Notes on the Use of Blockchains in Voting

Tom Ryan, May 2018

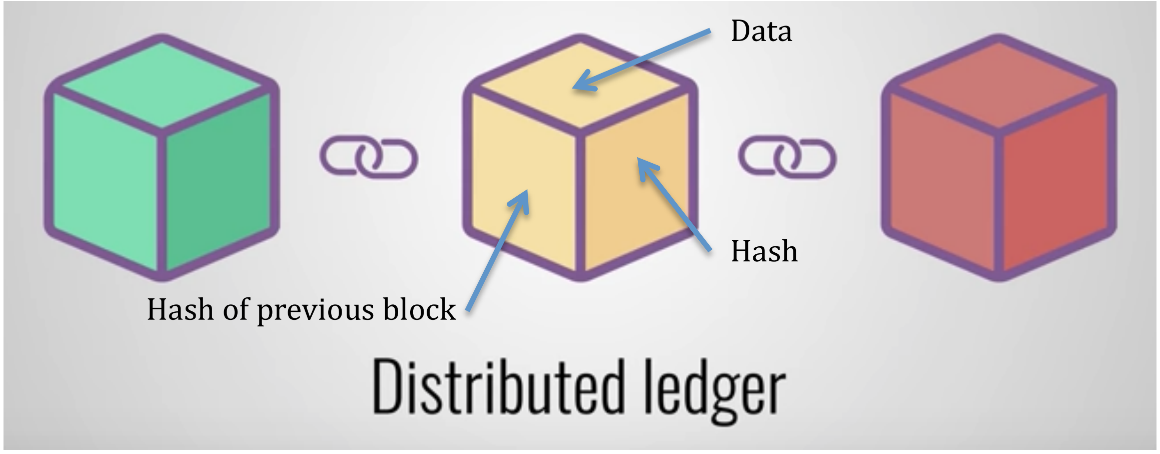
Blockchain developed in 1991 as a way to timestamp digital documents so it's not possible to backdate or tamper. Went pretty much unused until adapted to create Bitcoin in 2009.

Technically speaking, a blockchain is a linked list of blocks and a block is a group of ordered transactions. You can think of a blockchain as a subset of a database, or a distributed ledger, with a few additional properties.

Specific rules about how to put data into the database.

- Data cannot conflict with some other data that's already in the database (consistent),
- append-only (immutable), and the data itself is locked to an owner (ownable),
- Everyone agrees on what the state of the things in the database are without a central party (decentralized).

Blocks are sequenced in time. A "block" contains data, the hash of the block, and the hash of the previous block. Blocks are validated by "Proof of Work" that involves the solution to a complex cryptographic puzzle. "Miners" compete to solve the puzzle. The node that solves the puzzle adds the block, broadcasts the addition, and gets rewarded (at least in Bitcoin). Takes about 10 minutes on average. This complexity makes it "impossible" to intentionally corrupt a block then reconstruct all the remaining hash links without being detected.



Public, private and hybrid blockchains:

Each person that's authorized to add data to the blockchain has both a private key and a public key. The private key must be kept secret from everyone else, but the public key is available to anyone with access to the blockchain.

The private key is used in combination with the data a person wants to add to create a digital signature. The computers on the blockchain network can then use a person's public key to verify the private key was used to sign the data. That public key cannot, however, be used to determine the private key.

With blockchain voting, the information that registers on the blockchain shouldn’t include identifiable information. This means that information about the sender of the voting token has to be hidden. There are different ways to accomplish this, including zero knowledge proofs, ring transactions, or various encryption methods. Each has its benefits, drawbacks, and technical challenges. **True anonymity at the same time as verified identity is the big challenge of blockchain voting.**

Blockchain Trust Accelerator is an organization that promotes uses of blockchain technology:
The Blockchain is ***highly transparent***; a record of all transactions is permanently available. All users on the system can see in real time as new transactions are added to the database. Meanwhile, individual privacy is protected without jeopardizing the legitimacy of asset transfers since users work under numerical pseudonyms.

The Blockchain is also ***entirely auditable***. Every time a new transaction is added to the record, it is also cryptographically linked to every previous transaction. Therefore, the Blockchain ledger cannot be altered once it is verified. Since the record is both transparent and uncorrupted, a trail of digital breadcrumbs allows for monitoring and auditing of all the data within the network.

Blockchain Voting

THE FOLLOW MY VOTE WAY

The Voter

followmyvote.com

Downloads and installs the Voting Booth

Securely submits identity information for verification.

+

Registers for the election they qualify to vote in.

=

The voter has been authorized to cast a ballot by both the ID verifier and registrar.

The voter then votes and submits their ballot to a secure blockchain based ballot box, while retaining anonymity and ballot secrecy.

If a voter changes their mind, they have the ability to change their vote at anytime in the days leading up to the election.

(Election officials can decide to turn off or on this capability depending on laws and election rules)

Using their vote account, the voter can go into the ballot box and verify for themselves that their vote was cast as intended. The Voter can even audit each ballot in the ballot box to confirm the election results are accurate. All while retaining privacy and top level security.

Many companies promoting online voting, most involve blockchain: Voatz, Free and Fair, Follow My Vote, Blockchain Tech Corp, E-Vox (Kiev, Ukraine). Google developing cloud based blockchain apps

General lack of support from researchers/academics.

http://www.govtech.com/data/GT-OctoberNovember-Securing-the-Vote.html

Can Blockchain Bring Voting Online?

Ben Miller / Oct/Nov 2017

Voatz, a Massachusetts-based startup that has struck up a partnership with one of the few companies in the country that actually builds voting systems, has used a blockchain paradigm to run elections for colleges, school boards, unions and other nonprofit and quasi-governmental groups. Perhaps its most high-profile endeavor was authenticating delegate badges at the 2016 Massachusetts Democratic Convention.

The Voatz idea is to put a spin on bitcoin's approach to blockchain. The company thinks government could limit the blockchain miners — or validating peers, the term Voatz CEO Nimit Sawhney prefers — to a handful of trusted, verified partners. They wouldn't make money from their work the way bitcoin miners do.

"Your incentive to participate is essentially to help democracy and ensure we have better elections," Sawhney said.

The system can also work with paper ballots. Sawhney said his company has written a standard for incorporating those ballots into the blockchain, and in those situations, Voatz would augment the existing systems rather than replace them.

Voatz isn't the only company working on this. There's Follow My Vote, a Virginia-based company with its own blockchain-based platform. Then there's Blockchain Technologies Corp. in New York, and E-Vox in Kiev, Ukraine.

The Estonian government is considering blockchain voting. The Republican Party used it in Utah in 2016 for its primary voting. There are governments eyeing blockchain all around the world.

Benaloh sees many problems with blockchain. One of them is that the system trusts miners not to ignore votes, and to record them accurately, but he doesn't see a way to actually force them to do so.

"You're not necessarily trusting the blockchain miners to be honest about what they put. They might put something in the blockchain, like a transaction, that didn't really happen," Benaloh said. "So it's not a matter of honesty, it's a matter of agreeing on what's in the blockchain. Not whether what's in the blockchain is true."

And in fact, he can imagine some easy scenarios in which the miners could either be influenced or even have a direct interest in influencing the outcome of the election.

"Suppose the transactions are votes, and I am the leader of a movement to oppose a heavy tax on blockchain miners," he said. "If I'm going to vote in that referendum, then I have to convince some blockchain miner to pick up my vote and put it into the chain. In that case they may know who I am and they may say 'No, I don't want to do this,' and I may be disenfranchised."

Another criticism: There are ways for miners to increase their own influence. Because validating the blocks relies on computing power, if one miner is able to achieve computing power greater than half of the group of miners as a whole, they in effect win the ability to create the majority of the blockchain.

"If you have a majority of blockchain mining power, the most CPU cycles or whatever, you can take the blockchain basically in any direction you want," Benaloh said.

First U.S. election using blockchain in WV, military absentee voters and their families in two counties. VOATZ supporting West Virginia military voting. Fingerprint and facial recognition used to verify identities.

Charleston Gazette-Mail

Our soldiers deserve secure votes

- By Audrey Malagon May 6, 2018

Amid suspicions of interference in the 2016 elections, states must be more careful than ever to provide heightened security in this year's primaries. Yet, West Virginia has just introduced a more vulnerable form of voting for deployed military personnel.

West Virginia is now the first state to pilot blockchain technology, to allow some deployed soldiers to vote through mobile phones. Yet cyber security experts warn that this technology, also used for cryptocurrencies, poses dangers for voting. Instead of pioneering voting's future, West Virginia is paving the way for future election hacking.

Blockchain technology addresses only part of the security process currently used by those administering U.S. elections. It's like installing a high-tech lock and alarm system in your home, and then leaving a front door key and the alarm pass code under the doormat. The alarm system may work perfectly, but until the keys and pass codes are also secure, your home won't be secure, either.

Blockchains are designed to keep a tamper-proof record of transactions by essentially creating a list shared with a huge network of people at once. If anyone wanted to change an entry in the list, it would be very difficult, since they'd have to simultaneously change it on every copy.

The problem, however, is that blockchain technology in voting does nothing to make sure that correct information gets put on the list in the first place. If a vote is distorted before it's recorded, bad information gets on all the lists, and blockchain actually keeps that bad information secure. While this may not be obvious to the person voting, you can bet that hackers are aware of these vulnerabilities.

Secretary of State Mac Warner claims that this new voting process is "safe, secure and accurate," but statements put out by his office do little to support his claims.

One of the secure features Warner touts is using a phone's Touch ID to verify identity just before voting. This means elections officials contract out some of the security to individual phone manufacturers. During voting, a vote could be intercepted and intentionally recorded incorrectly. Or someone could pose as the voter and steal the vote.

Worse yet, Warner plans to spread the use of this technology, if it's "successful." Yet neither Warner's office nor Voatz, the mobile voting platform company, have clarified what they mean by success.

Will it be a success if the pilot program isn't hacked? How will they know the system has not been hacked? Are there plans to audit and make sure this hasn't happened? What's to keep potentially harmful interferers from waiting for a larger rollout to meddle in elections?

A better plan would be to invite independent cyber security experts to examine the technology or test its security. But, instead of taking such steps to test the technology before using it in West Virginia's elections, online voting in the state's primaries is already underway. In an effort to make voting faster and easier and advance new products, West Virginia is piloting practices that ultimately undermine election security.

In many ways, West Virginia demonstrates that its citizens and leaders care about election integrity. The state's in-person voting system aligns with many of the best practices outlined by election security organizations like Verified Voting.

West Virginia uses paper ballots or voting machines with a paper record, so that every voter can verify that the ballot they marked is the ballot that is cast while still maintaining voter anonymity. Election officials can conduct post-election audits of paper records, to ensure that the votes were interpreted and counted correctly.

By pushing deployed military to mobile app voting, we take away their right to verify that the ballot they cast is the ballot that's counted. With no paper ballot retained for recount or audit, we also exclude them from any authentic auditing process.

Soldiers fight every day to preserve our democracy. It's our responsibility to fight for the security of their votes.

Audrey Malagon is an associate professor of mathematics at Virginia Wesleyan University who works with Verified Voting to advocate for secure election practices.