Locked Doors and Open Windows: How Blockchain Can Protect Public Safety And Why Existing Security Measures are Relics.

by Build3 Foundation authors Kenneth Shultz, PE and Phillip Outland-Brock

What was once a form of security, the rite of sealing a professional's design, now serves only as a symbolic tradition. The 'stamp' signifying a professional's supervision and approval of a given engineered design has become obsolete when securing public safety. The loss of the security that stamps once offered creates an authorship dilemma. This dilemma introduces an existential threat to the mission of the NSPE, which is to create

*"...a world where the public can be confident that engineering decisions **affecting their lives** are made by **qualified and ethically accountable professionals**."* (National Society of Professional Engineers, 2015)

It's a dramatic statement. Stamps are sacred, or feel so to most people seeking licensure. Using that stamp to seal your first set of plans is a heavy feeling. It represents a huge leap of responsibility and potential consequences. The risks associated with applying your seal to anything have only increased over time, outpacing the level of protection that the existing regulations provide.

Existing Security Measures

The baseline security measure known to all engineers is licensure, first established in Wyoming in 1907 and eventually adopted by all 50 states over the next 40 years. (Luna, 2020)

The eligibility to sit for the licensure examination generally requires twelve years of combined education and work experience.

While regulated by the various state boards, a single two-inch circle acts as the publicly recognized signifier that a licensed engineer has supervised and released a design or specification. While the barrier to entry to becoming a licensed engineer is effectively high, the barrier to the illicit use of professional credentials is virtually nonexistent. This nonexistent barrier against unlawful credential use is due to the nature of our predominantly digital economy.

Offices all over the world throughout the supply chain handle documents generally trusted as the true copy of a qualified professional's design. We build cities from engineered designs trusting that no record was corrupted from the author's original along the entire supply chain of decisions.

We can't prove who authored the engineered documents, yet we use them to build trillions of dollars of infrastructure.

An Engineering Stamp Anyone Can Steal

To understand how low the barrier of entry is to the illicit use of professional credentials, you could follow these instructions:

1. Visit https://www.dpor.virginia.gov/LicenseLookup
2. Enter the author's name, "Kenneth Shultz," and note the license number.
3. Visit PEStamps.com and purchase a stamp with a name and license number for $10.

Caution: the above is an example only. Do not actually perform those steps, as they are illegal. The steps are shown for demonstration purposes only.

Some states require digital signatures, which slightly increase the level of security; however, none of the existing methods provide a surefire level of protection.

The 2016 paper published by NSPE, "Blockchain Technology: Implications and Opportunities for Professionals Engineers," states that "today, the institution of professional engineering is struggling for an interface with the digital world." (National Society of Professional Engineers et al. 5)

There are still engineering boards - whose **primary responsibility** is to **ensure technical competence** in engineering - that require physical applications mailed with paper checks. Have you had to dig out your checkbook for a $75 transaction lately? If so, we're willing to guess it wasn't at a place you associate with engineering.

How can we design a system that will, given those conditions, exhibit transparency to those willing to turn an ethically questionable blind eye? How can we prove if the seal hasn't been taken and used by someone else fraudulently? How do we ensure the practitioner's competence in making a judgment in a given field?

How is it handled now? Long story short: it's not, but losing control of your seal is still considered a criminal offense. Examine the chapters below from the state of Texas engineering regulations.

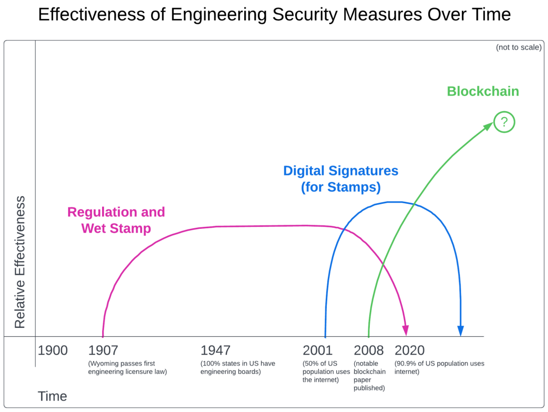
Chapter 137.33(d) makes it the engineer's responsibility to

"...secure their physical or electronic seals and signatures" (Texas Board of Professional Engineers and Land Surveyors, 2020, 70)

Chapter 137.37(a)(4) defines sealing misconduct **as subject to disciplinary action** if the regulant

"...allows others access to his or her electronic files containing his or her seal and/or electronic signature". (Texas Board of Professional Engineers and Land Surveyors, 2020, 71)

While it is eventually possible to catch an illicit use of your credentials, it is likely to be exposed by the damage it causes financially and to life safety. In that case, what recourse do you have when the damage has already been done? The burden of proof is on you.



Internet Usage Statistics from (Roser et al., 2015)

A Proposed Solution

So how does this all relate to blockchain technology? Blockchain technology can prove the authorship of digital documents offering a form of digital DNA. This mechanism is helpful and ***essential in due process for the industry.***

An excellent summary of the technology from Harvard Business Review states:

"With blockchain, we can imagine a world in which contracts are embedded in digital code and stored in transparent, shared databases, where they are protected from deletion, tampering, and revision. In this world, every agreement, every process, every task, and every payment would have a digital record and signature that could be identified, validated, stored, and shared…." (Harvard Business Review, 2017)

We must dismiss the two most well-known uses of blockchain. This article is not endorsing the use of blockchain as a cryptocurrency or an NFT.

Simply put, blockchain pairs a public key with a private key. Much like your email address, your public key is a unique identifier but is accessible to anyone with internet access. Consider your license number the public key.

However, unlike your email address, no private key or password is required to use your license number. This lack of a private key represents the fundamental security flaw in the system. It would be like anyone being able to send an email from your address without your knowledge or approval.

Blockchain allows for every single deliverable and document to be signed with a private key that only you can access. This private key creates a signature that can be verified by anyone using your public key (license number). These signatures are stored on a chain of transactions (a blockchain), creating a reliable chain of custody for every document.

For every transaction that occurs in the document's life, a hash is created that refers back to the last transaction and every transaction before that, creating a chain that verifies and reports itself along the way and ensuring that the author of each document is always verifiable. Any changes to the original document created by the engineer of record would break that chain, sounding alarm bells that the document has been altered.

Using blockchain to create a password for each license, we can resolve the authorship dilemma with little disruption to the industry or existing standards and practices. We have an opportunity to demonstrate a practical use-case of this technology and solve the authorship dilemma that has become a threat to the mission of the NSPE in the digital age.

To learn how to contribute to the open-source library or research with the Build3 community, visit https://www.build3.foundation.

References

Harvard Business review. (2017, January 01). *The Truth About Blockchain* [Print, Web]. Harvard Business Review. Retrieved December 06, 2022, from https://hbr.org/2017/01/the-truth-about-blockchain

Luna, M. (2020, February). *Catalysts for Regulation and Licensure in Engineering in the United States - American Society of Civil Engineers - Texas Section*. ASCE Texas Section. Retrieved December 6, 2022, from https://www.texasce.org/tce-news/catalysts-for-regulation-and-licensure/

National Society of Professional Engineers. (2015). *NSPE: Who We Are and What We Do | National Society of Professional Engineers*. National Society of Professional Engineers |. Retrieved December 6, 2022, from https://www.nspe.org/membership/nspe-who-we-are-and-what-we-do

National Society of Professional Engineers, Robles, PE, Chairman, D. R., Layton, Ph.D., PE, B., Beatty, PE, K., Begg, PE, W., Conway, PE, J., D'Amico, PE, F.NSPE, D., Davy, PE, F.NSPE, M., Ensz, PE, R., Evangelisti, PE, J., Hogan, PE, B., Maheady, PE, F.NSPE, T., Uddin, PE, R., & Williams, PE, C. (2016). *BlockchainTechnology: Implications and Opportunities for Professional Engineers* [A whitepaper of the 2015-2016 National Society of Professional Engineers' Financial Technologies Task Force].

Roser, M., Ritchie, H., & Ortiz, E. (2015). *Internet*. Our World in Data. Retrieved December 6, 2022, from https://ourworldindata.org/internet

Texas Board of Professional engineers and Land Surveyors. (2020, September 30). *Texas Engineering And Land Surveying Practice Acts and Rules Concerning Practice and Licensure*.