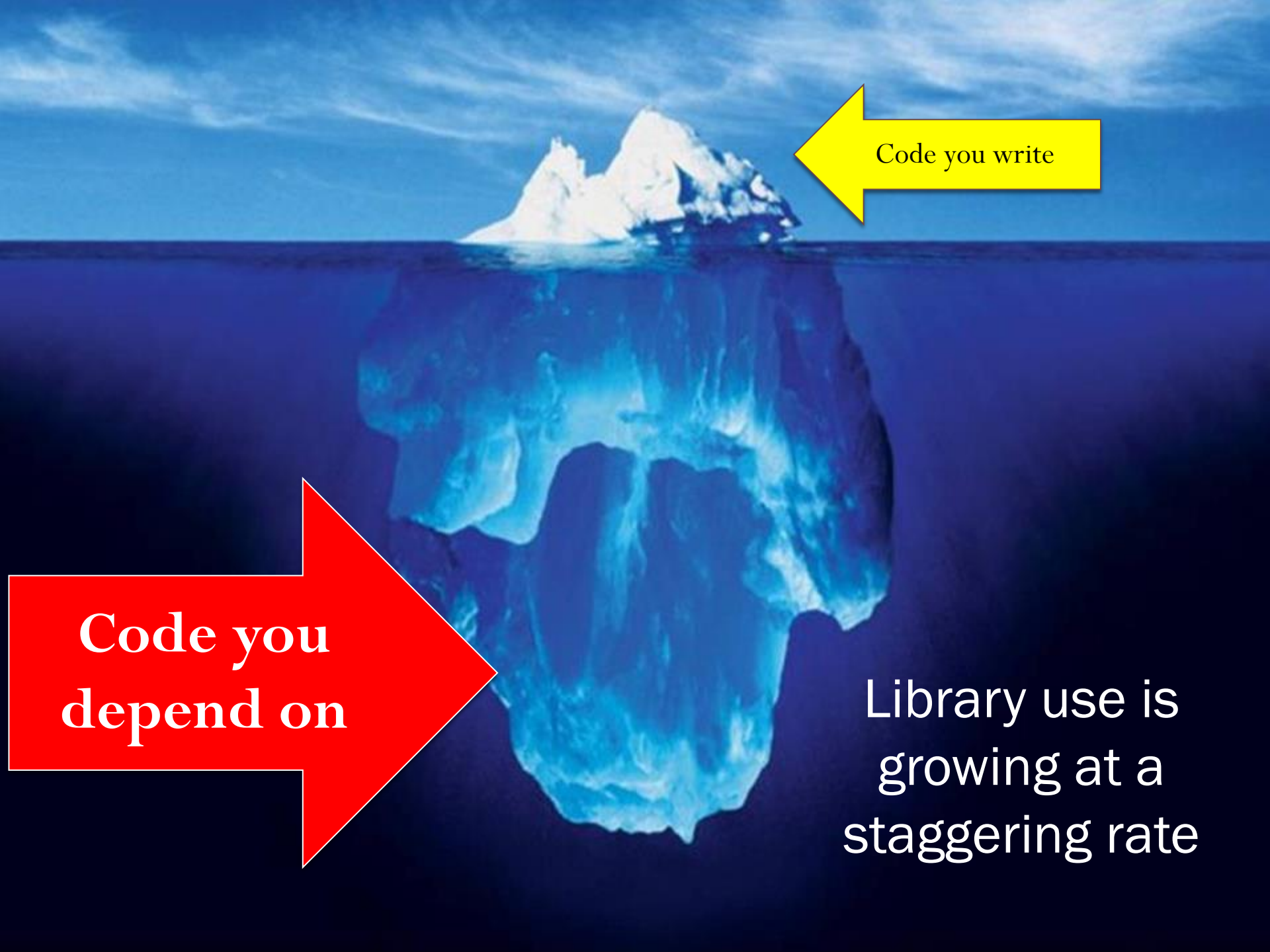


D: Centralization, 51% Attacks

Developer centralization



Code you write

Code you
depend on

Library use is
growing at a
staggering rate

Question

- Who controls the code you depend on?
- How many developers are there checking for its security?
- Would you bet your life savings on them?
- Case study



- Secures connections on a vast majority of sites
- Circa 2014, how many developers were maintaining this code?
 - John Walsh, "OpenSSL for example is largely staffed by one fulltime developer and a number of part-time volunteer developers ... to write, maintain, test, and review 500,000 lines of business-critical code. Half of these developers have other things to do."

It's all good, until it isn't

- Heartbleed OpenSSL bug (2014)



The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication

DARKReading

4/10/2014
02:10 PM

Heartbleed: Examining The Impact



Tim Sapio
Commentary

With Heartbleed, there's little hope of knowing if an asset was breached, if a breach can be identified, or what, if any, data was leaked. Here's how to defend against future attacks.

Yesterday saw the beginning of the most significant breaches in Internet security to date. I'm talking, of course, about the vulnerability that was discovered in OpenSSL (CVE-2014-0160), commonly known as [Heartbleed](#).

Securing the supply chain

- How many developers work on Solidity?
 - <https://blog.lamden.io/turing-incompleteness-and-the-sad-state-of-solidity-d5278ba4eda0>

Solidity development itself has 2 people working on it full time. The market cap of Ethereum is over \$25,000,000,000. Two people are working on the smart contracting system for a multi-billion dollar system that has unknown levels of attack vectors.

Developer/Owner trust in contracts

- Backdoors abound after DAO

Bancor Crashes After Hack, \$23 Million Stolen

🕒 July 10, 2018 10:50 am

The crypto broker platform is currently down for maintenance. Moreover Bancor has utilized a fail-safe mechanism to freeze all Bancor Network Tokens

- <https://www.trustnodes.com/2019/11/12/hackers-build-ethereum-google-sheets-sidechain-to-send-eth-by-email>

Hackers Build Ethereum Google Sheets Sidechain to Send ETH by Email

🕒 November 12, 2019 6:17 pm

They call it sheetcoin because this was meant as a jab “that points out how many ERC-20s have an owner account with admin privileges.”

After the DAO hack, the vast majority of smart contracts added a super-key that can over-ride user on-chain balances in that smart contract as was most famously illustrated when Bancor [over-rode accounts](#) after a hack.

Governance centralization

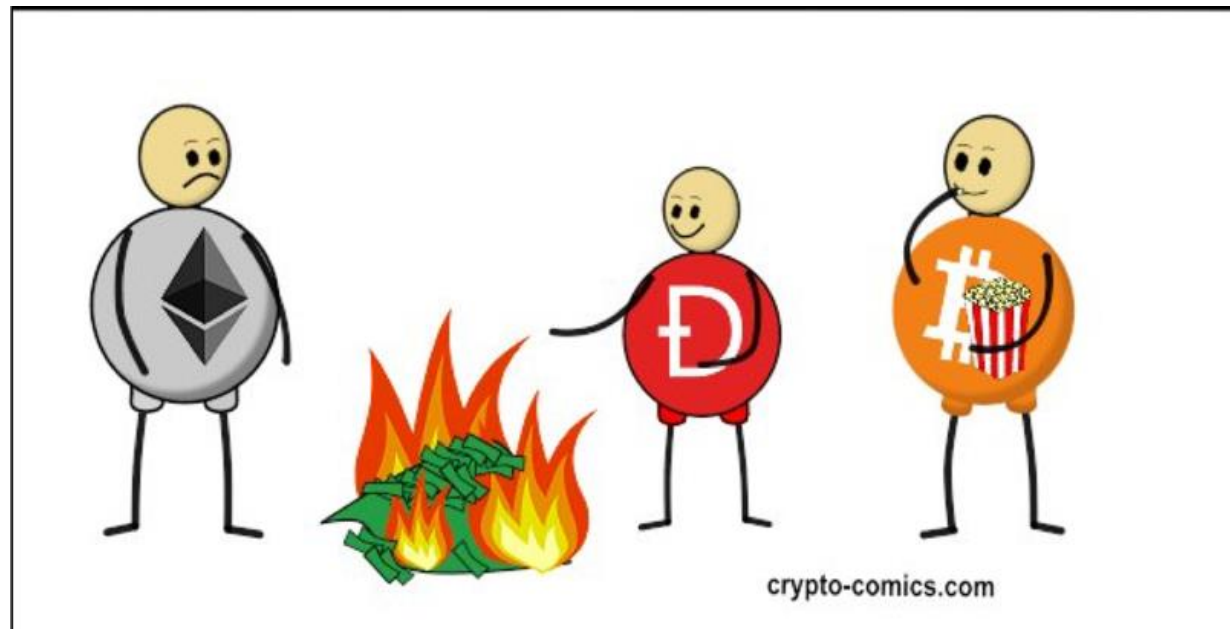
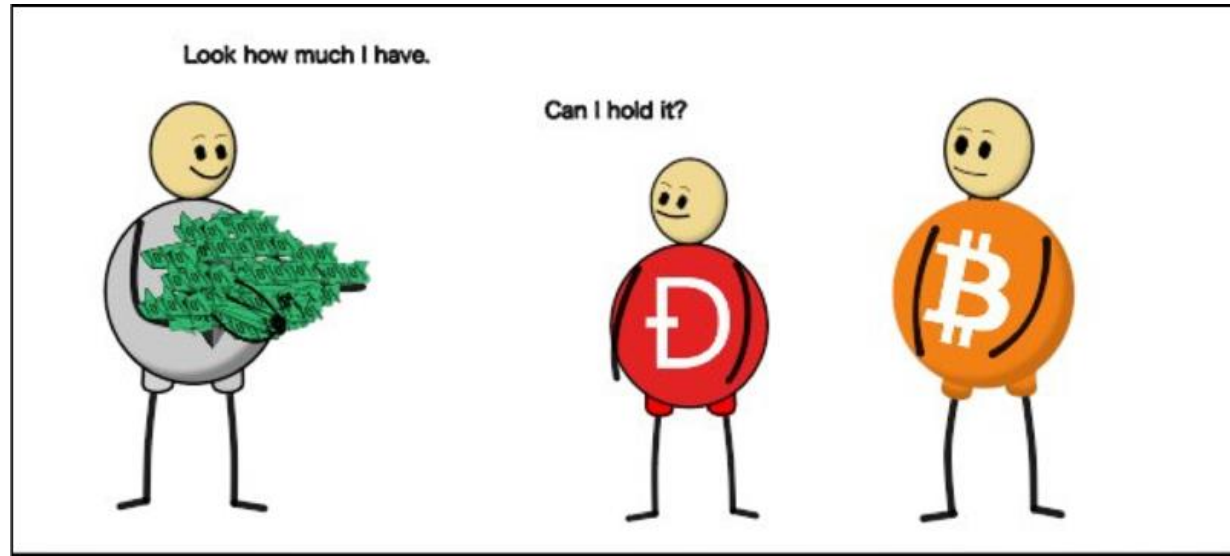
Governance in blockchains

- On-chain governance done via consensus protocol
- How is off-chain governance done?

The Blockchain Paradox

- "The very idea of blockchain governance can seem like a paradox wrapped in a dilemma. The paradox: "How do you change something which is 'immutable'?"
- <https://www.coindesk.com/the-blockchain-paradox>

But first, a story



The DAO

- Decentralized Autonomous Organization
 - Crowd-sourced venture-capital fund for funding future Ethereum projects
 - Completely virtual
 - Smart contracts written and deployed to run organization
 - Written by some of the top Ethereum developers
 - Initial funding period where people send ETH to get tokens representing voting stake (crowdsale or initial coin offering ICO)
 - Proposals to obtain funds for projects considered by the DAO
 - Members with tokens vote to approve these proposals.

DAO contract management

- `splitDAO()` function to create a "Child DAO"
 - Individuals or groups can join together to fund projects separately (i.e. create their own VC fund)
 - Child DAO can start raising funds and accepting proposals separately from others
 - Supports an "exit door"
 - Individuals or groups not happy with the DAO create their own Child DAO to exit contract and exchange their DAO tokens to get their ETH back
 - ETH sent to a specified address after a period of 28 days (similar to the DAO funding mechanism)
- Exploit
 - Attacking contract leverages vulnerability in split function to exchange a single token for its equivalent in ETH tens of thousands of times
 - Flaw is with the logic of the DAO smart contract itself (not the EVM)

Timeline

- 4/30/2016
 - Launched with 28-day funding window by German startup Slock.it
 - Several Ethereum Foundation members involved
- 5/2016
 - Raised \$150 million from 11,000 people (including a number of Ethereum Foundation members)
 - Ethereum valuation at the time was \$1 billion ($> 10\%$ of ETH in DAO)
- Early 6/2016
 - 50 project proposals received for funding, but DAO decides to hold off due to security issues in code
- 6/12/2016
 - Severe recursive call bug described by contract creator

● 6/17/2016

The DAO Attacked: Code Issue Leads to \$60 Million Ether Theft

Michael del Castillo (@DelRayMan) | Published on June 17, 2016 at 14:00 GMT

NEWS

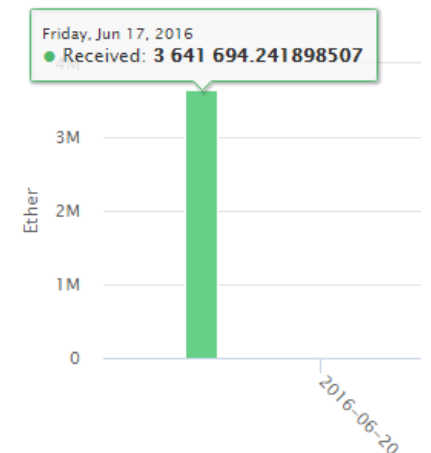
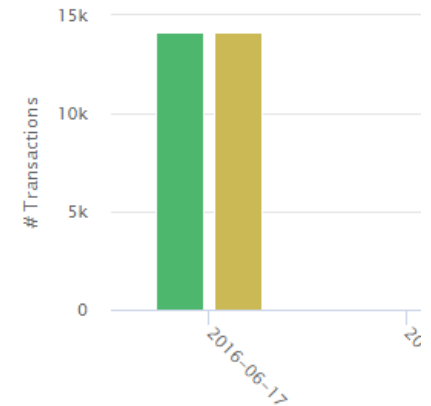
- Attacker takes out > 3.6 million ETH over several hours
 - $\sim 15\%$ of all ether in existence
 - Valued at $> \$60M$
 - Price of ETH plummets from $\$20$ to $\$13$

Ethereum Contract

0x304a554a310C7e546dfe434669

Transactions

Code / Source



- 6/17/2016
 - Attacker's contract
 - <https://etherscan.io/txsInternal?a=0x304a554a310c7e546dfe434669c62820b7d83490&p=200>





















Contract Internal Transactions

For Address [0x304a554a310c7e546dfe434669c62820b7d83490](https://etherscan.io/address/0x304a554a310c7e546dfe434669c62820b7d83490)

Sponsored:  - AAX - AAX - 5%+ interest rate on BTC saving. Visit [AAX.com](https://aax.com) now!

A total of 14,166 internal transactions found
(Showing the last 10k records only)

First < Page 200 of 200 > Last

Block	Age	Parent Txn Hash	Type	From	To	Value
1718916	1600 days 10 hrs ago	 0xd0307de8fd37da3ef1...	call	 TheDAO Token	  TheDarkDAO	258.056564760381731 Ether
		 0xd0307de8fd37da3ef1...	call	 TheDAO Token	  TheDarkDAO (0x304a554a310c7e546dfe434669c62820b7d83490)	.056564760381731 Ether
		 0xd0307de8fd37da3ef1...	call	 TheDAO Token	  TheDarkDAO	258.056564760381731 Ether
		 0xd0307de8fd37da3ef1...	call	 TheDAO Token	  TheDarkDAO	258.056564760381731 Ether
		 0xd0307de8fd37da3ef1...	call	 TheDAO Token	  TheDarkDAO	258.056564760381731 Ether

- 6/17/2016
 - Software fork immediately proposed by Buterin
 - <https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/>
 - Change code running on all full-nodes to disallow future transactions on both contracts

A software fork has been proposed, (with NO ROLLBACK; no transactions or blocks will be “reversed”) which will make any transactions that make any calls/callcodes/delegatecalls that reduce the balance of an account with code hash

0x7278d050619a624f84f51987149ddb439cdaadfba5966f7cfaea7ad44340a4ba (ie. the DAO and children) lead to the transaction (not just the call, the transaction) being invalid ...

- Attacker stops withdrawing once soft fork is proposed

- 6/2016
 - Attacker posts response
 - <https://pastebin.com/CcGUBgDG>

===== BEGIN SIGNED MESSAGE =====

To the DAO and the Ethereum community,

I have carefully examined the code of The DAO and decided to participate after finding the feature where splitting is rewarded with additional ether. I have made use of this feature and have rightfully claimed 3,641,694 ether, and would like to thank the DAO for this reward. It is my understanding that the DAO code contains this feature to promote decentralization and encourage the creation of "child DAOs".

I am disappointed by those who are characterizing the use of this intentional feature as "theft". I am making use of this explicitly coded feature as per the smart contract terms and my law firm has advised me that my action is fully compliant with United States criminal and tort law. For reference please review the terms of the DAO:

"The terms of The DAO Creation are set forth in the smart contract code existing on the Ethereum blockchain at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413. Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO's code. Any and all explanatory terms or descriptions are merely offered for educational purposes and do not supercede or modify the express terms of The DAO's code set forth on the blockchain; to the extent you believe there to be any conflict or discrepancy between the descriptions offered here and the functionality of The DAO's code at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413, The DAO's code controls and sets forth all terms of The DAO Creation."

A soft or hard fork would amount to seizure of my legitimate and rightful ether, claimed legally through the terms of a smart contract. Such fork would permanently and irrevocably ruin all confidence in not only Ethereum but also the in the field of smart contracts and blockchain technology. Many large Ethereum holders will dump their ether, and developers, researchers, and companies will leave Ethereum. Make no mistake: any fork, soft or hard, will further damage Ethereum and destroy its reputation and appeal.

I reserve all rights to take any and all legal action against any accomplices of illegitimate theft, freezing, or seizure of my legitimate ether, and am actively working with my law firm. Those accomplices will be receiving Cease and Desist notices in the mail shortly.

I hope this event becomes an valuable learning experience for the Ethereum community and wish you all the best of luck.

Yours truly,
"The Attacker"

- Eventually offers ETH to all miners/full-nodes who do not accept software fork

- 6/2016

- Software fork approved, but update pulled a few hours before deployment, due to a denial-of-service vulnerability

- Attacker can flood miners with transactions that will eventually be discarded without collecting any fees (bypasses gas mechanism)!
- <http://hackingdistributed.com/2016/06/28/ethereum-soft-fork-dos-vector/>

```
for(uint32 i=0; i < 1000000; i++) {  
    sha3('some data'); // costly computation  
}  
DarkDAO.splitDAO(...); // render the transaction invalid
```

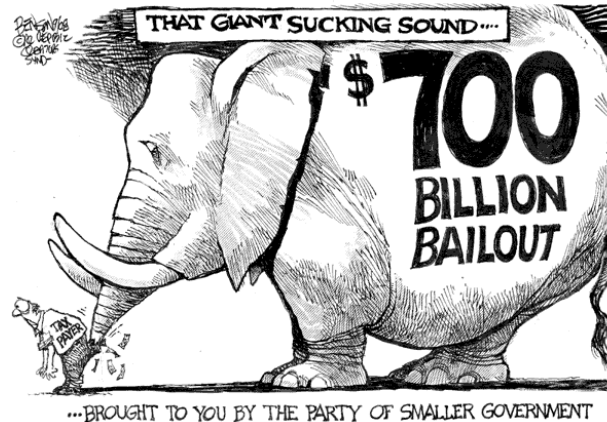
- Hard fork proposed

- Undo the transactions altogether and end the DAO (returning all money back to token holders)
- But, effectively a bailout for DAO token holders

Historical reference (2008 crash)

- Lehman took risks to make huge returns
 - When risks went south, asked for a government bailout
 - Didn't get one and failed
- But...
 - Eventually everyone else did

Emergency Economic Stabilization Act of 2008 :



COST OF 2008-2009 BANK BAILOUT*

Bank of America	\$3,496,780,985,709
Citigroup	\$2,591,415,050,066
Morgan Stanley	\$2,117,225,300,000
JPMorgan Chase	\$1,299,031,484,524

* Face value of federal loans, loan guarantees and bailout assistance (excluding repayments)
Source: Good Jobs First

- The exact thing that cryptocurrencies want to end!

2016 DAO

- The DAO and its investors took risks to make huge returns
- When risks went south, asked for an Ethereum Foundation bailout even though Ethereum worked exactly as intended
- Ethical discussion
 - Are DAO token holders like the banks?
 - Is the Ethereum Foundation like the government?
 - Was the DAO like the banks and considered "too big to fail"?
 - Is this doing what cryptocurrencies were intended to prevent?
 - What are the pros and cons of undoing the DAO transactions?

Cons

- "Code is law" - the original statement of the DAO terms and conditions should stand under any circumstances
- Blockchain should be immutable regardless of outcome
- Slippery slope
 - Once you modify/censor for one reason there is not a lot to keep you from doing it for other contracts
 - "Without an immutable censorship resistant ledger, a blockchain has very little value to offer."
- Ethereum Foundation developers were investors in the DAO
 - They propose bailing themselves out which is anathema to the ideas behind blockchains
 - <https://cryptohustle.com/5-reasons-why-the-dao-bailout-was-bad-for-ethereum/>

How hard forks justified the biggest bailout in cryptocurrency history



Chris Stewart [Follow](#)

Mar 21, 2017 · 2 min read

Pros

- "Code is law" is too drastic and humans should have the final say through social consensus
- Hacker should not be allowed to profit from exploit
- Slippery slope argument not valid as community is not beholden to past decisions, people can act rationally and fairly in each situation
- Not a bailout as money isn't being taken from the community, it is just a return of funds to the original investors
- If the community acts now it will make people that are unethical think twice before using Ethereum as their platform of choice (remember this for later)
- <https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/>

Aside: Formalism vs. Realism in legal governance

- Formalism
 - Law derived logically by examining the relevant facts, case law, and nothing else.
 - Law stands separate from social and political institutions
 - Law should derive from absolute principles
 - Much like advocates who insist on immutability at all costs
 - Judicial conservatism, Jeffersonian interpretation?
- Realism
 - Law is based on the decision of the courts, including any historical and social phenomena that influence that decision.
 - Anything that influences a judge is law
 - Law is a moving target, not inflexible dogma.
 - Much like advocates that insist on community-driven interpretation of the law
 - Judicial liberalism, Hamiltonian interpretation?

Put to a vote

- ~4.5% of those with ETH participate (results at <http://v1.carbonvote.com/>)

Vote YES:

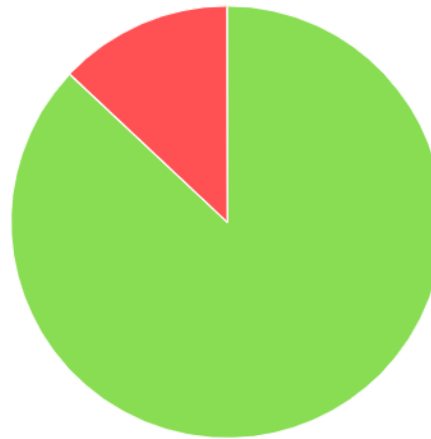
0x3039d0a94d51c67a4f35e742b571874e53467804

Vote NO:

0x58dd96aa829353032a21c95733ce484b949b2849

YES

Ether: 3964516.72178130761881221



■ YES ■ NO

NO

Ether: 577899.78346336959992868

19 Jul 2016 | 13:52 GMT

“Hard Fork” Coming to Restore Ethereum Funds to Investors of Hacked DAO

Facing a deadline to prevent the theft of \$40 million, The DAO tries to update its software. It's not so simple in a blockchain run by nobody in particular

By **Morgen E. Peck**

- 7/20/2016
 - Hard-fork deployed at Block 192,000 to avoid cashout by attacker on 7/27/2016
 - Funds from attacker contract given to a different smart contract whose sole purpose is to refund ETH to initial investors
 - 1 ETH = 100 DAO tokens

Ethereum Executes Blockchain Hard Fork to Return DAO Funds

At approximately 14:30 UTC today, China-based [ethereum](#) miner BW.com mined the ethereum blockchain's 192,000th block. Seconds later the mining pool also mined the first block on the new blockchain, which returned funds lost in the collapse of [The DAO](#) to an account available to its original investors.

The achievement, which returns approximately \$40m worth of ether from an account owned by an unknown hacker to a [new address](#), is being met with celebration by many members of the

ethereum community. However, the actual implications of the decision, which essentially showed that a supposedly immutable blockchain history can be altered, is yet to be seen.

- Others now want special treatment

“I made a bad contract in the first days ETH was online and lost 2K ETH with it, can I also get it back? Thanks!”

- Creates two versions of Ethereum

- Ethereum

- Those who adopted hard fork recommended by Ethereum Foundation

- Ethereum Classic

- Miners who refused to accept hard fork



Ethereum



Ethereum Classic

- What will the Ethereum Foundation look to "undo" in the future?
 - Tweet from 10/25/2019



Vitalik Non-giver of Ether ✓
@VitalikButerin



Suppose a popular smart contract wallet that a large portion of the ETH community uses gets hacked. This could be reverted by reverting all chain activity since the hack and doing a DAO-style HF to recover the funds. How much ETH must be at stake for you to support this?



14,577 votes · Final results

3:11 PM · Oct 25, 2019 · [Twitter Web App](#)

149 Retweets **376** Likes

Are blockchains that decentralized?



- Lessons from the DAO
 - Centralized management of software running the blockchain
 - Software update to roll back changes
 - Centralized ownership of full-nodes
 - Transactions rolled back via update that majority of full nodes accepted!
- (Later) Centralized ownership of miners
- Not the decentralized utopia that was imagined

Hard forking for fun and for profit (recovery)!

- Verge (4/2018)

Verge Coin Struck With A Severe Attack, Now Forced To Hard Fork

- Or...


 Stan Peterson  April 5, 2018  Altcoin News

Security

Buggy Verge crypto-cash gets hacked, devs go fork themselves, hard

Alt-currency's value tumbles amid malicious mining mishaps

By Shaun Nichols in San Francisco 6 Apr 2018 at 00:51

5  SHARE ▼

- "Verge activated an emergency hard fork intended to address the bug, but critics argued that the upgrade was merely a “band-aid” and did not eliminate the underlying vulnerability."
- Does this sound like the kind of governance you can invest in?

Compare to Bitcoin

- Recent theft (5/2019)

Hackers steal \$40 million worth of bitcoin in massive security breach

By Jordan Valinsky, [CNN Business](#)

Updated 10:30 AM ET, Wed May 8, 2019

- Rollback ledger?
 - Zhao (CEO of victimized Binance exchange), in response to questions about potentially issuing a rollback
 - “to be honest we can do that probably within the next few days but ... it may have some negative consequences in terms of destroying credibility for bitcoin”
 - Sirer, in response
 - “It takes only a handful of miners who will go along with a reorg. and perhaps they wouldn't do it for \$40 million, but there is a price at which they would do it...If it were to happen, it would undermine confidence in BTC, whose main claim to fame has always been security and immutability.”
- Pros and cons on Twitter thread
 - https://twitter.com/cz_binance/status/1125996197343154176

- Within the day



- Eventually apologizes 5/10/2019

- CZ will continue to communicate frequently with the crypto community via Twitter, even though he realizes that he sometimes might say the wrong things (like using "dirty words" such as "reorg"), for which he apologizes.

Aside

- Interesting counter-proposal to pull off a re-org of blockchain, keep Bitcoin purity, while deterring thefts in the future
 - <https://twitter.com/JeremyRubin/status/1125919526485254144>
 - Use private keys of hacked coins to sign old UTXOs of affected accounts and assign the BTC to miners
 - Miners have incentive to mine using these transactions!
 - Eventually miners will create a chain longer chain to undo transactions and obtain the hacked coins for themselves
 - Coins go to making the network more secure, reorgs to keep hackers from profiting at the same time, all within the rules of Bitcoin!
 - Must be done within several blocks to be feasible

Why hackers love BTC

- Mat Odell

"The reason bitcoin was stolen from binance and not any of the 100s of shitcoins they also offer is precisely because those chains are easy to rollback — or freeze — while bitcoin is not."

- <https://bitcoinist.com/binance-hackers-stole-bitcoin-superiority/>

But, people forget Bitcoin's history...

- August 15, 2010

<https://bitcointalk.org/index.php?topic=822.0>

- Block 74638 minted 184 billion BTC
- Code used for checking transactions did not account for integer overflow when summed!
- Way beyond original theoretical limit of 21 million BTC



Strange block 74638

August 15, 2010, 06:08:49 PM

Merited by vapourminer (1)

The "value out" in this block #74638 is quite strange:

Code:

```
      "hash" : "237fe8348fc77ace1
        "n" : 0
      },
      "scriptSig" : "0xA87C02384E1F18
    }
  ],
  "out" : [
    {
      "value" : 92233720368.54277039,
      "scriptPubKey" : "OP_DUP OP_HAS
    },
    {
      "value" : 92233720368.54277039,
      "scriptPubKey" : "OP_DUP OP_HAS
    }
  ]
},
"mrkl tree" : [
```

- Within 5 hours, software patch changing consensus rules to reject output value of all overflow transactions distributed to miners
 - Places a 21 million limit on transactions
 - Blockchain forked
 - Newer, "good" chain overtakes chain with overflow transaction at block 74691
 - <https://github.com/bitcoin/bitcoin/commit/d4c6b90ca3f9b47adb1b2724a0c3514f80635c84#diff-118fcbaaba162ba17933c7893247df3aR1013>

```

21 + static const int64 MAX_MONEY = 21000000 * COIN;
471 472         if (vin.empty() || vout.empty())
472 473             return error("CTransaction::CheckTransaction() : vin or vout empty");
473 474
474 - // Check for negative values
475 + // Check for negative or overflow output values
476 + int64 nValueOut = 0;
475 477         foreach(const CTxOut& txout, vout)
478 + {
476 479             if (txout.nValue < 0)
477 480                 return error("CTransaction::CheckTransaction() : txout.nValue negative");
481 +             if (txout.nValue > MAX_MONEY)
482 +                 return error("CTransaction::CheckTransaction() : txout.nValue too high");
483 +             nValueOut += txout.nValue;
484 +             if (nValueOut > MAX_MONEY)
485 +                 return error("CTransaction::CheckTransaction() : txout total too high");
486 +         }

```

Another accidental fork of Bitcoin...

- Bitcoin Core software version 0.8 released 3/2013
 - Inadvertently incompatible with version 0.7
 - Blockchain immediately forked
 - Two-chains operating separately from Block 225430
 - Within hours, operators via bitcoin-dev IRC channel decide to roll back to 0.7, then let 0.7 chain overtake 0.8
 - Operators of mining pools individually contacted and convinced to downgrade
 - Takes 24 blocks (6 hours) for 0.7 to overtake 0.8 chain

- Op-ed in Bitcoin Magazine that followed (3/2013)
 - <https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/>
 - *Bitcoin is clearly not at all the direct democracy that many of its early adherents imagined...if a centralized core of the Bitcoin community is powerful enough to successfully undertake these emergency measures to set right the Bitcoin blockchain, what else is it powerful enough to do? Force double spends to reverse million-dollar thefts? Block or even redirect transactions known to originate from Silk Road? Perhaps even modify Bitcoin's sacred 21 million currency supply limit?*
 - Irony
 - DAO fork happens only 3 years later



51% attacks

Centralization of mining resources

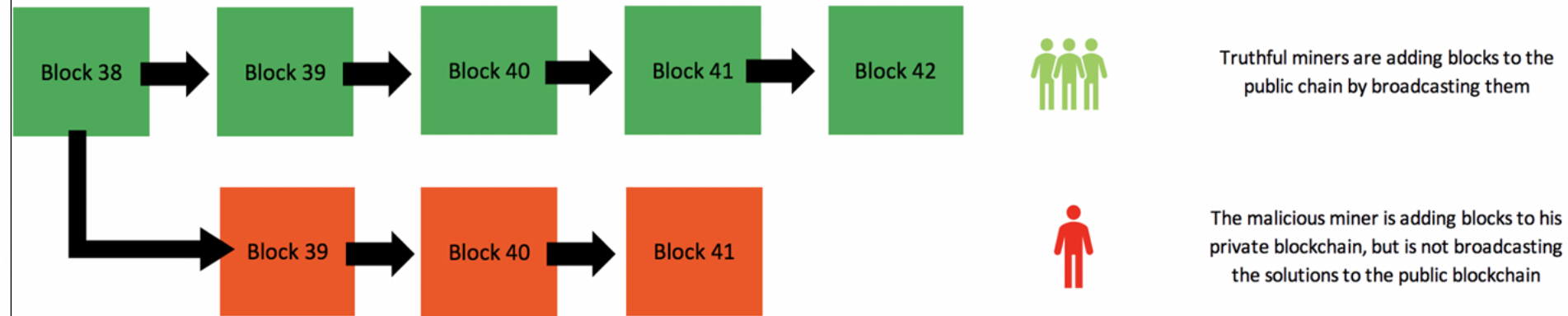
- Before: centralization of governance and software development
- Now: centralization of miners running the software
- But...
 - Malicious miners cannot forge transactions without private key
 - Block-mining delay prevents double-spending
 - Or does it?
 - Recall, longest-chain accepted by network
 - Assumption is that no one can control 51% of the mining resources
 - When assumption does not hold, double-spending is possible *using* the rules of the block-chain!

**Five Successful 51 Percent Attacks Have Earned
Cryptocurrency Hackers \$20 Million in 2018**

Jacob Godshall | Posted October 24, 2018

Step 1

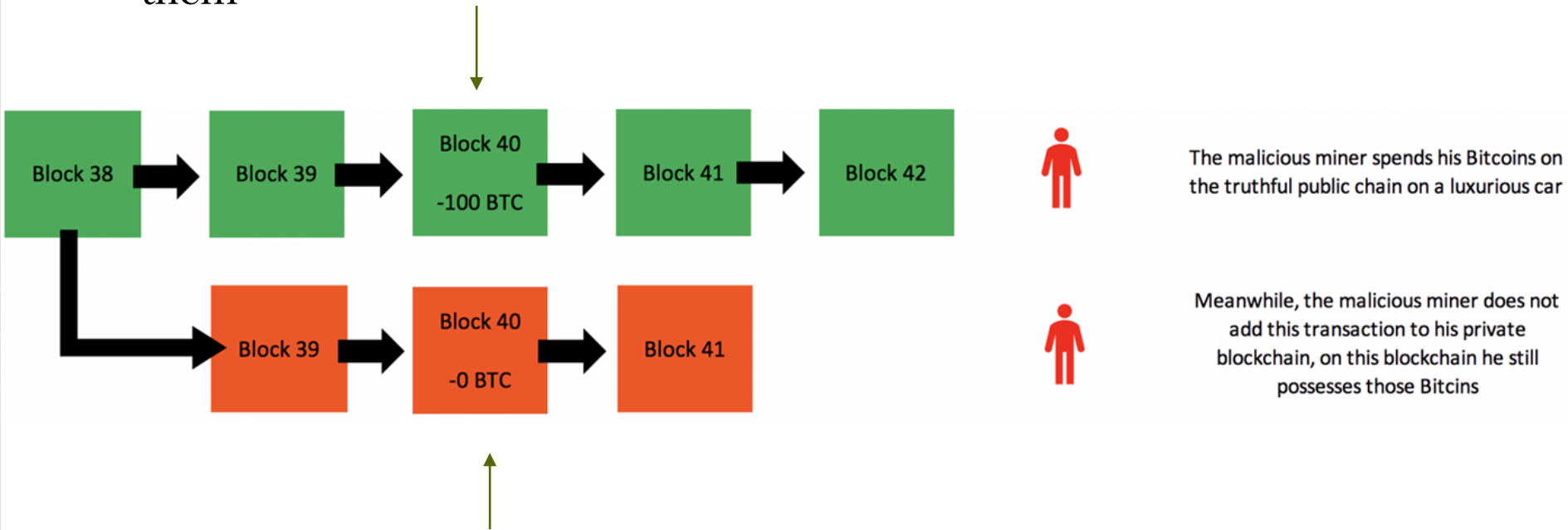
- Create a side-chain of your own transactions that mirrors main chain, but keep chain private



Figures via: <https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474>

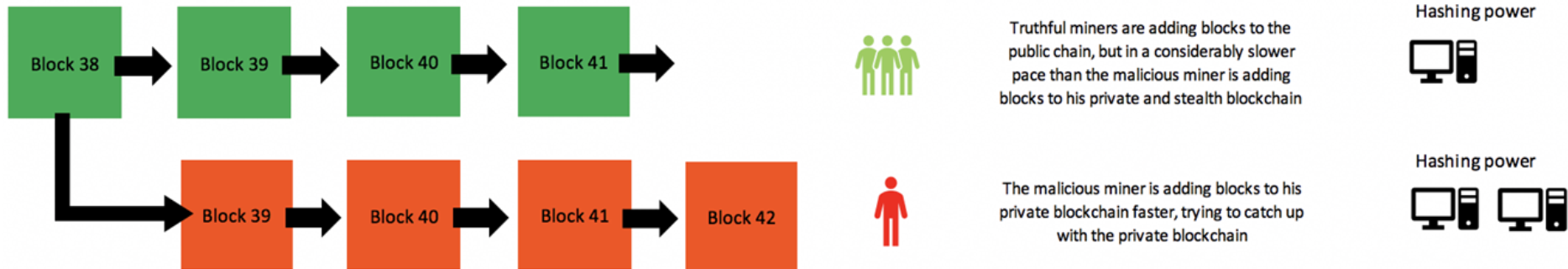
Step 2

- On main chain, go on a shopping spree (buy a car or some tokens)
 - But, create valid blocks in stealth chain without your transactions in them



Step 3

- The longest, heaviest chain will be accepted as current "truth"
- So co-opt 51% of mining resources
 - Maybe with the help of a cloud provider? (more later)
 - Work to build your chain faster than main chain
 - Adding blocks to private blockchain faster than main chain eventually allows you to create a longer chain



Or Step 3 even faster!

- Take down full nodes to get ahead...



Researcher kept a major Bitcoin bug secret for two years to prevent attacks

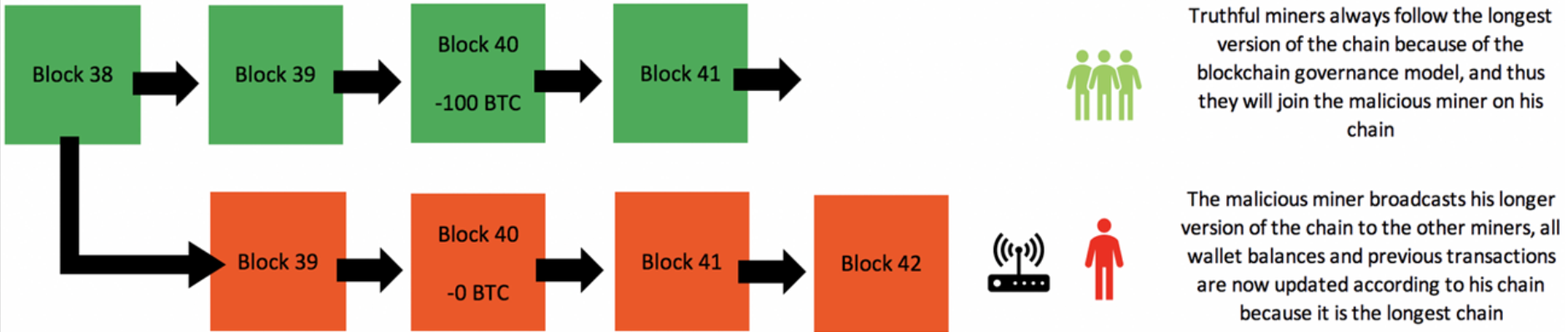
The INVDoS bug would have allowed attackers to crash Bitcoin nodes and other similar blockchains.



By [Catalin Cimpanu](#) for [Zero Day](#) | September 12, 2020 -- 10:25 GMT (03:25 PDT) | Topic: [Security](#)

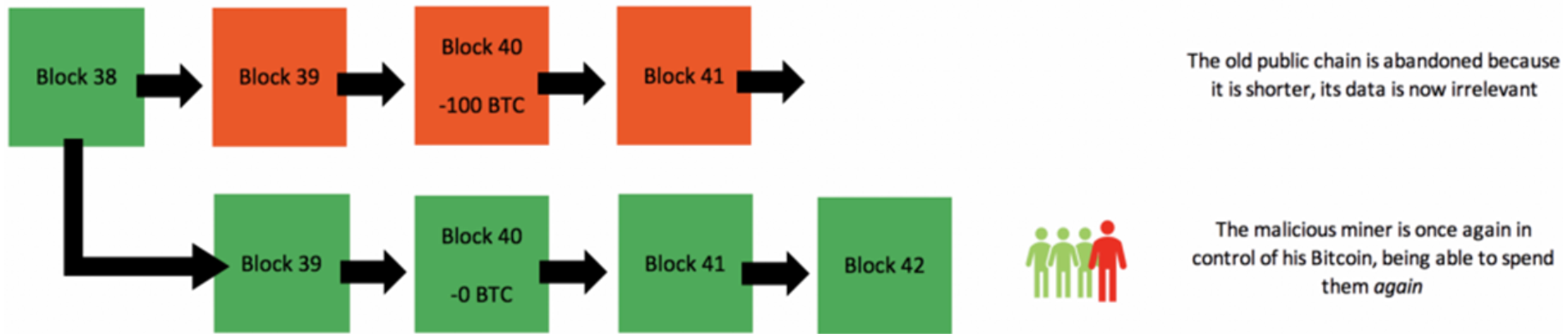
Step 4

- As soon as it is longer, broadcast your private stealth chain



Step 5

- Protocol sees that blocks are valid and the chain is longer
 - Must adopt it!
 - Old chain abandoned because it is shorter, rolling back the transaction
- Adversary can spend again



Motivates notion of confirmations

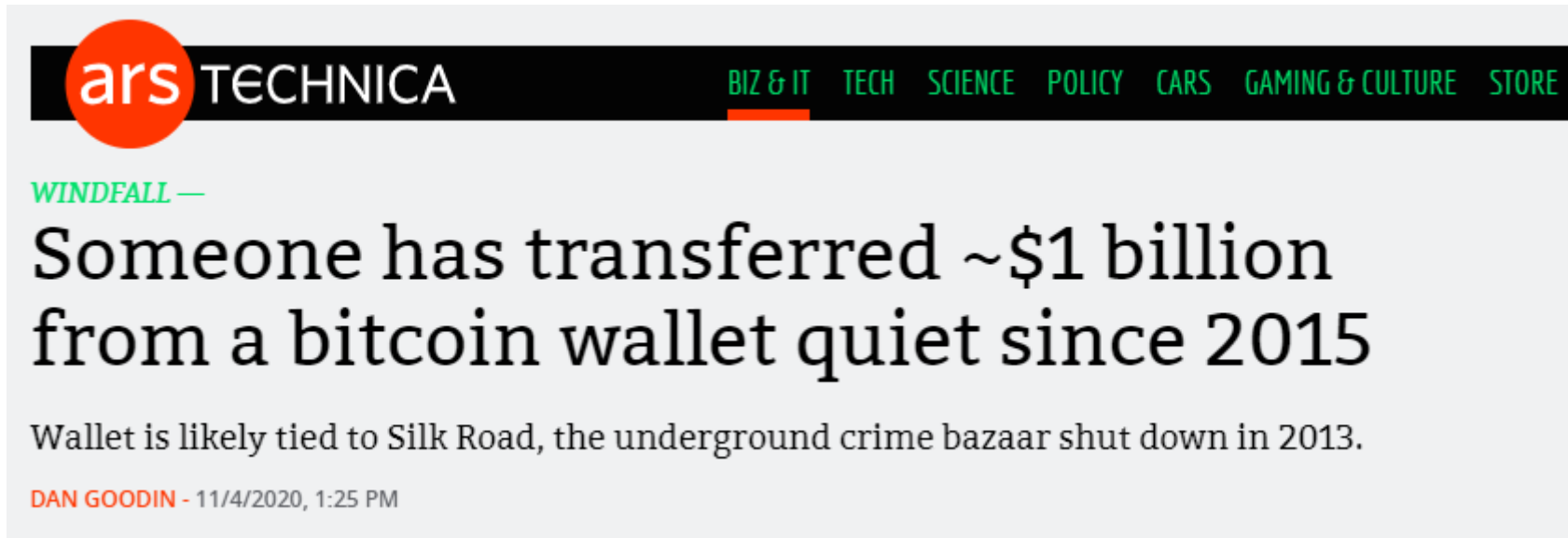
- Wait for a while to ensure history can not be rewritten!

How many Bitcoin Confirmations are Enough?

- 0 Payments with 0 confirmations can still be reversed! Wait for at least one.
- 1 One confirmation is enough for small Bitcoin payments less than \$1,000.
- 3 Enough for payments \$1,000 - \$10,000. Most exchanges require 3 confirmations for deposits.
- 6 Enough for large payments between \$10,000 - \$1,000,000. Six is standard for most transactions to be considered secure.
- 60 Suggested for large payments greater than \$1,000,000. Less is likely fine, but this is to be safe!

What about?

- Yesterday...



The image is a screenshot of the top portion of an Ars Technica article. At the top left is the Ars Technica logo, consisting of the word "ars" in white lowercase letters inside a red circle, followed by the word "TECHNICA" in white uppercase letters. To the right of the logo is a black navigation bar with several categories in green uppercase letters: "BIZ & IT", "TECH", "SCIENCE", "POLICY", "CARS", "GAMING & CULTURE", and "STORE". Below the navigation bar, the word "WINDFALL" is written in green uppercase letters, followed by a horizontal line. The main headline is in large, bold, black uppercase letters: "Someone has transferred ~\$1 billion from a bitcoin wallet quiet since 2015". Below the headline is a sub-headline in black text: "Wallet is likely tied to Silk Road, the underground crime bazaar shut down in 2013." At the bottom left of the article header, the author's name "DAN GOODIN" is written in red uppercase letters, followed by the date and time "11/4/2020, 1:25 PM" in black text.

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

WINDFALL —

Someone has transferred ~\$1 billion from a bitcoin wallet quiet since 2015

Wallet is likely tied to Silk Road, the underground crime bazaar shut down in 2013.

DAN GOODIN - 11/4/2020, 1:25 PM

Example: Ethereum Classic

- Small percentage of Ethereum full nodes refuse to undo transactions of the DAO re-entrancy hack
 - Hard fork that continues operating on old chain
 - Number of miners on Ethereum Classic very small
- Target of a 51% attack (1/2019)



Ethereum Classic

ALTCOINS

Coroner's Report on the Ethereum Classic [ETC] 51% attack; tracking the attacker's transactions on the blockchain



By Gareth Jenkinson

JAN 10, 2019

Ethereum Classic 51% Attack — The Reality of Proof-of-Work

"At time of writing, we have identified a total of 15 reorganizations, 12 of which contained double spends, totaling 219,500 ETC (~\$1.1M)."



Published 1 day ago on January 10, 2019

By Akash Girimath 

Bitcoin Gold

- Fork of Bitcoin to increase transaction throughput
- Attacked in 9/2018

Bittrex to Delist Bitcoin Gold Over 51% Attack

exchange Bittrex. The Seattle-based trading platform says they lost over 12,000 BTG during the network's 51% attack, and the firm had asked the BTG development team to compensate them for the loss.

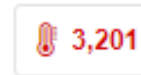
Bitcoin next?

Will Bitmain Stage A 51% Attack On The BTC Network?

The fate of the prototypical decentralized project could rest in the hands of two men.



By Paddy Baker — On Jun 25, 2018



The Chinese mining company Bitmain now controls over 40% of the BTC hashing power. This means that the company is approaching the hashing power required to control the Bitcoin network and – if it pleased – stage a 51% attack.

- Mining pools voluntarily reduce themselves to 40%
- Could a nation-state pull off an attack?

Do you need to be a nation state?

51% Attacks for Rent: The Trouble with a Liquid Mining Market

- Rent-a-miner attacks
 - <https://www.coindesk.com/51-attacks-for-rent%E2%80%8A-the-trouble-with-a-liquid-mining-market>
 - Use tens of thousands of dollars in computational resources over a short timeframe to obtain millions!
 - Much more profitable than legitimate mining (just bursty in its resource usage)
 - Q: Is this illegal or simply playing by the rules of Blockchain?

Now commonplace

Blockchain's Once-Feared 51% Attack Is Now Becoming Regular

- <https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular>

MAY 29, 2018 BY TONY SPILOTRO

Third Time's a Charm: Verge Suffers 51% Attack Yet Again

The privacy-focused cryptocurrency Verge, is quickly becoming a running joke within the cryptocurrency industry, after repeatedly suffering 51% attacks and having hackers exploit a vulnerability that's led to millions of dollars in Verge tokens being stolen.

- Can also be triggered via bug in code...

Privacy Coin Verge Succumbs to 51% Attack [Again]

 Josiah Wilmoth  22/05/2018  Altcoin News,

- "...the attacker manipulated a bug in the Verge code that allows malicious miners to set false timestamps on blocks and then rapidly mine new ones in quick succession."
 - \$1.75M lost in a few hours between blocks 2155850 and 2206272

← XVG block: 00000037f9d28dfe25a6bdf681ec8f51198b0503d084f654fba72ee70f75904a

Height	Difficulty	Confirmations	Size (kB)	Bits	Nonce	Timestamp
2200000	0.0002	6695	0.29	1e0ffff	3826299012	22nd May 2018 06:22:31

- Along with coordinated with a DDoS attack directed at several XVG mining pools.



it appears some mining pools are under ddos attack, and we are experiencing a delay in our blocks, we are working to resolve this.

♥ 574 8:17 PM - May 21, 2018



Krypton

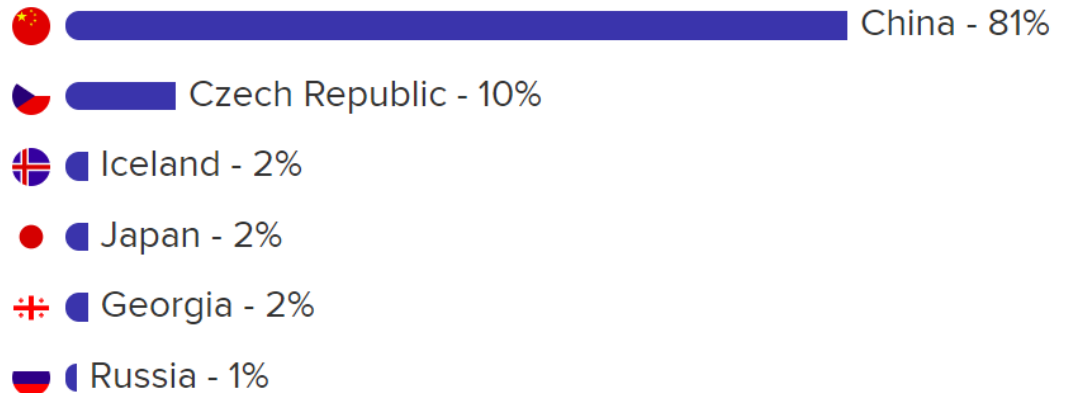
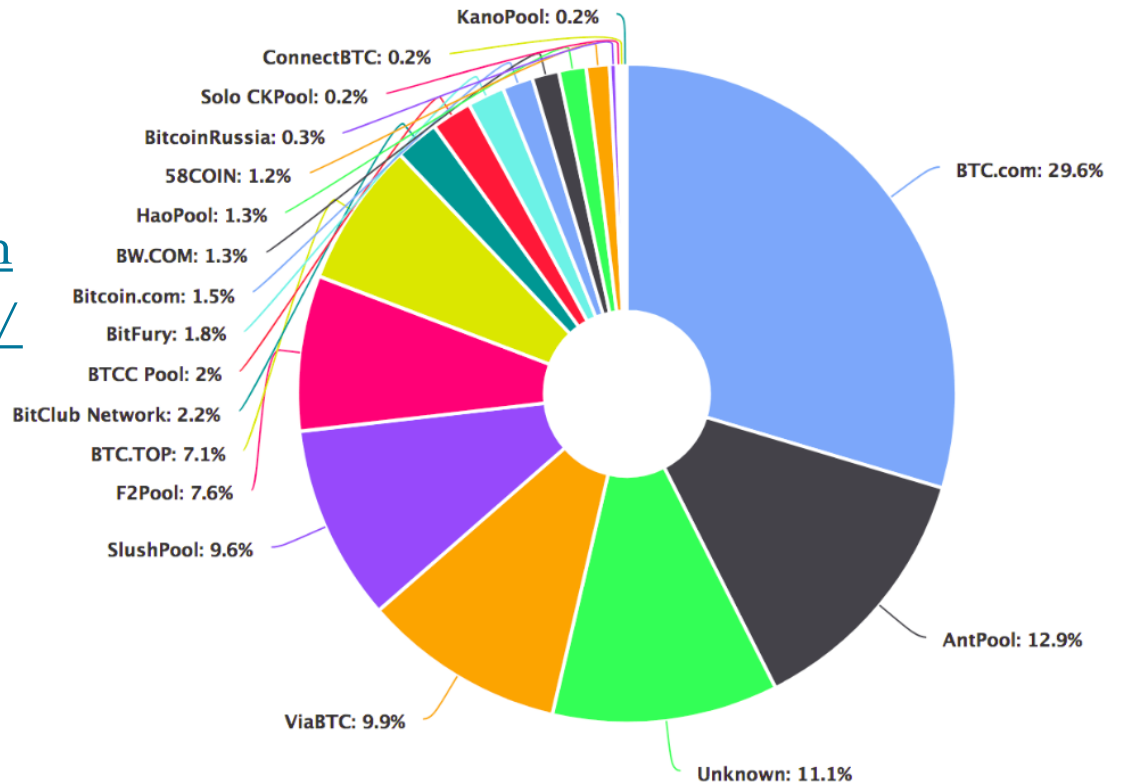
KRYPTON RECOVERS FROM A NEW TYPE OF 51% NETWORK ATTACK

🕒 August 26, 2016 👤 Rocky 📁 News

- Similar two pronged attack
 - Overpowering the network with at least 51% of the hashing power to roll back transactions and enable double-spend
 - Attackers rented miners for extra hashing power from Nicehash and used pool to conduct the attack!
 - DDoS-ing nodes to multiply network power.
 - Supernova mining pool and Krypton stats servers were also DDoS attacked to give the malicious miners an edge over the network.
 - Attacker sends KR to Bittrex, sells them for BTC and then rolled back the blockchain to reverse the transaction
 - 21,465 KR stolen from Bittrex by double spending on the network
 - Only ~\$4000 at the time

Mining centralization statistics

- Bitcoin (1/2019)
 - Mining pool distribution
 - <https://www.buybitcoinworldwide.com/mining/pools/>



Estimate 51% attack costs

- <https://www.crypto51.app>
- What if the NSA used all of its compute power to launch a 51% attack to undo N. Korean Bitcoin transactions?

Crypto51

About

PoW 51% Attack Cost

This is a collection of coins and the theoretical cost of a 51% attack on each network.

Learn More



Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	\$148.72 B	SHA-256	80,593 PH/s	?	0%

Alternate approach...Monero

- Avoid domination by mining pools by explicitly stacking the deck against mining operations using ASICs (9/2018)



Manufacturer Holds Cryptonight ASIC Firesale after Monero Hard Forks

- Does Monero become more or less vulnerable to 51% attacks?
 - Unclear
 - "Currently, it would be more profitable to dedicate your power to the chain than to attempt to defraud it. If confidence were overall lost in the chain, you wind up with nothing."
 - <https://www.ccn.com/binance-monero-mining-unprofitable-51-attack>

Ethereum 2.0: Towards Proof-of-Stake?

- Move towards Programmatic Proof-of-Work (ProgPoW) and Proof-of-Stake (PoS)
 - Reduce advantage of custom ASIC hardware for mining
- Ethereum's difficulty bomb to disable mining and move to proof-of-stake
- Easier said than done...
 - 9/2019

ETHEREUM'S BERLIN HARD FORK ARRIVES WITHOUT DIFFICULTY GROWTH

- Developers have voted several times to disable the difficulty time bomb, so that miners could get some grace time to seek block rewards.
 - The phasing out of mining is seen as an empty promise on the side of Ethereum's team
 - Inertia to maintain status-quo now in place

Devs vs. Miners

- Tension between developers, who want to limit ASIC dominance to make mining more decentralized and miners, who have invested significantly into ASIC who do not
- Initial deployment on Ropsten (10/2019)
 - "The Ropsten network showed what would happen if not all participants ... agree on moving forward. The test net split into two."
 - Despite moving on to another block production model, miners are influential enough to keep producing blocks.



By Joeri Cant

SEP 30, 2019

Early Arrival of Ethereum's Istanbul Hard Fork Causes Testnet Split
Huge miner pushing the non-forked chain



Mudit Gupta
@Mudit_Gupta



Which is the real ropsten?

The one supported by miners(s) that has the longest chain (non-istanbul fork)

OR

The one supported by the core devs but with smaller chain (istanbul fork)?

What will happen to the tokens that I issued on ropsten before the Istanbul fork?

1/

♡ 4 4:35 PM - Oct 5, 2019



[See Mudit Gupta's other Tweets](#)



Coming soon!

- Yesterday...

**Ethereum 2.0
Countdown Begins
With Release of
Deposit Contract**

Nov 4, 2020 at 15:38 UTC ▪ Updated Nov 4, 2020 at 16:33 UTC