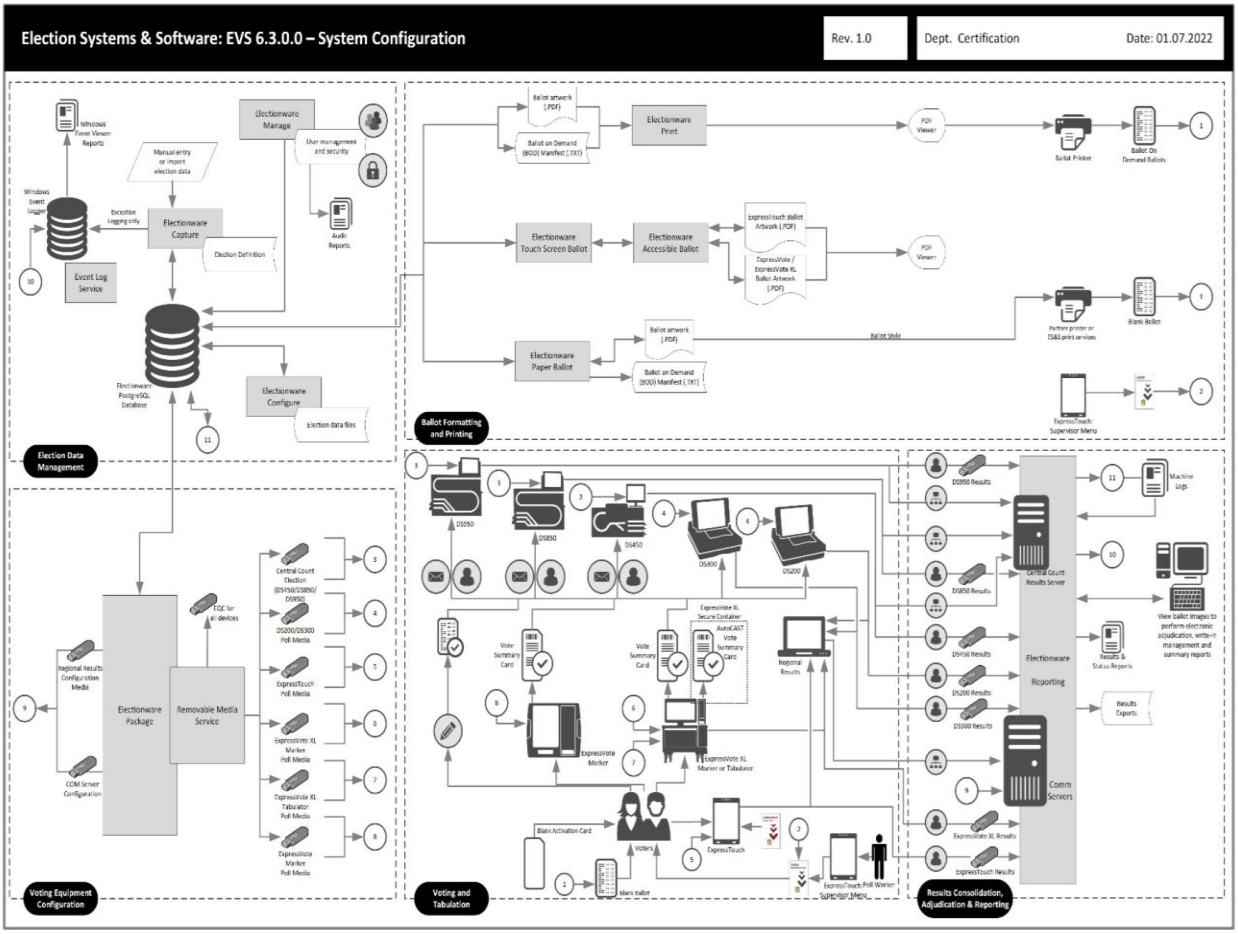
Electronic Voting and Blockchain Slide Notes

I'm Julie Baker, cybersecurity expert. I have spent over 30 years working in cyber – most of the time on Wall street for big banks like Citigroup, TD Bank and Deutsche Bank. I have even worked in Israel for 4 years setting up a cybersecurity innovation center there. A few other things to know about me:

- I am a retired chief information security officer
- I am the Congressional District 3 GOP Chairwoman
- RNC delegate
- Board member of the South Carolina Republican Assembly

And I want to talk to you today about why electronic voting is a really bad idea

Electronic voting, and this means using computers to cast votes, count votes and everything in between, is a bad idea and has been from the start. The picture you see below is of our current ES&S voting system in South Carolina – version 6.3.0.0



I will use this picture as a backdrop as I go into the reasons why electronic voting sucks

1. First is Complexity:

   We say in cybersecurity that Complexity is the enemy of security. The more complex a system is, the harder it is to secure. The voting systems in use today are all highly complex systems with many moving parts as you can see from the picture. Each part is a potential attack vector. Also contributing to this complexity is over 3-4 million lines of code just to count votes. Any developer or IT/IS expert can tell you that counting votes should not take 3-4 million lines of code. It is not possible for a person to analyze that many lines of code. AI could do it – but that's having the fox guard the hen house as far as I'm concerned

   Do you want a complex black box evaluating another complex blackbox? It's almost as if it is deliberately complex so as to avoid reviews and assessments.

2. Then there is the tendency towards centralization:

   Every move towards centralization in a voting system, by definition, means less local control. It means we the people have less control over our own voting. We have seen the risks from Federal involvement in our elections:

   - CISA is the federal Cybersecurity and infrastructure Security Agency that was weaponized against us
   - EI-ISAC and other ISACs – these are government/business consortiums for sharing information, but were again used for federal surveillance and control over our elections.
   - EAC (Election Assistance Commission) – the federal oversight body
   - The federal testing program for the current voting systems,
   - Federal laws like HAVA
   - not to mention the Center for Internet Security which manages albert sensors and gets federal funding

   and the list goes on.

   President Trump is working on fixing this. But this happens at the state level too - South Carolina has a fully centralized voting system – controlled from Columbia. Can central control ever be considered a good thing when it comes to voting?

3. Then there is the problem of an almost fully outsourced election process

   Our current voting systems are controlled by third parties some of which are not even US companies. ES&S, Dominion, Hart Intercivic – these are currently the three biggest voting companies and they are all largely private equity owned. This means we have no real visibility into investors, security posture or anything really. And these third parties use other

third parties - like Dominion using Serbian developers. What are the risks from an almost fully outsourced process? Like centralization risks, do we still have local control of our elections?

4. Next – these systems are opaque – there is no transparency:

   Current voting systems are what we call black boxes – in practical terms this means:

   - We have no access to the source code
   - We can't open the machines to see what hardware is inside.
   - We have no ability to test them or security assess the code/hardware ourselves.
   - Is there a cellular modem installed? No way to know

   Essentially we have no idea what is happening under the hood. voting companies make it very hard to get Cast Vote Records (CVRs) and audit logs, and you can't foia private companies. How can we trust what we can't see, what we can't audit?

5. Lastly Electronic Systems are Vulnerable:

   Software can be programmed to do just about anything and it can be manipulated on the fly and you would never know. It is also inherently vulnerable – developers write code and make mistakes. Even AI writes code that has mistakes. These mistakes become vulnerabilities or weaknesses that can be exploited by bad actors to gain unauthorized access. Every time software is changed, new vulnerabilities are introduced. Even supposedly air gapped systems can be compromised via USBs that have been infected with malware. This means it is not possible to have any electronic system that is 100% secure.

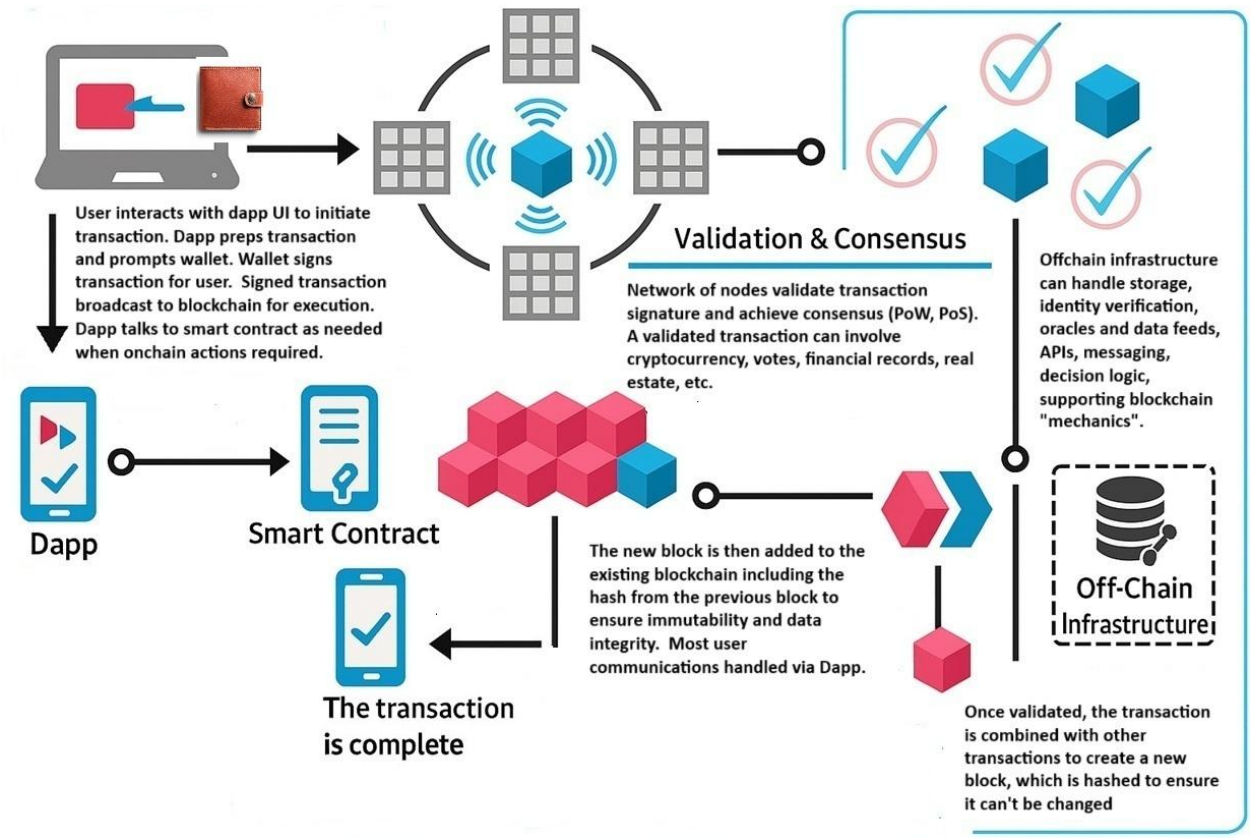
So electronic voting, using computers to vote is, in my oh so humble opinion, is irredeemably bad. Is there any way this can be fixed? There have been rumors that President Trump and Elon Musk have discussed the use of blockchain in voting to try to address these risks. There is also a mobile voting system being developed right now, potentially for use in the next election. Can these help us fix these problems?

So, let's talk about blockchain. Blockchain is a decentralized, meaning spread over lots of computers with no central authority, fully public and transparent, secure and immutable digital ledger. It records transactions whether they are financial transactions or votes or anything else. It is heavily used for cryptocurrencies like Bitcoin and Ethereum, but it is also being widely adopted for real estate and financial transactions and lots of other use cases.

It sounds wonderful indeed. These characteristics also make blockchain appealing for election integrity activists. Who wouldn't want a simple, secure, immutable, fully transparent,

decentralized system for voting, where no central authority can put their thumbs on the scale, right? But there is nothing new under the sun.

Take a look at this picture below.



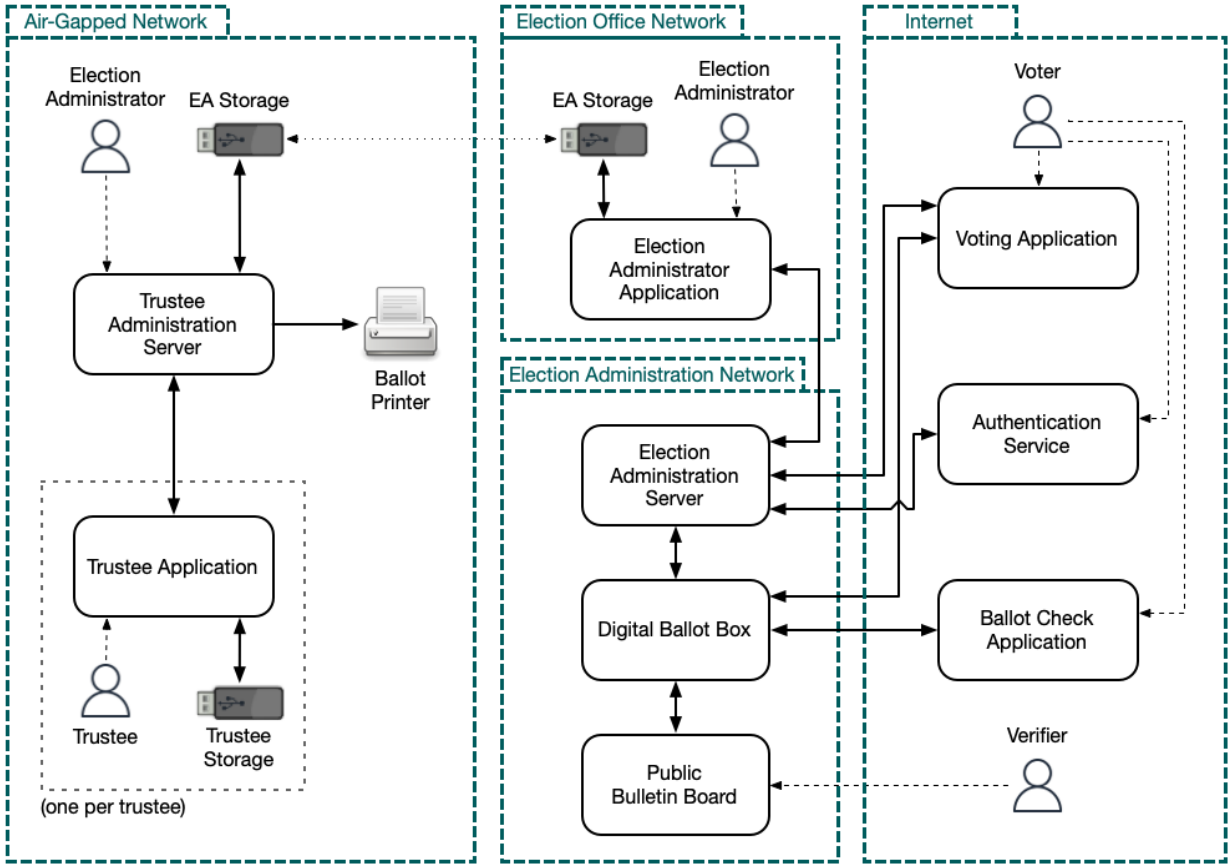
This blockchain ecosystem is more complex than the current electronic voting systems, especially around cryptography and how keys are managed and stored. Because it is never just the blockchain – it is always the blockchain ecosystem – everything that talks to the blockchain which includes many third parties and all the software that runs on the blockchain are vulnerable to attacks. You think it is fully transparent? You think it is fully de-centralized? Not necessarily because it is all in the implementation.

- Blockchain can be public (everyone can see everything, or private (only a few can see everything) or hybrid.
- It can be fully distributed more like a pure distributed blockchain or it can be fully centralized
- It can be permissioned where only a few can write to the blockchain or permissionless – all can write to the blockchain which is again the more “pure blockchain”

Also never forget that blockchain, and everything in the blockchain ecosystem is code. It is software, as well as hardware – just like the voting systems of today and just as vulnerable. And maybe I should mention all the real world examples of successful attacks against all the moving parts of this highly complex ecosystem. But there are too many examples - real world losses to the tune of hundreds of millions, even billions of dollars.

The Bybit attack was in February of this year – 1.5 billion was stolen. I get daily notices about attacks against applications, blockchain and cryptocurrency, mobile applications etc. The fact is - where the money is, the attackers will come. And equally true - where the votes are, the attackers will come…and the nation states. So nope, this is not an option for us.

Ok, so blockchain isn't workable, but what about Mobile Voting? Wouldn't it be amazing to be able to vote from your phone? Take a look at the picture below:



There is a "non-partisan" group funded by Tusk Philanthropies that are developing a mobile voting system that could potentially be used at the midterms (https://www.mobilevoting.org/about). Bradley Tusk also wrote a book that is very informative about the plans for mobile voting – Vote With Your Phone: Why Mobile Voting Is Our Final Shot at Saving Democracy.

I'll just give you some of the highlights.

- The folks behind this are not non-partisan – they are on the left.
- In their own words, they are not building a system that is more secure than the current systems, but one that is just as secure as the current systems – which is not secure at all as I have mentioned.
- The cryptography has strong ties to the NSA & DARPA not to mention Microsoft – do you think that is a good idea?
- There are foreign third parties involved in the development of this product – A Danish company is doing the development for example
- It is every bit as complex as the current voting systems, if not more complicated.
- They claim that you can view your ballot all the way through the process…at least until all those ballots get copied over to their "air gapped" system for final printing and tallying.
    - Even if they are displaying your ballot to you – how do you know that is what is being tallied?
- This is still vulnerable software with weaknesses that can be exploited.

which leads us to the real kicker

- It is meant to be a replacement for the current mail-in voting system that our president is trying to get rid of….Let me quote from their FAQ

"The technology we have developed mitigates the risk of voter fraud by following the same process used for mail-in voting…"

Do you think we have problems with fraud with the current mail-in voting process? If the answer is yes, then we don't want the electronic version of mail in voting – it is a recipe for fraud at scale.

Electronic voting – whether current systems, blockchain or mobile voting are bad news. Let's recap:

- We have the complexity problem –
  Mobile voting, blockchain voting and current systems all highly complex systems with lots of attack surface.
- We have the tendency towards centralization –
  Because it is all about the implementation for all of these systems.

  When Romania did their elections using blockchain in 2020 and again in 2024– they opted to use the EU's centrally controlled blockchain

Do we actually think nation states will opt to use a fully transparent, truly immutable, decentralized blockchain, or any system like that, for voting?

- We have the lack of transparency – the Black Box Risks
  There are major issues with transparency and auditability for all of these systems… they are black boxes – we have no idea what is happening inside
- Then there are the outsourcing or 3rd party risks
  Most of these systems are run by private entities, funded by opaque investors, with little independent security validation.
  Not to mention the foreign companies involved in our elections
- And lastly are the huge issues of software vulnerability –
  Every element of a blockchain ecosystem and mobile voting system are just like today's electronic voting systems -
  they are software and hardware.
  And all software has bugs. Even hardware has bugs
  Attackers know it and exploit that.
  History proves it by the sheer volume of attacks.

There is nothing new under the sun. And with the rise of AI and Quantum computing…all bets are off…there will be no more secrets. Think about this. Banks put aside 10s of millions even 100s of millions of dollars for fraud. They and other companies also buy cyber insurance because breaches will happen. It is not a matter of if but when. It is the reality because nothing is 100% secure and never will be.

How much fraud can you tolerate in an election? When it comes to elections you only have one shot at it. You have to keep the bad guys out 100% of the time – 100% prevention, which is not possible

So let's be clear. Blockchain and mobile voting might be innovative and cool, but they still have all the same issues that our current voting systems have. These issues are endemic to electronic voting. Electronic voting, in all its forms is irredeemably bad. It allows for cheating at scale. IIt is not possible to fix it.

So Nope! We need to say NO to blockchain voting. NO to mobile voting and NO to all forms of electronic voting. We need to say YES to paper. YES to hand-marked, hand-counted paper ballots.