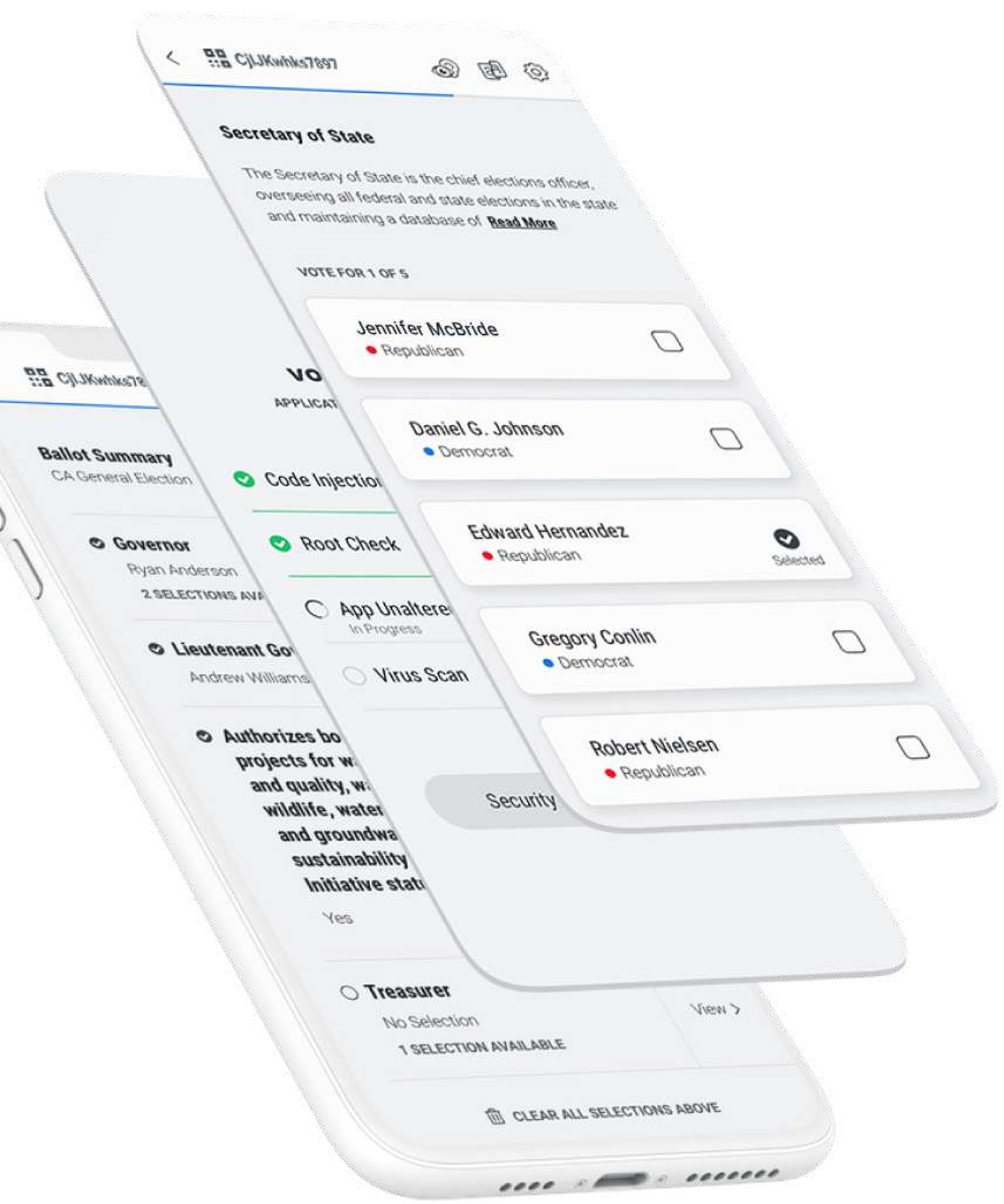
votingapp

Scan this code
for the long version

End-to-End Verifiable Voting



Introduction

End-to-end verifiable (E2EV) remote voting over public networks has not been a viable option for public elections due to system inabilities to adequately address security concerns, voter privacy issues, or a lack of true voter verifiability of cast vote records. [1, 2, 3] For these reasons voters of remote voting systems are required to sacrifice either security, secrecy/privacy, or verifiability for the convenience of using the system. The poll station and remote voting experiences have not been equal in these regards until now.

The voting app solution, relies on a variety of cryptographic techniques and voter authentication steps to give voters the privacy they deserve with the security required all while offering complete voter verifiability of their vote.

The Solution

An end-to-end verifiable (E2EV) system involves three key 'proofs' for vote verification.

- Marked As Intended - Voters can verify their choices are properly collected
- Stored as Marked - All observers can verify the collected marked ballot has not changed since marking
- Tallied as Stored - All observers can verify votes are not changed between storage and counting

The voting app solution provides all of these proofs without compromising voter privacy by utilizing a variety of cryptographic techniques including but not limited to asymmetrical key creation, hierarchical deterministic address protocoling (HDAP), cryptographic receipt generation, and by leveraging the inherent properties of data verification used by a permissions-based blockchain. While votes are stored and encrypted during live voting, a post processing step allows for complete vote decryption without compromising voter privacy or losing data verifiability.

How is this accomplished?

The voting app solution relies on two key aspects to accomplish the goals listed above. The basic architecture of the system requires a network of trusted components all sharing pre-provisioned keys and certificates with all data passed between components signed by multiple other components. As a result the system cannot be compromised by nefarious actors controlling a single component but only by controlling all components. Distributing the operation of the components between various mutually distrustful parties forces all components of the system to behave properly and honestly.

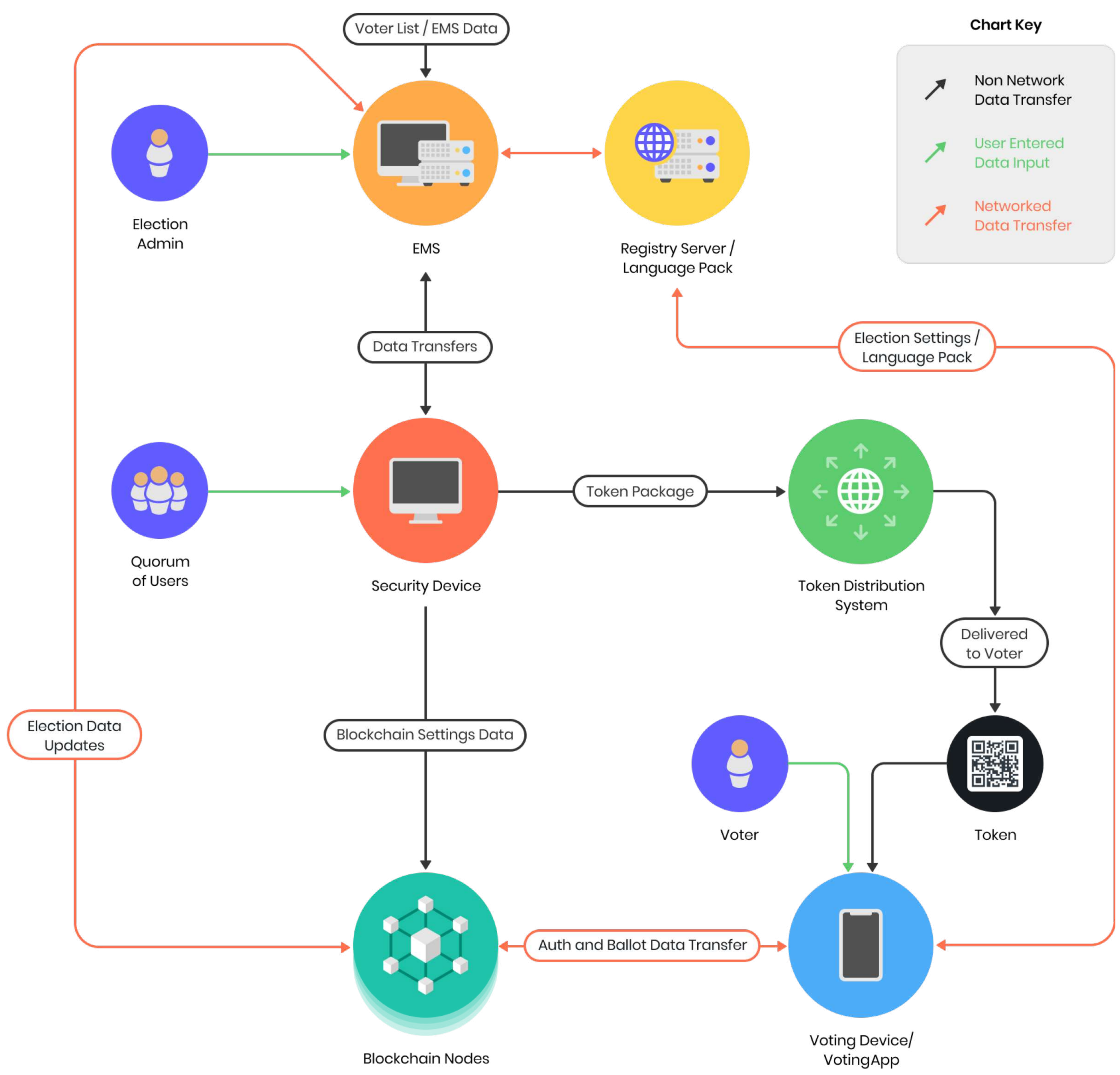


Figure 1: High Level Data Flow

Fully provisioned and operating election network. The communication paths shown represent data transfers during pre-election, live election, and post-election phases. It depicts the connections between components and distinguishes between networked traffic and manual data transfers. Detailed data workflow diagrams are available in the long version of this paper.

At the core of these components is an air-gapped, custom made security hardware device. The only place a link between individual voter data and ballot or marked ballot data exists is in this device. Even within the device there is a special security chip responsible for storing sensitive private keys that can never be accessed except to run validation operations against the stored data. Identifiable voter data cannot be retrieved from the device at any point. Additionally, for all critical operations run on the security device a quorum of users is required again to ensuring that no single bad actor can compromise any single election.

During the voting session a voter receipt is generated deterministically based upon the selections a voter made and some user-provided information. This makes each receipt unique, as well as ensures selections cannot be reverse engineered from the receipt alone. Voters retain this receipt after vote submission and can use it to verify the location of their stored vote on the blockchain, as well as the unchanged nature of their vote data when after the election the jurisdiction decrypts submitted votes and recreates all receipts. The one way nature of HDAP ensures voters can verify their receipt matches a recreated receipt but no one can use their receipt to verify actual selections and thus compromising voter privacy.

Figure 2: Receipt Generation

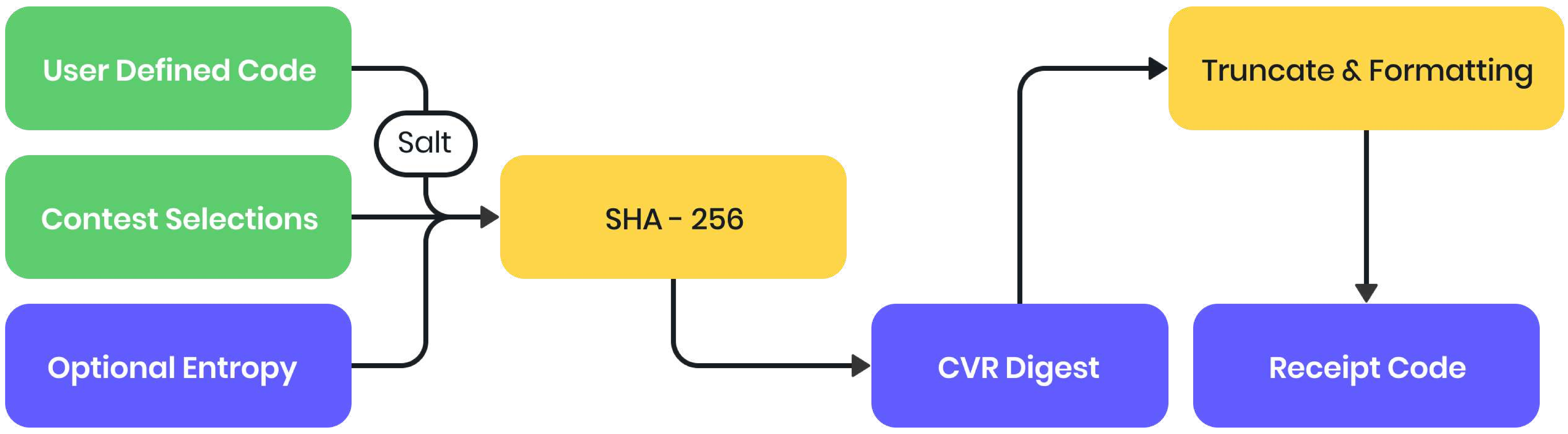
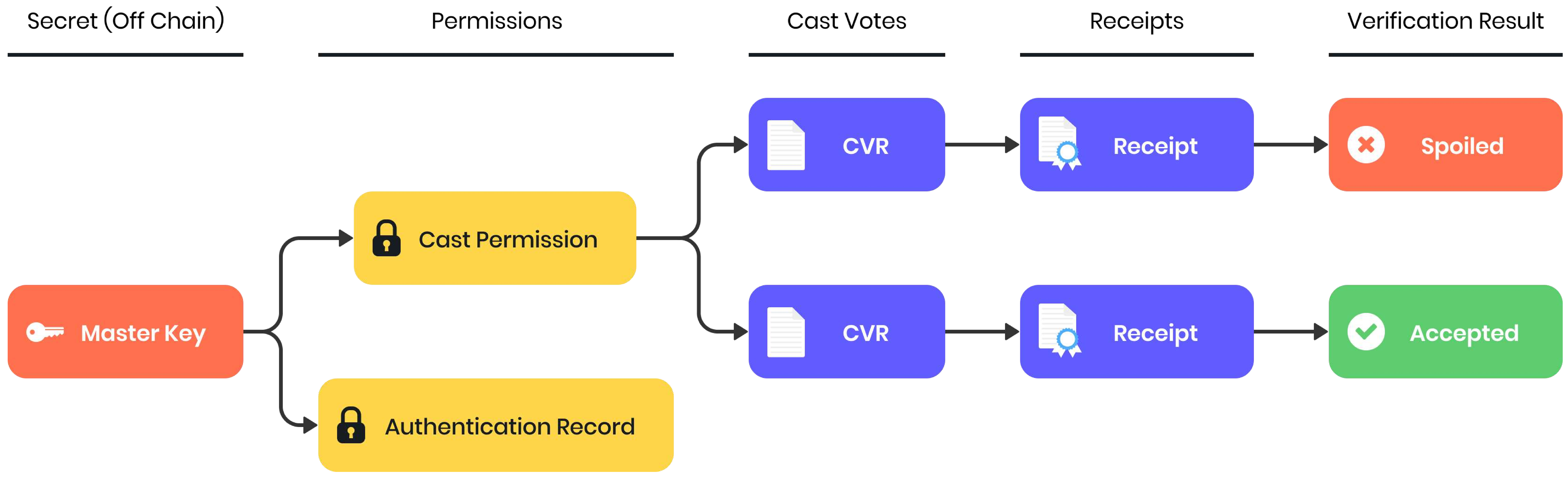


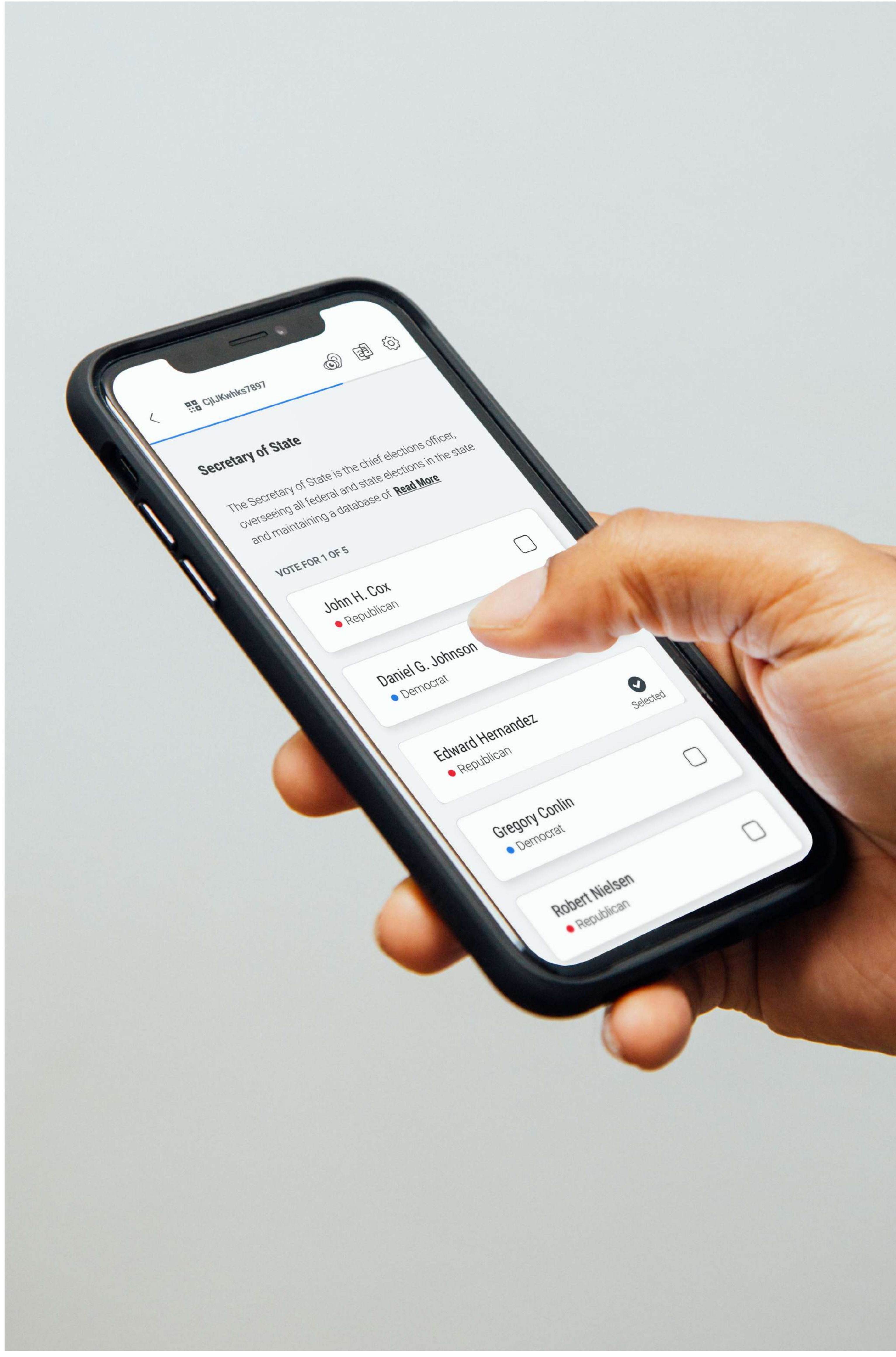
Figure 3: Address Structure



Conclusions

Currently there is only one system available for US public elections that allows for remote accessible voting while providing complete end-to-end-verifiability, all while maintaining voter privacy throughout the entire election cycle. Voters, election officials, and election observers can be assured an election run on the voting app solution is accurate, secure, and fully auditable.

For an in-depth look as well as further conclusions and discussion on future white paper topics see the long version of this paper at votingapp.com



References

1. Benaloh, J., Rivest, R., Ryan, P., Stark, P., Teague, V., & Vora, P. (2015). "End-to-end verifiability" (PDF). Retrieved July 9, 2021. https://escholarship.org/content/qt7c9994dg/qt7c9994dg_noSplash_97d64dc5a809c552701079250f47b4cb.pdf
2. Alvarez, R.M., Hall, T.E. (2004). "Point, click & vote: the future of Internet voting." Brookings Institution Press, Washington D.C.
3. Evans, D., Paul, N. (2004). "Election Security: Perception and Reality" (PDF). Retrieved July 14, 2021. https://www.academia.edu/1126471/Election_security_Perception_and_reality