The Key To Unlocking The Black Box:
Why The World Needs A Transparent Voting DAC

This paper details how improving the way a democratic society casts its votes can be accomplished through the development of a next generation voting platform, powered by BitShares, makers of the BitShares Toolkit for Building DACs (Decentralized Autonomous Companies).
**TABLE OF CONTENTS**

1) Introduction .............................................. 2
2) The Problem .............................................. 2 - 5
3) The History .............................................. 5 - 6
4) The Solution .............................................. 7 - 16
5) About Follow My Vote ................................. 17
1) INTRODUCTION:

We live in a world where many of us are no longer satisfied with the status quo. As such, there is seemingly room for improvement in all aspects of life.

Anyone with an analytical mind can observe the world around them and see opportunities to make certain things better. Whether it be something as simple as improving the design of a water bottle to fit better in one’s hand or as complicated as adding new and improved features to the design of an automobile, just because things are the way they are doesn’t mean they can’t be improved over time.

This paper details how improving the way a democratic society casts its votes can be accomplished through the development of a next generation voting platform, powered by BitShares, makers of the BitShares Toolkit for building DACs (Decentralized Autonomous Companies).

2) THE PROBLEM:

One would think that, in this day and age, democratic societies throughout the world would have figured out how to conduct legitimate elections where all those involved are able to come to an agreement on the outcomes. Yet, elections in the United States of America, arguably the greatest democracy in the world, has been plagued with accusations of illegitimacy stemming from all sorts of issues, such as flawed registration processes, inconsistent voter ID laws, cases of widespread voter fraud, non-sensible restrictions, vulnerable voting machine technology, and a general lack of transparency.

When it comes to the voter registration process in the United States, it is evident that people are willing to go to great lengths in an attempt to influence the outcome of elections by registering deceased citizens, criminals still incarcerated, purely imaginary people, and even their family pets.

In 2012, only to prove a point about how bad this situation is, Thomas Tolbert went as far as successfully registering his dog to vote as a member of the Democratic Party in Bernalillo County, New Mexico. The fact that this voter registration application was approved is utterly reprehensible and confirms the process is fundamentally flawed.

In the same year, a statewide voter fraud investigation was launched in Florida after a deceased woman’s name and signature was found on a Palm Beach County voter registration form that was gathered on behalf of the Republican Party. When digging deeper into the issue of rampant voter fraud in the U.S., it becomes apparent that voter registration issues aren’t always so blatantly obvious as the two aforementioned cases.
For instance, the latest **interstate voter cross check** program recently uncovered that there are over 6.9 million overlapping voter registrations between states in the U.S. Perhaps the most troubling thing about this statistic is that it only includes 28 states and does not take into account the three largest states: California, Texas and Florida. This duplicity means that it is currently possible for millions of people in the U.S. to vote multiple times in federal elections, a vulnerability that can be used by radical special interest groups who seek to gain an advantage for the candidates they chose to support in these elections. To make matters worse, when voters do show up to the polls, request their ballots, and vote in elections, their personal identities are not always verified.

At this point in time, there are a total of **19 states** in the United States that do not require voters to produce any sort of identification prior to voting in federal elections: California, Illinois, Iowa, Maine, Maryland, Massachusetts, Minnesota, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, Oregon, Pennsylvania, Utah, Vermont, West Virginia, and Wyoming. Also, when filling out absentee ballots in various states across the country, people do not have to provide proof of identification. This flaw in the ballot submission process has led to some people completing absentee ballots on other people’s behalf in order to influence the outcome of elections in one way or another, which is yet another form of voter fraud that seems to happen quite often.

Take Mike Marshall, for example, whom was **indicted in 2011** on 45 felony counts of voter fraud, forgery, and perjury relation to the 2010 election. Three of these cases concern applications for absentee ballots that Mike allegedly filled out for his son, brother, and a former roommate. But, when it comes to the voting laws in place that govern the way in which voters in the United States cast their votes, these issues with respect to fraudulent ballot submissions are only the tip of the iceberg.

These absentee ballots, once completed and sent in ahead of an election, cannot be changed. Therefore, those whom cast absentee ballots and subsequently change their minds about which candidate they wish to vote for in an election cannot update their ballots in the days leading up to the election, which means they might actually end up voting for a candidate they do not really support. Also, when a user casts their vote for their candidate of choice in an election, they only get to vote for one candidate for each political office. This is all fine and well when there are only two candidates participating in an election. However, the fact is that this is simply not the case in the many major elections.

For example, in the 2012 U.S. Presidential Election, the state of Virginia had **5 different candidates** on the ballot. With 5 different candidates to choose from, it is highly likely that some voters would have supported more than one candidate for President of the United States, yet they were forced to vote for only one candidate. Ultimately, this restriction may actually result in the candidate with the most supporters not getting elected. Many critics of this flaw in our current election
system would argue that this is exactly what happened in the 1992 U.S. Presidential Election.

In this election, Ross Perot ran as an independent candidate and received 19% of the votes. It was argued by some that the majority of the voters that voted for Ross Perot would have also supported George H. W. Bush whom received 38% of the votes in the same election. Yet, with 43% of the votes within the election, Bill Clinton was elected as President of the United States. If the aforementioned issues are not enough cause to call for the improvement of the way elections are run in the United States, the flaws in the technology that is being used to this day should be.

The reality is that some voting machines used in many elections hosted in the United States were capable of being hacked with relative ease; yet, the private companies responsible for developing these vulnerable voting machines have been awarded major contracts to host future elections within the United States.

One such company, Dominion Voting Systems, a company that acquired Premier Election Solutions (formerly Diebold Election Systems) in May 2010 and Sequoia Voting Systems in June 2010 currently has contracts to provide electronic voting systems to 600 jurisdictions in 22 states in the U.S. Both of these companies have developed voting machine technology used with known vulnerabilities in the past.

To further support these vulnerability claims, a security analysis study of the Diebold AccuVote-TS voting machine led by Professor Edward Felten of Princeton University revealed that one, whom gained physical access to this type of machine or its removable memory card, could install malicious code capable of stealing votes without being detected in as little as one minute. Voting machine vulnerabilities such as these leads one to believe that biggest offenders of election fraud are the voting machines themselves, not the voters.

With all this in mind, one may come to the realization that the only way to truly eliminate illegitimacy concerns due to the aforementioned issues is to ensure that elections are hosted transparently. Without transparency, being that one cannot independently audit the results of an election, there is absolutely no definitive way people can be assured their vote has been accurately recorded and properly stored in the system of record by the voting authority and/or that results of the election as a whole are actually legitimate.

The lack of transparency in elections can also lead to other issues, such as lack of voter turnout due to voter apathy, as many people feel that their vote doesn’t really matter because there is no way to determine whether or not their vote has been properly accounted for. Therefore, it comes to no surprise that, according to the Federal Elections Commission, the Federal Elections 2012 report states that only 58% of the population eligible to vote in the election actually voted.
In conclusion, it is clear that the voting industry is plagued with numerous issues, with one problem leading to another, beginning and ending in a black box where private companies with private interests tally the votes and control the outcome of elections. We must acknowledge that the key issue that needs to be solved is the lack of transparency in government run elections, in the Unites States and across the globe. If we can properly address this singular issue, we’d essentially solve all the other problems that plague the industry and would have the opportunity to begin hosting accurate elections that result in an agreeable consensus.

3. THE HISTORY:

The challenge of developing a sound process for hosting elections with agreeable outcomes is nothing new to the democratic societies of the world.

In their quest to develop a new and improved democratic nation where all of its citizens had the inalienable rights to life, liberty and the pursuit of happiness, when the Founding Fathers of the United States sat down and began drafting the [United States Constitution](https://www.whitehouse.gov/the-press-office/2015/09/29/founding-fathers-constitution), they intentionally avoided including anything in the constitution with respect to the citizens involvement in federal elections, deciding to leave it up to the states to decide how this should be handled. Although the Founding Fathers of the United States were arguably some of the smartest men in recent history, they could not even come to an agreement on whom should be given the right to vote or whether or not the act of voting should be considered a right or a privilege.

To address these gaps in our founding laws, states had to come up with their own voting laws starting with how their electors in the Electoral College would be selected and [what their responsibilities would entail](https://www.whitehouse.gov/the-press-office/2015/09/29/founding-fathers-constitution), which vary from state to state. Unfortunately, it seems that this decision made by the Founding Fathers of the United States resulted in the widespread inconsistencies between voting laws established by the states for hosting federal elections, a real problem that comes with its own set of challenges.

When it comes to the voting systems themselves, the technologies being leveraged by the states in hosting federal elections are no exception to the rule, as they vary from state to state as well.

As technology advances, states in the U.S. have generally chosen to evolve; and, the reality is that the U.S. taxpayers are the ones paying the bills. As a result of this forward progress, citizens voting in U.S. Presidential Elections are experiencing a rapid reduction in the availability of non-electronic voting systems.
The Key To Unlocking The Black Box: Why The World Needs A Transparent Voting DAC

Since 1980, punch card voting systems have been steadily losing their popularity and seem to be on their way out. Conversely, voting systems that utilize paper ballots combined with optical scanners have been on the rise since the early 1990’s.

At the turn of the century, the use of various electronic voting systems really took off. A decade later, mechanical lever machines, which were popular from 1960’s to the 1980’s, had become completely phased out in the United States. Paying for the advancement of these voting systems and adoption of electronic technologies come with a hefty price tag.

On a continual basis, government contracts are being awarded to private companies who are developing these advanced voting systems to be used in taxpayer funded elections. To put things in perspective, in 2010, Hart InterCivic (a developer of electronic voting machine technology), was awarded an $11.5 million contract by the Hawaii State Government to host the 2010, 2012, and 2014 elections. To put things into perspective, this contract is only for 3 elections cycles for one state that houses just 0.43% of the United States population.

With the 2016 U.S. Presidential and Congressional Elections right around the corner, it seems that the time has finally come to leverage the latest technology to develop a voting system that permits the hosting of secure and transparent elections with agreeable outcomes that makes efficient use of taxpayer money.
4) THE SOLUTION:

In today’s world, it is finally possible to host verified and transparent elections within an end-to-end voting system, while still respecting citizens right to privacy. This can be accomplished through the use of cryptography and blockchain technology encoded within a DAC.

DAC is a term that was first coined by the Founder and CEO of BitShares, Daniel Larimer, as a “Decentralized Autonomous Company.” But, in theory, a DAC could be thought as a product, as opposed to a company as the name would suggest; it is simply a software application that is created and launched by a software developer.

A DAC is referred to as a company because the developer has encoded a business model within the software that inherently generates profit for its users whom have invested in the product, which are referred to as the company’s token holders, as they have been awarded partial ownership of the product for their investment in the form of tokens of the company. Where permitted by law, the product is able to generate profits for its token holders because, in order to use the services the software provides, one must also invest in the product by purchasing tokens of the company and use those tokens to pay the transaction fees associated with each service the software provides. As services are provided and tokens are spent to pay for transaction fees, the tokens are destroyed.

As tokens of the DAC are destroyed, the total number of tokens that have been issued to the users of the product is reduced, which makes the value of each token left in existence go up. This increase in value (equity-per-token) can be considered profits earned by the product’s token holders, similar to the way dividends are paid to shareholders within a traditional company.

Although tokens of the company are being purchased and used to pay for services the software provides, it is important to point out that a DAC is not a legal entity or person like a traditional company, as the company exists entirely as a decentralized transaction ledger maintained by a network of individual computers that are owned by regular people all over the world. This network of computers that powers the product is managed by 101 users, which are referred to as delegates within the DAC, as they have been appointed to their positions by the other users within the DAC through a continuous voting process; and, these delegates take turns verifying that each transaction on the transaction ledger is legitimate on behalf of the other users, hence the name delegate.

A delegate is viewed as a coveted position within the DAC, as the company allocates tokens to delegates over time as a form of compensation for the costs associated with powering the product (i.e. verifying transactions on behalf of the people). The number of tokens each token holder has determines how many votes are given to the delegates they choose to support. The 101 users that have the most token holder
votes get the opportunity to serve as delegates. Being that token holders can change their votes at any point in time for any reason, delegates can be voted in and out of their positions at any point in time, as delegate vote totals will naturally fluctuate within the DAC. Operating in this way gives the end user base collective control of the company and allows the DAC to continue to provide its services to the users of the software without relying on any single individual (such as a CEO) to accomplish its goals; this makes DACs autonomous in nature.

Using the BitShares Toolkit for building DACs, any software developer with the necessary coding skills can create a DAC; and, DACs can be built with various types of business models. For example, BitShares suggests that DACs are a great fit for all types of business models, such as banking, stock exchanges, insurance, lotteries, auctions, music, and voting. Regardless of what business model the developer chooses to encode into to the DAC, the product should performs services for the end user(s) that adds value to their lives so that people actually want to use it.

Ultimately, the only things that have true value are those that sustain and defend society. A voting DAC provides a service that allows people to vote in elections that are secure, transparent, and free from corruption, which begs the question:

What better way to defend a society than by developing a DAC using the voting business model?

4.1) Voting DAC Benefits:

The benefits of using a DAC for hosting elections are inherent in a DACs design, as it embodies many of the characteristics that a legitimate electronic voting system requires: security, accuracy, transparency, anonymity, forgiveness, fairness, and efficiency.

4.1.1) Security:

Contrary to popular belief, cryptography is not a new concept, as cryptography technology has been in use for decades. For instance, cryptography technology is actively being applied to secure all types of communications in today's modern world, such as ATM card and ecommerce transactions.

DACs use asymmetric encryption, which requires two separate keys that are mathematically related. One of these keys is shared by both parties involved and can be made public, which is why it is called a public key. The other key is kept secret by one of the two parties involved, and is therefore called a private key. The combination of public and private key is described as a key pair.
Therefore, a DACs asymmetric encryption method is ideal for use in a transparent voting system, as it provides a secure way for voters to register to vote, request ballots, and cast their votes in elections and allows others to verify their activity as legitimate in an effort to prevent fraudulent activity that would otherwise corrupt the results of an election, all while protecting the voter’s right to privacy.

When a user creates an account within a DAC, they are given a public key and a private key. Although the user will be given both, the system and users within it will only know what that users public key is, meaning that the owner of the account is the only person who will know what their private key is. The user’s private key will be used to control the account and submit requests to the system. Therefore, if a user loses their private key, being that they are the only person who knows what their private key is, they will need to create a new account in order to use the system. By leveraging cryptography technology in this way, the system is secure; even if a thief knew your public address, it would take them billions of years with a supercomputer to compute your private key.

4.1.2) Accuracy:

Once a user's account is created, the user can register their account if they wish to secure a username of choice. Otherwise, their public key will serve as their identity within the software application. Additionally, if a user wishes to do so, they can enter various demographic credentials (i.e. age, country of citizenship, etc.) and connect with other account holders outside of the system, in order to have their
account credentials verified; these account holders are users that wish to serve as account verifiers to validate certain user credentials (i.e. the U.S. government, Republication Party, Democratic Party, etc.). Once verified, these account verifiers will confirm the user’s credentials inside of the system, at which point these credentials will officially be associated to the user’s account.

As a user’s account credentials are verified, users become eligible to request ballots to vote in various elections. Users can also request to create elections if they wish to do so. During the election creation process, the user must specify what account credentials voters must have in order to vote in their election. Thus, when a user requests a ballot to vote in an election, the electronic voting system must verify that the user has the appropriate account credentials prior to providing the user with a ballot. Also, once a user has been given a ballot, they cannot request another ballot for the same elections. These rules ensure that only those that are allowed to vote in certain elections have the ability to do so and prevent users from voting more than once in an election.

When a user submits their ballot in an election, they are simply requesting to add new information to this electronic voting system. This request (in addition to all of the aforementioned types of requests) will be submitted to the electronic voting system in the form of a transaction that must be verified by a delegate within the system. During this process, the user can rest assured that their ballot will not be tampered with, as cryptography and blockchain technology prevents the user’s ballot from being intercepted and modified (even by a delegate) prior to being stored in the electronic voting system.

Before a delegate can verify a user’s ballot submission as a legitimate transaction, the delegate must first verify that they have a copy of the most up to date version of the electronic voting system. Once the delegate has verified they have the most current version of the software, the delegate must verify that the user’s ballot submission (the transaction) is legitimate. If so, the transaction will become part of the official transaction ledger, meaning the ballot will be stored within the electronic voting system and the user’s the vote will be added to the results of the election. Even though delegates serve as the gatekeepers of the system, it’s important to point out that a delegate’s power is limited.

Delegates cannot vote on someone else’s behalf, nor can they approve illegitimate transactions or override the rules of the system in any way, which means that delegates have no control over the results of the election. However, they do have the ability to approve one or more transactions at the same time, which are referred to as blocks. These blocks of transactions are stored within that electronic voting system in chronological order (based when the delegates approved them) and are connected to one another in a way that would resemble a chain, hence the name blockchain.
Every block in the blockchain contains a hash or ID number of the previous block. This has the effect of creating a chain of blocks from the very first block to the current block. Each block is guaranteed to come after the previous block in chronological order because the previous block's ID number would otherwise not be known. Each block is nearly impossible to modify once it has been in the chain for a while because every block after it would also have to be regenerated.

Although the delegates are responsible for creating and maintaining the blockchain, it is actually a public transaction ledger that can be viewed by any user within the DAC at any time. In other words, the blockchain is the transactional database shared by all the users of the DAC that lives within a software application on the computers of its users around the world that have the ability to connected to the internet. Thus, the DAC, the electronic voting system, and the blockchain can be thought of as all one and the same things.

4.1.3) Transparency:

A full copy of the DACs blockchain contains every transaction ever performed within the electronic voting system. With this information, one can find out how many votes each candidate had at any point in history. This means that anyone at any time could audit the results of an election to ensure the authorities hosting the election accurately reported the outcome. Without transparency, being that one can’t independently audit an election, how can they be assured the results are legitimate? The harsh reality is in the fact that they can’t. Thus, without transparency, the voters do not control the outcome of the election; the voting authority that tallies the votes and reports the vote totals to the voters is really the one whom controls the election.
4.1.4) Autonomy:

The great thing about a DAC is that it is completely controlled by the users, meaning that it is decentralized in nature. Although the rules of which the DAC operates by is initially encoded in the software by the original software developer, the reality is that the software is open source software that can be updated by any user at any time. This means that, by editing the code, the users can update the rules of the software as they see fit. However, in order for a user’s update to take affect, each delegate must agree to the new rules by updating their version of the software from their existing version to the newer version that incorporates the user’s recent change. These rules make the DAC a self-policing system that prevents the software from being hacked and highjacked.

4.1.5) Anonymity:

Being that the DAC uses cryptography technology to issue private keys to account holders that are used to perform user operations within the software (i.e. requesting a ballot) and public keys to control the verification of user operations as legitimate transactions to be added to the blockchain, users can be assured that their identities will be protected and therefore remain anonymous.

4.1.6) Forgiveness:

In the days leading up to an election, DAC users can complete their ballots ahead of time. Users can also can access and update their ballots at any time by changing whom they wish to vote for prior to the end date of an election. This rule ensure that, when an election ends, the users’ vote are much more likely to reflect who they really want to win the election.

4.1.7) Fairness:

In a DAC, users will be able to vote for every candidate they support for a particular office, as opposed to forcing users to vote for one and only one candidate per office. This rule will naturally ensure that the candidate that has the most support among all voters actually wins the election, leveling the playing field for all candidates.

4.1.8) Efficiency:

A DAC’s goal is to maximize revenue from transaction fees by increasing the value provided by the transactions while minimizing the cost of operations. When it comes to the crypto-equity aspect of a DAC, instead of creating ‘coins’ (i.e. bitcoins, which is the currency being used in the Bitcoin payment system), DACs have tokens much like a corporation. A token is nothing more than a percentage of a whole. There are many ways to allocate tokens; one approach with respect to token allocation will be covered in the next section of this whitepaper.
4.2) The Follow My Vote Voting DAC:

In the near future, Follow My Vote will be developing the first voting DAC in history using the BitShares DAC Toolkit, which will be called the VOTE DAC. Development will happen in stages, with the first stage being the development of a proto-DAC. A proto-DAC is a software product/company that doesn’t implement the full feature set of the ultimate company, but which allows the trading of tokens in one or more future companies while they are under development. With this in mind, we will refer to the partial ownership the VOTE DAC as a VOTE or VOTES, similar to how one would refer to owning shares of a traditional company.

4.2.1) VOTE Allocation:

The VOTE allocation of Follow My Vote’s voting DAC will include 10 billion VOTES. Half (50%) of the VOTES (5 billion to be exact) will be allocated over time to delegates that will be responsible for maintaining the blockchain throughout the life of the company, starting with 50% allocated within the first year of operations and 50% of the remaining VOTES thereafter, year over year.

The other 5 billion VOTES will be allocated up front to, among other things, cover the cost of the development of the DAC itself and marketing necessary to acquire its initial user base. The breakdown of the up-front VOTE allocation will be as follows:
4.2.2) BitShares PTS: 1.5 billion VOTES

BitShares PTS, is a simple minable crypto-currency (similar to Bitcoin) that was created to allow people to advertise their interest in receiving free token samples in future DACs. Per the BitShares social consensus, 30% of VOTES that are initially allocated will be distributed to those who have supported the BitShares industry by owning its BitShares PTS tokens.

A snapshot date will be announced at some point prior to the release of the VOTE proto-DAC; and, a snapshot will be taken of the ownership of BitShares PTS. A “snapshot date” is like a date of record for a stock dividend. Anybody who owns BitShares PTS on that snapshot date is given a proportional stake in the new DAC. Thus, those interested in supporting Follow My Vote should invest in BitShares PTS prior to the VOTE DAC snapshot date.

4.2.3) BitShares AGS: 1.5 billion VOTES

BitShares AGS is similar to BitShares PTS in that both were ways of volunteering to receive free promotional samples from the developers of new DACs. The difference is that BitShares AGS can no longer be bought or sold, as the owners are those whom contributed into an industry development fund while the industry was still in its infancy. Per the social consensus, 30% of VOTES that are initially allocated will be distributed to BitShares AGS owners in proportion to their ownership of AGS.

4.2.4) Follow My Vote: 1.5 billion VOTES

Follow My Vote will be spending a considerable amount of resources to develop the VOTE DAC and acquire new account holders upon its release. Thus, 30% of VOTES that are initially allocated will be distributed to Follow My Vote to cover these costs.

4.2.5) NuSpark: 50 million VOTES

NuSpark is a startup incubator in Blacksburg, VA, that has supported Follow My Vote in since their early stages of development by providing them with dedicated office space to conduct business operations. NuSpark will continue to support Follow My Vote by further educating the Blacksburg community and surrounding areas about cryptography and blockchain technology in an effort to encourage the use of the VOTE DAC. For their continued support, NuSpark will receive 1% of the initial allocation of VOTES.

4.2.6) Virginia Tech: 50 million VOTES

Virginia Tech is also located in Blacksburg, VA. Similar to NuSpark, Virginia Tech will be supporting Follow My Vote by further educating the Blacksburg community and surrounding areas (in addition to the Virginia Tech faculty and student body)
about cryptography and blockchain technology in an effort to encourage the use of
the VOTE DAC. For their support, Virginia Tech will receive 1% of the initial
allocation of VOTES.

4.2.7) New River Valley: 400 million VOTES

Follow My Vote will be promoting the emergence of the cryptography and
blockchain technology to the U.S. citizens living in New River Valley. Residents of
Blacksburg, Christiansburg, and Roanoke, VA, will have an opportunity to claim
VOTES during a series of promotions to encourage the use of the VOTE DAC. A total
of 8% of VOTES that are initially allocated will be distributed in this way.

4.3) DAC Use Cases:

There is massive potential for software developers to revolutionize various
industries by developing DACs that create value by providing various services to
end-users. The possibilities are endless.

For illustrative purposes, we’ve taken the liberty to list several use cases for DACs
developed using the voting business model:

Hosting Elections:
- Governments:
  o Federal
  o State
  o County
  o City
  o Town
  o School
- Proxy Voting:
  o Corporations
  o HOA’s

Establishing Consensus:
- Belief Statements/Opinion Polling:
  o Government Organizations
  o News Media Outlets
  o Lobbyists
  o Political Campaign Strategists
- Focus Groups:
  o Startup Companies
    ▪ New Product Development
  o Established Corporations
    ▪ New Product Development
    ▪ Existing Product Modification
In conclusion, a voting DAC is the key to solving the transparency problem current electronic voting systems face today. Thus, the VOTE DAC has the potential to become a game-changing technology and the voting platform of the future.

By investing in BitShares PTS prior the VOTE proto-DAC snapshot date, you have an opportunity to get in on the ground floor and secure a stake in all DACs that Follow My Vote plans to develop in future, as snapshots for future Follow My Vote DACs will be taken of the VOTE DAC, in addition to BitShares PTS.

Additionally, once the VOTE proto-DAC is released, regardless of whether or not you missed out on an opportunity to invest in BitShares PTS prior to the snapshot date, VOTES of the VOTE proto-DAC will be traded on crypto-currency exchanges (i.e. Cryptsy.com, Bter.com, etc.), at which point all one needs to do is purchase VOTES in order to become involved in this investment opportunity of a lifetime.

Keep in mind that this field is still in its infancy. Thus, one would be wise to seek out and invest in companies developing these emerging technologies.

Seize this moment. The time is now.
5) About Follow My Vote:

Follow My Vote was born on the 4th of July in 2012, founded on the principles of freedom, as a tribute to the Founding Fathers of the United States.

We’re a nonpartisan organization on a mission to change the world. We develop applications intended to improve our world by effectively gauging popular demand.

As a first step towards fulfilling our mission, Follow My Vote is taking on the challenge of improving elections around the world for everyone involved by developing the voting platform of the future, which will exist as a Decentralized Autonomous Company (DAC) that provides end-to-end transparency into the results of any and all elections hosted within it by utilizing blockchain and cryptography technology.

With this voting DAC, our goal is to begin unlocking the black boxes that elections are being hosted within today, allowing voters to audit election results while respecting each voter’s right to privacy, in order to ensure that each vote in every election truly counts.

The Follow My Vote Family's Core Values:

-Honesty
-Integrity
-Transparency

As we work to develop our first of many voting DACs in the days ahead, we wish to leave you with a quote that we hope makes a lasting impression:

'It's Not the People Who Vote that Count; It's the People Who Count the Votes'
- Joseph Stalin