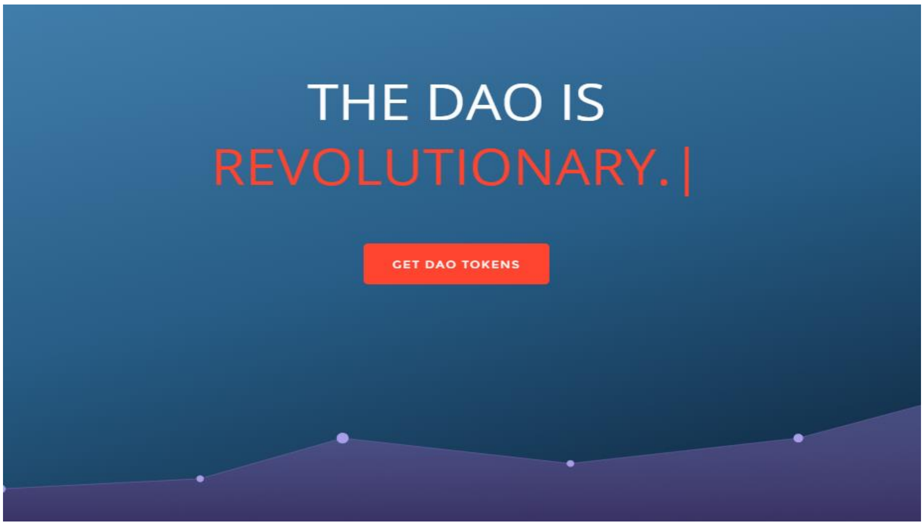
Revisiting "The DAO"

22 November 2017



(Source: DaoHub)

Abstract

In this piece, we revisit "The DAO" and the events following its failure. We analyse what happened to the various buckets of funds inside The DAO, on both sides of the chainsplit that it caused. We identify US$140 million of unclaimed funds still inside what is left of The DAO.

Key points

- *The DAO hacker appears to control tokens worth approximately US$60 million.*
- *There are currently around US$140 million of unclaimed funds still inside The DAO withdrawal contracts.*
- *In June 2017, the USD value of unclaimed funds inside The DAO was higher than the value of the amount initially raised in May 2016.*
- *After a 10 January 2018 deadline, around US$26 million of the funds may no longer be available to be claimed.*

BitMEX Research

Filtering out the hype with unbiased, evidence-based reports on the crypto-coin ecosystem.

BitMEX Research is also active on Twitter and Reddit.

research.bitmex.com

Previous reports:

The implications for Bitcoin of the new Bitcoin Cash difficulty adjustment mechanism
(16/11/17)

The Litecoin vs. Dogecoin hash-rate wars of 2014 and implications for Bitcoin vs. Bitcoin Cash
(16/11/17)

Trading Tip: Attempt to obtain free Bitcoin Cash on Bitfinex
(12/11/17)

Non Empty Smaller Block Data By Mining Pool
(01/11/17)

Overview

In the early summer of 2016, a project called "The DAO" generated a substantial amount of excitement in the crypto space. DAO stands for Decentralized Autonomous Organization, and to the confusion of many, The DAO (as the group styled its name) consumed that entire moniker for itself. The DAO was to be an autonomous investment fund, investing in projects determined by the token holders. The fund was to be governed by a "code is law" philosophy, as opposed to the centralised top-down control mechanisms in traditional investment funds, where key individuals matter.

Many believed this novel approach would lead to superior investment returns. Although it is a unique and potentially interesting approach, expecting strong investment returns at this point may be somewhat naive.

The fund raised Ethereum tokens worth approximately US$150 million at the time, around 14% of all the Ether in existence, with investors presumably expecting spectacular returns. The downside risk was expected to be minimal or even zero, since one was supposed to be able to withdraw one's Ethereum from The DAO whenever one wished. In reality, doing so was a complex and error-prone process.

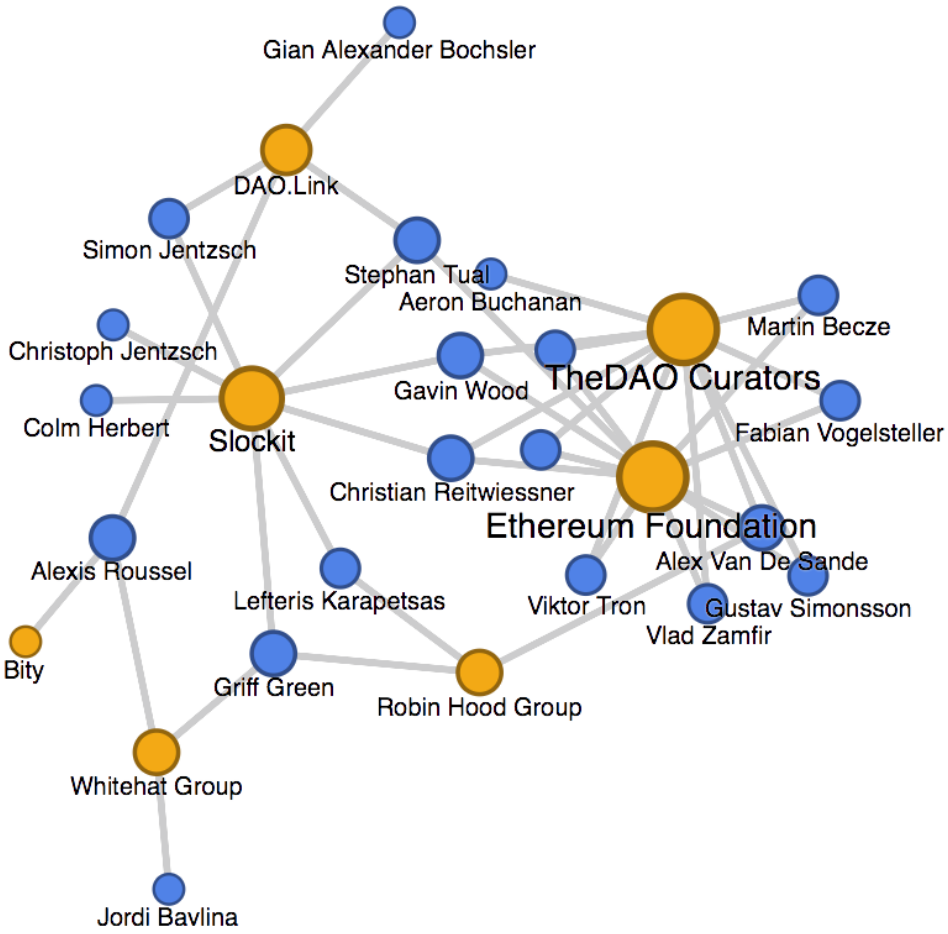
Problems with The DAO

As it turns out, The DAO was fundamentally flawed on several levels, as many in the Ethereum Foundation pointed out before the exploit was discovered. For instance:

- **Economic incentives** — The incentive model of the project was poorly thought out. For example, there was little incentive to vote "no" on investment proposals, since "no" voters became invested in approved projects. Those that did not vote did not become exposed to the project. Additionally, there was no stated mechanism for forcing successful projects to contribute profits back into The DAO.
- **Token viability** — The creation of new projects would have ended up creating new classes of DAO tokens, such that each class was entitled to different risks and rewards. This meant that the tokens would not be fungible, an issue poorly understood by exchanges and the community.
- **Buggy code** — The code did not always implement what was described or intended. The smart-contract code did not appear to be adequately reviewed. The coders did not appear to fully grasp its language, Solidity, nor some of the states the contract could reach.

A few weeks after the conclusion of the token sale, a hacker found an exploit in the code that allowed them to access The DAO's funds and drain some of it into a child DAO over which the hacker potentially had significant control. This led to an Ethereum hardfork, which was an attempt to prevent the hacker from controlling the funds and to return the funds to the initial investors. Since some in the Ethereum community were unhappy about this, it lead to the chainsplit between ETH and ETC.

The main groups and individuals related to The DAO



Network map of the main groups and the individuals involved in The DAO. There are other Ethereum foundation members with no association with The DAO, who are excluded from the diagram. Blue circles represent individuals; yellow circles represent organizations.
(**Source:** BitMEX Research)

	Description	People involved
DAOHub.org	A DAO community website promoting The DAO, hosted by DAO.link.	Felix Albert, Auryn Macmillan, Boyan Balinov, Arno Gaboury, Michal Brazewicz, Taylor Van Orden, Des Donnelly, Daniel McClure (source)
Slock.it	Slock.it wrote the code for The DAO and the company was hoping to develop smart locks. Slock.it was expected to be financed by The DAO.	Stephan Tual, Lefteris Karapetsas, Griff Green, Christoph Jentzsch, his brother Simon Jentzsch, Gavin Wood, Christian Reitwießner (source)
The hacker	The exploiter of The DAO.	Anonymous
DAO token holders (DTH)	Individuals from the general public who contributed to The DAO crowd sale or purchased DAO tokens on the open market.	22,873 account holders (source)
The DAO curators	Third-party arbitrators separate from Slock.it who manage disputes or emergency situations arising from The DAO.	Taylor Gerring, Viktor Tron, Christian Reitwießner, Gustav Simonsson, Fabian Vogelsteller, Aeron Buchanan, Martin Becze, Vitalik Buterin, Alex Van de Sande, Vlad Zamfir, Gavin Wood (resigned as a DAO curator prior to the exploit) (source)
Bity	A Swiss based cryptocurrency exchange in partnership with Slock.it. The exchange publishes WHG announcements. (source)	Alexis Roussel (source)
DAO.Link	A Swiss-registered joint venture of Slock.it and Bity, which hosts the DAOHub website.	Stephan Tual, Simon Jentzsch, Alexis Roussel (source)

Robin Hood Group (RHG)	The original “white hat” group, which secured the majority of The DAO funds pre-fork.	Publicly: Alex Van de Sande, Griff Green, Lefteris Karapetsas Stephan Tual claims: “individuals from the eth foundation, devs, security experts, ethcore, slock, etc.” (source)
Whitehat Group (WHG)	The organisation that took ownership of ETC from the RHG. The WHG has close ties to Bity.	Only publicly known members are Jordi Baylina and Griff Green (source)
The Ethereum Foundation	Non-profit foundation behind the creation of Ethereum.	Many individuals including some of the founders of Ethereum (source)

The DAO timeline

In order to fully understand and account for the proper ownership of the funds, we must revisit the provenance of The DAO funds before, during, and after the hardfork.

Date	Event	Movement of funds
30 April 2016	The DAO crowdsale is launched. (source)	
25 May 2016	The DAO crowd sale concludes.	~11.5 million pre-fork ETH raised.
17 June 2016	The DAO is drained into a child DAO by the hacker. (source)	~3.6 million pre-fork ETH drained to hacker’s child DAO.

A child DAO can be split from the main DAO as part of The DAO’s governance process, similar to a spin-off company.

The splitting process was exploited by the hacker using a recursive-call exploit, which drained more funds from the parent DAO than intended. The owner of a newly formed child DAO cannot withdraw those funds immediately but must wait for a voting period to end before securing those funds and being able to freely transfer them.

This voting period gave the Ethereum community a window of opportunity to attempt to reclaim the funds by attempting to exploit the hacker's child DAO using the same vulnerability. This, however, might have resulted in perpetual splitting and a DAO war, whereby the funds would be stuck in limbo forever as long as neither the hacker nor RHG gave up. This process could be easily scripted so would not take much effort on either side.

One way to solve this would be the implementation of a softfork to censor the hacker's transactions, preventing them from participating in this war and quickly allowing the funds to be recovered.

Date	Event	Movement of funds
21 June 2016	RHG begin "DAO Wars" and are able to recover a majority of the funds. (source)	~8.1 million pre-fork ETH drained into the RHG's child DAOs using the same vulnerability.
24 June 2016	DAO Wars softfork proposed to secure attacker's ~3.6 million pre-fork ETH. (source)	Would have censored transactions to prevent hacker from accessing their child DAO.
28 June 2016	Critical flaw discovered in DAO Wars softfork, which is then abandoned (source)	

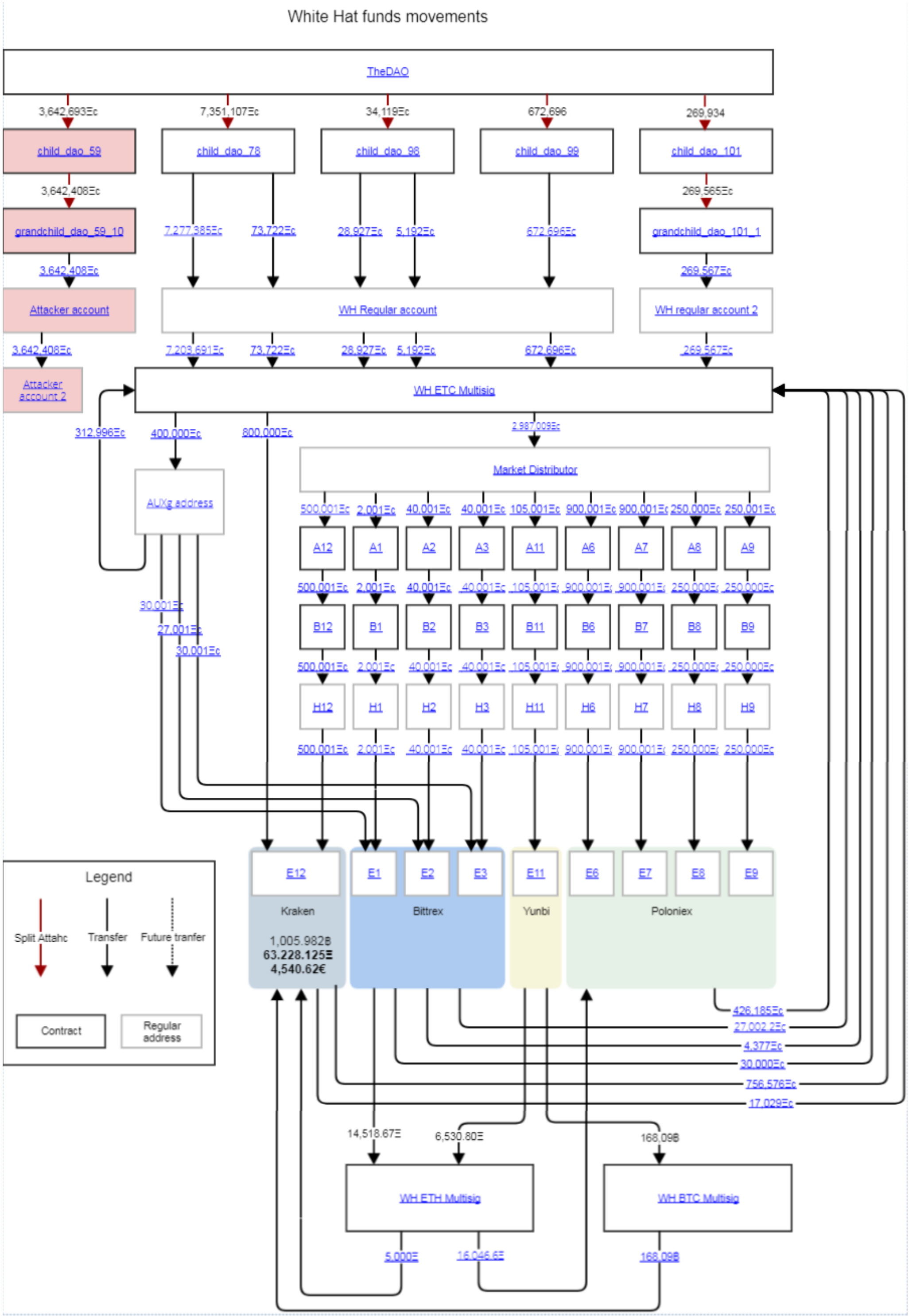
At this point, the RHG had managed to secure around 70% of the funds by exploiting other child DAOs, but in order to guarantee the ability to reclaim the remaining 30% (around 3.6 million pre-fork ETH), a hardfork was the only possibility. Moreover, the softfork proposal was found to have critical security vulnerabilities and was quickly scrapped.

Date	Event	Movement of funds
20 July 2016	Hardfork is implemented, effectively undoing the effects of The DAO hack and making DTH whole on the forked ETH chain. Implemented via two withdrawal contracts. (source, source)	~11.5 million post-fork ETH returned to DAO withdraw contract, which can be claimed by DTH based on their current DAO token balances.
20 July 2016	ETC, the not-forked chain, continues to be mined.	The RHG and The DAO hacker will eventually have access to ETC in child DAOs.

After the fork, there are two chains in parallel universes: ETH, where the hack is undone, and ETC, where the hack remains. The RHG have still secured around 70% of the ETC, and could have continued the attack on the ETC chain using the aforementioned "DAO Wars" limbo strategy, but decide not to. To refund DTH on the ETH chain, a withdrawal contract is used, which DTH must call to claim their ETH.

Date	Event	Movement of funds
23 July 2016	ETC is listed on Poloniex; other exchanges follow suit. ETC/USD reaches a third of ETH/USD. (source)	n/a
9 Aug 2016	The RHG hands ownership of the ETC funds to the WHG. The WHG receive funds in their ETC multisig wallet as the ETC child DAOs mature. (source)	~8.1 million ETC secured by the WHG.
10 Aug 2016	Unannounced, WHG/Bity use Bity's "verified money service business" account to attempt to tumble and swap 3 million ETC on four exchanges for ETH, BTC, and EUR. (source)	Poloniex freezes 2.3 million ETC, Kraken trades but freezes 1.3 million worth of ETC, Bittrex trades and processes 82,000 ETC, and Yunbi trades and processes 101,000 ETC.
12 Aug 2016	After the majority of the tumbled ETC is frozen, WHG/Bity announce that they have decided not to sell the ETC for ETH, and instead will distribute ETC to DTH. (source)	Bity trade back BTC, ETH, and EUR into ~1.5 million ETC, bringing their balance back to ~8.1 million ETC.

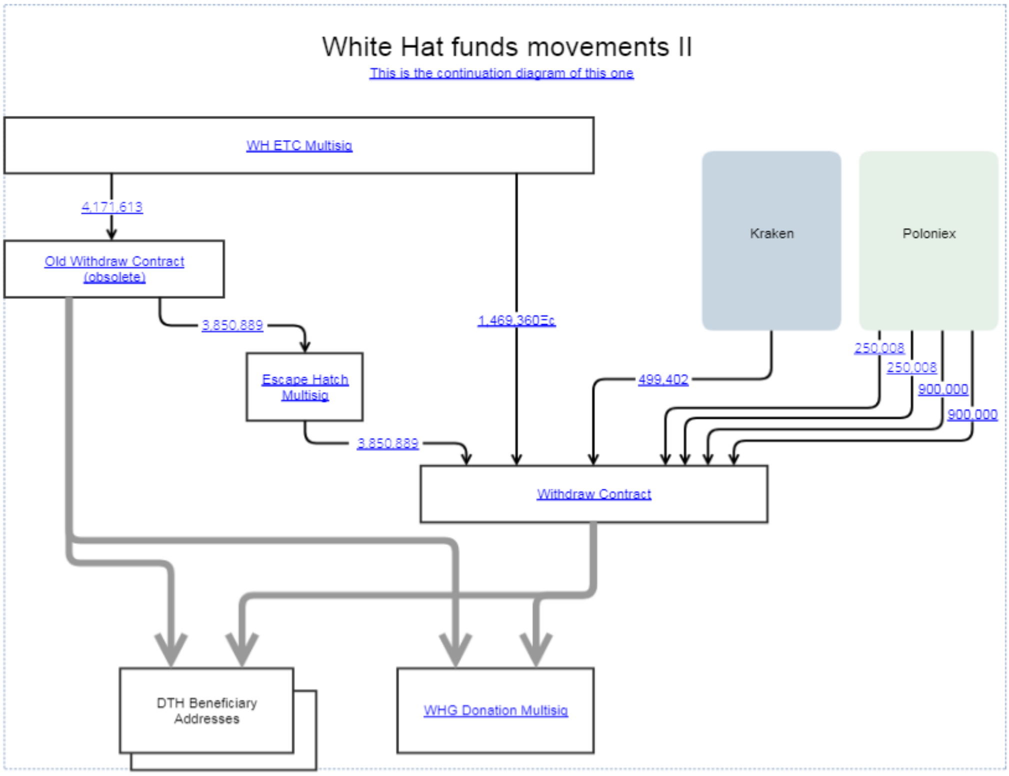
Figure 1 – Graphical illustration of the above transactions



(Source: Gliffy)

Date	Event	Movement of Funds
26 Aug 2016	Bity announce launch of the “whitehat withdrawal contract”. (source)	n/a
30 Aug 2016	Bity announce that the first version of the whitehat withdrawal contract is published. (source)	~4.2m ETC transferred from WHG to the withdrawal contract, ~0.6 million claimed by DTH. DTH are entitled to receive funds based on their DAO token balance at the time of the hardfork, not the current token balance as is the case for ETH.
30 Aug 2016	Bity announce that second version of whitehat withdrawal contract is published. (source)	~3.8 million ETC transferred from old contract to new contract.
6 Sept 2016	Bity announce that the remaining ETC (including that which was attempted to be traded on exchanges, and some from matured child DAOs) is transferred to the whitehat withdrawal contract. (source)	~4.3 million ETC transferred from WHG exchange accounts and multisig into withdrawal contract. During the time these trades were made, the price of ETC dropped in value relative to ETH, BTC, and EUR, causing the trade back into ETC to yield an additional 700,000 of ETC that was added to the whitehat withdrawal contract. The exact details of these on-exchange swaps were not made public.

Figure 2 – Graphical illustration of the above transactions



(Source: Gliffy)

Date	Event	Movement of funds
6 Sept 2016	DAO hacker moves the funds from his “dark child DAO”. (source)	~3.6 million ETC Secured by hacker
6 Sept 2016	DAO hacker donates some ETC to the ETC development fund. (source)	1,000 ETC sent to ETC developer fund.
25 Oct 2016 to 7 Dec 2016	DAO hacker tumbles funds into many different accounts, potentially swapping to different currencies. (source)	~0.3 million ETC tumbled by hacker.

At the time of writing, the hacker has not touched the vast majority of the drained ETC, and is sitting on a stash of 3,360,332 ETC worth US$58 million.

One feature of the whitehat withdrawal contract is that a limit is set for the ETC funds to be withdrawn (originally set to three months, expiring on 30 January 2017). Due to the large proportion of the funds that were not claimed within the given three months, this period was extended twice.

Date	Event	Movement of funds
30 Jan 2017	Bity extend the ETC whitehat withdrawal contract deadline to 14 April 2017. (source)	n/a
14 April 2017	RHG extend the ETC whitehat withdrawal contract deadline to 10 January 2018. (source)	n/a
10 Jan 2018	ETC whitehat withdrawal contract deadline.	?

There have been no major events since; the vast majority of ETH funds have been withdrawn by DTH, as has the majority of ETC.

The unclaimed funds

As of 19 November 2017, approximately US$140 million in funds remains unclaimed, as the approximate breakdown below indicates.

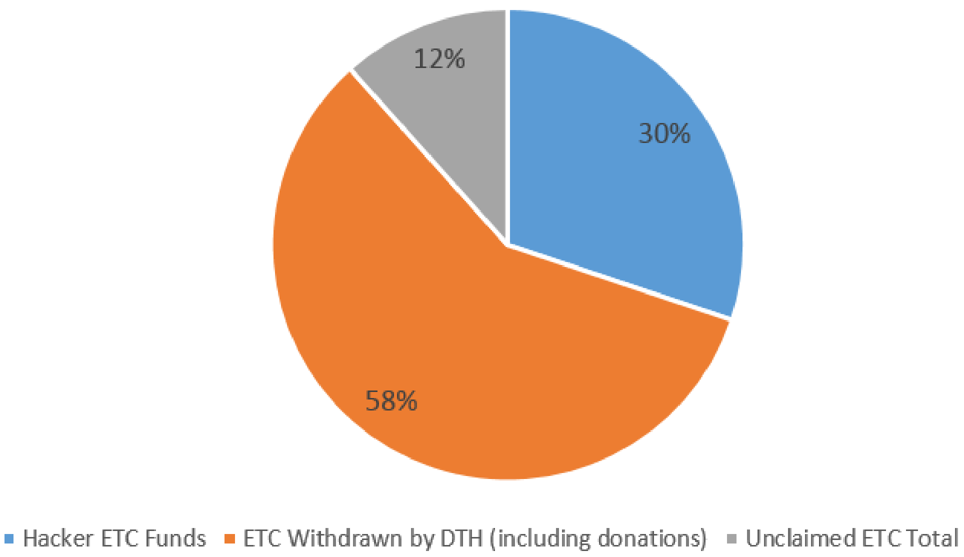
Bucket	ETH	Unclaimed US$ million	Percent
Claimed balances			
ETH withdrawn by DTH	11,286,046		97.3%
Unclaimed balances			
Unclaimed ETH in DAO Withdraw (source)	235,414	86.6	2.0%
Unclaimed ETH in DAO ExtraBalance (source)	76,204	28.0	0.7%
Unclaimed total	**311,618**	**114.7**	**2.7%**
Claimed & unclaimed			
Total funds	11,597,664		100.0%

DAO-related funds on the ETH side of the fork, calculated at a USD/ETH price of $368.
(**Source:** BitMEX Research, Ethereum blockchain)

Bucket	ETC	US$ million	Percent
Hacker funds			
ETC retained by Hacker	3,642,408	66.6	30.1%
WHG Funds			
ETC withdrawn by DTH (including donations)	7,035,319		58.2%
Unclaimed ETC (source)	1,405,072	25.8	11.6%
WHG total	**8,440,391**		**100.0%**
Hacker & WHG funds			
Total funds	**12,082,799**		

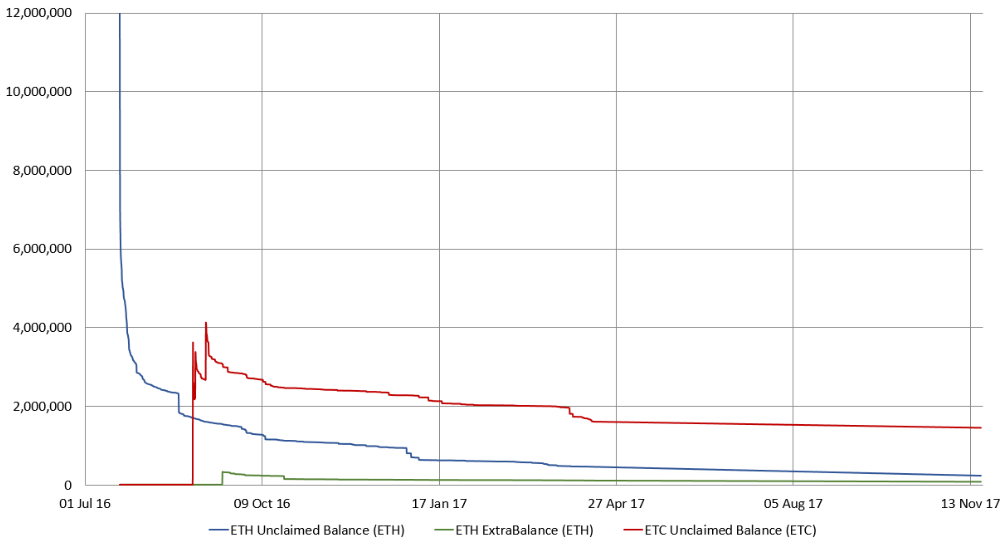
DAO-related funds on the ETC side of the fork calculated at a USD/ETC price of $18.30.
(**Source:** BitMEX Research, Ethereum Classic blockchain)

Figure 3 – DAO-related funds on the ETC side of the fork

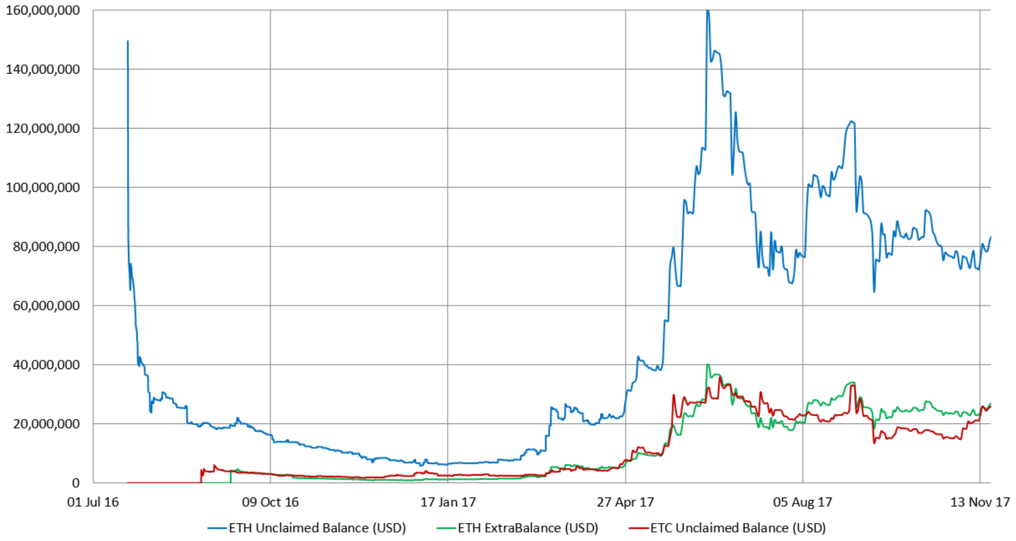


DAO-related funds on the ETC side of the fork.
(**Source:** BitMEX Research, Ethereum Classic blockchain)

Figure 4 – Unclaimed DAO balances over time for ETH and ETC



Unclaimed DAO balances over time for ETH and ETC.
(**Source:** BitMEX Research, GitHub)



Unclaimed DAO balances over time, in USD.
(**Source:** BitMEX Research, Coinmarketcap, GitHub)

As the chart above illustrates, at the Ethereum price peak in July 2017, the USD value of unclaimed Ethereum inside DAO withdrawal contracts was even higher than the US$150 million initially raised.

Withdrawal contract "gotchas"

Whilst the notion of a withdrawal contract sounds binding, all of the unclaimed funds are still in the control of the owners of those contracts.

Safety hatches

All three withdrawal contracts have "safety hatch" mechanisms, meaning the owners of these contracts have the ability to withdraw all of the funds at any time.

- DAO Withdraw and DAO ExtraBalance owner: DAO Curators Multisig
- Whitehat Withdrawal Contract owner: WHG Address

Whilst The DAO curators have not indicated this is planned, it may be tempting to appropriate these funds if it is deemed that no more withdrawals will take place. The WHG, in contrast, have designed their contract specifically to ensure this happens.

Whitehat deadline

The whitehat withdrawal contract also has a timeout system for when DTH are able to withdraw their funds. This deadline will expire on 10 January 2018 (although it has been extended twice before), so attempts to withdraw after this deadline may be denied.

What next for the US$26 million of unclaimed ETC?

The next obvious question is what happens to the unclaimed funds on 10 January 2018.

There are four clear options at present:

1. Have WHG/Bity keep the funds as payment for their service, returning some of the ETC.
2. Donate the funds to a charity or the "community", perhaps the ETC, DTH, or ETH community.
3. Extend the deadline again.
4. Commit to allowing withdrawals indefinitely, as with the ETH withdrawal contracts.

An official response from Bity suggests that they may lean towards option two:

> *"We feel that these funds should be donated to the DAO token-holders community where they originated from. After six months, we want to be able to donate these unclaimed funds to a community-wide effort, like a foundation supporting smart-contracts security. We want these funds to be used to develop the future of structures of decentralized governance, DAOs, and smart contracts. We will see what options are available at the time."*

Of course, questions of who represents the DTH community will arise, and the transparency of spending the funds may come into question. Due to the anonymity of whoever is behind WHG, it may be difficult for the community to properly audit the spending of these unclaimed funds.

Additionally, this arbitrary deadline that prevents individuals from claiming funds that are rightfully theirs may result in future legal action. Given that, there is a possibility that WHG is only left with option 3 or 4, and will potentially allow ETC withdrawals to continue in perpetuity.

However, January 2018 will be over 18 months after The DAO, a long time in the crypto space. In addition to this, the price of both ETH and ETC has risen considerably since The DAO. Therefore, some DTHs may forget about their tokens in all the excitement and wealth generation, which is prevalent in the Ethereum ecosystem.

Disclaimer

Transacting on BitMEX is not offered or available to any resident of (I) the United States of America, (ii) Cuba, Crimea and Sevastopol, Iran, Syria, North Korea, Sudan, or any other sanctioned jurisdiction, or (iii) any jurisdiction where the services offered by BitMEX are restricted.

This material should not be the basis for making investment decisions, nor be construed as a recommendation to engage in investment transactions and is not related to the provision of advisory services regarding investment, tax, legal, financial, accounting, consulting or any other related services, nor is a recommendation being provided to buy, sell or purchase any good or product.

Any views expressed are the personal views of the authors of the report. BitMEX (or any affiliated entity) has not been involved in producing this report and the views contained in this report may differ from the views or opinions of BitMEX.

The information and data herein have been obtained from sources we believe to be reliable. Such information has not been verified and we make no representation or warranty as to its accuracy, completeness or correctness. Any opinions or estimates herein reflect the judgment of the authors of the report at the date of this communication and are subject to change at any time without notice. BitMEX will not be liable whatsoever for any direct or consequential loss arising from the use of this publication/communication or its contents.

BitMEX