TESTIMONY OF SHAMSH HADI
CEO OF ZORROSIGN, INC.

BEFORE THE U.S. HOUSE COMMITTEE ON ADMINISTRATION

HEARING ON *2020 ELECTION SECURITY: PERSPECTIVES FROM VOTING SYSTEM VENDORS AND EXPERTS*

JANUARY 9, 2020

Chairperson Lofgren, Ranking Member Davis and members of the Committee — thank you for affording me the opportunity to submit testimony to the committee as part of the committee's hearing on 2020 Election Security. My name is Shamsh Hadi and I am the CEO of ZorroSign, Inc. - a company based in San Francisco, CA. ZorroSign is the pioneer of electronic signature technology and the developer of ZorroSign DTM, a unified platform built on blockchain technology, and incorporates a complete Electronic Signature and Digital Transaction Management solution. ZorroSign's unique Document 4n6 (forensics) technology offers post-execution fraud detection and verification and authentication of electronic signatures and documents using blockchain security tokenization.

I would like to outline for the committee how blockchain technology can be employed by voting machine vendors across the country to significantly enhance and upgrade the security and reliability of electronic voting systems. Obviously, the goal of any legislative effort to improve and ensure the security of our elections this year should encourage or require the use of available technologies that are reliable, easily integrated into existing software systems, saves time, eliminates fraud and cost effective.   Blockchain technology meets all of these criteria.

Throughout my career in the high-tech industry, and especially through my work as CEO of a technology company that lives and breathes data and security, I have come to learn that blockchain can and should be an essential component to any election security framework. In my testimony, I would like to share with the committee my views on how blockchain can and should be an essential feature of a nationwide election security framework.

According to a paper issued in February of 2019 by the National Institute of Standards and Technology (NIST Annual Manufacturing Series 300-6), *"blockchain is a distributed storage framework that is virtually tamper resistant, has a native synchronization-discrepancy-resistance mechanism and is already highly praised in the financial world."*

In its simplest form, blockchain is a shared fixed ledger for recording transactions. The concept of blockchain can and has been extended to have the highest levels of security and privacy protecting the sensitive information and identities of authorized individuals in a network who have permission to access the content stored in the ledger.

Blockchain is a digital record where all transactions are recorded in the order of occurrence and where the next record is linked and related to the previous record. It is a continuous database of records that can only be added to and never edited or deleted. In layman's terms, blockchain allows government agencies to secure and validate a digital asset, such as a voting record, enabling the enforcement of ownership or authenticity.

The noteworthy characteristics of a blockchain are:

- Indelible: The most important and distinctive property of blockchain. Once a transaction is written into a block, it can never be erased or modified by anyone, including the person who wrote the transaction.

- Globally Readable: Anyone who has permission to view the transaction can read what it contains and everyone sees exactly the same content.

- Accept Rules Based Rights: Any chosen party can write into the blockchain if it respects the predetermined rules set out for that transaction.

- Strictly Ordered: There is no ambiguity of the transaction. The audit trail will clearly show which block of data came first and which came second.

In its February 2019 paper, NIST noted that because blockchain *"…is tamper resistant and the blocks are timestamped, a blockchain is a robust solution to prove the existence of a specific asset at a certain time during the product lifecycle"* and "*a safe way to track both the existence and ownership of a digital asset at a certain time."*

There is a plethora of practical applications of blockchain in the real world. For the purposes of this hearing, I would note that blockchain has a very real and pertinent application when it comes to electronic voting: voter registration, personal identity, and voting records. Please note that blockchain is NOT Bitcoin. Cryptocurrency like Bitcoin uses blockchain technology, but they are not the same. Blockchain is not cryptocurrency or Bitcoin. Rather, Bitcoin uses blockchain to secure transactions and publicly record them in a distributed ledger.

Blockchain is important because it has unique qualities that set it apart from other transaction database management systems. Specifically, blockchain is being used today in private, permissions-based decentralized systems that are secure, trusted and automated with standards that can now surpass bank grade security. Ultimately, blockchain technology helps make digital transactions more secure, faster and less expensive.

One of the conclusions of the February 2019 NIST paper was that *"Due to its tampering resistance, blockchain is an ideal candidate to record and secure data exchanges."* As someone who has spent the better part of my career working on and with blockchain, I wholeheartedly agree with NIST's conclusion.

In terms of how blockchain can specifically be employed to enhance and upgrade election security, I would note that blockchain can and should be utilized by electronic voting systems to store the voting record of each voter. If the goal is to ensure that our elections in 2020 are true, fair and honest, then recording each voter's voting record on blockchain where the record cannot be altered is highly recommended. Blockchain technology could help centralize the U.S. election process by validating the voter, and making counting votes more secure and efficient because the ledger would clearly identify who voted and where the vote came from.

If the committee is going to consider setting national standards for electronic voting systems, then blockchain technology should be an essential feature of any national regulation. As I explained earlier, the employment of blockchain technology in electronic voting system would be one of the most effective ways to lower voter fraud rates and create a tamper proof audit trail — thereby significantly safeguarding the integrity of the voting process. Implementing blockchain technology into voting systems allows for the highest levels of security and privacy, protecting the sensitive information and identities of individuals in a network who have permission to access the content stored in the ledger. If voting systems across the country are going to go digital — and more and more jurisdictions are doing just that — then blockchain technology would be an effective way to help make voting transactions more secure, faster and less expensive. The employment of blockchain technology as a required feature of an electronic voting system would prevent the unauthorized view/review, re-distribution of voting records, ensure unbroken chain-of-custody and provide a clear audit trail for every voter in every election.

To conclude, the thoughtful and intentional employment of blockchain within electronic voting systems in the U.S. would protect the fabric of our democracy and maintain confidence in the integrity of our elections.

Thank you for your time and consideration. I would be happy to answer any questions committee members might have, either in person or in writing.