future internet

MDPI

Communication

A Public Infrastructure for a Trusted Wireless World

Renee Carnley and Sikha Bagui *

Department of Computer Science, University of West Florida, Pensacola, FL 32514, USA; rcarnley@uwf.edu
* Correspondence: bagui@uwf.edu

Abstract: The novelty of this work lies in examining how 5G, blockchain-based public key infrastructure (PKI), near field communication (NFC), and zero trust architecture securely provide not only a trusted digital identity for telework but also a trusted digital identity for secure online voting. The paper goes on to discuss how blockchain-based PKI, NFC, and the cloud provide a roadmap for how industry and governments can update existing frameworks to obtain a trusted digital identity in cyberspace that would provide secure telework and online voting capabilities.

Keywords: e-voting; blockchain technology; identity, credential and access management (ICAM); Internet of Things (IoT); mobile devices; public key infrastructure (PKI); near field communication (NFC); smart card; 5G; telework

1. Introduction

The COVID-19 pandemic turned an unprepared world upside down. Millions worldwide were either out of work or teleworking for the first time. Businesses had to adapt quickly, and the first few months were wrought with one mishap or the other. A mobile world filled with an exploding volume of Internet of Things (IoT) was not prepared to securely handle working from home. Safeguards that are in place on the premises of government and industry are not in place at their employee's homes. Moreover, all of this happened during an election year for the United States (US).

Citizens of the US were warned that they would put their lives as well as the lives of others in danger if they voted in person at the polls. They were also warned of the unreliability of voting by mail while at the same time being told of the safety of voting by mail. Then there were all of the claims of voter fraud [1]. US citizens either took a side or were confused about the right thing to do. This left many asking why, in this 21st century, in a technological age where majority of the business transactions are taking place online, we do not have the capability to cast votes online [2]. The primary reasons are privacy, tampering, and security. How do we allow individuals to vote online and prove their identity? How do we allow them to vote only once? How do we keep their vote private? How do we keep our voting systems tamper-proof from hackers [3]? We do this by utilizing the ideas first put forth within the Mobile Identity, Credential, and Access Management(ICAM) framework. These ideas will be elaborated upon throughout this paper [4].

Since the pace of the usage of IoT has increased within industry at the same rate as that of personal devices, it is high time for trusted digital identities that can scale from on-site to the cloud to personal residences. A digital identity is the computerized representation of an entity that exists in the physical world. This entity may be a person, organization, application, or device. As telework becomes more and more the norm, with smart phone users increasing annually and the mobile web flourishing, it is critical to implement stronger security. From personal devices to industry to government, the internet has become the primary means of modern communication. People want secure communication. US citizens want to vote online. This has further increased the need for a method of tracking and securing these devices. An organization must not only know the identity of the users on

check for updates

Citation: Carnley, R.; Bagui, S. A Public Infrastructure for a Trusted Wireless World. *Future Internet* **2022**, *14*, 200. https://doi.org/10.3390/fi14070200

Academic Editor: Paolo Bellavista

Received: 2 June 2022
Accepted: 27 June 2022
Published: 30 June 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

their networks and have the capability of tracing the actions performed by a user, but the organization must also trust the system providing this knowledge. Online retailers are faced with the challenge of authenticating a card remotely and proving that the person making the purchase is the actual card holder. A person cannot claim their transaction is fraudulent if they cannot prove it was not them making the online purchase.

Hence, the novelty of this work lies in examining how 5G, blockchain-based public key infrastructure (PKI), near field communication (NFC), and zero trust architecture securely provides not only a trusted digital identity for telework but also provides a trusted digital identity for secure online voting. This paper goes on to discuss how blockchain-based PKI, NFC, and the cloud provide a roadmap for how industry and governments can update existing frameworks to obtain a trusted digital identity that would provide secure telework and online voting capabilities. A framework is provided for trusted digital identity in cyberspace.

Section 2 presents a summary of blockchain-based PKI followed by a description of NFC and digital identities. Section 3 discusses the challenges. The usage of cloud computing and the types available are defined to offer context for how many organizations are currently facing their telework challenges. Section 4 presents an examination of how blockchain-based PKI, NFC, and the cloud may provide a roadmap for how industry and governments can update existing frameworks to obtain a trusted digital identity that would provide secure telework and online voting capabilities. Section 5 presents a framework for updating the existing frameworks. Section 6 discusses the security within the system and Section 7 presents the conclusion and future work.

2. Background

Securing anything online begins with a trusted digital identity. Then, the trusted digital identity must be utilized via mobile devices. The technology found best suited for mobile devices is radio frequency identification (RFID) that will work over short distances and is readily available already many on smart devices.

2.1. Near Field Communication (NFC)

Near field communication (NFC) is a more simplistic implementation of radio frequency identification technology. Involving two wireless devices, NFC operates via short-range frequencies within five to ten centimeters. There are two modes: active and passive. An active mode device starts the communication. This device is referred to as the initiator. The initiator generates its own power and sends information by amplitude shift keying. Within the passive mode, the device is referred to as the target and uses the radio frequency field from the initiator as the power for its communication [5].

2.2. Blockchain

The foundation of blockchain began with a paper published by Stefan Konst in 2000 that provided instructions for implementing cryptographically secured chains and then grew in popularity in 2008 by Satoshi Nakamoto's creation of bitcoin. Blockchain offers several key benefits such as transparency, trust, cost reduction, transaction improvements, and security [6]. Blockchain is defined as 'a peer-to-peer, distributed ledger that is cryptographically secure, append-only, immutable, and updatable only via consensus or agreement among peers' [7].

Blockchain became popular since it was the technology behind Bitcoin. Bitcoins are a type of electronic cash used as a digital currency on the internet. Bitcoin spelled with an uppercase 'B' references the cryptocurrency payment network, protocols, and blockchain. When spelled with a lowercase 'b', bitcoin refers to the units of bitcoin. For example, Sally is sending Bob 1.5 bitcoins [8].

A block is an assortment of transactions which are arranged logically. A transaction is the transference of digital currency from a sender's account to a receiver's account. A block can consist of more than one transaction [7]. Block 0, or the genesis block, is the first block

on the blockchain. The genesis block within Bitcoin was hardcoded at the time of creation with the message 'The Times 3 January 2009 Chancellor on brink of second bailout for banks.' Each block contains a hash of the previous block's message hash, linking each block together in a chain and providing additional security that the previous block's transaction has not been tampered with. The Bitcoin blockchain uses the SHA-256 algorithm as its hash. The SHA-256 algorithm generates a unique, fixed-size 256-bit hash [6].

2.3. Public Key Cryptography

Public key cryptography is the same as asymmetric cryptography. The two terms can be used interchangeably. Public key cryptography began in 1976 with a paper publication by Whit Diffie and Martin Hellman describing a method of establishing a common key in a secure manner over an insecure channel [9].

Each entity (person or device) that uses public key cryptography has a key pair that consists of a public key and a private key. Private keys are secret and known only to their owners. They are protected by a passphrase and can be stored on separate hardware cryptographic devices such as smart cards. Private keys are used for proving the identity of an entity. Public keys are made known openly and are distributed to all hosts with which the entity wants to securely communicate. The two keys are mathematically dependent, but the private key cannot be derived from the public key. The data encrypted with the public key can only be decrypted with the private key and vice versa. Since the public key is shared freely, a method to ensure the authenticity of the public key is created through a public key certificate. A public key certificate is an electronic document used to prove the ownership of a public key. This ensures trust that the public key belongs to the entity it is associated with. This is most commonly done using the X.509 standard. X.509 is a standard defining the format of the digital certificates used to validate the ownership of a public key. This standard allows interoperability among numerous tools and applications among vendors [10].

2.4. Nonrepudiation

Nonrepudiation is the assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. Public key cryptography provides nonrepudiation via a digital signature. A digital signature is a means of identifying the sender of a digital message, similar to the way a written signature on a paper or document proves authorship. Using public key cryptography, a sender, Bill, uses his private key to digitally sign a message. The receiver, Jill, uses Bill's public key to confirm the message's signature so that she can trust it came from Bill. If Bill wants to send a private message to Jill, Bill encrypts the message with Jill's public key. Only Jill can decrypt the message with her private key ensuring that only Jill reads the message. Bill digitally signs the message with his private key so that Jill can assure herself the message came from Bill. This is how public key cryptography allows a means of authenticating the identity of one another [11].

2.5. Digital Certificate

Digital certificates are electronic credentials that bind a user's, computer's, or service's identity to a public key by providing information about the subject of the certificate, the validity of the certificate, and the applications and services that can use the certificate. Digital certificates can be used for authentication, encryption, and digital signing. Certificates issued in PKIs are structured to meet these objectives based on standards established by the Public Key Infrastructure (X.509) Working Group (PKIX) of the Internet Engineering Task Force (IETF) [10].

2.6. PKI

Public key infrastructure (PKI) has been around for decades as a means to identify and authenticate individuals and machines. Traditionally, the identification of an individual

has been done through the use of a smart card and a personal identification number (PIN). The PIN is entered in addition to a smart card to prove that a person is who they claim to be. A smart card is about the size of a credit card and requires the use of a smart card reader, which makes the use of the smart card on mobile devices cumbersome. Industry, especially the United States Department of Defense (DoD), wants a lighter, more mobile-friendly solution. Since PKI provides everything necessary to securely communicate with an established and trusted digital identity in a static environment, it simply needs updating to accommodate the dynamic mobility of today. PKI provides the groundwork for creating and handling digital identities at the scale IoT requires.

The root certificate is the foundation of trust for PKI, which is why it is also called the root of trust. In order for a certificate to be trusted it must originate from a trusted source. A certificate is signed by a root certificate issued by a program run under strict guidelines. Many well-known root certificates are distributed in operating systems such as Microsoft and Apple. A root certificate is invaluable because any certificate signed with its private key is automatically trusted [12].

A credential service provider (CSP) establishes and maintains the enrollment records and binding authenticators of a digital identity within a PKI. They were formed in order to meet the challenge of linking a digital identity to a single precise person or thing. A CSP can meet one of three identity assurance levels (IALs) [13]:

IAL1: Invalid or unverified digital identity. There does not have to be a link to a real person or thing.

IAL2: There is some proof that the digital identity is real. The proof can be remote or physically present identity proofing.

IAL3: The digital identity is verified and validated by an authorized and trained CSP representative by the physical presence of the real person or thing [13].

A certification authority (CA) is an entity that certifies an identity with a public key. Basically, the CA is the method of generating the digital identity through providing a certificate. Certification is a binding that occurs in the form of a signed data structure called a public key certificate. A CA is an authority on the process of certification. The issuing CA digitally signs certificates, ensuring integrity; therefore, a CA must be trusted by both the issuer of the certificate and the owner of the certificate [14]. A CSP must provide security management services for key generation and storage.

A validation authority (VA) is the authentication system within PKI. It verifies the validity of a digital certificate by following the requirements of the X.509 standard. A VA manages the certificate revocation list (CRL) issued by the CAs and provides online certificate status protocol (OSCP) functions. Some VAs may also provide access control and authorization services [14].

2.7. Zero Trust Architecture (ZTA)

Zero trust architecture (ZTA) is an enterprise cybersecurity approach that is built on a novel model for cybersecurity principles and network security known as 'zero trust' (ZT). Zero trust architecture moves security away from a perimeter-based security model to one that focuses on the security of individual transactions. Continually evaluating the people and entities on a network broadens the range of protection to accommodate the dynamic modern world that is constantly moving between on-premises and cloud networks. This approach is comprised of logical components that, once implemented, can improve the security posture of any classification or sensitivity level network [15].

2.8. Fifth-Generation Cellular Communications Technology (5G)

Fifth-generation cellular communications technology is referred to as 5G. Fourth-generation cellular communications technology (4G) is still widely used, and in fact, many parts of the world are still using 3G and 2G. It will take some time before 5G is available universally [16], and 5G improves upon previous cellular technologies by improving a mix of existing access radio technologies combined with newer technologies such as utilizing

a new spectrum band. These updates will allow 5G subscribers to access services from anywhere and anytime, with high data rates, low latency, and increased quality of amenities. There will be a new range of services available for the first time such as virtual reality, augmented reality, ultra-high definition, 3D videos, and autonomous driving [17].

3. Challenges

Currently, the internet is like the Wild West. There are millions of unknown devices connected anonymously. Even if elections were not a consideration and before COVID-19 forced masses into teleworking, employers and employees wanted to use their personal devices to perform work-related activities. This was also known as bring your own device (BYOD). The built-in anonymity of cyberspace makes identity one of the largest challenges that cybersecurity experts face [18]. Managing and having trust in the identity of a user is desired knowledge by governments, industry, and individuals. In the technologically rooted social and business environments of the modern world, identity can be faked or impersonated. People want to know that the person they have been chatting with on social media or flirting with on dating sites is who they say they are. People want to trust that the email they just opened is really from their bank as it claims. Industry and governments want to know that the person they allowed onto their network or access to their websites is who they say they are. People want to believe in their electoral process and trust that fraud has not occurred. A digital identity sometimes referred to as an electronic identification (eID) is the cyberspace equivalent to a person's or entity's real-life identity. An entity can be an industry, a government, or a thing. Basically, anything that connects to a network requires a digital identity. The authentication and authorization validation process of a PKI requires a strong trust that must have meaning and be quantifiable. Since trust is more of a social construct, giving it meaning and finding measurements within an electronic system proves challenging. PKI's relying on the correct usage of public/private key pairs depends upon there being a chain of trust among certificate authorities (CA). A public key certificate is issued as the public component of these key pairs and is often associated with personal identity verification (PIV) card. These CAs are the third-party servers providing the certification path to authentication. Path validation and path construction are essential to the proper management of trust within PKI [19].

Implementing an electronic voting (e-voting) system in every city across a state and within every state across the country will take a tremendous number of resources. There will need to be collaboration amongst government and industry. Before the e-voting system will work, the ICAM framework [20] will need to be instantiated in order to have an eID.

4. Literature Review

The idea of using blockchain for an e-voting system is not new. There is the Universiti Tun Hussein Onn Malaysia (UTHM) e-voting system. It is based on common blockchain concepts from Nakamoto and offers no registration process as a method to ensure anonymity. A group of students from UTHM designed the e-voting system using the web browser as the frontend of the system, where it was never explained how a voter would be authenticated. Then, the browser acting as the client sends the user's vote to the blockchain e-voting system's backend [21].

An e-voting system using blockchain that consists of a voter list, administration management services, and election preparation services has also been proposed [22]. It hails all of the integrity benefits and warns of the risks of central authority control but using no trusted digital identities. There is nothing similar to PKI to ensure the integrity of the system nor ensure the system itself is tamper-proof.

Blockchain as a service for e-voting has also been proposed. It works by using a permissioned Proof-of-Authority (POA) blockchain that consists of two types of nodes: a district node and a bootnode. A district node represents a voting district, while the bootnode is a service that allows the districts to communicate with each other. This system allows the users to authenticate themselves as well as authenticate their vote [23]. It would

take little effort for individuals to vote multiple times within this proposed blockchain as a service e-voting machine.

Another idea for blockchain-based e-voting is e-vote-as-a-service. This system would be hosted within a cloud and is business/corporation-structured. It does have a clear voter authentication mechanism using tokens and places voters from a list into a pool. The purpose of this pool seems to be a way to loosely define a county or a district so the e-vote can be a service. The voting session established by the use of a token can provide some voter anonymity until the vote is placed on a blockchain via the blockchain configurator [24].

Building upon the e-vote-as-a-service is the blockchain e-voting within a smart city concept called smart e-voting. The proposed framework relies heavily upon existing blockchain infrastructures and Dijkstra's algorithm for trust [25]. However, it is quick to see that a random trust value does not provide the same level of trust that a PKI framework can provide. Blockchain-based PKI has built-in trust that meets all tenets of ZTA.

Finally, there is VoteChain, which is, as its name makes clear, a blockchain-based e-voting system. VoteChain makes use of three nodes and a gateway node. This blockchain network consists of a 6-core processor, 1 TB SSD storage, and a 1 Gbps local area network. Each vote block has the previous block's hash value, proof of work, and a root of the Merkle tree of votes. Each vote contains a hash of the entire vote, timestamp, vote data, voter identification, which is a unique ID to verify a user's identity, and a one-time password [26]. This system would not work in the real world. Not all voters have 1 Gbps networks, nor do they have multicore processors, much less 6-core processors. Plus, how many voters want their name tied to their vote?

5. A Roadmap for Updating Existing Frameworks to Obtain Trusted Digital Identities

In order to manage the vast number of devices, in addition to making people feel confident that a machine such as an e-voting system or a person is who they say they are, companies must deploy digital-credentialing systems and methods. Since trust is more of a social construct, giving it meaning and finding measurements within an electronic system proves challenging. The existing self-sovereign identities of the internet must be changed. Public key infrastructure (PKI) has been around for decades as a means of identifying and authenticating individuals and machines. A PKI will provide the policies, roles, software, hardware, and procedures necessary to create, manage, distribute, use, store, and revoke digital certificates. The most important aspect of PKI is that it establishes the identities of people, devices, and services [14]. However, PKI is outdated and in need of a facelift. Blockchain provides a mechanism to update PKI in order to meet the demands of a mobile 21st century. The PKI framework, as it currently exists, has vulnerabilities. Reporting unauthorized certificates is a time-consuming and labor-intensive effort that leaves a CA open to a man-in-the-middle (MITM) attack. If the CAs are not operating correctly, the introduction of encryption has no value. Blockchain-based PKI techniques provide methods to secure the CA vulnerabilities immediately in real time [27].

In order to affectively implement blockchain within PKI, establishing trust would be necessary to instantiate security measures against interference, breach, and eavesdropping [28]. A considerable vulnerability to PKI applications and platforms is their dependence on a centralized cloud. PKI, in its current form, is centralized, relying on trusted third parties. Decentralizing and incorporating blockchains provides the means of overcoming several of the problems linked with the centralized cloud approach. Provenance and other startups are using blockchain to promote trust in product transactions from the source to the customer [29]. Blockchains can cryptographically sign transactions and verify the originator's cryptographic signature to guarantee a message's origin [29]. Blockchains also provide secure traceability of certifications and other relevant data in supply chains. Blockchain's public availability ensures transactions can be linked to identify vulnerable mobile devices [28]. Suitable for registering time, location, price, parties, and data, as they move through the supply chain, blockchain-based PKI systems will help strengthen mobile device security [29]. A blockchain-based PKI running on a 5G network

will allow for significantly improved performance and capabilities within mobile devices. Blockchain-based PKI's authentication service will improve because 5G will employ higher and more directional frequencies such that the data signals can transmit more precisely using less energy [16].

In addition, blockchain-based PKI allays several deficiencies of the existing CA within PKI, the primary deficiency being the centralization of the CA [30]. Following the Identity, Credential, and Access Management (ICAM) framework laid out in Trusted Digital Identities for Mobile Devices, the CA can be made distributed [20]. A distributed system is where all of the parties work together as a single coherent system. It has qualities of centralization and decentralization. There is still a central authority that has some control over the other parties in governing processes, yet the other parties can make many of their own decisions and work autonomously. Distribution improves availability, reliability, fault tolerance, performance, and scalability [7].

Blockchain-based PKI utilizing NFC, as proposed in the ICAM framework [20], allows PKI to solve the challenges faced with online voting and BYOD. The ICAM system provides the authentication/authorization piece to the blockchain-based PKI e-voting system (BPES). Once authenticated through the ICAM and the BPES e-voting frontend, as shown in Figure 1, the BPES e-voting frontend presents a ballot based on where the authorized user is registered to vote. The ballot displayed will contain the user's city, county, state, and national choices for the current election. The frontend can be presented on a screen in-person at a voting poll or via a website.

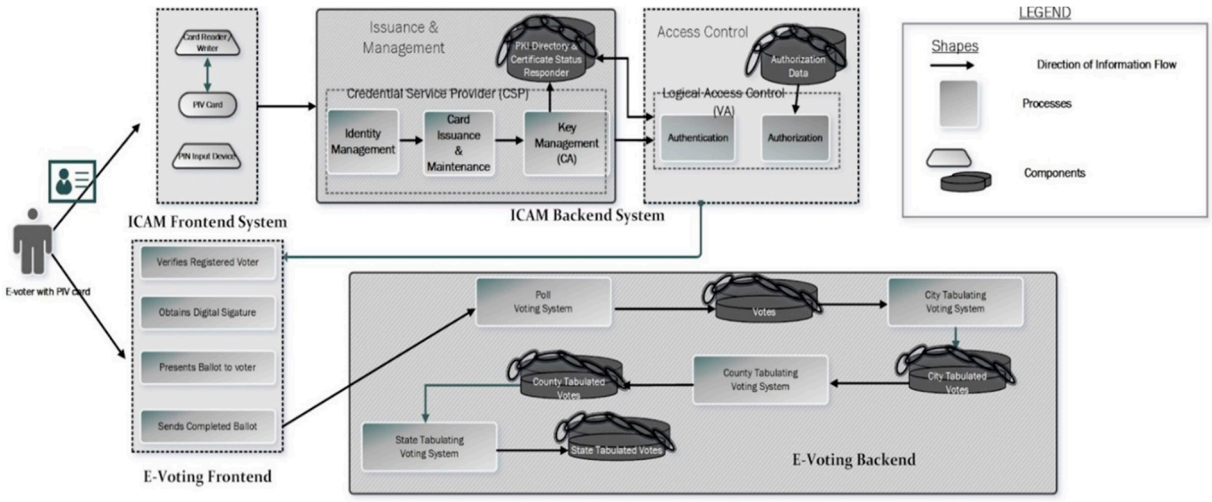

Figure 1. BPES integrated with the ICAM system.

Other blockchain-based e-voting systems have already been proposed using HTTP and WebSocket [31]. BPES would utilize HTTPS and other defense in-depth per the tenets of ZTA such as those explained within [32]. Incorporated with NFC capabilities, the website can be accessed via a mobile device. Once the user is finished, the filled-out ballot is sent to the e-voting backend, as shown in Figure 1. The vote for one user is contained on one BPES blockchain. It does not contain any identifying information about the voter. It only contains the voter's selection digitally signed by the e-voting frontend. This digital signature allows for the nonrepudiation and traceability of the ballot's origin. The integrity of the ballot is guaranteed through blockchain's security and transparency.

The city's BPES would be independent yet connected to the county's BPES, as shown in Figure 2. The city may have any number of poll voting systems that act independently of the county system. However, one primary city system in the county will send a tally to the county system. A county has votes during an election that include their county or cities in addition to any votes necessary at the state level. The results for each county are added to a blockchain on a similar state system working in conjunction with the county's

independent system for the votes the state needs. Basically, the county-centralized system sends the tally of their county's state votes on the blockchain part of the state's system, much like the city did to the county system. The blockchain would look like Figure 3 but would be one county's votes, and that county would not be anonymous. It would include that county's digital ID. It would be an extra security protocol, as that county's public key would sign the blockchain, providing a means of nonrepudiation and integrity for each county. This would allow one to know where the votes came from and if the votes had been tampered with.

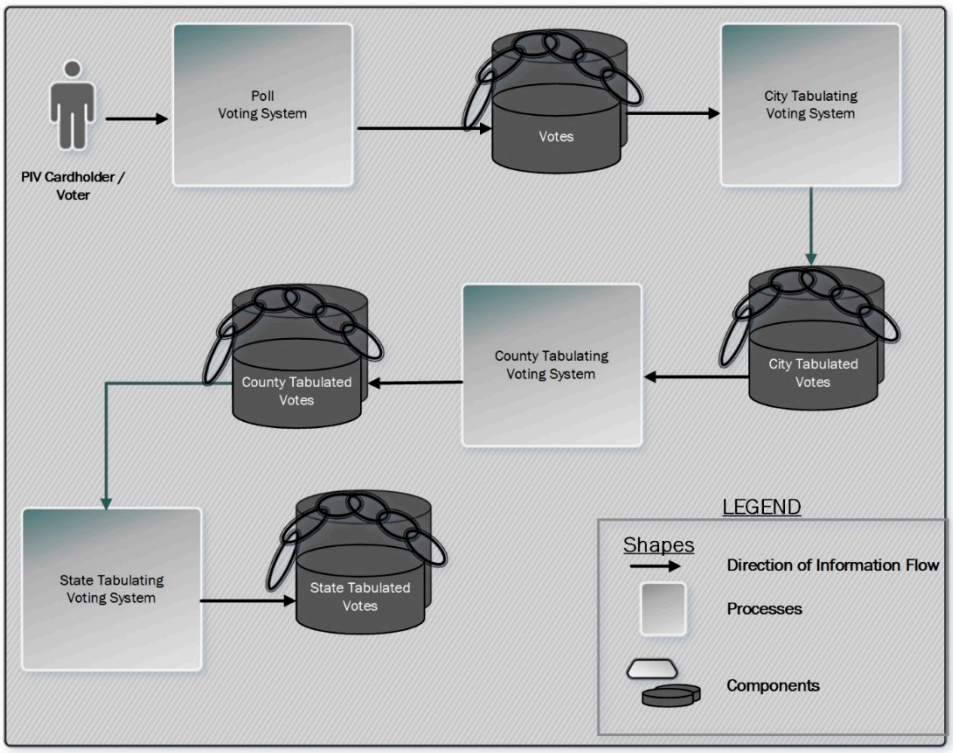

Figure 2. BPES city, county, and state integration.

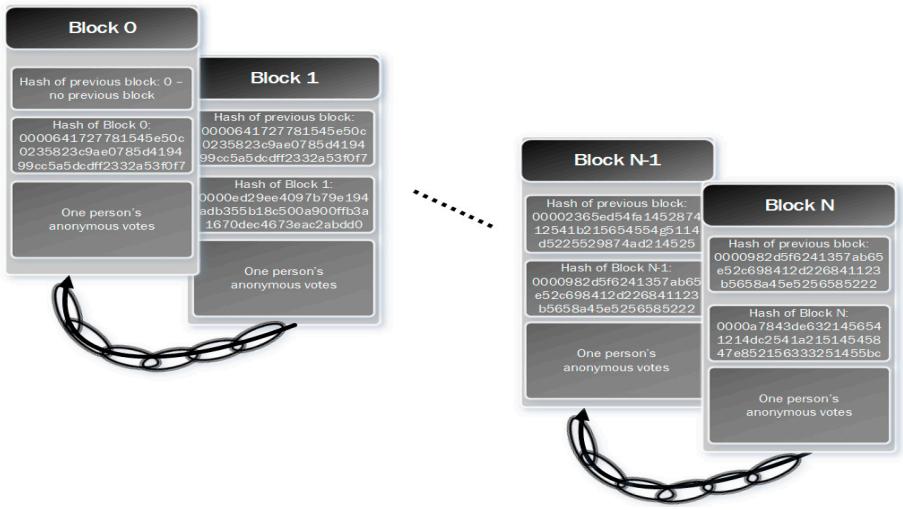

Figure 3. An example of the BPES blockchain.

BPES relies on a distributed system shown in Figure 4, with each system having a trusted ICAM digital ID all working interdependently. A central system maintains the tallies as necessary on each level with each central system forming another distributed system at

the higher levels. This allows each system to retain a certain amount of independence while still functioning as a whole for a county, state, or national system. Not only does BPES provide a means for the autonomy of city, state, and federal entities but it also provides a means for trust and verification by city, state, and federal entities as well. The BPES provides the validation of a tamper-proof election through encryption.

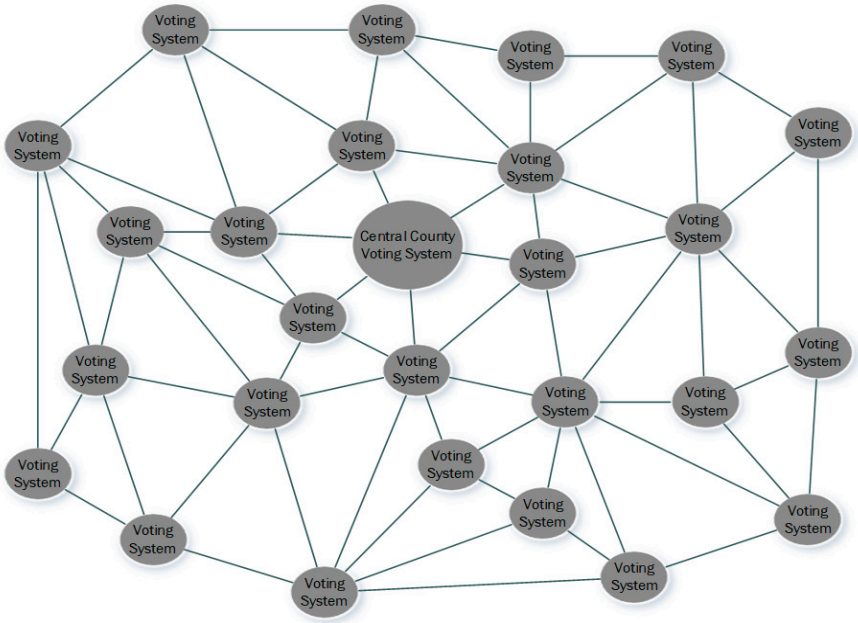

Figure 4. Distributed online e-voting within a county as well as in-person voting working simultaneously.

The state voting system would look much like Figure 2 but would consist of a distributed system made of the central blockchain-based PKI e-voting system from each county within the state. Each county's central system would keep their county's particular votes and send on to the state's central system the state and federal votes. Then, the state's central system would keep that state's particular votes and send on to the federal central system that state's votes. This would work for any nation state, but using the US as an example, all 50 states' BPES central systems would form an additional distributed system at the federal level, systems within systems that function interpedently.

This enables the BPES to provide full functionality with all IoT things because ICAM ensures that the same security mechanisms that an employer has on their premises, for example, are utilized when their employees are teleworking. Therefore, utilizing ICAM with BPES guarantees the same level of security that is in place while voting in person is there when voting online regardless of the device used to cast a vote. A cryptographic challenge response protocol based on PKC and PKI has been developed for protecting NFC tags from attacks. This proposed framework consists of using symmetric cryptography [27]. A digital identity given to an e-voting system within a blockchain-based PKI such as BPES ensures the confidentiality, integrity, availability, and traceability of online voting. Several experiments are being conducted with blockchain e-voting systems, but there are several concerns with a purely blockchain voting system [24]. A blockchain-based PKI provides the trusted digital identity lacking in a blockchain-only e-voting system. Utilizing the ICAM framework, a city/county can gather their election results. There would be a variety of polling places across the county collecting citizens' votes. The ICAM system, following all of the tenets of the framework, would be the frontend that would confirm a person's identity online. Each polling location system would digitally sign the blockchain, adding another layer of defense to the blockchain-based PKI e-voting machine, whether it be an online system or within a physical location for in-person voting. The system would work seamlessly both for in-person and online voting.

6. Security within the System

Java card is an industry standard technology platform developed by Sun Microsystems (now Oracle) to enable Java-based applications that run on smart cards. These Java-based applications are called applets. Java card helps developers build, test, and deploy smart-card-based applications quickly and efficiently with an object-oriented programming model and off-the-shelf development tools. Since Java Card 3.0, the card has been extended to support a Web application model with servlets running on the card and TCP/IP as basic protocol. The virtual machine and runtime environment have been upgraded as well to support multithreading and hierarchical class loaders. The Java Card platform can run on contact and contactless devices since it runs on secure elements that power the card emulation mode in NFC. NXP Semiconductors makes a smart card using the Java Card Open Platform (JCOP) operating system. The JCOP operating system has a Java Card Virtual Machine (JCVM). NXP's smart cards are more popular in Europe than in the United States. The most popular smart card using NXP's JCOP is MiFare [33].

Applying digital certificates to online voting systems following the ICAM framework ensures the integrity and availability of each system. The built-in security of modernizing PKI with blockchains ensures that every system can be checked for fraud and the tampering of a citizen's vote. In the traditional method of voting, citizens must show identification to vote. If traditional methods of identification such as driver's license and passport were updated using a Java Card that has a digital certificate, then citizens could utilize the ICAM Framework to cast their votes online with confidentiality and security. Only the system that verifies the identity, the verification authority, would need to confirm the identity of the citizen to ensure they may vote and vote only once; then, the voting system would ensure the confidentiality of the vote by only recording the votes with no identities attached. Again, the votes would be secured and stored within the system using blockchain-based PKI so that the integrity and security of the registered votes are ensured. Any attempts to alter a blockchain would be easily detected and the blockchain technology would revert to the untampered, originally cast vote.

7. Conclusions and Future Work

If an e-voting system is to be trusted, government and industry must make an investment to updating cyberspace and voting systems that will instill confidence. The internet must reform for the modern age. The technical solution for a public infrastructure that creates a trusted cyberspace requires a collaboration of many people, organizations, industry, and governments across the globe. Public key cryptography provides everything we need to securely communicate with other identities. The public keys give us confidentiality and integrity of data. Successfully implementing a digital identity using a public key requires a public key infrastructure. No one trusts their competitor's PKI system [34].

An updated blockchain-based PKI founded on the ICAM framework [20] provides the governance necessary for digital credentials that establish a confidence level that government, industry, and the public will trust. The world wants reliable online and mobile environments. Confidence is at the root of a heterogeneous environment, but action must be taken that does not break the existing systems in use. Remote identity authentication needs assurance that the identification of an individual is authentic. The path has been identified, and now that path must be followed through a collaboration of industries, governments, and individuals around the globe.

Future work would require utilizing the tools and technologies available at our disposal today to instantiate an ICAM authentication and authorization system that has a trusted digital identity. The ICAM system provides the foundation that BPES can then be built upon. These are all key steps that will ensure accurate and trustworthy vote counts.

Author Contributions: Conceptualization: R.C. and S.B.; Methodology: R.C.; Software, R.C.; Validation, R.C. and S.B., Formal Analysis, R.C.; Investigation, R.C.; Resources, R.C.; Data Curation, R.C.; Writing—original draft preparation, R.C.; Writing—reviewing and editing, S.B.; Visualization—R.C.

and S.B.; Supervision—S.B.; Project Administration—S.B. and R.C.; Funding Acquisition—NA. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Isaacs-Thomas, I. How Risky Is in Person Voting? Here's How to Navigate Your Options during a Pandemic. Available online: https://www.pbs.org/newshour/health/how-risky-is-voting-in-person-heres-how-to-navigate-your-options-during-the-pandemic (accessed on 29 December 2020).
2. Graham, J. No, You Can't Vote for the President Online. Here's Why. Available online: https://www.usatoday.com/story/tech/2016/11/08/why-cant-we-vote-president-online/93454572/ (accessed on 29 December 2020).
3. Branaccio, D.; Shin, D.; Soderstrom, E. Why Aren't We Voting Online? Available online: https://www.marketplace.org/2020/11/02/online-voting-election-hacking-attempts-malware-internet-connection/ (accessed on 29 December 2020).
4. Carnley, P.R. *Mobile Identity, Credential, and Access Management Framework*; Dakota State University: Madison, SD, USA, 2020.
5. Matsumoto, S.; Reischuk, R.M.; Szalachowski, P.; Kim, R.H.; Perrig, A. Authentication challenges in a global environment. *ACM Trans. Priv. Secur.* **2017**, *20*, 1–34. [CrossRef]
6. Gates, M. *Blockchain: Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money*; Wise Fox Publishing: London, UK, 2017.
7. Bashir, I. *Mastering Blockchain*, 2nd ed.; Packt Publishing Ltd.: Birminghan, UK, 2018.
8. *Ethereum, Bitcoin, Blockchain, and Cryptocurrencies Resources*; Wise Fox Publishing: London, UK, 2018.
9. Paar, C.; Pelzl, J. *Understanding Cryptography*; Springer: New York, NY, USA, 2010.
10. Adams, C.; Lloyd, S. *Understanding PKI Concepts, Standards, and Deployment Considerations*; Pearson Education, Inc.: Boston, MA, USA, 2003.
11. Batten, L.M. *Public Key Cryptography*; Wiley: Piscataway, NJ, USA, 2012.
12. Mayes, K.; Markantonakis, K. *Smart Cards, Tokens, Security, and Applications*, 2nd ed.; Springer: Cham, Switzerland, 2017.
13. Grassi, P.A.; Fenton, J.L.; Lefkovitz, N.B.; Choong, Y.-Y.; Greene, K.K.; Danker, J.M.; Theofanos, M.F. NIST Special Publication 800-63A. Available online: https://doi.org/10.6028/NIST.SP.800-63a (accessed on 1 June 2017). [CrossRef]
14. Ballad, B.; Ballad, T.; Banks, E.K. *Access Control, Authenticatin, and Public Key Infrastructure*; Sudbury, M.A., Ed.; Jones & Bartlett Learning, LLC: Burlington, MA, USA, 2011.
15. NIST. *Draft (2nd) NIST Special Publication 800-207 Zero Trust Architecture*; U.S. Department of Commerce: Washington, DC, USA, 2019.
16. Allen, J. What is 5G and Is it for Me? *Am. J. Fam. Law* **2020**, *14*, 63–66.
17. Madhusanka Liyanage, I.A. *A Comprehensive Guide to 5G Security*; John Wiley & Sons Ltd.: Hoboken, NJ, USA, 2018.
18. Rivera, R.; Robledo, J.G.; Larios, V.M.; Avalos, J.M. How Digital Identity on Blockchain can contribute in a smart city environment. In Proceedings of the 2017 International Smart Cities Conference (ISC2), Wuxi, China, 14–17 September 2017; pp. 1–4.
19. Rahoof, P.N.L.I.T. Trust structure in public key infrastructure. In Proceedings of the 2017 2nd International Conference on Anti-Cyber Crimes, Abha, Saudi Arabia, 24 April 2017.
20. Carnley, P.R.; Rowland, P.; Bishop, D.; Bagui, S.; Miller, M. Trusted Digital Identities for Mobile Devices. In Proceedings of the 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Calgary, AB, Canada, 17–22 August 2020.
21. Rosasooria, Y.; Mahamad, A.K.; Saon, S.; Mat Isa, M.A.; Yamaguchi, S.; Ahmadon, M.A. E-Voting on Blockchain using Solidity Language. In Proceedings of the 2020 Third International Conference on Vocational Education and Electrical Engineering (ICVEE), Surabaya, Indonesia, 3–4 October 2020.
22. Tas, R.; Tanrıöver, Ö.Ö. A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting. *Symmetry* **2020**, *12*, 1328. [CrossRef]
23. Hjálmarsson, F.Þ.; Hreiðarsson, G.K.; Hamdaqa, M.; Hjálmtýsson, G. Blockchain-Based E-Voting System. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018.
24. Bellini, E.; Ceravolo, P.; Damiani, E. Blockchain-Based E-Vote-as-a-Service. In Proceedings of the 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), Milan, Italy, 8–13 July 2019.
25. Rathee, G.; Iqbal, R.; Waqar, O.; Bashir, A.K. On the design and Implementation of a Blockchain Enabled E-voting Application within IoT-Oriented Smart Cities. *IEEE Access* **2021**, *9*, 34166–34178. [CrossRef]
26. Pandey, A.; Bhasi, M.; Chandrasekaran, K. VoteChain: A Blockchain Based E-Voting System. In Proceedings of the 2019 Global Conference for Advancement in Technology (GCAT), Bangalore, India, 18–20 October 2019.

27. Matsumoto, S.; Reischuk, R.M. IKP: Turning PKI around with decentralized automated incentives. In Proceedings of the 2017 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 22–26 May 2017; pp. 410–426.
28. Robey, C. Whom do you trust? Part 2 blockchain technology & smart contracting. *Contract Manag.* **2017**, *57*, 18–27.
29. Kshetri, N. Can blockchain stregthen the internet of things. *IT Prof.* **2017**, *19*, 68–72. [CrossRef]
30. Singla, A.; Bertino, E. Blockchain-based PKI solutions for IOT. In Proceedings of the 2018 IEEE 4th International Conference on Collaboration and Internet Computing, Philadelphia, PA, USA, 18–20 October 2018; pp. 9–15.
31. Al-Maaitah, S.; Qatawneh, M.; Quzmar, A. EVoting System Based on Blockchain Technology: A Survey. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 200–205.
32. Kumar, R.; Sharma, R. Leveraging blockchain for ensuring trust in IoT: A survey. *J. King Saud Univ. Comput. Inf. Sci.* **2021**, *in press*. [CrossRef]
33. NXP. Products. Available online: https://www.nxp.com/ (accessed on 25 September 2019).
34. Stokkink, Q.; Pouwelse, J. Deployment of a Blockchain-Based Self-Sovereign Identity. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1–7.