Some Security Risks for DLT

Zhiniang Peng
pengzhiniang@360.cn

360 INTERNET SECURITY CENTER

Virtual machine Vulnerability

Security research on smart contract platforms (EOS and Neo)

30+ bugs are founded in two month

US$200,000+ bounty from the vendors

The virtual machine vulnerability need more attention

Type of Vulnerabilities

Denial of Service

Fork

Remote code execution

Denial of Service

NEO VM Exponential Expansion

Push A:	A	
Dup:	A	A
Append:	AA	
Dup:	AA	AA
Append:	AAAA	
Dup:	4A	4A

…

Exponential expansion make the node out of memory (DOS)

Other vulnerabilities lead to DOS (with real case):

- Buffer Overflow
- Null Pointer Dereference
- Out-Of-Memory
- Dead Loop
- ……

Fork

Division results different between C# and neo-python code

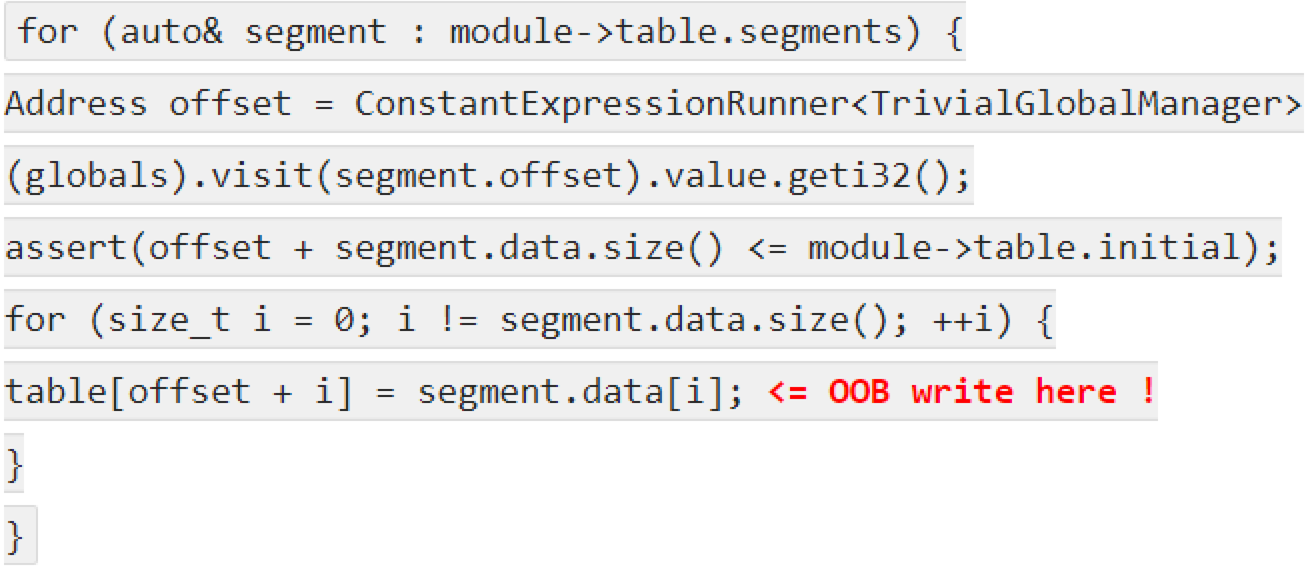
- C# implementation
- Python implementation

Other vulnerabilities lead to fork:

- Out of bound memory read
- Subjective error: time/memory usage
- Uncertainty in float point computation
- updates
- ......

Remote code execution

At libraries/chain/webassembly/binaryen.cpp (Line 78),Function binaryen_runtime::instantiate_module:



```
 for (auto& segment : module->table.segments) {
Address offset = ConstantExpressionRunner<TrivialGlobalManager>
(globals).visit(segment.offset).value.geti32();
assert(offset + segment.data.size() <= module->table.initial);
for (size_t i = 0; i != segment.data.size(); ++i) {
table[offset + i] = segment.data[i]; <= OOB write here !
}
}
```

To achieve Remote Code Execution

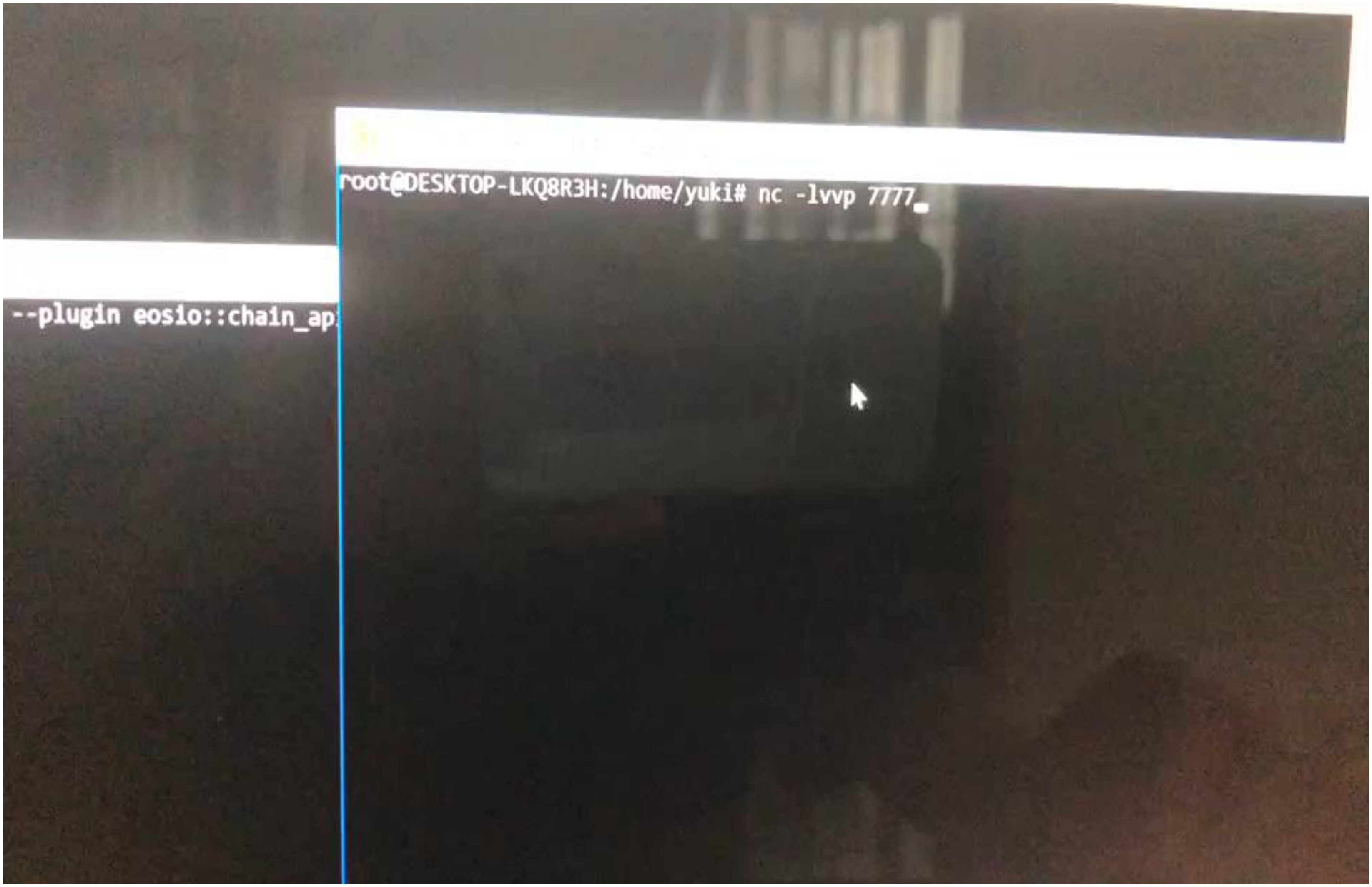
1. The attacker uploads malicious contracts to the nodeos server.

2. The server nodeos process parses the malicious contracts, which triggers the vulnerability.

3. Use Just in time complier to bypass the mitigation techniques such as DEP/ASLR on 64-bits OS.

4.Once successfully exploited, attacker can run arbitrary code on nodeos.

The Proof of Concept Video



```
root@DESKTOP-LKQ8R3H:/home/yuki# nc -lvvp 7777_
```

```
--plugin eosio::chain_ap
```

Blockchain node attack surface

1. Webassembly interpreter and JIT compiler

2. RPC

3. Smart contract

4. Protocol and logic vulnerabilities…

5. Others

Mining Related Attacks

Why this topic?

- security of consensus mechanism is critical
- Need more attention
- Security of mining is a good starting point

Basis of Mining

Finding hash(block)<target

Winner has reward!

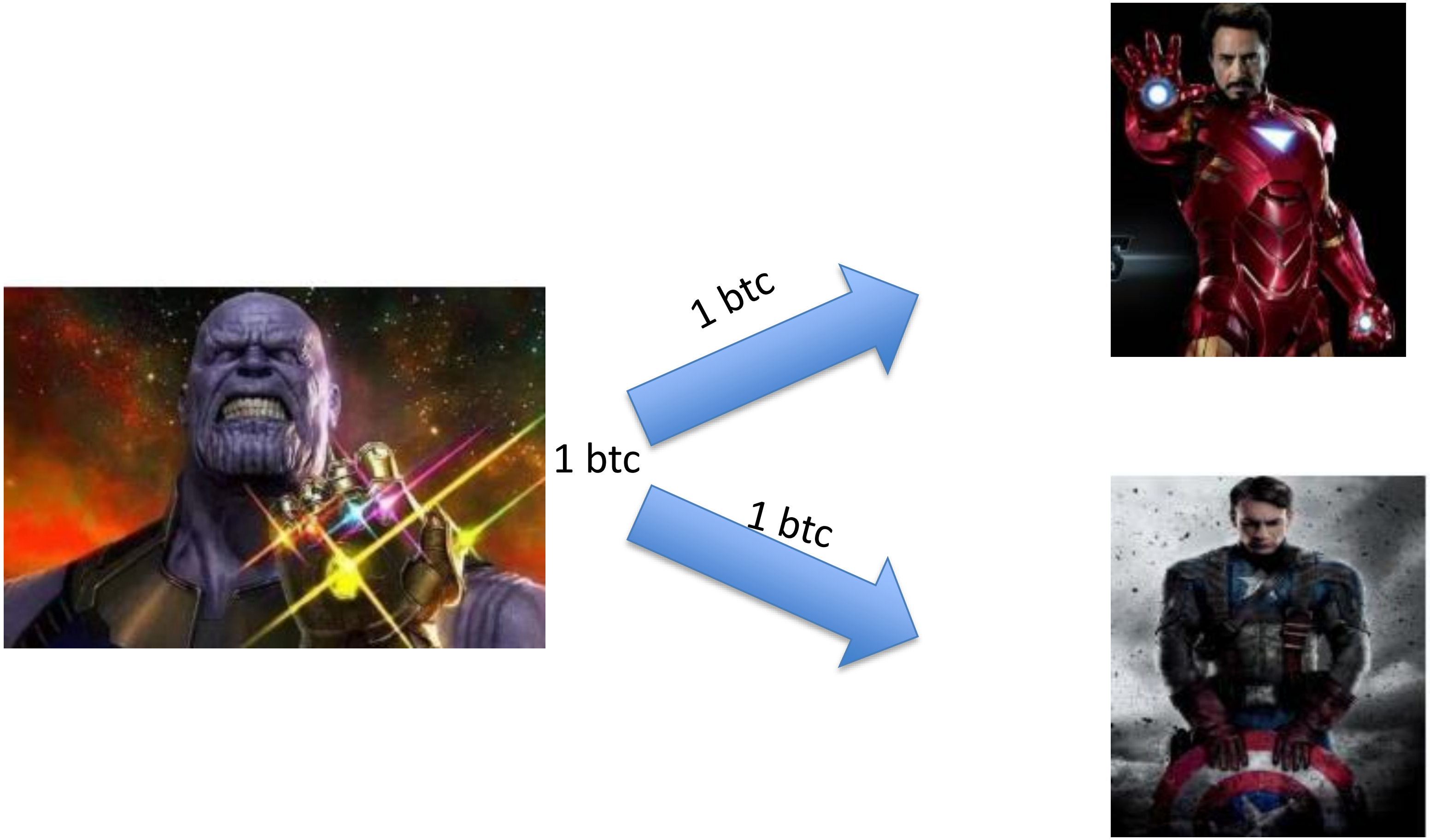
The basis of POW consensus

Randomly select producer of the next block based on hashpower

Mining has a huge attack surface

- Double spend attack
  - 51% attack
- Coin hopping attack
- Attacks against the mining pool
  - Fake miner attack

Double spend attack



1 btc

1 btc

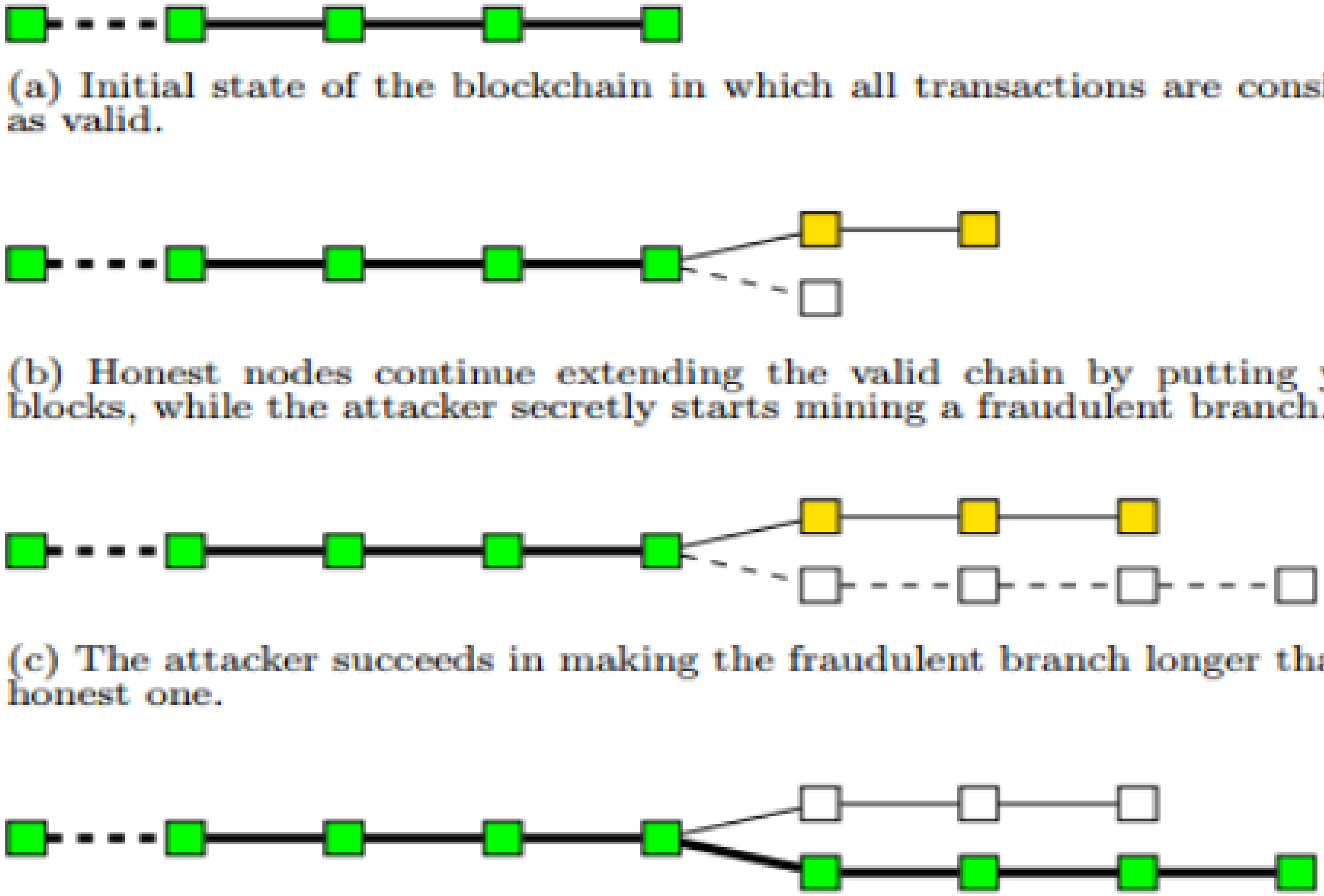
1 btc

Double spend attack

There are many way to perform double spend attack:

- Finney attack
- Race attack
- Brute force attack
- Vector 76 attack
- **51% attack**
- …

51% attack



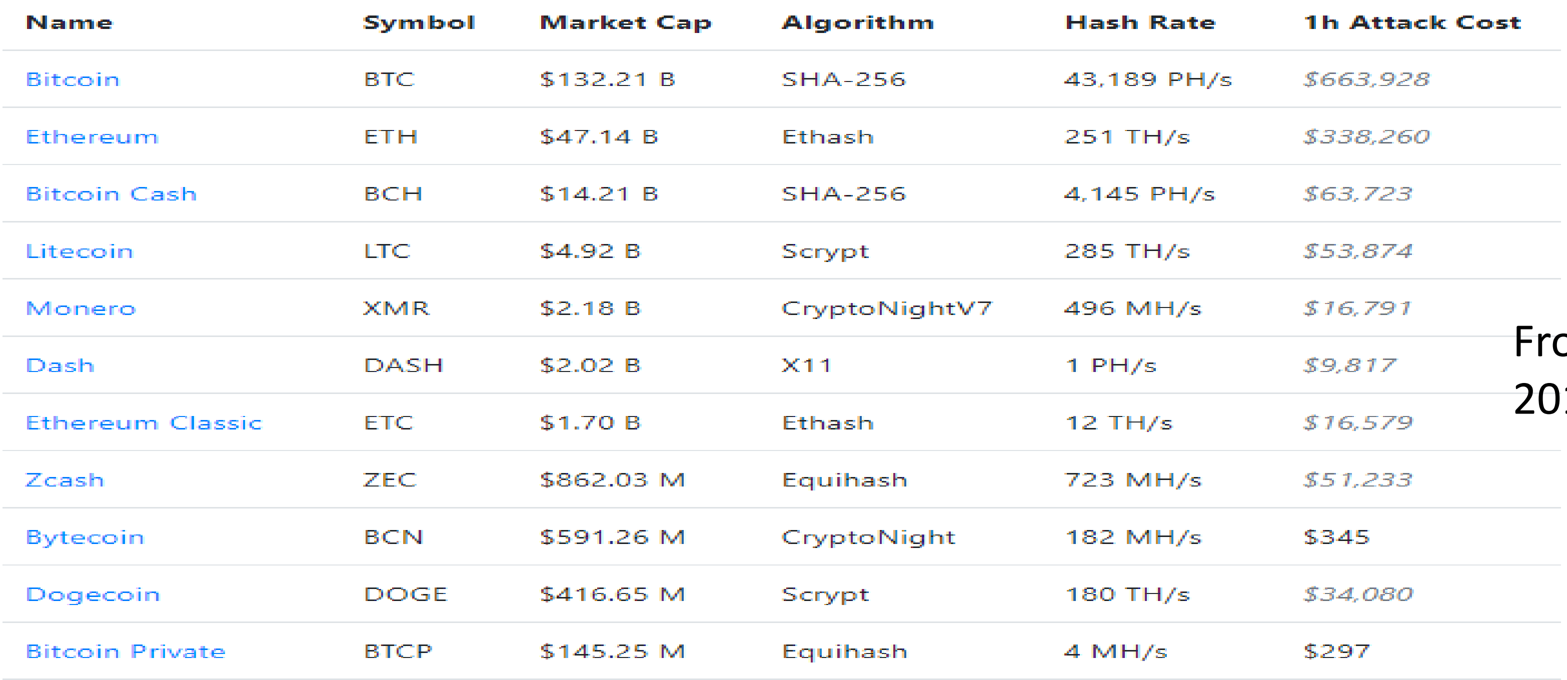
(a) Initial state of the blockchain in which all transactions are considered as valid.

(b) Honest nodes continue extending the valid chain by putting yellow blocks, while the attacker secretly starts mining a fraudulent branch.

(c) The attacker succeeds in making the fraudulent branch longer than the honest one.

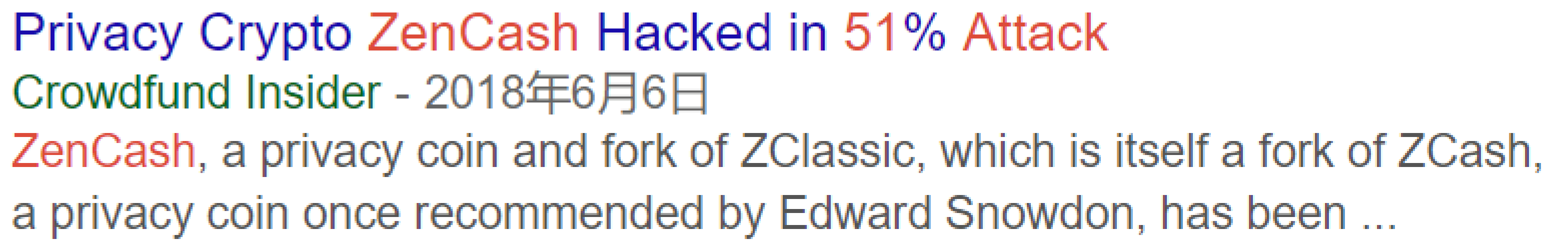
(d) The attacker's branch is published and is now considered the valid one.

51% attack is practical



Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost
Bitcoin	BTC	$132.21 B	SHA-256	43,189 PH/s	$663,928
Ethereum	ETH	$47.14 B	Ethash	251 TH/s	$338,260
Bitcoin Cash	BCH	$14.21 B	SHA-256	4,145 PH/s	$63,723
Litecoin	LTC	$4.92 B	Scrypt	285 TH/s	$53,874
Monero	XMR	$2.18 B	CryptoNightV7	496 MH/s	$16,791
Dash	DASH	$2.02 B	X11	1 PH/s	$9,817
Ethereum Classic	ETC	$1.70 B	Ethash	12 TH/s	$16,579
Zcash	ZEC	$862.03 M	Equihash	723 MH/s	$51,233
Bytecoin	BCN	$591.26 M	CryptoNight	182 MH/s	$345
Dogecoin	DOGE	$416.65 M	Scrypt	180 TH/s	$34,080
Bitcoin Private	BTCP	$145.25 M	Equihash	4 MH/s	$297

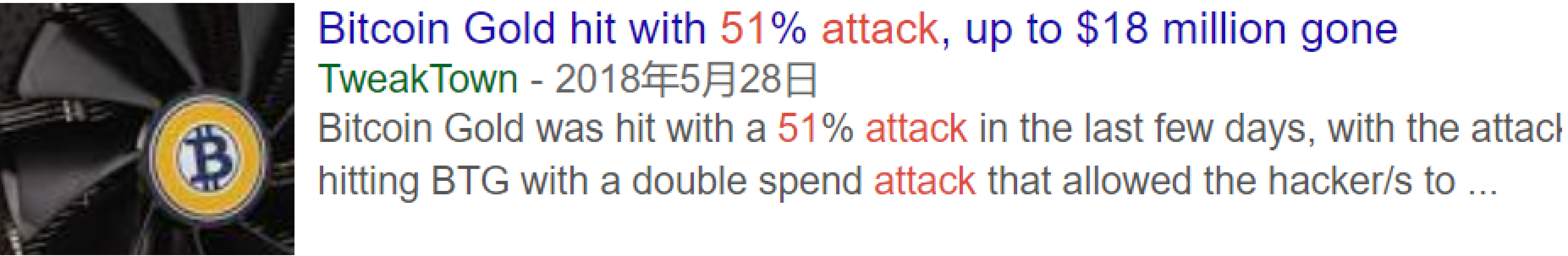
From: crypto51.app
2018/7/23



Privacy Crypto ZenCash Hacked in 51% Attack

Crowdfund Insider - 2018年6月6日

ZenCash, a privacy coin and fork of ZClassic, which is itself a fork of ZCash, a privacy coin once recommended by Edward Snowdon, has been ...



Bitcoin Gold hit with 51% attack, up to $18 million gone

TweakTown - 2018年5月28日

Bitcoin Gold was hit with a 51% attack in the last few days, with the attacl hitting BTG with a double spend attack that allowed the hacker/s to ...

Coin hopping attack

Mining difficulty is dynamic

the more hashpower, the harder

DAA (difficulty adjustment algorithm)

Coin hopping attack

miner hopping between two coins the get more mining profit.

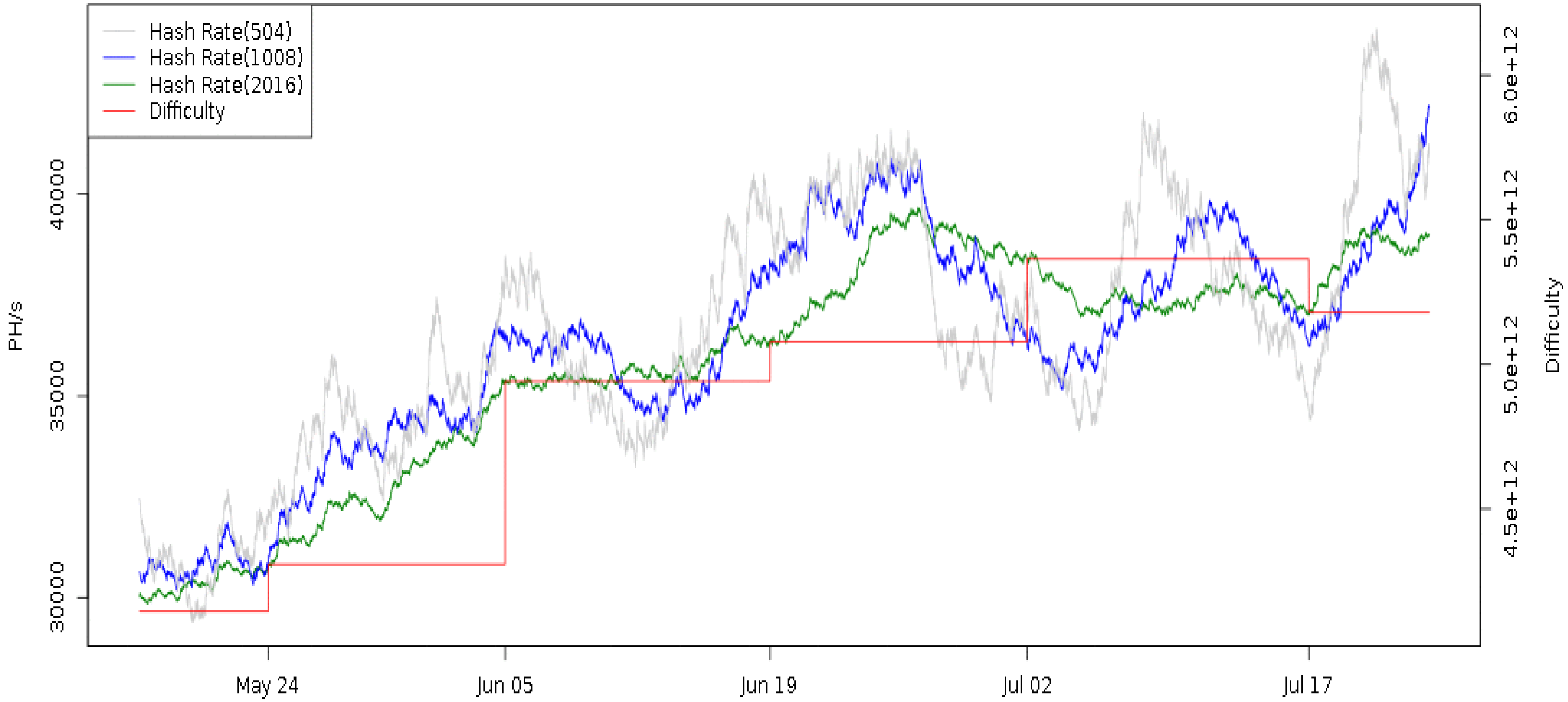
Difficulty adjustment algorithm

360 INTERNET SECURITY CENTER

Every M blocks ($M = 2016$ for Bitcoin) the difficulty is recalculated as

$$D_{i+1} = D_i \cdot \frac{M \cdot |\Delta|}{S_m}$$

Bitcoin Hash Rate vs Difficulty (2 Months)

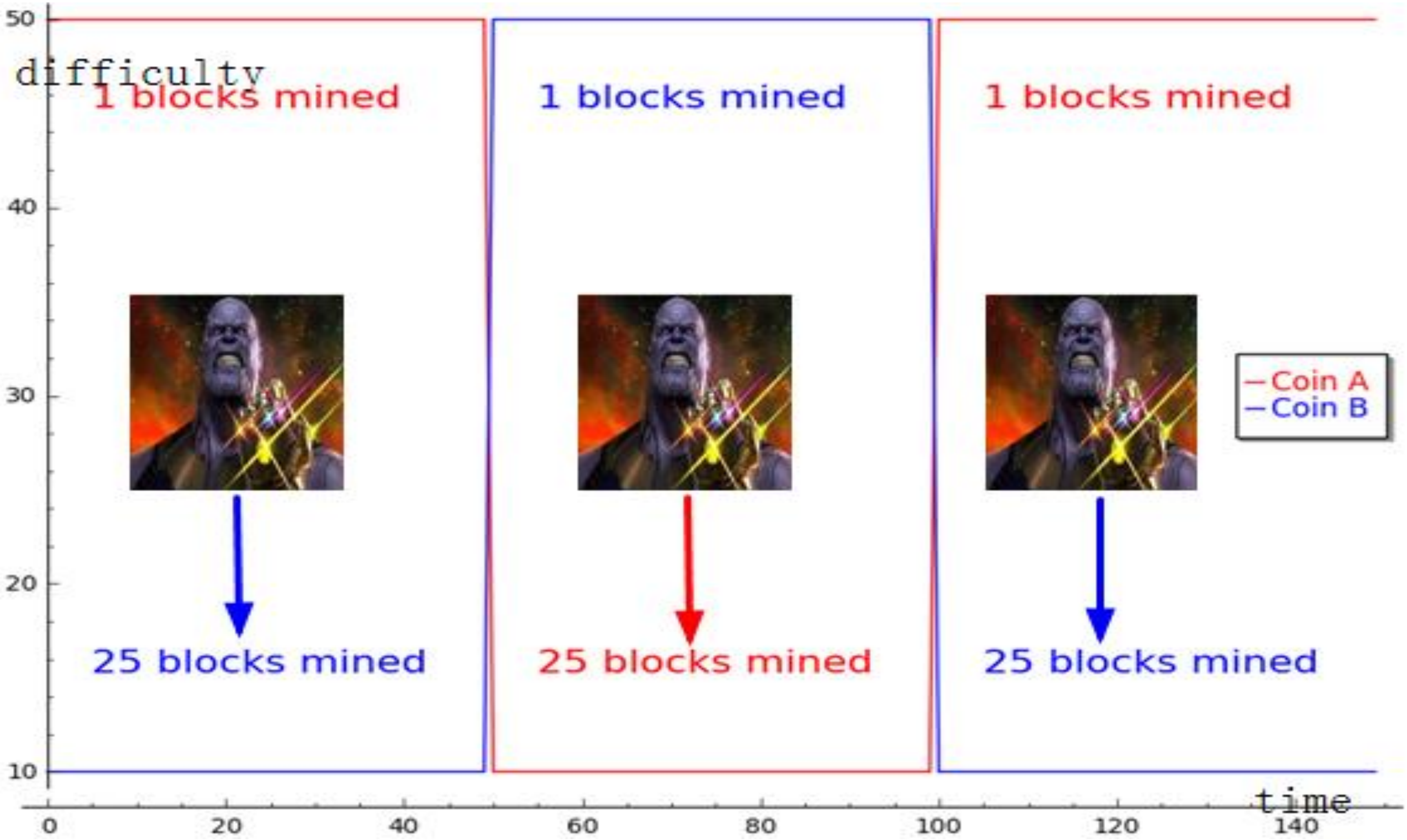


Coin hopping attack

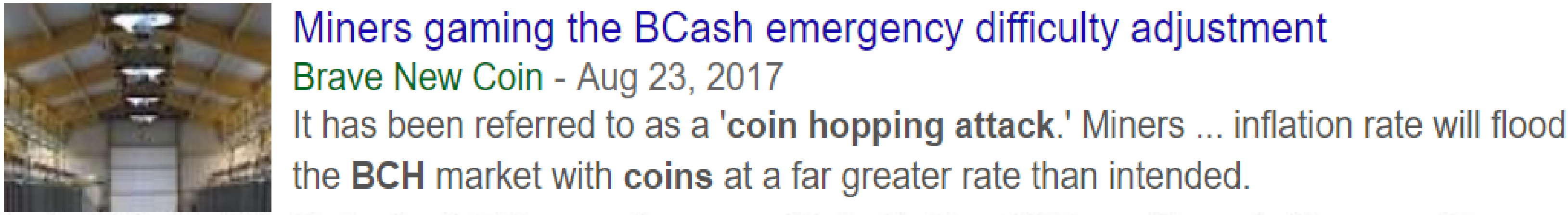
Attacker hashpower: 4X

Hashpower of honest miner for coin A: 1X

Hashpower of Honest miner for coin B: 1X



BCH emergency difficulty adjustment

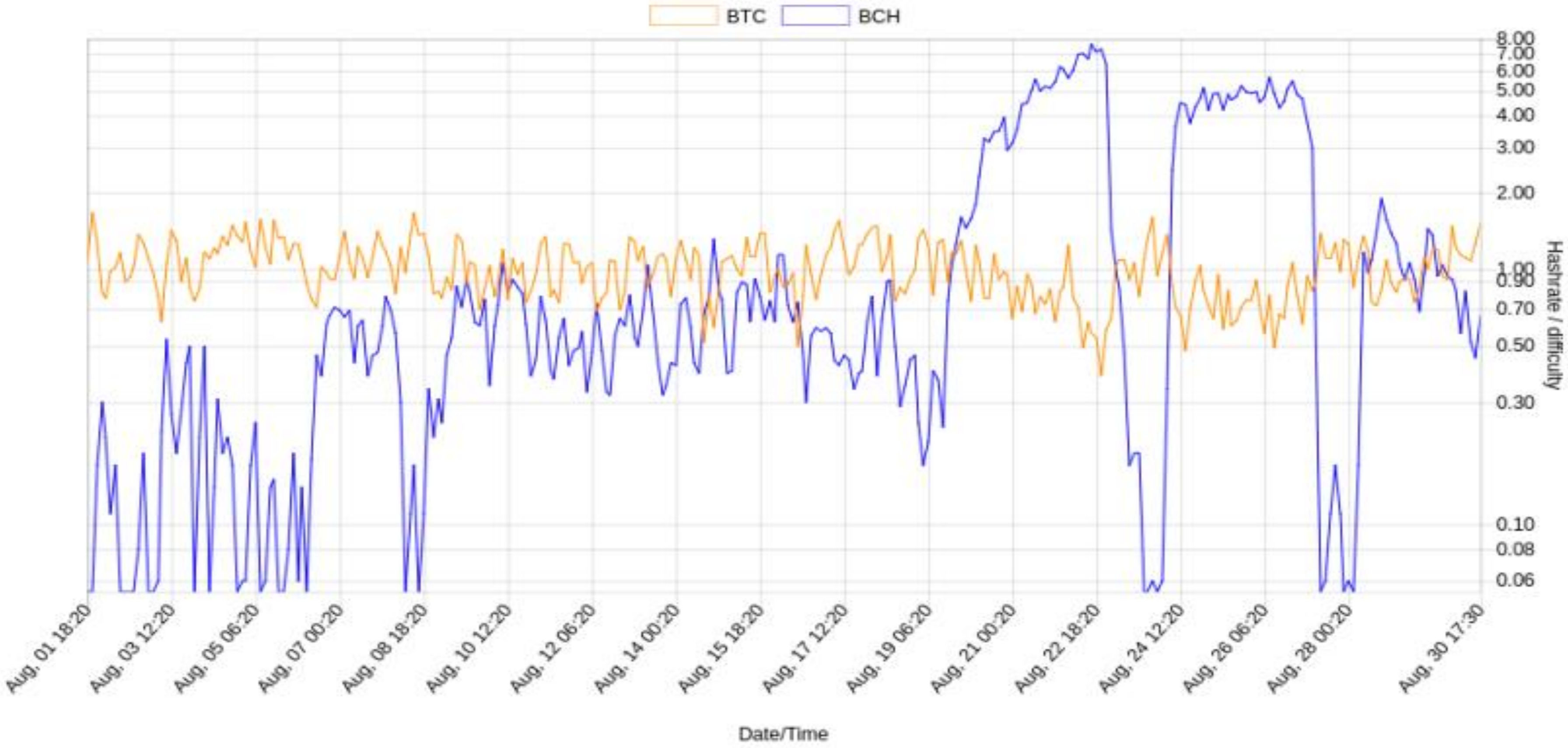


Miners gaming the BCash emergency difficulty adjustment

Brave New Coin - Aug 23, 2017

It has been referred to as a '**coin hopping attack**.' Miners ... inflation rate will flood the **BCH** market with **coins** at a far greater rate than intended.

Hashrate divided by difficulty. A ratio of > 1.0 means (on average) faster blocks, < 1.0 slower. (log scale, 3h averages)



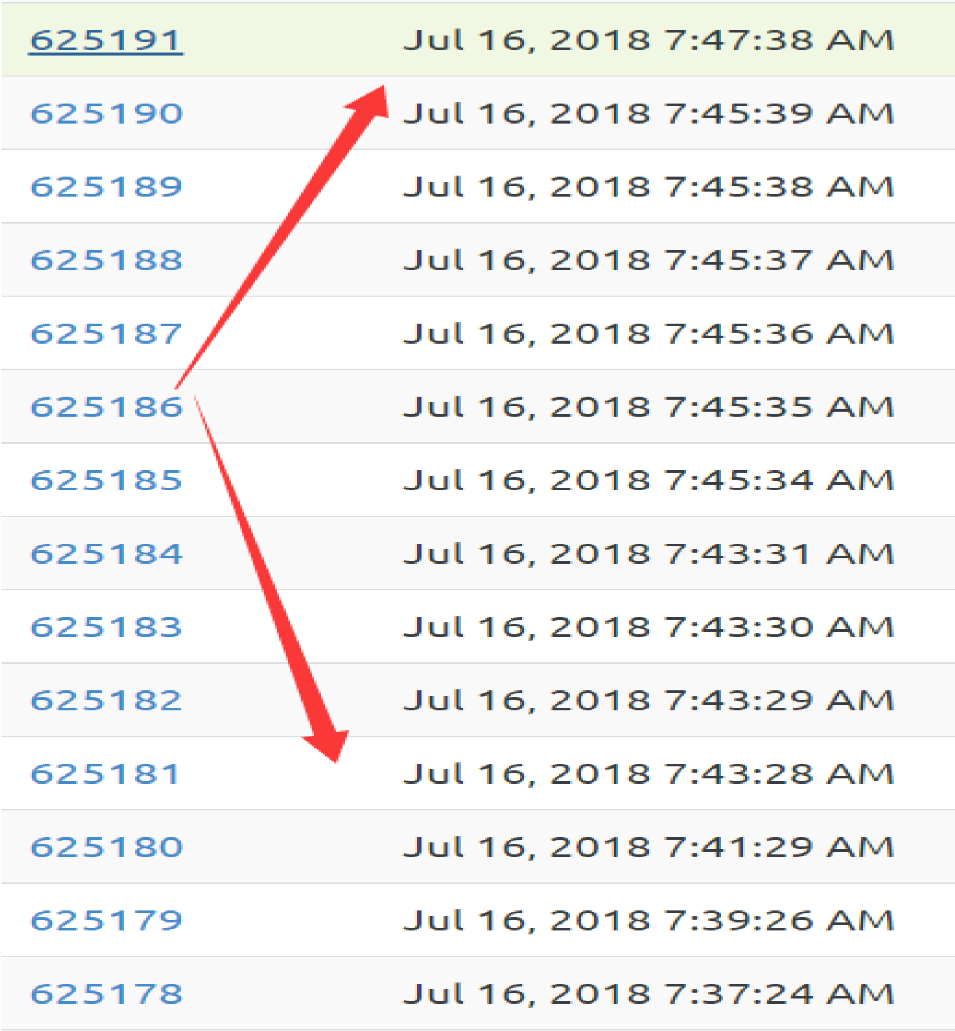
Coin hopping happens everyday

Event 10x attacker for altcoin

Advance tricks:

- **Time manipulation**
- **Time hijacking**
- **Block withholding**
- **Block discarding**
- **Selfish mining**
- **……**

10X attacker on bitcoin candy:
1 second per block



625191	Jul 16, 2018 7:47:38 AM
625190	Jul 16, 2018 7:45:39 AM
625189	Jul 16, 2018 7:45:38 AM
625188	Jul 16, 2018 7:45:37 AM
625187	Jul 16, 2018 7:45:36 AM
625186	Jul 16, 2018 7:45:35 AM
625185	Jul 16, 2018 7:45:34 AM
625184	Jul 16, 2018 7:43:31 AM
625183	Jul 16, 2018 7:43:30 AM
625182	Jul 16, 2018 7:43:29 AM
625181	Jul 16, 2018 7:43:28 AM
625180	Jul 16, 2018 7:41:29 AM
625179	Jul 16, 2018 7:39:26 AM
625178	Jul 16, 2018 7:37:24 AM

Mitigations

Enhanced DAA:

Zawy difficulty algorithm
Digshield algorithm
Dark Gravity Wave
MIDAS
……
Some altcoin has other own DAA

Very Hard to achieve:

1. resistant to all types of attacks
2. mathematically eliminate attacker's advantage
3. constant block rate

Test your DDA with simulator:

https://github.com/edwardz246003/DAA_simulator (Monte Carlo based)

Attacks against the mining pool

There are many attacks against the mining pool :

Pool hopping attack

Block withholding attack

smart contract enhanced attack

Fake miner attack

…

Equihash verifier bug

Equihashverify:

https://github.com/joshuayabut/equihashverify

used by z-nomp

Wrong implementation of Equihash algorithm

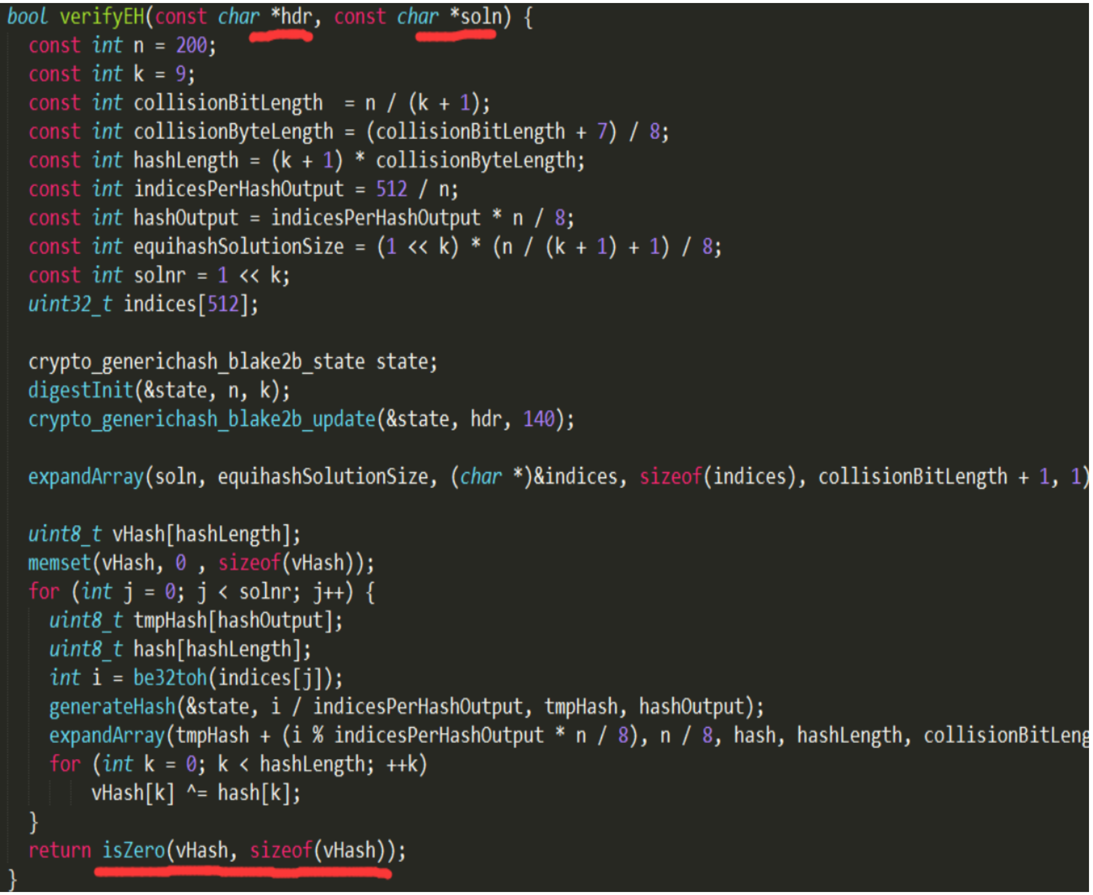
Attacker can generate fake shares to cheat mining pool

Affected altcoin:

Zcash, Bitcoin Gold, Zencash, Bitcoin Private, Zclassic, Komodo, Hush, BitcoinZ, Bitcoin Candy, NewBTG, Bitcoin Faith, Bitcoin nano, Bitcoin pizza, Bitocin world ……

Equihash verifier bug

Finally some software bug ☺



```
bool verifyEH(const char *hdr, const char *soln) {
  const int n = 200;
  const int k = 9;
  const int collisionBitLength  = n / (k + 1);
  const int collisionByteLength = (collisionBitLength + 7) / 8;
  const int hashLength = (k + 1) * collisionByteLength;
  const int indicesPerHashOutput = 512 / n;
  const int hashOutput = indicesPerHashOutput * n / 8;
  const int equihashSolutionSize = (1 << k) * (n / (k + 1) + 1) / 8;
  const int solnr = 1 << k;
  uint32_t indices[512];

  crypto_generichash_blake2b_state state;
  digestInit(&state, n, k);
  crypto_generichash_blake2b_update(&state, hdr, 140);

  expandArray(soln, equihashSolutionSize, (char *)&indices, sizeof(indices), collisionBitLength + 1, 1)

  uint8_t vHash[hashLength];
  memset(vHash, 0 , sizeof(vHash));
  for (int j = 0; j < solnr; j++) {
    uint8_t tmpHash[hashOutput];
    uint8_t hash[hashLength];
    int i = be32toh(indices[j]);
    generateHash(&state, i / indicesPerHashOutput, tmpHash, hashOutput);
    expandArray(tmpHash + (i % indicesPerHashOutput * n / 8), n / 8, hash, hashLength, collisionBitLeng
    for (int k = 0; k < hashLength; ++k)
        vHash[k] ^= hash[k];
  }
  return isZero(vHash, sizeof(vHash));
}
```

hash(hdr,x_1)^ hash(hdr,x_2) ^…^ ^…^.hash(hdr,x_{512})

does not check duplicate

$\{x_1=1,x_2=1,x_3=1,\ldots,x_{512}=1\}$

Exploitation: https://github.com/edwardz246003/equihash_attacker

Closing thoughts

Blockchain security is very complex

more than traditional software security

Any attack is possible

If the outcome is enough

Is Proof of stake safer?

I don’t think so

New technologies are coming in blockchain industry

with new attacks!

Thanks

360
WWW.360.cn

SAFETY FIRST