Implications of Decentralized Autonomous Organization on Political Campaign Finance Regulations

Ayzha D. Ricks
Computer Science Department
University of Houston
Houston, United States
wardayzha@gmail.com

Keshav Kasichainula
Computer Science Department
University of Houston
Houston, United States
kkasichainula@uh.edu

Weidong Shi
Computer Science Department
University of Houston
Houston, United States
wshi3@uh.edu

***Abstract*—The Federal Election Commission (FEC) is the regulating authority over the monies that U.S. citizens are allowed to give to political candidates and parties. However, preexisting loopholes in FEC regulation allow for contributions to be made in situations that do not require donors to disclose their identity, a term coined as "dark money". The increase of dark money in campaign financing and the ability of political spending to influence voter perspectives and decisions puts the credibility of the political finance system at stake. Additionally, with the introduction of blockchain, decentralized autonomous organizations (DAOs) and smart contracts to political financing these technologies collectively can serve as a new vehicle for bad actors to use. In this paper, the effects of blockchain and smart contracts on political finance are examined through four use cases to demonstrate how these technologies can extend anonymous, foreign interference in political campaign financing and further cripple public trust in it.**

***Index Terms*—Federal Election Commission (FEC), dark money, blockchain, decentralized autonomous organization (DAO), smart contracts**

I. Introduction

A. Dark Money in the Political Finance Arena

In the political campaign finance arena, the Federal Election Commission (FEC) is the regulating authority that both political candidates and their sponsors must answer to Guidelines put in place by the FEC dictate how monetary contributions can be made to candidates and parties, how much can be made and how they must document their actual spending of these donations. Ideally, with such a system in place, the likelihood of candidates being able to "sell" the offices that they hold or vie for by making deals with individuals who have political motives should be deterred but this is not often the case. In fact, current political campaign finance regulations set by the FEC may actually help cultivate an environment where bad actors may be able to come together and form partnerships or relationships with one another. One of the contrivances that helps make this possible is "dark money". The term "dark money" refers to political spending to influence the decision of a voter, where the donor is not disclosed, and source of money is unknown" [2].

Dark money has seen an increase in its involvement in political campaign financing since the paramount ruling in the 2010 Supreme Court case versus Citizens United, in which it was ruled that it was lawful for super political action committees (super PACs) to receive money from nonprofit organizations and corporations [3]. It was already established that super PACs could receive an unlimited amount of contributions, and many of them do, often bringing millions in contributions for candidates that they and their supporters vie for.

What makes this problematic is the fact that the FEC does not require nonprofits and corporations to disclose the identities of their donors, so if an anonymous individual has illegal political motives or desires to exert some sort of unlawful influence on the political campaign system, they can use these entities to fund the super PACs which will in turn push the candidates that support their platform, good or bad.

Additionally, the FEC recently approved the acceptance of bitcoins as a form of contributions to candidates and committees, which may further exacerbate existing threats or loopholes in the political campaign finance system. The introduction of cryptocurrency such as bitcoin and other blockchain-related technologies coupled with preexisting regulation loopholes can collectively help disminish the effectiveness of the guidelines established and the convenience that these integrated technological solutions should have. This paper examines possible uses cases in which the utilization of the aforementioned technologies could result in a more disastrous situation if the proper consideration and risk mitigation for these things are not put into place, similar to that seen in the 2016 U.S. presidential election hack orchestrated by Russia [6] [11] [8].

B. Development from Blockchain to DAO

"Blockchain" refers to a digital ledger of transactions that are maintained by a network of computers that only add transactions when they can come to terms of agreement with one another on how the transactions should be ordered. Key features about a blockchain are its immutability, decentralized nature and privacy.

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

What makes a blockchain immutable is the capability of being able to add a block of transactions to the ledger in such a way where the ordering cannot be changed once it has been added. What makes this possible is the hashing of a block of transactions prior to it being added to the ledger. A new block of transactions will contain the previous hash that represents all transactions added to the ledger thus far and a new hash is created once the current block is added. Due to the nature of hashing, if a bad actor were to try to change the ordering of transactions in a previous block, this would result in a change to the hash. Hashes are checked before new blocks are added, meaning a discrepancy in the hash of previously added transactions would not go unnoticed.

In terms of being decentralized, blockchains operate without a central authority by allowing computers that do "proof-of-work" to engage in computationally-intensive calculations to verify the validity of the blocks being added to the ledger and allowing them to govern what transactions are added and in what order and at what time [9] [13]. The authority given to these network nodes is safeguarded by requiring the nodes to reach a "consensus" on the block of transactions to be added based on the proof-of-work calculations that are done.

Blockchains offer a level of privacy by being able to mask the identities of its users through its utilization of blockchain addresses for transactions. These blockchain addresses can be viewed to the same similitude as bank account numbers. The ledger records what blockchain address is sending or receiving bitcoins to or from another address but offers a certain degree of anonymity.

As blockchain technology developed over time, this paved the way for the integration of smart contracts into its environment. Smarts contracts can be viewed as terms or conditions that must be met in order for transactions to be executed on the ledger. When utilized in a blockchain environment, they can help serve as a middleman in determining whether a transaction should be executed or not between two parties. Smart contracts can be written as computer code that can then be added to the ledger to even ensure the integrity of the contract and deter attempts to change it. Utilization of smart contracts allow entities trading bitcoins and other cryptocurrencies more autonomy in setting the terms of their agreements with one another.

A decentralized autonomous organization (DAO) is an organization in which transactions executed on behalf of the entity are governed by smart contracts. Since a DAO is governed by smart contracts, this allows transactions to be fully automated and membership to the DAO may include individuals, organizations or even other DAOs [12]. Ethereum [7], a blockchain platform that specializes in decentralized applications that can be executed in its environment, is one of the most notable platforms on which DAOs can be executed.

C. DAOs in the Political Finance Arena

The scope of this paper is to examine the implications of a politically motivated DAO on FEC campaign finance regulations. Our thought is that by using blockchain technologies such as DAOs, the credibility of the electoral process can be undermined and preexisting loopholes in regulations can be taken advantage of. In such a situation, the expectation is that the DAO will be utilized to fulfill or promote politically incentivized transactions between two or more parties. There are four use cases that are expounded upon to showcase how blockchain technology could be used maliciously to circumvent checks and balances set by the FEC.

Political DAO may be defined as: a distributed ledger or blockchain based virtual entity setup to fulfill or promote politically incentivized transactions where the transactions can be automated using smart contracts, and operations of the DAO is sustained by decentralized infrastructure for computing, communications and book keeping.

We can look at the comparison of Dark money,super PACs, and political diriven DAO in Table 1

II. DARK MONEY BACKGROUND AND PROBLEM

A. Open Secrets Data Sets

Dark money's rampant increase in the political campaign finance system can be attributed to the outcome of the Supreme Court ruling in Citizens United v FEC in 2010. Since then, its presence in the political campaign system became more apparent with every election cycle.

Looking into the Open Secret's Center for Responsive Politics website, we can see that dark money's existence in elections grew since the 2012 election cycle, one of its prominent years being in 2016. In fact, in the 2016 election cycle the amount of dark money determined to be flowing through the political campaign system was estimated around $39.84 million. Due its widespread growth during this election cycle, this is the election cycle of interest in this paper.

Open Secret's define dark money as "funds from outside groups such as nonprofit organizations or super PACs that are raised in support of or against a candidate" [1]. However, these funds cannot be raised in coordination with the monies contributed to a candidate's official campaign committee. To further examine the extent of dark money according to political party, datasets from Open Secrets containing the amount of dark money raised per election in 2016 were examined. The intention of this analysis was to see if the effects of dark money on political parties and campaigns could lead to implications of potential effects of dark money on political campaign financing when coupled with smart contracts and DAOs. Data taken from Open Secrets in CSV format which contained information on the overall amount of money and dark money that 2016 candidates received was used to generate Table 1 and Table 4.

Table 1 showcases the outcome of 2016 election races according to the political party that won and also happened to raise the most money. This allows us to examine the effects of dark money on the election race outcomes for the two major U.S. political parties, the Democratic Party and the Republican Party. The column "Winning Party" entails which political party won the race ("R" for Republican and "D" for Democratic). The column "Top Raised/Winner" entails

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

	Super PACs	Dark-money groups	Crypto currency DAO
Type of entity	Regulated by FEC	Nonprofit	DAO
Disclosure of contributors required	Yes	No	No
Disclosure of expenditures required?	Yes	Through tax filings	No
Limits on dollar amount of contributions?	None	None	No
Can be wholly political?	Yes	No	Yes
Coordination with candidates?	Impermissible	Impermissible	Not in public

TABLE 1: Dark money (501(c)) groups and super PACs compared

whether or not the candidate that had the most amount of dark money raised in their favor also went on to win the election race ("Y" for instances where this is true and "N" for instances where this is false).

Table 1 showcases the outcome of 2016 election races according to the political party that won and also happened to raise the most money. This allows us to examine the effects of dark money on the election race outcomes for the two major U.S. political parties, the Democratic Party and the Republican Party. The column "Winning Party" entails which political party won the race ("R" for Republican and "D" for Democratic). The column "Top Raised/Winner" entails whether or not the candidate that had the most amount of dark money raised in their favor also went on to win the election race ("Y" for instances where this is true and "N" for instances where this is false). Table 4 illustrates a detailed breakdown of dark money spent for or against the Democratic Party and Republican Party in each 2016 election race. The columns "For Dems" and "For Reps" represent dark money that was contributed in favor of each political party respectively while "Against Dems" and "Against Reps" represents the contrary. From data in Table 4 , a third table was generated to further analyze whether or not a political party that had the most dark money raised in its favor for an election race also had one of their candidates win that respective election. Or, in the event their candidate did not win, did another candidate win that had less dark money contributed to oppose their campaign (which would mean the first candidate received more opposition in the form of dark money given against their campaign). Table 3 contains the columns "TopSupWins" and "MoreOpp" to explore these scenarios. In the event that the candidate that raised the most dark money did not win, "TopSupWin" has a value of "N" for no ("Y" is for yes), and in this case "MoreOpp" will either have a value of "Y" for yes and "N" for no.

B. Influence of Money on 2016 Election Campaigns

Based on Table 1 , Table 4 and Table 2 , a couple of data analyses were performed to determine what effects, if any, dark money had within these race outcomes in a statistical way. In Figure 1, the frequency of 2016 election race wins according to candidates that raised the most overall money is examined.

From this, we can see a majority of the time that a candidate won the race they also happened to have raised more money than their competitors. This occurs in the dataset about 127 times (roughly 78% of the time) and does not occur only in about (13% of the time). The bar "Outcome Unknown" indicates 2016 elections where this could not be determined since there was only campaign finance information available for one candidate. This signals to us that money does indeed play a factor in election race outcomes.

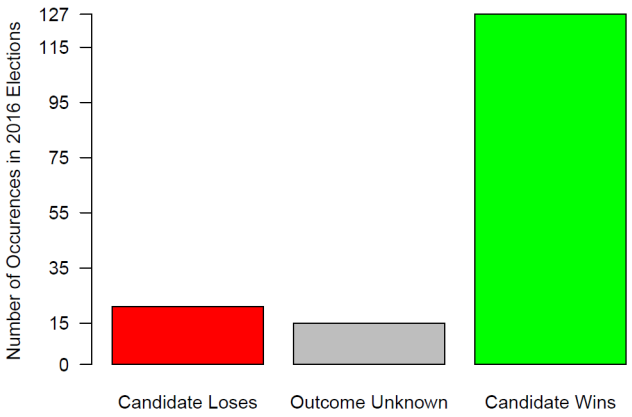

Fig. 1: 2016 Election Race Results for Candidates that Received the Most Money.

Figure 2 illustrates the amount of dark money raised in favor of or against a political party based on information from Table 4 . As seen in the figure, most of the dark money raised in the 2016 election cycle was in the form of opposition against the Democratic Party. Additionally, the second highest amount of dark money raised was in the form of support for the Republican Party. We examine the relationship between money raised for a political party and against their competition to determine if there is any correlation in these relationships

Two correlation tests were performed to determine if there is a relationship: 1) dark money raised for Democrats and against Republicans and 2) dark money raised for Republicans and against Democrats. From the former correlation test, a correlation coefficient of 0.907095 is obtained which means that there is some positive correlation between an increase in dark money raised for Democrats and an increase in dark money raised against Republicans. As for the latter correlation test, a correlation coefficient of 0.8373681 is also obtained. This brings us to a similar conclusion as the first test, as dark money raised for the Republicans increases so does the amount of dark money raised against the Democrats. This proves there is some level of significance to the interaction between dark money raised for a political party and against their competitors.

From this, we draw the notion that dark money given in the form of bitcoins or other cryptocurrencies may have a similar

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

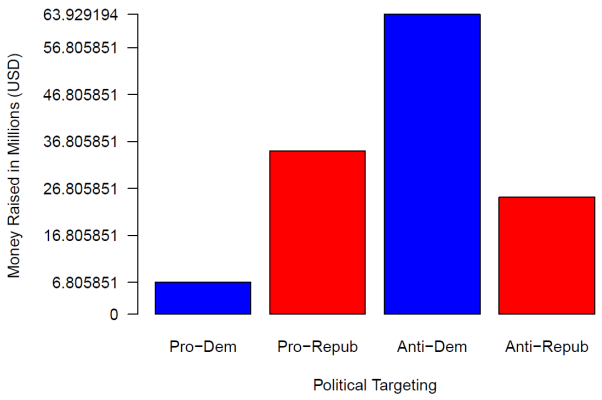

Fig. 2: Top Dark Money 2016 Elections According to Political Party Support

impact, especially when utilized in conjunction with smarts contracts and DAOs.

III. CASE STUDIES

In this section we will be discussing the different ways the DAO contract can be used to bypass the FEC regulations on the political financial system.

A. Bounty Check Protocol

The use case of a DAO contract would be as a ”Bounty Check” service. The main aim of this service would be to help verify and transfer the bounty after completion of the task.

Let’s understand the bounty check service with an example. For this example, let us assume we have a candidate with the name Alice and opposition candidate Bob. Bob would like to promote a social media post against Alice. Bob sets the requirements of the task that the social media post should get 100 likes/shares/retweets causing debate over a hot topic. Bob would pay the entity A ”x” amount of tokens for finishing the task. Algorithm 1 gives the pseudo code of the execution.

The bounty check algorithm accepts two arguments. The first argument is *ct*, which is the information about the contract’s DAO address. The second argument is *daoC*, which holds the list of competitors for the DAO contract (i.e., DAO address, number of shares, etc.). The contract will keep comparing the *deadline* and the current time to check if it needs to decide a winner. In a case that the *deadline* is more than the current time, then contract returns failed as there is still time left. Lines 4 through 16 are used to determine a winner when *deadline* passes.

The *for* loop runs through the *daoC*, and examines the value *daoC.[dCount].Criteria* to check how many have succeeded to meet the requirements mentioned above. For the above step, we assume that the DAO is feed with external data regarding the likes/shares/retweets for different social media posts. In the case that DAO doesn’t have a continuous stream of data, it would contain code to call web bots to search for social media platforms. In a case, there is no winner determined. *winners* is assigned NULL value, and the bounty goes back to Bob.

From the above example, one of the most noticeable entity is the fact that throughout the process, nowhere has the name of the donor been put out in public. And with the help of DAO, one can spread negative propaganda against the opposition without being directly tied to this act. The use of DAO helps with circumventing the FEC regulation that requires super PAC’s to disclose their donors. Any bad actor can use a DAO do their bidding and not be directly associated with any of the dealings.

The DAO can either move or not move the reward tokens to another DAO address based on the contract specifications. Users can exchange and verify completion of the contract without even knowing the entity at the other end of the exchange.

By using political DAOs, conspirators against a political figure or party may solicit funds and opposition to help overthrow their competition. Additionally, for these politicians or parties, hot topics or key issues and the viewpoints they desire to present to voters on them can be promoted without direct ties being made to a sole party or candidate. This circumvents FEC regulations that require super PACs to disclose their donors because if a bad actor or co-conspirator utilizes a DAO (or third-party via a DAO) to do their bidding for a preferred super PAC, it is practically untraceable. Additionally, the DAO can be used as a vehicle for super PACs to target opposing candidates or parties and wage attacks and criticism on their platforms without a direct connection being made to their organization.

The DAO will either move or not move the reward tokens to another DAO address, based on contract specifications. It should also be noted that users within a DAO may exchange tokens and verify completion of the contract without even knowing who the other entity they are in partnership with is. The smart contracts that govern this protocol could serve as the intermediary to verify the accounts of competitors without revealing their true identities or online personas.The Bounty Check Protocol also leaves enrollment in the competition and verification of contract completion up to the DAO, demonstrating that two entities in a DAO contract do not even need to communicate directly with one another to ensure a contract is completed meanwhile ensuring that predetermined terms and arrangements are met. We next consider the case where bad actors conspire with candidates to ”buy” legislation.

B. Check Record Protocol

In Algorithm 2 we consider the situation in which a bad actor bribes a candidate in return for ”x” amount of tokens.

The bribe helps entice candidate voting in favor of law/legislation that the party is vying to pass through. Check Record Protocol uses DAO as a medium of a contract between the co-conspirators and also monitor the fulfillment of the terms. *tpa* represents the DAO address that will receive the tokens on behalf of the candidate. Using a DAO address

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

associated with shell corporations or non-profit helps to evade FEC regulations on identifying the donor.

Function *votecheck* runs once the legislative bill has passed and the data for the voting is available. It checks if candidate A has voted in the agreed manner with the Bad Actor B. This information is verified and fed into the DAO via the variable $data_{feed}.Criteria$ and compared with the value *ct.Criteria* to determine if its in agreement with the B's desired vote. Once verified *tpa* receives the reward tokens as promised by B from the contract's DAO address and the contract closes. A message *m* is returned to *votecheck* that contains the reward tokens distributed, the DAO address of the recipient, and the timestamp. In a scenario where the vote is not in favor of B's agenda or deadline has passed for the contract that will result in protocol failing and no reward tokens getting dispensed.

Above-discussed functionality mirrors the idea of contract acting as an escrow for tokens until the fulfillment of the terms of reward or exchange. The escrow helps in providing security for the tokens and ensuring that one party getting cheated into paying up.

C. Crypto-Service Protocol

Crypto-Service Protocol utilizes DAO to serve as a medium in which bad actors hide under the mask of anonymity to carry out crimes and/or financial transactions. The methodology outlined by the protocol mentioned in further paragraphs has drawn ques from 2018 Indictment by Special Counsel Rober Mueller on the 2016 Presidential Race hack by Russian spies [4]. Crypto-Service Protocol outlines how DAO address and smart contracts [5] have the potential to help in highly-organized attacks. The attacks can involve multiple cyber-attack vectors and conspirators. And throughout this still maintaining the anonymity.

If you take a look at the Algorithm 3 we can see two main functions governing how cryptocurrency flows in and out of the crypto-wallet(identified as funds) for Bad Actor B. The first function, *exchangeCoin,* helps in distributing tokens when service from DAO requests payment. The DAO address for service is an argument for *exchangeCoin* and variables related to *serviceDao* are checked. In case a payment is due, the number of tokens gets transferred from *funds* to *servicesDao*. And the tokens remaining with B are updated. *m*, a message containing all the transaction details get sent back to *exchangeCoin*.

Function *sale* takes two arguments.

- *data_leak*, the DAO address selling stolen or leaked information.
- *buyerDao*, the DAO address which is looking to buy the information.

Let's assume that Bad Actor Bob is selling stolen data. First, a flag called *paid* is set to see if the buyer has met the requirements before transferring data. If not, then the value of *Tokens* for *buyerDao* is tallied against *Data_price* to ensure that the buyers intend on paying and a temporary wallet gets created for the transaction to take place and the *Paid* flag is set to true.

Once *Paid* is set to true, the tokens received by Bob gets transferred to *funds*, and the number of tokens that the buyer has left is updated. *Stolen_data* which contains the information, is encapsulated in a message and sent to the buyer. To record proof of the transaction, *sale* returns a message *m* to be recorded to the ledger. And something to keep in mind is that the stolen data could involve some level of encryption, and segmentation of data into multiple messages takes place over the network. This level of encryption is done to evade detection and message falling into the wrong audience.

This functionality in the DAO can be used to automate payments to services such as anonymous domain name purchases and hosting since payments are only tied to a DAO address and not an entity (unless one know's which DAO address is owned by whom). Additionally, payments from such a DAO address can be used to facilitate services that allow bad actors leverage for their crimes. For example, once a domain name has been acquired and set up to be hosted, Bad Actor B may exploit this service by hosting malware and phishing sites on the domain and since the purchase was anonymous it cannot be traced back to them [4].

In Mueller's indictment, it is cited that Bitcoin was primarily used to purchase servers, register domains, and make other payments to further the hack ([4], p. 22). Additionally, it was via the use of a registered domain under the name "dcleaks.com" that hackers were able to disclose stolen information from the Democratic National Committee ([4], p. 13). The usage of bitcoins also allowed hackers to keep a low profile and evade greater scrutiny (in regards to identities and sources of funds) that would have otherwise been drawn by going through traditional financial institutions [14, p. 22]. Cryptocurrency was also used to lease a virtual private server, which served as a proxy when in communication with home-grown malware used to infect the computers of several DNC members, logging keystrokes and taking screen captures that were reported back to the hackers ([4], p. 9,13). Additionally, the hackers fabricated social media accounts that were used to help release stolen information and deter suspicion of who facilitated the leaks to other entities. With such a significant use-case as this, the usage of a DAO to help facilitate political espionage or to target political parties and candidates is not far-fetched. Foreign interference was given a green light into the affairs of American political campaigns via the assistance of blockchain technologies. If one wanted to use these technologies to serve as a platform for conducting political espionage and waging war against political parties, it would prove to be a viable option.

IV. Conclusion

Dark money has become an influential force on political campaign financing. Data from 2016 election cycle results from Open Secrets showcases how dark money has not only shaped the political campaign financing system but also the likelihood of certain parties or candidates winning races. This idea can be extended even further when blockchain technology such as a DAO and smart contracts are used. The

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

protocols outlined in this paper entail how dark money can utilize DAOs and smart contracts to continue to circumvent FEC regulations and extend the reach of bad actors with political incentives.

As blockchain technology increases its integration within federal government and the services and processes it oversees, the functionality and scope of its usage need to be considered. Utilizing technology such as DAOs and smart contracts within the political campaign finance arena has the potential to introduce new security risks and FEC regulation loopholes that can further cripple the political campaign finance process and the electoral system that intertwines with it. Additionally, a DAO platform in political campaign finance may actually be more inviting to conspirators because it offers a level trust without them having to have it in their co-conspirator.

There is work being done to mitigate this by Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) [10], however this is just the tip of the iceberg when it comes to tackling voting or election-related cybersecurity risks pertaining to blockcahin. Before blockchain utilization in political campaign finance becomes widespread, more focus needs to be put on how to deter and even detect foreign interference within the political campaign finance process.

REFERENCES

[1] Center for responsive politics. dark money basics: Total outside spending with no disclosure of donors. www.opensecrets.org/dark-money/basics.

[2] Center for responsive politics. *Dark Money Basics* .opensecrets.org,. www.opensecrets.org/dark-money/basics.

[3] Center for responsive politics. Follow the Shadow of Dark Money .opensecrets.org,. www.opensecrets.org/dark-money/shadow-infographic.php.

[4] U.S. Department of Justice. UNITED STATES OF AMERICA v. VIKTOR BORISOVICH NETYKSHO, Et. Al. The United States Department of Justice, 13.

[5] Maher Alharby and Aad van Moorsel. Blockchain-based smart contracts: A systematic mapping study. *CoRR*, abs/1710.06372, 2017.

[6] Adam Badawy, Kristina Lerman, and Emilio Ferrara. Who falls for online political manipulation? *CoRR*, abs/1808.03281, 2018.

[7] Vitalik Buterin. A next-generation smart contract and decentralized application platform .github, ethereum foundation. github.com/ethereum/wiki/wiki/White-Paper, November 2013.

[8] National Intelligence Council. Assessing russian activities and intentions in recent us elections, 6 Jan 2017.

[9] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[10] Department of Homeland Security. protect2020. 25 July 2019.

[11] Commitee on Foreign Relations United States Senate. Putin's asymmetric assault on democracy in russia and europe: Implications for u.s. national security. 25 Jul 2019.

[12] Toshendra Kumar Sharma. What is decentralized autonomous organization (dao) how dao works? www.blockchain-council.org/blockchain/decentralized-autonomousorganization-dao-dao-works/, January 2018.

[13] et al. Wei, Cai. Decentralized applications: The blockchain-empowered software system. *IEEE*, 6, 12 Oct 2018.

V. APPENDICES

Race	Top Raised/ Winner	Winning Party
President	N	N
Pennsylvania Senate	N	N
Florida Senate	Y	N/A
Nevada Senate	Y	Y
Indiana Senate	Y	N/A
North Carolina Senate	N	N
Ohio Senate	Y	Y
New Hampshire Senate	Y	N/A
Missouri Senate	Y	Y
Wisconsin Senate	N	Y
Nevada District 3	Y	N/A
Arizona Senate	Y	N/A
Illinois Senate	Y	N/A
Iowa District 1	Y	N/A
Pennsylvania District 16	Y	Y
Michigan District 8	Y	Y
Florida District 26	Y	N/A
Georgia District 3	Y	N/A
Nevada District 4	Y	N/A

TABLE 1: Top Overall Money 2016 Elections Statistics Database File.

Race	TopSupWins	MoreOpp
President	N	N
Pennsylvania Senate	N	N
Florida Senate	Y	N/A
Nevada Senate	Y	Y
Indiana Senate	Y	N/A
North Carolina Senate	N	N
Ohio Senate	Y	Y
New Hampshire Senate	Y	N/A
Missouri Senate	Y	Y
Wisconsin Senate	N	Y
Nevada District 3	Y	N/A
Arizona Senate	Y	N/A
Illinois Senate	Y	N
Iowa District 1	Y	N/A
Pennsylvania District 16	Y	Y
Michigan District 8	Y	Y
Florida District 26	Y	N/A
Georgia District 3	Y	N/A
Nevada District 4	Y	N/A
California District 21	Y	Y
Maine District 2	N	N
Michigan District 1	Y	N/A
Alabama Senate	Y	N/A
New Jersey District 5	Y	N/A
Minnesota District 8	Y	N/A
Kansas District 1	Y	N/A

TABLE 2: Top Dark Money 2016 Elections Political Party Statistics.

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

Race	For Dems($)	Against Dems($)
President	2,519,664	13,589,713
Pennsylvania Senate	1,056,236	7,852,814
Florida Senate	115,512	8,941,103
Nevada Senate	496,945	3,982,661
Indiana Senate	0	5,092,896
North Carolina Senate	297,048	4,965,508
Ohio Senate	2,458	5,277,597
New Hampshire Senate	10,330	2,868,321
Missouri Senate	0	3,555,060
Wisconsin Senate	506,944	2,521,374
Nevada District 3	2,630	0
Arizona Senate	11,484	300,150
Illinois Senate	633,416	0
Iowa District 1	19,447	697,520
Pennsylvania District 16	0	665,780
Michigan District 8	0	713,612
Florida District 26	3,251	27,800
Georgia District 3	0	0
Nevada District 4	79,552	0
California District 21	12,463	563,623
Maine District 2	78,066	67,762
Michigan District 1	9,210	544,263
Alabama Senate	0	0
New Jersey District 5	87,238	0
Minnesota District 8	11,805	354,450
Kansas District 1	0	0

TABLE 3: Top Dark Money 2016 Elections Political Party Statistics - Cont.

Race	For Reps($)	Against Reps($)
President	10,665,491	15,733,767
Pennsylvania Senate	2,441,910	1,780,984
Florida Senate	949,363	183,824
Nevada Senate	3,249,780	283,006
Indiana Senate	2,838,388	0
North Carolina Senate	506,156	2,161,909
Ohio Senate	1,572,299	209
New Hampshire Senate	1,583,563	220,276
Missouri Senate	422,122	0
Wisconsin Senate	785,997	556,311
Nevada District 3	817,125	1,239,106
Arizona Senate	1,269,762	3,507
Illinois Senate	550,150	7,285
Iowa District 1	359,331	2,131
Pennsylvania District	72,035	0
Michigan District 8	0	0
Florida District 26	622,255	0
Georgia District 3	651,152	0
Nevada District 4	16,748	500,801
California District 21	6,815	12,463
Maine District 2	111,194	322,896
Michigan District 1	23,007	0
Alabama Senate	67,954	0
New Jersey District 5	27,292	322,234
Minnesota District 8	49,099	0
Kansas District 1	202,046	199,861

TABLE 4: Top Dark Money 2016 Elections Political Party Statistics.

Algorithm 1 Bounty Check Protocol

```
1: function BOUNTY_CHECK(ct,daoC)
2:   if ct.Deadline > current_timestamp then
3:     retrun fail
4:   if ct.Deadline <= current_timestamp then
5:     for dCount ← 0, dCount ⇐, dCount++ do
6:       if daoC[dCount].Criteria does not meet
   data_feed.Criteria then
7:         continue
8:       else
9:         if daoC.Criteria does meet data_feed.Criteria then
10:          winner[winner.Lenght+1 ← daoC[dCount]
11:          winner[last_index].Tokens ← ct.Reward
12:          continue
13:  if winner.Length = 0 then
14:    winner ← NULL
15:  m ← ct + winner + current_timestamp + ct.Reward
16:  return m
```

Algorithm 2 Check Record Protocol

```
1: function VOTECHECK(tpa)
2:   if ct.Deadline < current_timestamp then
3:     retrun fail
4:   else
5:     if ct.Deadline <= current_timestamp then
6:       voteFavor ← data_feed.Criteria
7:       if voteFavor == ct.Criteria then
8:         tpa.Tokens ← ct.Reward
9:         ct.Reward ← 0
10:        Close ct
11:        m ← + ct + tpa + current_timestamp + tpa.Tokens
12:      else
13:        if voteFavor ! = ct.Criteria then
14:          return fail
```

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

Algorithm 3 Crypto-Service Protocol

```
1: function VOTECHECK(serviceDao)
2:   if serviceDao.payment_due == current_timestamp then
3:     serviceDao.Tokens ← funds
4:     funds ← funds - serviceDao
5:     servicesDao.service_paments ← True
6:     return m
7:   else
8:     return m
9: function SALE(data_leak,buyerDao)
10:  data_leak.Paid ← False
11:  if buyerDao.Tokens >= data_leak.Data_price then
12:    data_leak.Tokens ← buyerDao.Tokens
13:    data_leak.Paid ← True
14:    if data_leak.Paid is True then
15:      funds ← data_leak.Tokens
16:      buyerDao.Tokens ← buyerDao.Tokens - funds
17:      data_leak.Message ← data_leak.Stolen_data
18:      buyerDao.Message ← data_leak.Message
19:      m ← data_leak + buyerDao + timestamp +
   data_leak.Tokens
20:      return m
21:  else
22:    return fail
```

978-1-7281-5092-5/19/$31.00 ©2019 IEEE