

- Story of the Heist part I
- Blockchain and DAO theory
- Story of the Heist part II
- Discussion



The DAO launched on 30th April, 2016, with a 28-day funding window.

The DAO was a digital decentralized autonomous organization and a form of investor-directed venture capital fund.

The DAO had an objective to provide a new decentralized business model for organizing both commercial and non-profit enterprises.

It was instantiated on the Ethereum blockchain, and had no conventional management structure or board of directors.

The code of the DAO is open-source.

The DAO: Terms and Conditions

By Creating DAO tokens through interaction with The DAO's smart contract code, you expressly agree to all of the terms and conditions set forth in that code. If you do not understand or do not agree to those terms, you should not Create DAO tokens.

[...]

The DAO's smart contract code governs the Creation of DAO tokens and supercede any public statements about The DAO's Creation made by third parties or individuals associated with The DAO, past, present and future. The software code currently available at <https://github.com/slockit/dao> is the sole source for the terms under which DAO tokens may be created.

watch the statistics

The DAO has been created

1164.01 M

DAO TOKENS CREATED

11.99 M

TOTAL ETH

220.65 M

USD EQUIVALENT



1.50

LAST EXCHANGE RATE
ETH / 100 DAO TOKENS

0 -

NEXT PRICE PHASE

0 -

SINCE CREATION PERIOD ENDED
CREATED 28 MAY 09:00 GMT

Thank you all for your contribution

0xbb9bc244d798123fde783fcc1c72d3bb8c189413

DO NOT SEND ETH TO THIS ADDRESS
THE CREATION PHASE IS OVER, NO NEW TOKENS WILL BE GENERATED

Check Your Balance

ADDRESS ✓ ADDRESS

Enter the Ethereum address account used to create DAO tokens

CHECK

A Call for a Temporary Moratorium on “The DAO”

DRAFT (v0.3.2)

Dino Mark, Vlad Zamfir, Emin Gün Sirer
dino at smartwallet dot org, vlad@ethereum.org, egs@cs.cornell.edu
May 26, 2016
(revised May 30, 2016)

Over the past 3 weeks a Distributed Autonomous Organization (DAO) known simply as ‘The DAO’ and implemented as a smart contract on the Ethereum blockchain, has raised 11.5 million Ether, valued at \$150 million at the time of writing. This is the largest crowd-funding event in history. The DAO now controls 16% of the total supply of Ether. It is arguably the most visible project in the Ethereum ecosystem.



Emin Gün Sirer
@el33th4xor



Following

The DAO is an excellent solution to the non-existent problem of Kickstarter absconding with the funds.

RETWEETS

22

LIKES

44



10:21 AM - 14 May 2016



Stephan Tual [Follow](#)

Slock.it Founder, Blockchain and Smart Contract Expert, Former CCO Ethereum

May 26, 2016 · 3 min read · Unlisted

Proposal #1—DAO Security, Redux

I'm really excited to announce we are making available not one, but two Proposals to the DAO. Both have their code finalized the first one was already submitted to the Curators for addition to the whitelist following the formal procedure.

The first Proposal is a completely revised Proposal for DAO.Security. Initially, we had in mind for DAO.Security to include all aspects of what constituted the 'security' of the DAO, including the establishment and management of a Bug Bounty Program and several 3rd party audits of the DAO code itself.

Friday
June 17 2016

Exactly 44 years after
Watergate...

This is not a drill...

The DAO is being attacked.

**It has been going on for 3-4 hours, it
is draining ETH at a rapid rate.**

THE ATTACKER



MOVES 3.6 M ETHER INTO A 'CHILD DAO'

PANIC ENSUES....

TRADING IN ETHER IS HALTED ON THE MAJOR EXCHANGES

ATTEMPTS ARE MADE TO SWAMP THE NETWORK WITH SPURIOUS TRANSACTIONS

IT SEEMS THAT ALL \$220M WILL SOON BE LOST

Enter our unlikely Hero....



Vitalik Blogs :

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
hash0x7278d050619a624f84f51987149ddb439cdaadfba5966f7cfaea7ad44340a4ba (ie. the DAO and children) lead to the transaction (not just the call, the transaction) being invalid, starting from block 1760000 (precise block number subject to change up until the point the code is released), preventing the ether from being withdrawn by the attacker past the 27-day window. This will provide plenty of time for discussion of potential further steps including to give token holders the ability to recover their ether.

DAO token holders and ethereum users should sit tight and remain calm.
Exchanges should feel safe in resuming trading ETH.

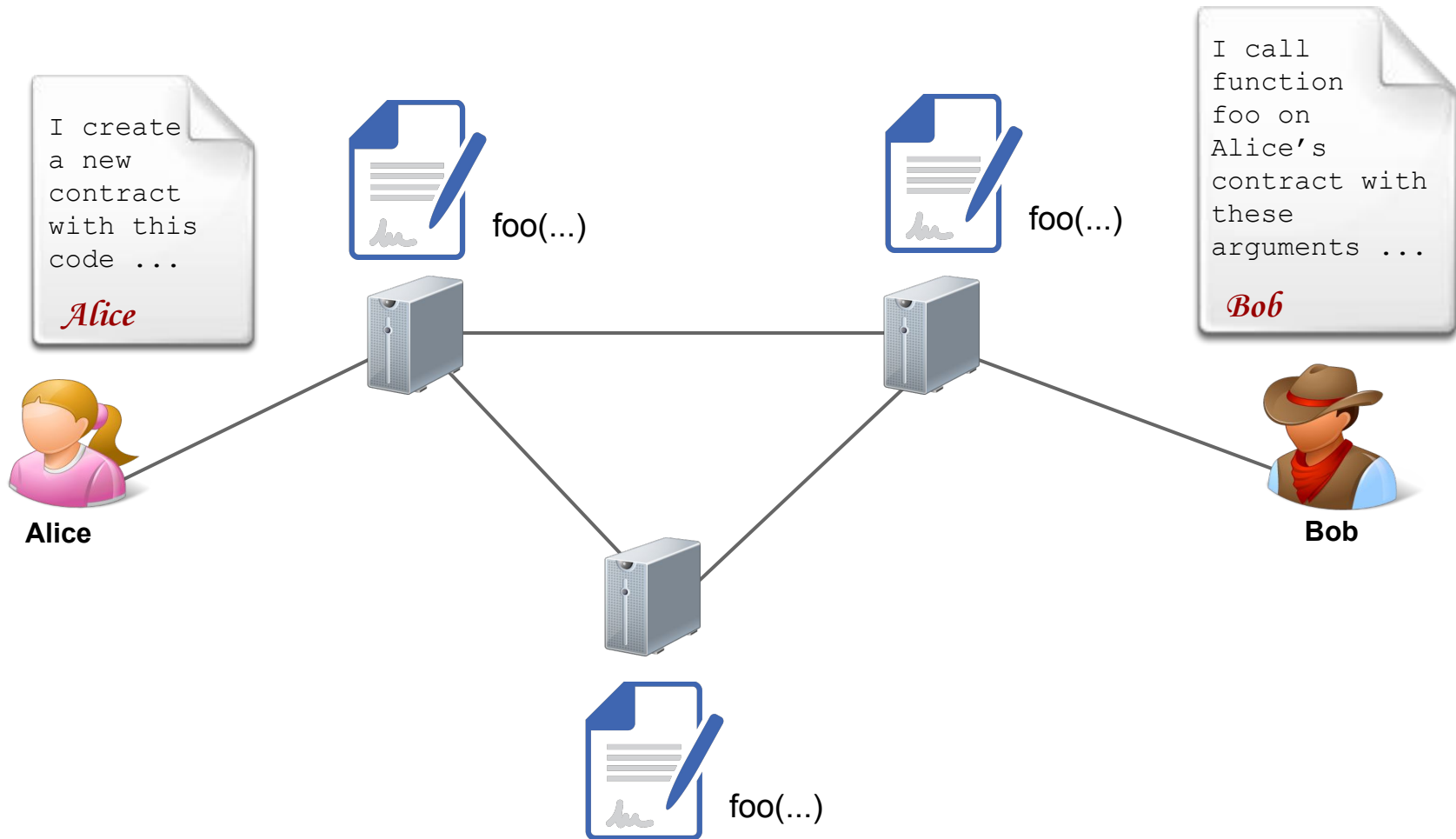
....and the attack stops

**This pause in the action gives us chance to explain
Blockchains, DAOs and Forks**

FEATURES OF THE BLOCKCHAIN

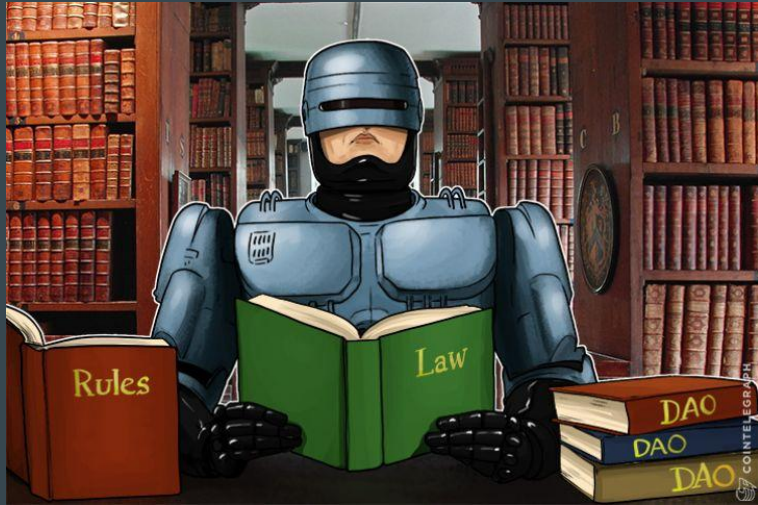
- The network is resilient
- The system is censorship / tamper proof
- A Shared Ledger gives transparency
- The ledger is append only, it is seen as immutable





Decentralised Autonomous Organisations (DAO)

A Business organisation run according to rules specified in a smart contract



The DAO contains some kind of internal property that is valuable in some way, and it has the ability to use that property as a mechanism for rewarding certain activities.

- Outsiders can see the governance algorithm
- It may use voting or prediction markets to choose policy

How to Steal \$50M - the exploit in detail

...

```
// Burn DAO Tokens
```

```
Transfer(msg.sender, 0, balances[msg.sender]);
```

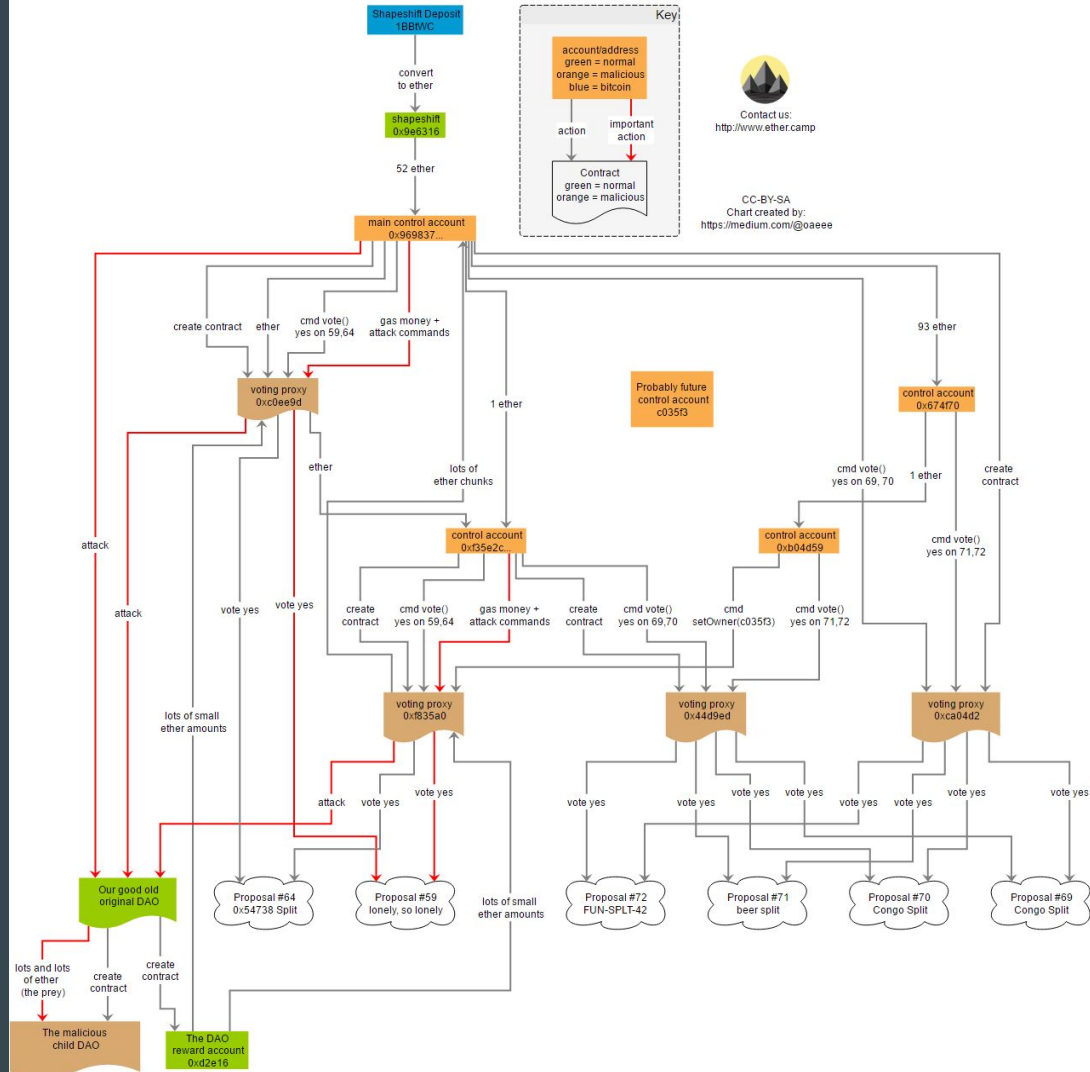
```
withdrawRewardFor(msg.sender); // be nice, and get his rewards
```

```
totalSupply -= balances[msg.sender];
```

```
balances[msg.sender] = 0;
```

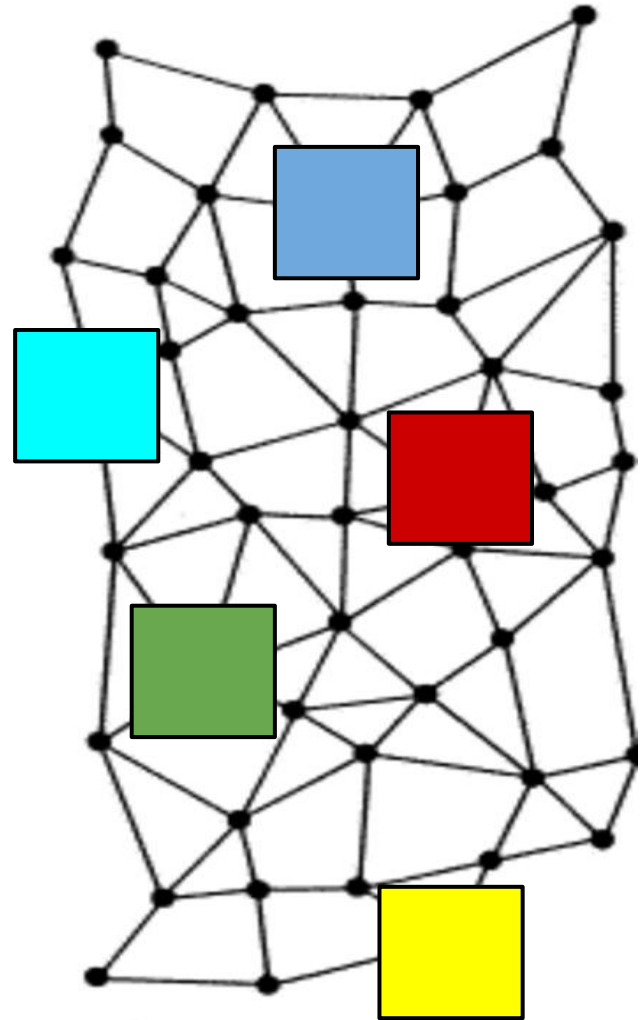
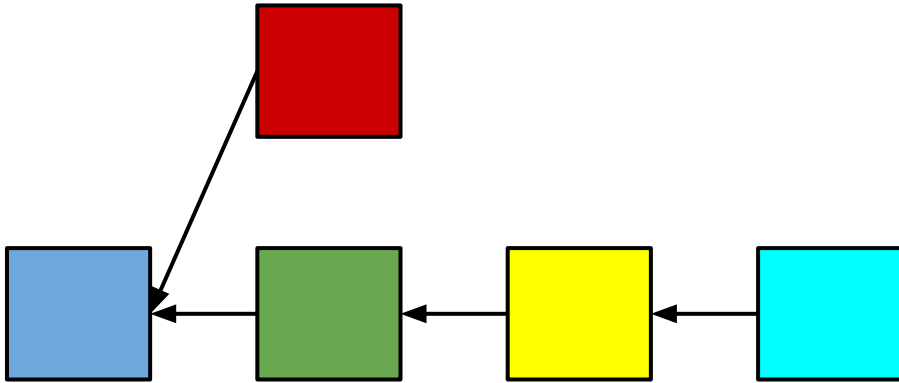
```
paidOut[msg.sender] = 0;
```

```
return true;
```



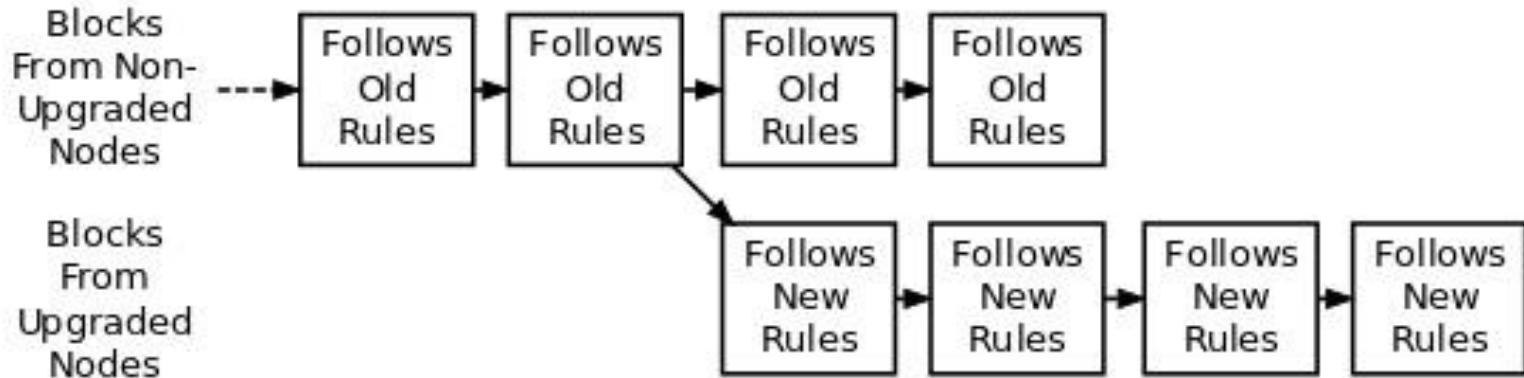
Forks

The blockchain is forking all the time as there are slight disagreements about the ordering of transactions, but the underlying protocols and mechanisms ensure that these forks are reconciled quickly and we have one absolute agreed upon version of events.



Hard and Soft forks are permanent

We ask the users of the system to change their software and follow a new set of protocols.



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

Funds in the DAO are still vulnerable...



The Robin Hood Group Successfully drains the DAO

DAO is now mostly empty. 7.2M ether have been secured so far. The community needs to help by identifying the rest.

[https://etherscan.io/address/0xb136707642a4ea12fb4bae820f03d2562ebff487 ...](https://etherscan.io/address/0xb136707642a4ea12fb4bae820f03d2562ebff487...) - alex van de sande

===== 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"

===== END SIGNED MESSAGE =====

About Carbonvote.com

Carbonvote.com was initiated during the DAO hard fork and conducted vote in a secure web-page fashion with the feature that the voting conducted did not require coins to leave voters' wallets. It had been a great source of reference when the community decided to go with the fork. Our thanks to all that participated in the last and our first round of the vote in DAO hard fork.

Once again, Carbonvote.com is a community initiated project dedicated to be an important source of reference in a quantitate way, to offer suggestions to the directions of Ethereum for developers and the Ethereum Foundation. We are open to feedbacks to improve in order to better serve the purpose.

If you are looking for historical votes, please visit <http://v1.carbonvote.com>.

Hard Fork Day

Previous

Block Number: 1920000 (2 hours ago)

- Hash: 0x4985f5ca3d2afbec36529aa96f74de3cc10a2a4a6c44f2157a57d2c6059a11bb
- Difficulty: 62,413,376,722,602
- Miner: [bw](#)
- Gas Limit: 4,712,384
- Gas Usage: 1.8% (84,000 of 4,712,384)
- Time: 2016-07-20 15:20:40 (2 hours ago)
- Uncle Hash: 0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347
- Root: 0xc5e389416116e3696cce82ec4533cce33efccb24ce245ae9546a4b8f0d5e9a75
- Tx Hash: 0x7701df8e07169452554d14aadd7bfa256d4a1d0355c1d174ab373e3e2d0a3743
- Size: 976 bytes
- Extra: dao-hard-fork (Raw: 0x64616f2d686172642d666f726b)
- Nonce: 0xbede87201de42426
- Reward: 5.00168 Ether

End of the Story

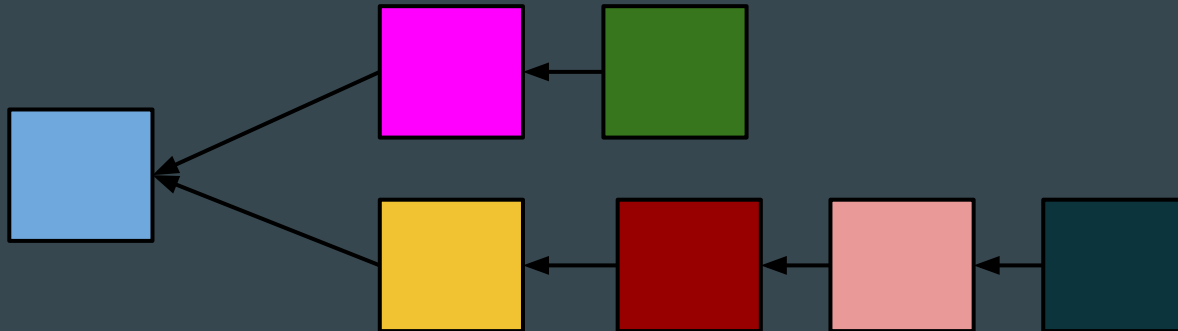
Of course not, we need a sequel....

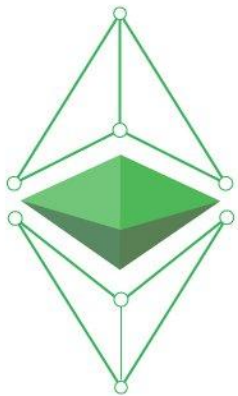
Ethereum

CLASSIC



phneep.com





ethereum
classic

ETH and ETC



On the 5th September the attacker withdrew his ETC from the Dark DAO

The attacker donated 1,000 ETC to an address associated with ETC development.

The Robin Hood Group kindly ask that the recipient of these funds deposit the 1000 ETC to the withdraw contract so it can be distributed to its rightful owners.

Attacker's Account 10/5/2017

Address

0x5e8f0e63e7614c47079a41ad4c37be7def06df5a

Balance

3360332.0323 ETC

\$21,237,298

\$22,144,589 (today)

Movement of funds continuing

07 Dec 2016, 01:23

50000.0000 ether

0x52a12a7daaa2ad99c9263399aaaf8ccdb54171af

06 Dec 2016, 03:19

30000.0000 ether

0xde284c656834bf9f75e1094c059e99beffd4da3a



Bitcoin Address

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

Summary

Address [1M2aaNN3GTw6dy13uScodHaQ8Egr6xr6Ew](#)

Hash 160 [dbaef57a72243859c056175cedf54c2b6d3efa4f](#)

Tools [Related Tags](#) - [Unspent Outputs](#)

Transactions

No. Transactions 59

Total Received **148.5228178 BTC**

Final Balance **50.32070393 BTC**

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

Transactions (Oldest First)

[Filter](#) ▼[d785e3c9f93939002639859a0eda78b741616f31917330bd5e1585af39894740](#)

2017-04-07 11:34:59

[1M2aaNN3GTw6dy13uScodHaQ8Egr6xr6Ew](#)

[1LyHiDUxMDMZx8jUVJANWZ7E2WNpWVRqMr](#)
[1L725GwXwWMZ2xHPRwg3SkirrSkW2C5rMK](#)

20.15 BTC

1.75521913 BTC

-21.485593 BTC[cbab44b87afb88a05c00234dd1a13ec1d26666909b6abf8a364b44a7f7bf87d](#)

2017-01-13 04:02:50


[1M2aaNN3GTw6dy13uScodHaQ8Egr6xr6Ew](#)

[1NXpyeKpd5ziYVtWbWojQ63QRGdQmAbLao](#)
[1MNNak3Ya2wqixfoKAUobHPXmLYMysDa2v](#)

25 BTC

0.42175603 BTC

-21.44914531 BTC
























Payment Request

Donation Button

Address	bc1qjkn9k4qjqshj5k3fkgx5p3nhzxjq90cpah4vy 
Format	BECH32 (P2WPKH)
Transactions	2
Total Received	50.32067244 BTC
Total Sent	50.32067244 BTC
Final Balance	0.00000000 BTC

Transactions

Hash	08f1dcd0371b544dacc3901e42ddc278519f...	2019-09-07 08:30
		
bc1q704a5kpwkvrgwn2...	0.10040243 BTC 	bc1q5wrnnlfe9ml3jsavv... 0.00322267 BTC 
bc1qvn3nzum38mhrf8...	0.10040244 BTC 	bc1q5gzvv3qd0yg6cng... 0.00359361 BTC 
bc1q6yf9zk9kwjcqcqk...	6.00640104 BTC 	bc1q3q6d6gzmgwjy78... 0.00875804 BTC 
bc1q432lq5wcz9vnpdj...	0.09920768 BTC 	bc1q77yr0r04wkkrut9... 0.01092553 BTC 
bc1quwv8tncaxq04xkej...	0.10043280 BTC 	bc1q6nwg20uq9zpe2th... 0.02051807 BTC 
bc1qt803evvdzp7xcnxq...	0.10025031 BTC 	bc1qs604c7jv6amk4cx... 0.03560141 BTC 
bc1qqxr5rx965qm0wm...	0.10100000 BTC 	bc1qn5nqxfm5p35pwm... 0.04399288 BTC 
bc1q5zp5n47nl99lt56u...	11.12073724 BTC 	bc1qxzmh69zv3pvuwa... 0.04403251 BTC 
bc1qrr24xuh5jv8947hrn...	4.46631106 BTC 	bc1qza0gjh0r7fq8d3ld... 0.04925245 BTC 
bc1qczfegsu8keqg5ztn...	0.20084850 BTC 	bc1q7r2ruh88euhgtxpr... 0.07603806 BTC 
Load more inputs... (64 remaining)		Load more outputs... (162 remaining)

What about the Robin Hood Group ?

- Did they return all the ETC correctly ?
- Did they dump a large amount of ETC onto the exchanges in an attempt to sabotage ETC ?

At no point did the group intend to “go rogue.” - Bity.SA

Who is the bad guy ?

He followed the rules of the DAO

He didnt want a split of the Ethereum community

His actions have prompted research into provable code, and safer patterns in smart contracts



He violated one of the basic concepts of the blockchain

He split the Ethereum community

His associates may have attempted to sabotage Ethereum Classic



Questions of Governance

The chaotic response to the DAO attack showed the lack of a governance mechanism

How do we deal with things we don't like ?

Should we change things we don't like ?

Who is 'we' anyway ?

Meatspace Law versus Blockchain Law

- Can a DAO be considered a company, If not, can that be enforced ?
- How do we determine the jurisdiction of the users of the DAO, and the DAO itself ?
- Are changes to the DAO's behaviour legal given the terms and conditions ?
- Are smart contract developers liable for the behaviour of code they write ?
- Are miners accountable if they mine illegal transactions ?

“The DAO is empty.”

老子

Dao de Jing, late 4th century B.C.