whats going on with bcc? Im out of the loop


PATTAYA city



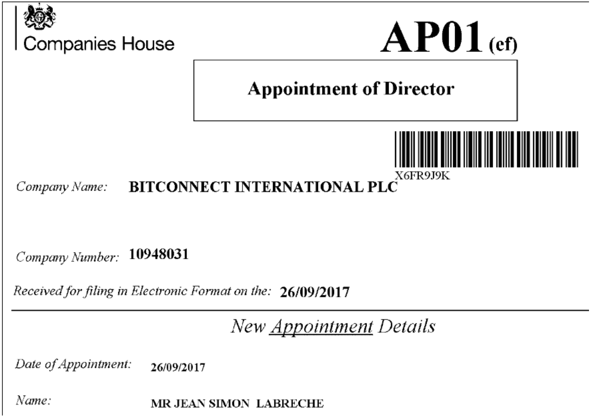
Je soutiens La Presse

EXCLUSIF **Publié le 02 février 2018 à 08h05** | Mis à jour le 02 février 2018 à 12h45

Dirigeant d'une entreprise frauduleuse ou victime d'un vol d'identité?

Jean-Simon Labrèche à Pattaya, en Thaïlande, en marge d'une grande conférence de BitConnect, en octobre dernier

PHOTO TIRÉE DU COMPTE FACEBOOK DE JEAN-SIMON LABRÈCHE



Companies House

AP01 (ef)

Appointment of Director

X6FR9J9K

Company Name: **BITCONNECT INTERNATIONAL PLC**

Company Number: **10948031**

Received for filing in Electronic Format on the: **26/09/2017**

New Appointment Details

Date of Appointment: **26/09/2017**

Name: **MR JEAN SIMON LABRECHE**

Stranger Danger

- Being sued simultaneously in Florida, the UK, and Quebec.
- Listed as “Director”
- Youtube is also listed as a Defendant
- Why am I telling you this?
- I hope it will help you with your term papers