2017 15th Annual Conference on Privacy, Security and Trust

Alice in Blockchains: Surprising Security Pitfalls in PoW and PoS Blockchain Systems

Dr. Thomas P. Keenan, FCIPS, I.S.P., ITCP
Professor, Faculty of Environmental Design
Adjunct Professor, Department of Computer Science
University of Calgary
Calgary, Alberta, Canada
keenan@ucalgary.ca
(Revised Sept. 20, 2017)

Abstract—**If, as most experts agree, the mathematical basis of major blockchain systems is (probably if not provably) sound, why do they have a bad reputation? Human misbehavior (such as failed Bitcoin exchanges) accounts for some of the issues, but there are also deeper and more interesting vulnerabilities here. These include design faults and code-level implementation defects, ecosystem issues (such as wallets), as well as approaches such as the "51% attack" all of which can compromise the integrity of blockchain systems. With particular attention to the emerging non-financial applications of blockchain technology, this paper demonstrates the kinds of attacks that are possible and provides suggestions for minimizing the risks involved.**

Keywords—blockchain, PoW, PoS, vulnerabilities, hacking, software defects, security, governance, cryptography

I. SCOPE OF THIS RESEARCH

There are currently two major implementation philosophies for blockchain systems: Proof of Work (PoW, used by Bitcoin) and Proof of Stake (PoS, used by PeerCoin and Nxt). PoW relies on a network of miners who solve increasingly difficult mathematical problems, and in the process, maintain the integrity of the blockchain. A PoS system, which is less common, assigns the right to "forge" (in the sense of a blacksmith) the next block based on the ownership of the items. So, if there are 1000 units and I own 500 of them, there is a 50% chance I will be chosen, in a pseudo-random fashion, to forge the next block.

Alice and Bob, our classic crypto-communicators, are probably on pretty solid ground moving their assets around via major blockchain systems like Bitcoin and Ether and maybe even Peercoin and Nxt. The total value of all Bitcoins in existence is currently over $18B U.S. dollars, so if there were fundamental mathematical flaws that allowed double spending or theft, we surely would have heard about them.

It is important to understand that the blockchain is a general technology that can be used to keep track of anything of interest. Besides money, blockchain technology has been used for everything from tracking counterfeit blue jeans to validating land titles to securing the integrity of medical records. Walmart is testing it to expedite removing recalled products from the shelves. Instead of being a technology that simply encodes monetary value, the blockchain is really a platform for representing and systematizing trust. This is important because some of the mis-conceptions around blockchain security derive from thinking of it as "only Bitcoin" or "only money" when it's so much more.

II. ATTACKING PROOF OF WORK AND PROOF OF STATE SYSTEMS

A. Why the blockchain has a shady reputation

If the underlying structure of the major blockchain systems is sound, why are there so many scandals? Bad code and bad people. Bitcoin exchanges like Tokyo-based Mt. Gox and Hong Kong's Mycoin failed spectacularly. The largest, and most instructive what-not-to-do lessons come from Mt. Gox, which lost almost half a billion dollars in cryptocurrency value in 2011 and went out of business. Reports say that the firm's internal software was a disaster, with no version control mechanism. According to one account, "any coder could accidentally overwrite a colleague's code if they happened to be working on the same file." [1] The concept of development sandboxes seems to have eluded this company. They tested patches on their live production system, which was handling people's real money.

Also on the "people are your biggest problem" front, the 2014 attack on UK-charted cryptocurrency trading company Bitstamp that resulted in the theft of almost 19,000 Bitcoins, involved extended and ultimately successful phishing attacks via Skype directed at company officials, as well as a server compromise. Classic hacking techniques can certainly be directed against blockchain systems.

One vulnerability that could only have happened in the blockchain world is the collapse of the Decentralized Autonomous Organization (DAO), a kind of virtual venture capital fund. The DAO was instantiated on Ethereum, a very popular distributed application platform. For a while, $60M worth of Ether cryptocurrency was being held hostage by someone who exploited a flaw in the underlying open-source code. Since participating investors agreed in advance that "the heck with courts, the code is the law" this posed an awkward problem. A controversial "hard fork" recovered most of that value, but also did significant philosophical and reputational damage to Ethereum. It is important to note that the source code for the DAO was always publicly accessible on Github, so one moral of this story is to read the defining code for smart contracts very, very carefully.

In July 2017, "an unknown attacker exploited a critical flaw in the Parity multi-signature wallet on the Ethereum network"

978-1-5386-2487-6/17/$31.00 ©2017 IEEE
DOI 10.1109/PST.2017.00057

[2] thereby stealing $31M US of the cryptocurrency. In response, “a group of benevolent white-hat hackers from the Ethereum community rapidly organized” [2], and drained the remaining $150M US that was at risk, on behalf of the rightful owners. It was like the good guys robbing the bank to prevent a bank robbery!

The fault here was not with Ethereum or the Parity multi-signature wallet system, but rather “a vulnerability in the default smart contract code that the Parity client gives the user for deploying multi-signature wallets.” [2]

The take-away from all these debacles is that the ecosystem surrounding a blockchain project is important, as is the knowledge and ethical standards of the people in charge of it.

B. *Types of attacks on blockchain systems*

Consider the much-touted Hyperledger system, which is open-governed but has backing from companies including IBM. Digging down into the code and instructions, which is posted at [3] discloses potential landmines for blockchain developers, especially those trying to create “self-executing contracts” by writing code in the Go language.

As just one example, while debugging codechain code, it is common to “implement mapping of the fabric-couchdb container port to a host port” which “allows the visualization of the database via the CouchDB web interface (Fauxton).” [3] Yet, as noted in the same document, leaving this mapping in place in a production environment could allow “outside access to the CouchDB containers” thereby compromising privacy and possibly even security.

Even if all code is properly brought up to production standards, and no mathematical flaws are found, there are significant security issues surrounding blockchain. For example, there’s the so-called “51% attack”.

In a PoW system, the integrity of the blockchain is maintained by a cadre of “miners” who are compensated with small amounts of value in return for doing increasingly difficult mathematical calculations. If a single entity, or a group of colluding ones, controlled more than 51% of the total processing power, they could hijack the blockchain and arbitrarily validate transactions of their choosing by adding them to the blockchain.

In the early days of “mom and pop miners,” such collusion was unlikely. However, a report in the *New York Times* showed that in April 2016, “over 70 percent of the transactions on the Bitcoin network were going through just four Chinese companies, known as Bitcoin mining pools.” [4] So the 51% attack is more than hypothetical, even for a well-established cryptocurrency like Bitcoin. Imagine how much more vulnerable a company would be if, for some reason, it tried to build and maintain its own private PoW blockchain.

III. MITIGATING RISK THROUGH RELIANCE ON EXTERNAL BLOCKCHAIN RESOURCES

One lesson for companies is that attempting to build and maintain their own private blockchain infrastructure may be perilous. Aside from the risks of getting something wrong, an adversary with sufficient computing resources could overwhelm you. Suppose, and this is not totally hypothetical, your company makes designer jeans in China for $20 and sells them in the U.S.A. for $200. You cleverly decide to put all the valid garments on a PoW blockchain, so there is a publicly verifiable, immutable way to tell real from counterfeit garments. Your competitor, who also has access to that factory, wants to sell these jeans for $50 and simply gets enough computing power to swamp your little blockchain and add his bogus products to it.

This is why companies like Berlin-based ascribe GmbH, (which tracks the authenticity of limited edition artworks), are piggy-backing on the Bitcoin blockchain, inscribing their ownership claims on that network. This is good idea since it leverages all the energy of the Bitcoin miners to maintain integrity through the PoW paradigm.

Suppose ascribe GmbH had instead used a PoS blockchain, which does have some advantages. Some people argue that the 51% attack makes little sense in a PoS environment because someone who has a large stake, and is therefore more likely to be chosen to forge a block, would be diminishing his own value disproportionately by corrupting the blockchain.

That is actually the result of limited thinking, i.e. assuming that the items on the blockchain are simply monetary units. Since the blockchain can be used for anything, there may indeed be an incentive to do a 51% attack on a PoS blockchain.

If there were 100 legitimate copies of an art print, and I owned 51 of them, I would be probably be diminishing the value of my holdings if I hijacked the blockchain and put on another 100 counterfeit ones. However, it is not clear that the reduction in value would be proportional, as it would be in the monetary case. If those 100 artworks were worth $100 each, and I own 51, I start with $5,100 in value. Hijacking the PoS blockchain and putting another 100 on the market might lower their value, but not by half. Say they were worth $80 now, and I now own 151 (my original 51 plus the 100 counterfeit copies). That’s 151*$80 or $12,080, a tidy profit.

IV. EMERGING VULNERABILITIES IN THE APPLICATION OF THE BLOCKCHAIN

There are numerous impediments to the adoption of blockchain approaches in general and cryptocurrencies in particular.

These include:

- wallet and other ecosystem issues
- dark pool vs. transparency
- the problem of retrieving lost credentials
- the human factor in all its glorious manifestations (pride, greed, envy, gluttony, wrath, sloth and yes, even lust can be found in various blockchain tales)
- the (illusion of) privacy and anonymity

Issues surrounding privacy and anonymity were explored in greater depth in a presentation given by the author at the RSA Asia Pacific Japan conference on July 20-22, 2017 [5]

That presentation notes that there are circumstances where the owner of a wallet deliberately discloses his or her personal or corporate identity, together with an address that allows people to pay into it. An example would be a charity or political group that is seeking funds and needs to tell supporters where to pay them. Of course, the dark side of this is Ransomware. Victims of this crime are often given a Bitcoin address to submit their payment, which supposedly will trigger the release of their files.

There are also circumstances where the identity of the wallet owner can be inferred from collateral information, for example if it is mentioned in a signed blog posting. In addition, while knowing your public address will not allow someone to steal your funds, as was noted in a Reddit post, "If an attacker knows your address, s/he can see the addresses paying you and those you pay… An attacker might be able to use that information against you by lying to you, or pretending s/he's one of those people, for example." [6] This poster also notes that by monitoring your transactions an attacker might deduce valuable business information.

At a computer security summer school for graduate students in Europe, we conducted experiments on recorded Tor network traffic to see if some information could be deduced from transaction graph analysis. While we did not publish the results, we had some success where the volume of traffic between two sites was high enough. Similar approaches can be applied to weaken the anonymity of blockchain transactions. For example, if a transaction splits into two outputs, one of 2.00000000BTC and one of .68255982 BTC an observer might deduce that the first is a purchase and the second is the "change" and make use of that information.

V. SPECIAL CONSIDERATIONS RELATING TO NON-FINANCIAL INFORMATION

In a way, it's wonderful that the first widespread blockchain applications have been financial ones. People pay very careful attention to their money, and, with the exception of fiascos like Mt. Gox and the DAO, blockchain concepts have stood up well and proven their value and reliability in this arena.

As we start applying blockchain technology for everything from medical records to land titles to our very identities, new issues will arise. Timeliness is certainly one, since there are complaints about processing delays in cryptocurrency systems. In a life or death situation like an emergency room, users cannot wait around for miners to validate the next block in a chain.

Privacy will take on an even greater importance, as evidenced by the September 2017 Equifax breach, which saw the personal (and largely unchangeable) data of 140M Americans stolen by hackers. As we trust the blockchain with "things more important than money" there will be thorny social and legal issues. As just one example, it's currently pretty clear who to sue in a major corporate privacy breach. In the multi-party world of the blockchain, lawyers might be hard pressed to decide where in the world to file a suit, and who should be the defendant. Rules of evidence will also need rethinking since "going to the bank with a warrant" won't work anymore.

The blockchain may also thwart governments seeking citizen's information. The "it's just not available" argument used by Apple in the San Bernardino case may apply widely.

VI. MOVING TOWARDS BEST PRACTICES IN BLOCKCHAIN APPLICATIONS

Numerous public and private entities are at work developing guidelines for the adoption of blockchain technology for both financial and non-financial applications. A reasonable place to start is the document published in January 2017 by the European Union Agency for Network and Information Security. [7]

This report makes concrete recommendations in 13 areas:

- Key management
- Cryptography
- Privacy
- Code review
- Consensus Hijack
- Sidechains
- Permissioned chain management
- Denial of service
- Wallet management
- Scalability
- Governance controls
- Smart contracts
- Interoperability

While all these are sensible and well thought out, it is clear that they would only have minimized the risk and damage of some of the cryptocurrency catastrophes that we have already seen, and might not really apply directly to non-financial applications. As we move to using blockchain technology for life-critical applications as well as for protecting sensitive information such as health data, we will need to develop even better practices as well as auditing procedures.

Above all, since the human factor has often been the source of problems, we will need to give substantial attention to how people interact with blockchain technology. The opportunities of blockchain-based applications to change our lives for the better are amazing, but so are the risks.

REFERENCES

[1] McMillan, R., The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster", accessed Aug 6, 2017 at https://www.wired.com/2014/03/bitcoin-exchange/

[2] Quereshi, H. "A hacker stole $31M of Ether—how it happened, and what it means for Ethereum," Freecodecamp.org, Jul 20, 2017, accessed Aug 6, 2017 at https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce

[3] Hyperledge/fabric, "Getting Started", accessed Aug 6, 2017 at github.com/hyperledger/fabric/blob/master/docs/source/getting_started.rst

[4] Popper, N., How China Took Center Stage in Bitcoin's Civil War, New York Times, Jun 29, 2016, accessed Aug 6, 2017 at https://www.nytimes.com/2016/07/03/business/dealbook/bitcoin-china.html

[5] Keenan, T.P., "Security Implications of Using Blockchain Technology for More than Money", RSA Asia Pacific Japan Conference, accessed Aug 6, 2017 at https://www.rsaconference.com/writable/presentations/file_upload/fle1-f01_security-implications-of-using-blockchain-technology-for-more-than-money.pdf

[6] "Bob Alison" on www.Reddit/com retrieved Sept 20, 2017 at https://www.reddit.com/r/Bitcoin/comments/2fc82s/is_publically_posting_your_wallet_address_safe/

[7] ENISA, "Distributed Ledger Technology & Cybersecurity - Improving information security in the financial sector", accessed Aug 6, 2017 at https://www.enisa.europa.eu/publications/blockchain-security