## H.B.5417 – Oppose – Solution in Search of a Problem, at Our Expense

**Government Administration and Elections Committee** **Luther Weeks**
**Testimony – February 27, 2019** **Luther@CTVotersCount.org**
**334 Hollister Way West, Glastonbury, CT 06033**

Chairs and members of the Committee, my name is Luther Weeks, Executive Director of CTVotersCount, a Certified Moderator, and a Computer Scientist.

I do not consider myself an expert on blockchain, yet I have studied blockchains at a basic level and reviewed several evaluations by scientists I trust. I do claim to be an expert on solving problems, especially with technology.

> Experience Pertinent to this testimony: I have a B.S. in Mathematics from Clarkson University, an M.S. in Computer Science from Rensselaer Polytechnic Institute, and am a Master Fellow of the Life (Insurance) Management Institute. I have a 35-year career building, evaluating, purchasing and implementing computer systems and new technology. For 9 of those years I was a Director of Strategic Planning for the Travelers Computer Science Division and for 8 years worked for two start-ups, designing, developing, and marketing data communications software to large enterprises and government agencies. I keep up with election technology and security issues, daily exchanging ideas with nationally recognized experts in computer science and computer security.

This is bill represents a classic mistake – a "hot" technology solution in search of an undefined problem. This proposal defines no problem and limits the solution to one over-hyped technology. Better to have the problem clearly defined and then solicit proposals to solve the problem – solutions technical and otherwise.

The way to solve problems is to define the problem, create a team of experts on the subject matter, with technical problem solvers, and experts who have solved similar problems for other states and nations - then let them brainstorm, evaluate and propose effective solutions.

If there is a problem to be solved, it is likely there is a solution - if so, it almost certainly does not depend on blockchains, and likely does not need any "hot" technology.

Finally, I am concerned that this Task Force includes two experts on blockchain technology. 1) If there are to be experts on the Task Force, there should be computer scientists and computer security experts as well. 2) If there are blockchain experts then they should be subject to strong ethics requirements to preclude conflicts of interest before and after their participation on the Task Force. The Task Force should also provide several, noticed well in advance, opportunities for public oral and written comments.

I have attached an article on blockchain by a recognized election security expert, Harvard Professor Bruce Schneier on the value of blockchain technology in general, ***There's No Good Reason to Trust Blockchain Technology.*** Here are a some pertinent quotes by Prof Schneier:

> *The circumvention of trust [by using a blockchain] is a great promise, but it's just not true…*
>
> *Private blockchains[1] are completely uninteresting…In general, they have some external limitation on who can interact with the blockchain and its features. These are not anything new; they're distributed append-only data structures with a list of individuals authorized to add to it. Consensus protocols have been studied in distributed systems for more than 60 years. Append-only data structures have been similarly well covered. They're blockchains in name only, and—as far as I can tell—the only reason to operate one is to ride on the blockchain hype...*

[1] Note: Based on its characteristics and the author's definition, a voter registration system would likely only be able to employ a, so called, *private blockchain.*

> *Do you need a public blockchain? The answer is almost certainly no. A blockchain probably doesn't solve the security problems you think it solves. The security problems it solves are probably not the ones you have. (Manipulating audit data is probably not your major security risk.) A false trust in blockchain can itself be a security risk. The inefficiencies, especially in scaling, are probably not worth it. I have looked at many blockchain applications, and all of them could achieve the same security properties without using a blockchain—of course, then they wouldn't have the cool name.*

Also pertinent is this recent article in MIT Technology Review:

**Once hailed as unhackable, blockchains are now getting hacked**
https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

Thank you

The complete article by Professor Schneier:

## There's No Good Reason to Trust Blockchain Technology
**https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/**

**WIRED OPINION** ***Bruce Schneier 02/06/19***

In his 2008 white paper that first proposed bitcoin, the anonymous Satoshi Nakamoto concluded with: "We have proposed a system for electronic transactions without relying on trust." He was referring to blockchain, the system behind bitcoin cryptocurrency. **The circumvention of trust is a great promise, but it's just not true.** Yes, bitcoin eliminates certain trusted intermediaries that are inherent in other payment systems like credit cards. But you still have to trust bitcoin—and everything about it.

> ***ABOUT:*** *Bruce Schneier is a security technologist who teaches at the Harvard Kennedy School. He is the author, most recently, of* Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*.*

Much has been written about blockchains and how they displace, reshape, or eliminate trust. But when you analyze both blockchain and trust, you quickly realize that there is much more hype than value. Blockchain solutions are often much worse than what they replace.

First, a caveat. By blockchain, I mean something very specific: the data structures and protocols that make up a *public* blockchain. These have three essential elements. The first is a distributed (as in multiple copies) but centralized (as in there's only one) ledger, which is a way of recording what happened and in what order. This ledger is public, meaning that anyone can read it, and immutable, meaning that no one can change what happened in the past.

The second element is the consensus algorithm, which is a way to ensure all the copies of the ledger are the same. This is generally called mining; a critical part of the system is that anyone can participate. It is also distributed, meaning that you don't have to trust any particular node in the consensus network. It can also be extremely expensive, both in data storage and in the energy required to maintain it. Bitcoin has the most expensive consensus algorithm the world has ever seen, by far.

Finally, the third element is the currency. This is some sort of digital token that has value and is publicly traded. Currency is a necessary element of a blockchain to align the incentives of everyone involved. Transactions involving these tokens are stored on the ledger.

**Private blockchains are completely uninteresting. (By this, I mean systems that use the blockchain data structure but don't have the above three elements.) In general, they have some external limitation on who can interact with the blockchain and its features. These are not anything new; they're distributed append-only data structures with a list of individuals authorized to add to it. Consensus protocols have been studied in distributed systems for more than 60 years. Append-only data structures have been similarly well covered. They're blockchains in name only, and—as far as I can tell—the only reason to operate one is to ride on the blockchain hype.**

All three elements of a public blockchain fit together as a single network that offers new security properties. The question is: Is it actually good for anything? It's all a matter of trust.

Trust is essential to society. As a species, humans are wired to trust one another. Society can't function without trust, and the fact that we mostly don't even think about it is a measure of how well trust works.

The word "trust" is loaded with many meanings. There's personal and intimate trust. When we say we trust a friend, we mean that we trust their intentions and know that those intentions will inform their actions. There's also the less intimate, less personal trust—we might not know someone personally, or know their motivations, but we can trust their future actions. Blockchain enables this sort of trust: We don't know any bitcoin miners, for example, but we trust that they will follow the mining protocol and make the whole system work.

Most blockchain enthusiasts have a unnaturally narrow definition of trust. They're fond of catchphrases like "in code we trust," "in math we trust," and "in crypto we trust." This is trust as verification. But verification isn't the same as trust.

In 2012, I wrote a book about trust and security, *Liars and Outliers*. In it, I listed four very general systems our species uses to incentivize trustworthy behavior. The first two are morals and reputation. The problem is that they scale only to a certain population size. Primitive systems were good enough for small communities, but larger communities required delegation, and more formalism.

The third is institutions. Institutions have rules and laws that induce people to behave according to the group norm, imposing sanctions on those who do not. In a sense, laws formalize reputation. Finally, the fourth is security systems. These are the wide varieties of security technologies we employ: door locks and tall fences, alarm systems and guards, forensics and audit systems, and so on.

These four elements work together to enable trust. Take banking, for example. Financial institutions, merchants, and individuals are all concerned with their reputations, which prevents theft and fraud. The laws and regulations surrounding every aspect of banking keep everyone in line, including backstops that limit risks in the case of fraud. And there are lots of security systems in place, from anti-counterfeiting technologies to internet-security technologies.

In his 2018 book, *Blockchain and the New Architecture of Trust*, Kevin Werbach outlines four different "trust architectures." The first is peer-to-peer trust. This basically corresponds to my morals and reputational systems:

pairs of people who come to trust each other. His second is leviathan trust, which corresponds to institutional trust. You can see this working in our system of contracts, which allows parties that don't trust each other to enter into an agreement because they both trust that a government system will help resolve disputes. His third is intermediary trust. A good example is the credit card system, which allows untrusting buyers and sellers to engage in commerce. His fourth trust architecture is distributed trust. This is emergent trust in the particular security system that is blockchain.

What blockchain does is shift some of the trust in people and institutions to trust in technology. You need to trust the cryptography, the protocols, the software, the computers and the network. And you need to trust them absolutely, because they're often single points of failure.

When that trust turns out to be misplaced, there is no recourse. If your bitcoin exchange gets hacked, you lose all of your money. If your bitcoin wallet gets hacked, you lose all of your money. If you forget your login credentials, you lose all of your money. If there's a bug in the code of your smart contract, you lose all of your money. If someone successfully hacks the blockchain security, you lose all of your money. In many ways, trusting technology is harder than trusting people. Would you rather trust a human legal system or the details of some computer code you don't have the expertise to audit?

Blockchain enthusiasts point to more traditional forms of trust—bank processing fees, for example—as expensive. But blockchain trust is also costly; the cost is just hidden. For bitcoin, that's the cost of the additional bitcoin mined, the transaction fees, and the enormous environmental waste.

Blockchain doesn't eliminate the need to trust human institutions. There will always be a big gap that can't be addressed by technology alone. People still need to be in charge, and there is always a need for governance outside the system. This is obvious in the ongoing debate about changing the bitcoin block size, or in fixing the DAO attack against Ethereum. There's always a need to override the rules, and there's always a need for the ability to make permanent rules changes. As long as hard forks are a possibility—that's when the people in charge of a blockchain step outside the system to change it—people will need to be in charge.

Any blockchain system will have to coexist with other, more conventional systems. Modern banking, for example, is designed to be reversible. Bitcoin is not. That makes it hard to make the two compatible, and the result is often an insecurity. Steve Wozniak was scammed out of $70K in bitcoin because he forgot this.

Blockchain technology is often centralized. Bitcoin might theoretically be based on distributed trust, but in practice, that's just not true. Just about everyone using bitcoin has to trust one of the few available wallets and use one of the few available exchanges. People have to trust the software and the operating systems and the computers everything is running on. And we've seen attacks against wallets and exchanges. We've seen Trojans and phishing and password guessing. Criminals have even used flaws in the system that people use to repair their cell phones to steal bitcoin.

Moreover, in any distributed trust system, there are backdoor methods for centralization to creep back in. With bitcoin, there are only a few miners of consequence. There's one company that provides most of the mining hardware. There are only a few dominant exchanges. To the extent that most people interact with bitcoin, it is through these centralized systems. This also allows for attacks against blockchain-based systems.

These issues are not bugs in current blockchain applications, they're inherent in how blockchain works. Any evaluation of the security of the system has to take the whole socio-technical system into account. Too many blockchain enthusiasts focus on the technology and ignore the rest.

To the extent that people don't use bitcoin, it's because they don't trust bitcoin. That has nothing to do with the cryptography or the protocols. In fact, a system where you can lose your life savings if you forget your key or download a piece of malware is not particularly trustworthy. No amount of explaining how SHA-256 works to prevent double-spending will fix that.

Similarly, to the extent that people do use blockchains, it is because they trust them. People either own bitcoin or not based on reputation; that's true even for speculators who own bitcoin simply because they think it will make them rich quickly. People choose a wallet for their cryptocurrency, and an exchange for their transactions, based on reputation. We even evaluate and trust the cryptography that underpins blockchains based on the algorithms' reputation.

To see how this can fail, look at the various supply-chain security systems that are using blockchain. A blockchain isn't a necessary feature of any of them. The reasons they're successful is that everyone has a single software platform to enter their data in. Even though the blockchain systems are built on distributed trust, people don't necessarily accept that. For example, some companies don't trust the IBM/Maersk system because it's not *their* blockchain.

Irrational? Maybe, but that's how trust works. It can't be replaced by algorithms and protocols. It's much more social than that.

Still, the idea that blockchains can somehow eliminate the need for trust persists. Recently, I received an email from a company that implemented secure messaging using blockchain. It said, in part: "Using the blockchain, as we have done, has eliminated the need for Trust." This sentiment suggests the writer misunderstands both what blockchain does and how trust works.

**Do you need a public blockchain? The answer is almost certainly no. A blockchain probably doesn't solve the security problems you think it solves. The security problems it solves are probably not the ones you have. (Manipulating audit data is probably not your major security risk.) A false trust in blockchain can itself be a security risk. The inefficiencies, especially in scaling, are probably not worth it. I have looked at many blockchain applications, and all of them could achieve the same security properties without using a blockchain—of course, then they wouldn't have the cool name.**

Honestly, cryptocurrencies are useless. They're only used by speculators looking for quick riches, people who don't like government-backed currencies, and criminals who want a black-market way to exchange money.

To answer the question of whether the blockchain is needed, ask yourself: Does the blockchain change the system of trust in any meaningful way, or just shift it around? Does it just try to replace trust with verification? Does it strengthen existing trust relationships, or try to go against them? How can trust be abused in the new system, and is this better or worse than the potential abuses in the old system? And lastly: What would your system look like if you didn't use blockchain at all?

If you ask yourself those questions, it's likely you'll choose solutions that don't use public blockchain. And that'll be a good thing—especially when the hype dissipates.