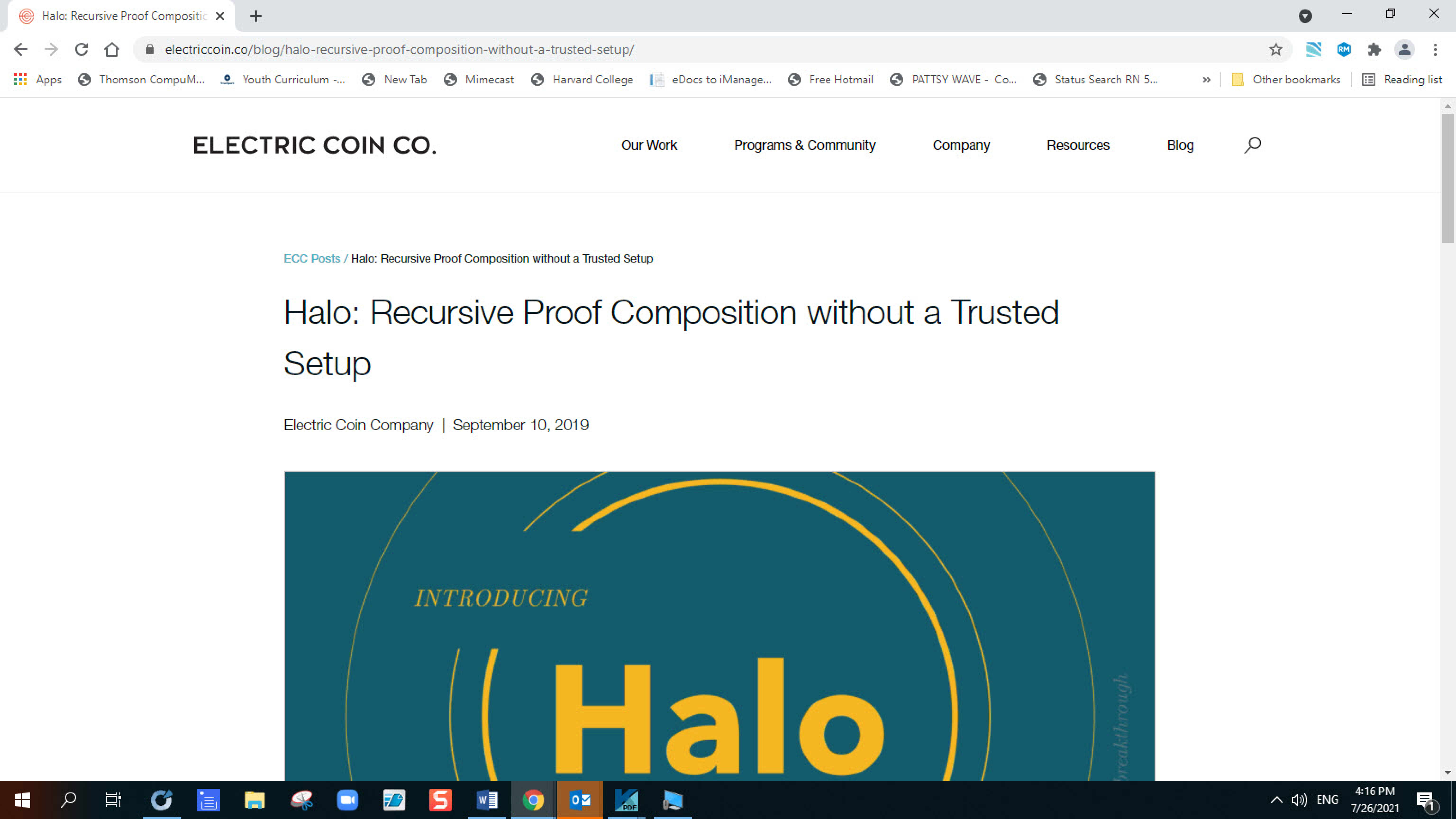
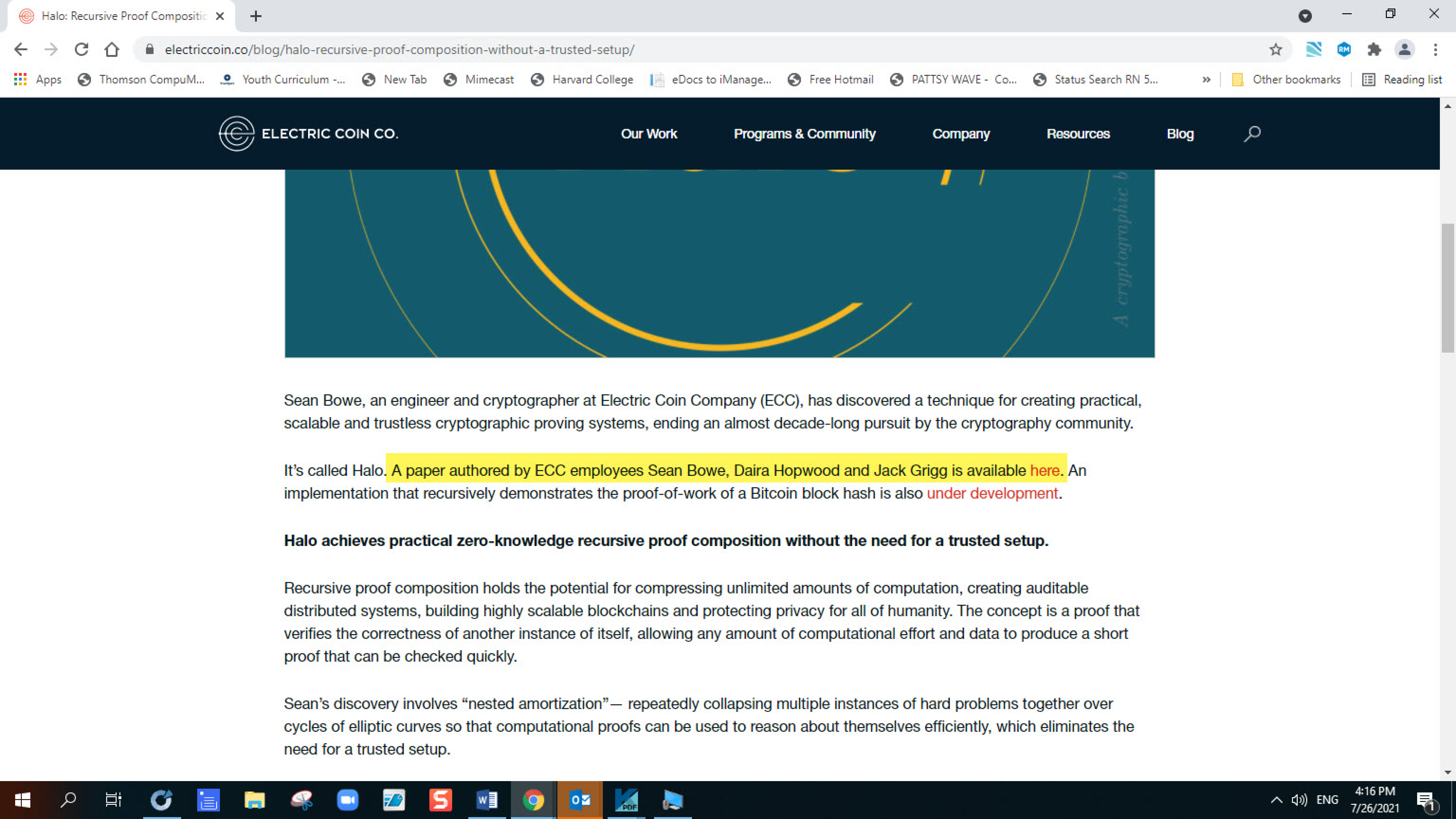


ECC Posts / Halo: Recursive Proof Composition without a Trusted Setup

Halo: Recursive Proof Composition without a Trusted Setup

Electric Coin Company | September 10, 2019



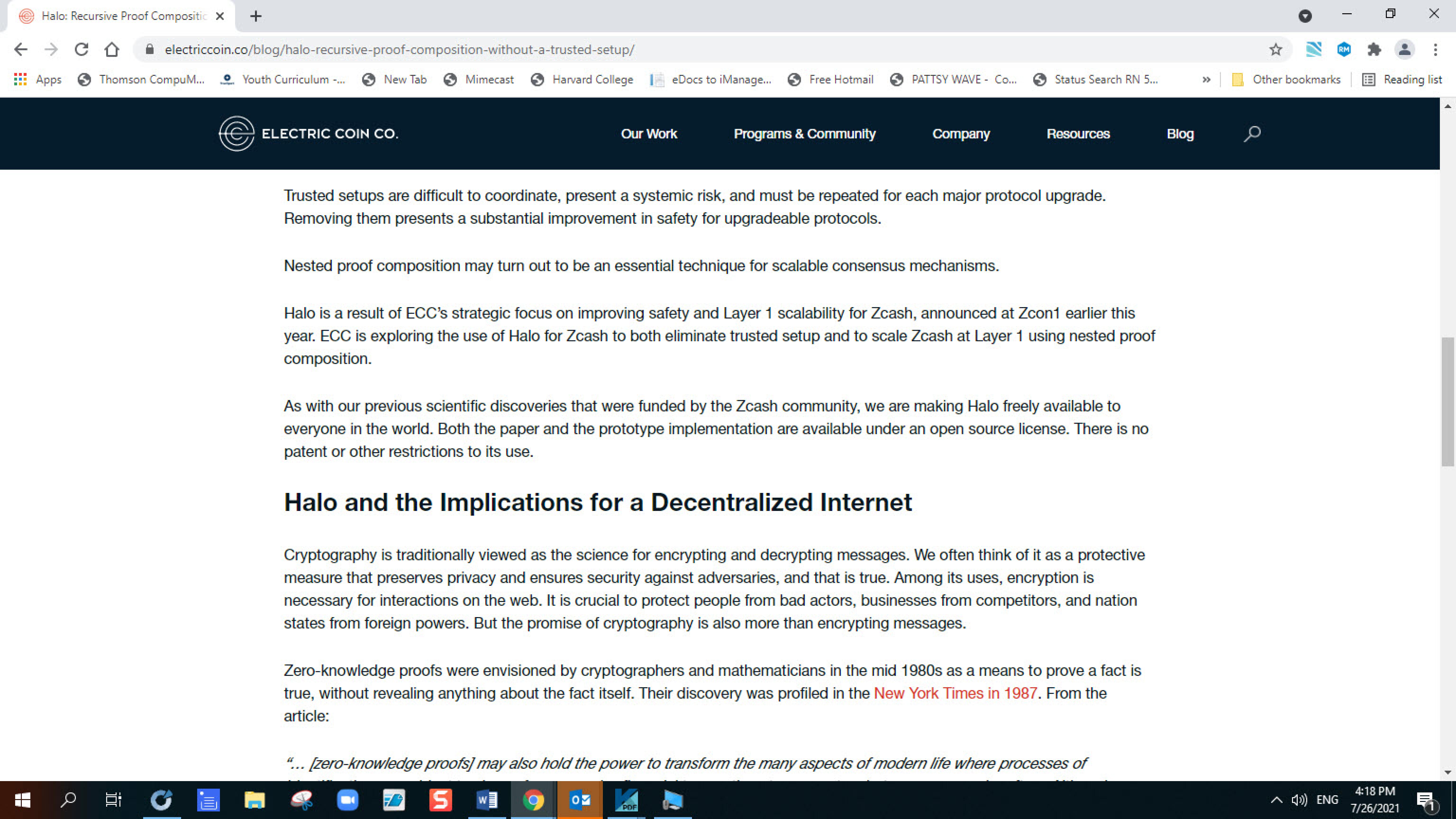
Sean Bowe, an engineer and cryptographer at Electric Coin Company (ECC), has discovered a technique for creating practical, scalable and trustless cryptographic proving systems, ending an almost decade-long pursuit by the cryptography community.

It's called Halo. A paper authored by ECC employees Sean Bowe, Daira Hopwood and Jack Grigg is available here. An implementation that recursively demonstrates the proof-of-work of a Bitcoin block hash is also under development.

Halo achieves practical zero-knowledge recursive proof composition without the need for a trusted setup.

Recursive proof composition holds the potential for compressing unlimited amounts of computation, creating auditable distributed systems, building highly scalable blockchains and protecting privacy for all of humanity. The concept is a proof that verifies the correctness of another instance of itself, allowing any amount of computational effort and data to produce a short proof that can be checked quickly.

Sean's discovery involves "nested amortization"— repeatedly collapsing multiple instances of hard problems together over cycles of elliptic curves so that computational proofs can be used to reason about themselves efficiently, which eliminates the need for a trusted setup.



Trusted setups are difficult to coordinate, present a systemic risk, and must be repeated for each major protocol upgrade. Removing them presents a substantial improvement in safety for upgradeable protocols.

Nested proof composition may turn out to be an essential technique for scalable consensus mechanisms.

Halo is a result of ECC's strategic focus on improving safety and Layer 1 scalability for Zcash, announced at Zcon1 earlier this year. ECC is exploring the use of Halo for Zcash to both eliminate trusted setup and to scale Zcash at Layer 1 using nested proof composition.

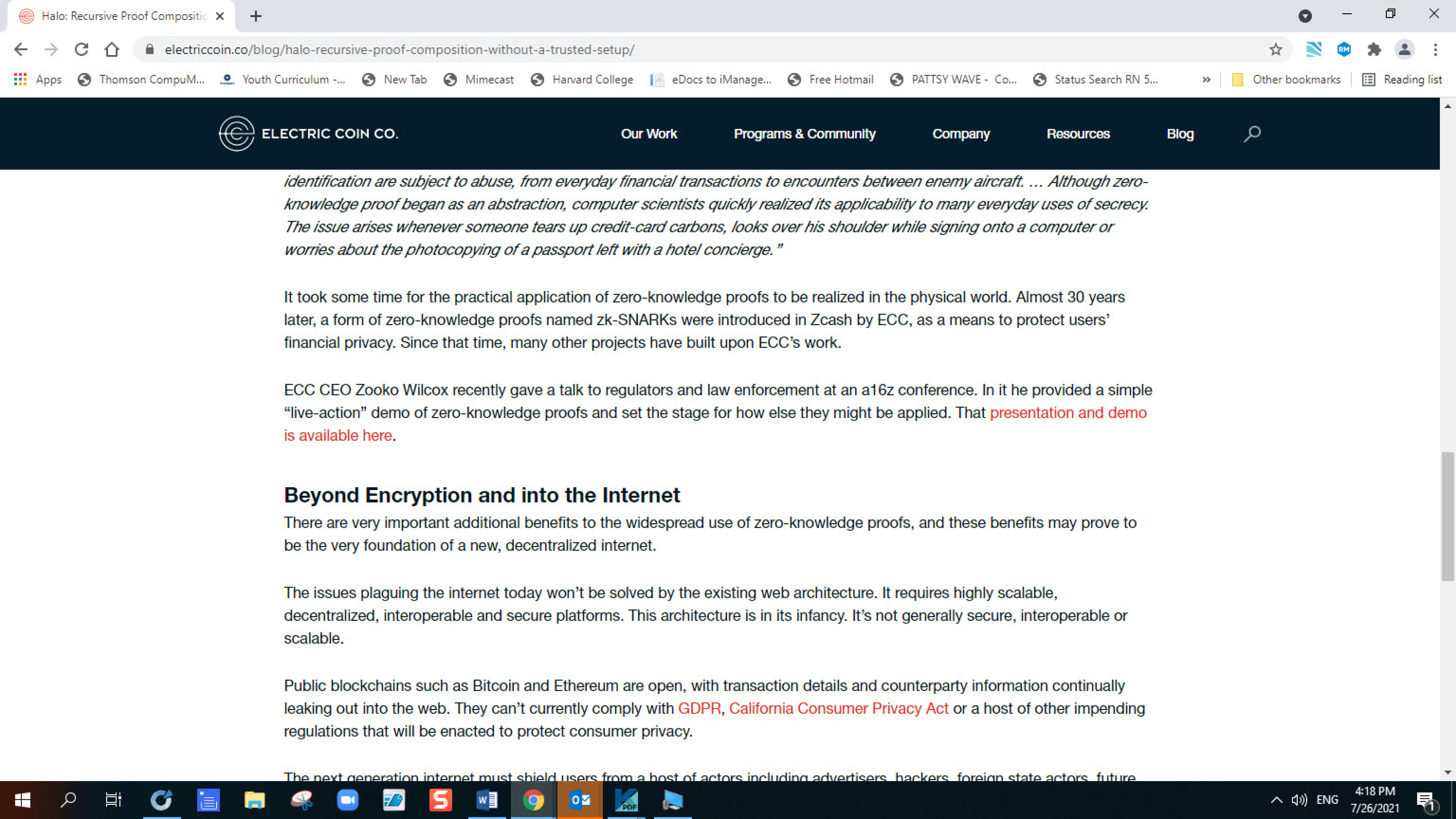
As with our previous scientific discoveries that were funded by the Zcash community, we are making Halo freely available to everyone in the world. Both the paper and the prototype implementation are available under an open source license. There is no patent or other restrictions to its use.

Halo and the Implications for a Decentralized Internet

Cryptography is traditionally viewed as the science for encrypting and decrypting messages. We often think of it as a protective measure that preserves privacy and ensures security against adversaries, and that is true. Among its uses, encryption is necessary for interactions on the web. It is crucial to protect people from bad actors, businesses from competitors, and nation states from foreign powers. But the promise of cryptography is also more than encrypting messages.

Zero-knowledge proofs were envisioned by cryptographers and mathematicians in the mid 1980s as a means to prove a fact is true, without revealing anything about the fact itself. Their discovery was profiled in the New York Times in 1987. From the article:

"… [zero-knowledge proofs] may also hold the power to transform the many aspects of modern life where processes of



identification are subject to abuse, from everyday financial transactions to encounters between enemy aircraft. … Although zero-knowledge proof began as an abstraction, computer scientists quickly realized its applicability to many everyday uses of secrecy. The issue arises whenever someone tears up credit-card carbons, looks over his shoulder while signing onto a computer or worries about the photocopying of a passport left with a hotel concierge."

It took some time for the practical application of zero-knowledge proofs to be realized in the physical world. Almost 30 years later, a form of zero-knowledge proofs named zk-SNARKs were introduced in Zcash by ECC, as a means to protect users' financial privacy. Since that time, many other projects have built upon ECC's work.

ECC CEO Zooko Wilcox recently gave a talk to regulators and law enforcement at an a16z conference. In it he provided a simple "live-action" demo of zero-knowledge proofs and set the stage for how else they might be applied. That presentation and demo is available here.

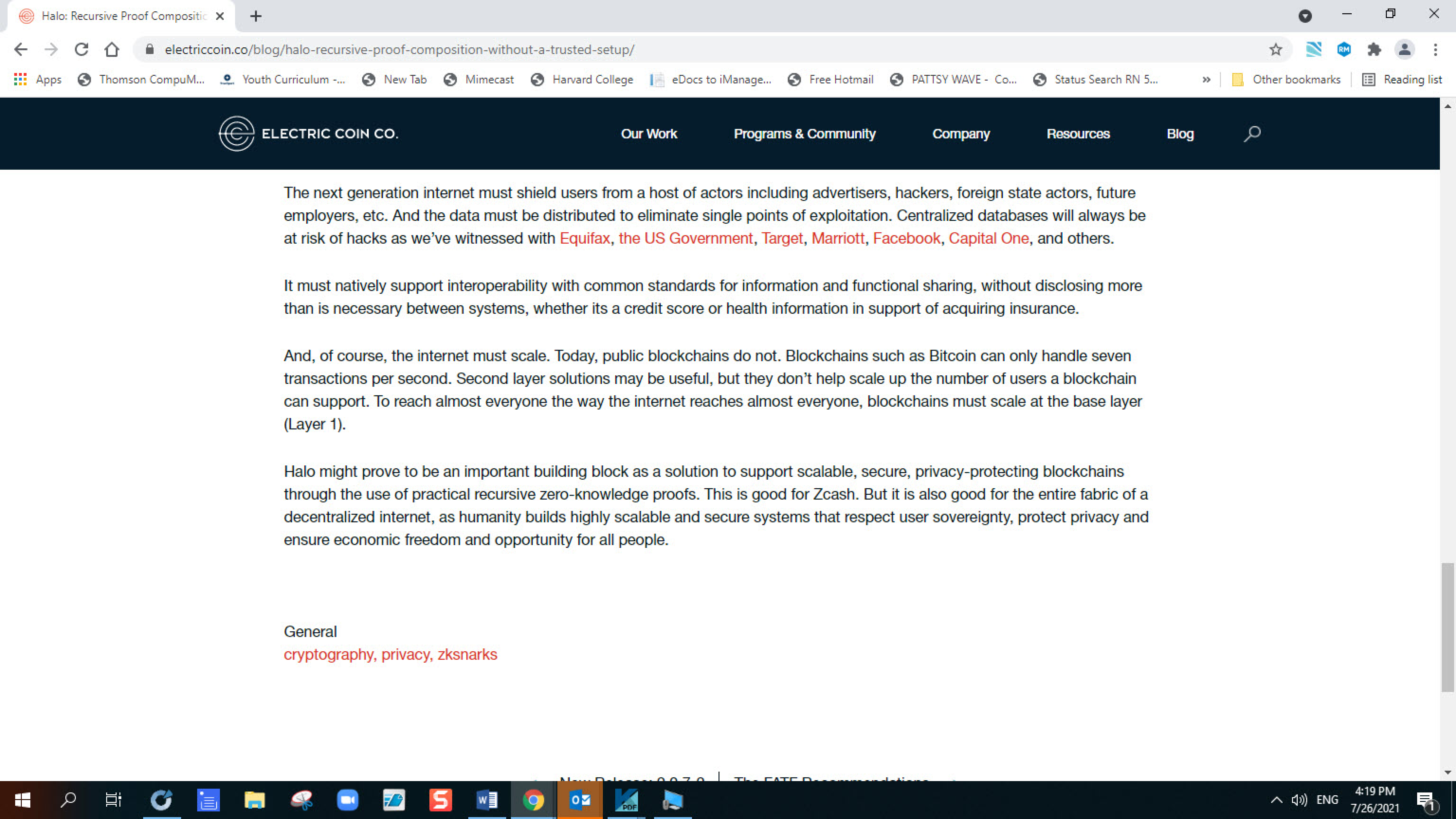
Beyond Encryption and into the Internet

There are very important additional benefits to the widespread use of zero-knowledge proofs, and these benefits may prove to be the very foundation of a new, decentralized internet.

The issues plaguing the internet today won't be solved by the existing web architecture. It requires highly scalable, decentralized, interoperable and secure platforms. This architecture is in its infancy. It's not generally secure, interoperable or scalable.

Public blockchains such as Bitcoin and Ethereum are open, with transaction details and counterparty information continually leaking out into the web. They can't currently comply with GDPR, California Consumer Privacy Act or a host of other impending regulations that will be enacted to protect consumer privacy.

The next generation internet must shield users from a host of actors including advertisers, hackers, foreign state actors, future



The next generation internet must shield users from a host of actors including advertisers, hackers, foreign state actors, future employers, etc. And the data must be distributed to eliminate single points of exploitation. Centralized databases will always be at risk of hacks as we've witnessed with Equifax, the US Government, Target, Marriott, Facebook, Capital One, and others.

It must natively support interoperability with common standards for information and functional sharing, without disclosing more than is necessary between systems, whether its a credit score or health information in support of acquiring insurance.

And, of course, the internet must scale. Today, public blockchains do not. Blockchains such as Bitcoin can only handle seven transactions per second. Second layer solutions may be useful, but they don't help scale up the number of users a blockchain can support. To reach almost everyone the way the internet reaches almost everyone, blockchains must scale at the base layer (Layer 1).

Halo might prove to be an important building block as a solution to support scalable, secure, privacy-protecting blockchains through the use of practical recursive zero-knowledge proofs. This is good for Zcash. But it is also good for the entire fabric of a decentralized internet, as humanity builds highly scalable and secure systems that respect user sovereignty, protect privacy and ensure economic freedom and opportunity for all people.

General
cryptography, privacy, zksnarks