Using Digital Signatures to Improve Election Integrity

(Technical Paper)

Nostr, Bitcoin and the Co-Production of Technology and Policy

(STS Paper)

A Thesis Project Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science

University of Virginia, Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree

Bachelor of Science, School of Engineering

Ethan Steere

Fall, 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignment

Signature Ethan Steere Date 12/13/2023

Ethan Steere

Approved ____ Date __________

Brianna Morrison, Department of Computer Science

Approved ____ Date __________

Travis Elliot, Department of Engineering and Society

Introduction

My STS paper examines Nostr and Bitcoin through the lens of Co-Production of Technology and Policy. Each technology was created out of frustration with the status quo. For Bitcoin it was bank bailouts after the 2008 financial crisis and for Nostr it was the aggressive social media censorship during Covid. Each system intelligently leverages computer networks and cryptography to construct an unstoppable network. In cadence with the "*Trust Systems, Not People*" ethos of Bitcoin and Nostr, my technical project hopes to create provably secure elections.

Technical Topic: Using Digital Signatures to Improve Election Integrity (CS 4991)

Elections were once scarce, but are now a part of governance for most nations. This presents challenges as the voting population has grown. We must manage elections on the scale of hundreds of millions or billions of votes in the span of a few days. Paper ballot methods introduce human error and proprietary electronic voting systems are laughably insecure (Halderman, 2022). I propose a system of broadcasting signed votes called "Election Security Standard" that ensures perfect auditability.

First, each voter will need to generate a Schnorr key pair. The public key will be used to verify signatures and the private key will be used to create them. The public key is called public because it must be public for anyone to be able to verify the signature. The private key is called private because it can be used to create trusted, signed data. Only the key generator should have this ability! Instead of filling out a paper ballot, voters will go to the voting office to give their public key which is then added to the public ESS database. With this public key, anyone will be able to validate the signature you create for your ballot with the private key. Each voter can check that the correct key is added before leaving the voting office. At home, voters will make their choice and use their private key to sign the digital ballot. After uploading to the ESS website, the digital ballot and signature will be automatically associated with your row in the database. Any government adhering to this system would not be able to change any of the votes without being immediately busted with incontrovertible evidence.

To finish this project, I will need to finalize the ballot payload specification and choose a signature algorithm. Next, I will implement a stable version of the software that could be run out of the box by any interested government. Finally, I will need to do load testing to estimate the cost of running this system for comparison with paper ballots.

STS Topic: Bitcoin and Nostr: Can Software Change Policy?

Introduction

Early January 2009, a sequence of 2000 ones and zeros was sent out of an unknown computer with an encoded message: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." This was the genesis block of Bitcoin. Bitcoin is revolutionizing finance, but more importantly demonstrates the outsized impact software can have on social and political issues. The influence is clear in projects like Nostr, which hopes to secure freedom of speech through a decentralized social media protocol. I firmly believe both of these projects will not just improve the security of human freedom, but also set a new standard against all recorded history.

Co-Production of Science and Social Order

In STS literature, the co-production of science and social order emphasizes the effect that politics can have on technological development and vice versa. This theory posits that scientific research and its application are shaped by social and political factors, and in turn, these factors are also influenced by scientific knowledge (Sendell, 2011, p152). Bitcoin was clearly influenced by bank bailouts of the 2008 crisis given the contents of the genesis block. Nostr was similarly created to address the censorship of alternative narratives during the Covid-19 Era (Castillo, 2023). The distributed nature of Bitcoin and Nostr make them impervious to shutdown, effectively overriding any laws pertaining to speech and monetary policy.

Digital Signatures

Digital Signature Cryptography is ubiquitous in all computer systems and is the centerpiece of both Bitcoin and Nostr. A digital signature is a piece of data that allows a receiver of a message to be sure that a message came from a known sender. A sender will generate two keys, which are just really large numbers. Then, the sender will make one key public. When the sender wants to send a message they will take the private key and perform the signing operation on the message data to produce a signature. The receiver can check that the signature, message, and public key satisfy a mathematical invariant specified by the chosen signature scheme. A robust digital signature scheme will ensure that a signature is impossible to create for a public key without the private key and that any signature validation will fail if the message is altered.

Digital signatures are the lynchpin of decentralized systems because they are a robust and permissionless source of identity and message authenticity. There is no need to contact any central authority, server, or database to create a key pair and sign messages. You could, in theory, do key generation and signing on paper although that’s not feasible in practice. Nostr uses digital signatures to ensure authenticity for all messages. Bitcoin uses digital signatures to allow users to guard access to their coins.

Bitcoin

It is understandably difficult to conceptualize how Bitcoin works when it's described as a "digital currency." Bitcoin is a list of transactions between accounts from which account supply and total currency supply are inferred. Bitcoin holders digitally sign transactions and broadcast them to their peers. These proposed transactions are added in blocks of one or more transactions. A block can only be added to the Blockchain if its digest meets certain requirements. The process of shuffling Block contents to achieve the required digest and reward is called mining. Mining was designed to be difficult so that individual bad actors could not create blocks more quickly than the rest of the honest miners. Furthermore, a bad actor would need to forge the digital signature of the account under attack, which is an implausible task. Overpowering the current hashrate would require a herculean effort of clandestine semiconductor fabrication

Traditional government currencies operate in a much different manner. The validity of the government currency transaction ledger is determined by the government's Central Bank. Central banks abuse this authority by adding transactions without a proper source of funds. This increases the supply of currency and devalues existing currency over time. In the United States about one third of the federal budget is derived from printed Dollars (US Treasury, 2023). This is undeniably a problem for citizens around the world, but many of those with the ability to enact change are dependent on the system and therefore have little incentive to push reform.

Bitcoin, created out of frustration with this Monetary Policy, now seems to be the only way to change monetary policy. Bitcoin is innate, without opinions or any care for anything said by anyone. No matter how powerful you are on Earth, you can't continuously mine Bitcoin blocks faster than the global community of miners. Bad policy created Bitcoin and now Bitcoin is the only option for remediating said policy. There is clear Co-Production of Technology and Social Order when analyzing Bitcoin and Monetary Policy.

Nostr

Nostr, short for "*Notes and Other Stuff Through Relays*," provides a standardized format for distributing internet content. At a traditional social media company, one's account is a row in a database and the platform ensures only your posts are displayed under your name. The platform can then censor content, misattribute content, or delete your account and following altogether. Nostr opts to use digital signatures as a source of identity and has the solely providing hosting bandwidth. With Nostr, you can easily port all of your content between Relays without losing any of your following. Consumers of content follow their creators public key, not their account at that Relay. Through the use of cryptography as a mechanism for identity, a content creator could only be cut off from his following by completing the impossible task of shutting down all Nostr relays.

Nostr is a nascent technology, but still has already gained traction. So far, there have been more than 100 Million events from over 300,000 public key pairs (Nostr Band, 2023). It's unknown how many people browse Nostr activity without posting.

As Nostr rises, the influence that the law has on the content citizens produce and consume will wane. A good case study for government intervention in content creation was the New York Post article about Hunter Biden's Laptop. After this story went live on all New York Post social media accounts, the FBI sent agents to popular social media companies like Meta, Twitter, and Google stating that this was disinformation spread by Russia (Oliver, 2023). As a result, Facebook, Instagram, Twitter, and Youtube all prevented the story from being shared, discrediting the reporting. Many Americans were not aware of the story as a result. Any attempt of suppression tactics would fall flat on Nostr, as the New York Post could have used a different relay outside of U.S. influence.

Conclusion

Both Bitcoin and Nostr are incredibly clever technologies that leverage computer networking and cryptography to build systems of hitherto impossible robustness. Both were a result of frustration with government policy. Bitcoin was born out of frustration with the crony bank bailouts in 2008 and Nostr was born out of aggressive social media censorship in the Covid Era. Each protocol now stands as the best chance of changing the bad policy that motivated their creation. The new science of distributed protocols is shifting political power dynamics around the world. The clear political motivations and consequential for the creation of these networks demonstrate the Co-Production of Scientific Knowledge and Political Power.

References

1. Castillo, Michael del. “Meet @Fiatjaf, the Mysterious Nostr Creator Who Has Lured 18 Million Users and $5 Million from Jack Dorsey.” *Forbes*, 30 May 2023, www.forbes.com/sites/digital-assets/2023/05/30/bitcoin-social-network-nostr-creator-fiatjaf-/?sh=d2981ab11c0d. Accessed 7 Oct. 2023.
2. Halderman, J. Alex, and Drew Singall. *Security Analysis of Georgia’s ImageCast X Ballot Marking Devices*. 1 July 2021.
3. “Nostr Stats.” *Stats.nostr.band*, stats.nostr.band/. Accessed 7 Oct. 2023.
4. Oliver, Ashley. “FBI “Engaged in Deception” with Hunter Biden Laptop, Missouri v. Biden Attorney Says.” *Washington Examiner*, 10 Aug. 2023, www.washingtonexaminer.com/news/justice/fbi-engaged-in-deception-hunter-biden-laptop. Accessed 7 Oct. 2023.
5. Swedlow, B. (2011). Cultural coproduction of four states of knowledge. *Science, Technology, &amp; Human Values*, *37*(3), 151–179. https://doi.org/10.1177/0162243911405345
6. “Your Guide to America’s Finances.” *Fiscaldata.treasury.gov*, 2023, fiscaldata.treasury.gov/americas-finance-guide/.