IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 9, Issue 9, September 2020

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

Securing Government Services; Blockchain Strategy in the course of Pandemics

Hussam Elbehiery[1], Khaled Elbehiery[2]

Associate Professor, Department of Computer Science, October 6 University (O6U), Egypt[1]

Professor, Department of Computer Information Systems, Park University, USA[2]

ABSTRACT: Early 2020 has seen the emergence of coronavirus or COVID-19 outbreak, the sudden explosion and uncontrolled worldwide spread have shown the limitations of existing healthcare systems to timely handle public health emergencies, fortunately, innovative technologies such as blockchain and Artificial Intelligence (AI) have emerged as a promising solution to help fighting the pandemic situation. Blockchain helps with protecting user privacy and ensuring reliable medical supply chain during the outbreak tracking, but with the predicting behavior of than the human mind of AI, the outcome is almost accurate early detection of the outbreak. This paper is a manifestation of an extensive survey on the use of blockchain and AI together for combating coronavirus (COVID-19) as a pandemic situation and epidemic as well. The research paper begins with a survey of the recent on fighting the coronavirus utilizing blockchain and AI in a wide range of applications, followed by an introduction to a new conceptual architecture and highlighting the key solutions that integrates blockchain and AI focusing on coronavirus situation supported by a case study. And lastly, we shed some lights on the challenges that might be encountered and the guidelines to deal with the same circumstances or even worse in the future.

KEYWORDS: Digital Transformation, e-ID, Digital Identity, eGovernment Services, Business Intelligence, Coronavirus, E-Voting, Cybersecurity, Critical Infrastructure, and Blockchain.

I. INTRODUCTION

Technology is evolving exponentially and it is no longer something separate from everyday life with the goal to improve the way our devices and systems communicate, cybersecurity on the other hand is one of the biggest bridges yet to cross. Developing technologies are pioneered by the private sector, the public sector represented in the local or state government could harness these technologies to deliver beneficial services that improve citizens' lives in different approaches such as:

- Provide services more effectively and efficiently
- Find new solutions to policy challenges
- Commercialize some public services and develop fresh sources of revenue.
- Facing the new pandemics like COVID-19

The Digital transformation is not just about new technologies, but it requires an overhaul of organizational structures, governance, work processes, culture, and mindset, in addition to securing those services with a strong cybersecurity infrastructure. To create this qualified digitally enabled public sector, governments have five critical areas to consider:

1.1 Customer Experience

Governments need to reimagine how digital transformationcan be used to enhance the citizen's end-to-end experience of public services. This requires the adoption of a 'citizen-first' culture and mindset in designing policies and delivering services. The ultimate goal is to improve service quality, promote transparent and efficient interaction, enhance the level of public trust in government, and drive better citizen outcomes. Social media and mobile platforms are replacing traditional channels as a means to interact with government, report concerns and provide feedback. Artificial intelligence (AI) can help deliver services to citizens, using chatbots to complete transactions within government websites. It can help improve urban planning by optimizing routes for transport operators, reducing commuters' journey times; provide educational support to students based on their individual learning needs; and enable online self-referral and screening, signposting citizens to social services based on their needs and eligibility.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

1.2 Public Value

In an environment of uncertain growth and rising demand, governments must find sustainable ways to finance public services and infrastructure to optimize the return on public investment.Digital technologies create opportunities to explore new models for providing services, improve management of resources through smarter spending, and link the money invested in programs and services to the outcomes they produce for citizens, boosting accountability and trust. Blockchain technology can help track how money is spent through the system. Predictive analytics and text mining can make an important contribution to the smart management of public resources by anticipating problems and enabling preventative action — for example, identifying taxpayers at risk of nonpayment.

1.3 National Security

The threats from terrorist groups and other non-state actors are increasing and made more complex through digital technology. Today, conflicts are waged not only on the battlefield but on public transport, on social media and in cyberspace. Governments have a responsibility to safeguard their citizens from a whole range of threats, enabling them to live and work without fear. Digitalization is both a hindrance and a help in this struggle. As governments embrace digital technologies and become more interconnected with partner organizations and smart devices, new vulnerabilities arise that can be exploited by cyber attackers. Terrorists, fraudsters and hackers can jeopardize the delivery of essential public services and the smooth running of civil society, including the election process. On the other hand, digital technologies and better data sharing provide a sophisticated means of combating threats. Defense organizations are investing in AI and machine learning; cyber weapons and threat detection programs; cybersecurity apparatus; robotics and digital tools to make them nimbler and more effective. Governments are introducing information security management systems to safeguard the data they keep and increasingly rely on. Governments must also exploit the power of cloud computing to increase their own computing capacity, support secure biometric identification programs and provide safe payment platforms for citizen transactions.

1.4 Future Workforce

Economic growth, social cohesion and equality of opportunity rely on a country's workforce being skilled and ready to embrace the needs of 21st-century employers. Governments need to build the skills and capabilities of their own employees in order to drive greater efficiencies, elevate customer focus and strengthen diversity and inclusion.
Mobile technologies can help agencies empower their workforce to do their jobs more effectively. As a high proportion of public sector employees regularly work outside the office, they can be equipped with devices such as smartphones, tablets, and laptops to perform their duties wherever they're located.While governments prepare their own workforces for the digital age, technological changes such as automation and AI have far-reaching implications for the future of work, economies and society in general. Governments must adopt, update and strengthen policies to mitigate adverse social and economic consequences — such as the displacement of workers in some lower-skilled jobs, and widening social inequality.

1.5 Smart Infrastructure

Many of today's most fundamental challenges — urbanization, globalization, pollution, water shortages and climate change — can be tackled with smart infrastructure developments such as connected cars, electric vehicles, smart power grids, energy-efficient buildings, Internet of Things (IoT) networks and open data portals. Many emerging countries need new infrastructure to support their growing populations and increased economic activity, while mature markets must renew deteriorating or inefficient infrastructure. Smart infrastructure offers a way to harness the latest technologies to obtain maximum value and efficiency and create resilience and sustainability. Governments must also pursue policies to encourage a thriving digital economy. This involves working with private businesses to provide enhanced 4G and forthcoming 5G networks, and data centers; create high digital literacy among citizens; promote digital inclusion; and enable secure access to services, through digital identification systems [1].

II. DIGITAL GOVERNMENTAL SERVICES

While individuals can use traditional forms of identification in face-to-face transactions, these forms of identification are less useful for conducting business on the Internet. To address this challenge, many governments are creating national electronic identification (e-ID) systems—a collection of technologies and policies that enable individuals to electronically prove their identity or an attribute about their identity to an information system. These systems can help reduce identity theft and enable individuals to use online applications more securely in a variety of industries such as health care and banking. Individuals can use an e-ID to authenticate to online services, securely communicate online, purchase goods and services, and create legally-binding electronic signatures, such as to sign a contract. Businesses can

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

use identity management functions to better interact with their customers on the Internet, such as to authenticate users to online applications or to verify the ages of their customers.
Finally, government can use e-IDs to streamline egovernment services, allow individuals to sign and submit forms online, and offer innovative services.A national e-ID system will provide a platform for the public and private sectors to develop a wide array of innovative and productivity-enhancing products and services online that require one's identity, or an aspect of one's identity to be confirmed. Policymakers should embrace the opportunity to create an innovation-driven approach to a national e-ID system that balances competing interests, improves privacy and security for users, and combines the strengths of both the public and private sector.

2.1 Benefits of e-ID Systems

Reducing duplication and multiple identities Building an ID system can help eliminate multiple functional identities, or credentials issued by different government departments or agencies, for voting, paying taxes, or accessing social benefits. Further, data on target beneficiaries from a complete and reliable ID register can be shared with select departments or agencies to ensure the efficient and inclusive delivery of social and economic services at different levels of administration. The linking mechanism between national ID and Civil Registration and Vital Statistics (CRVS) systems varies between countries and depends on three main factors: Scope of population coverage, Organization, and Digitization. Various countries have adopted different approaches and business processes to successfully link their CRVS and national ID systems. Fig. 1 offers a visual representation of a national ID system as a water tank with inlet and outlet taps used to update information on births and deaths. In the interest of completeness, national ID systems should also include people migrating in and out of the country [2].

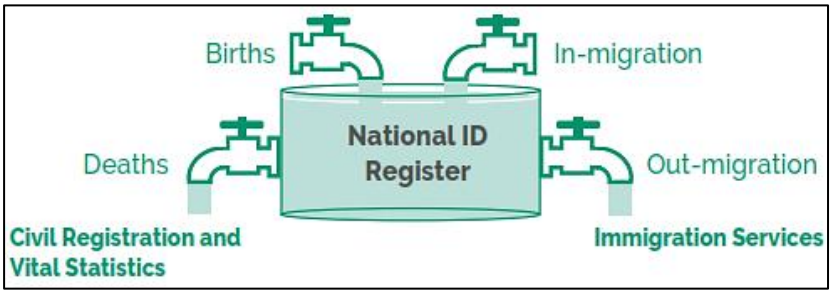

Fig. 1, Visual representation of a national ID system with update mechanisms

2.2 Digital Government Services

Digital government services (also called e-government) are defined as service delivery within government — as well as between government and the public — using information and communication technologies. When implementing digital services, innovators can meet challenges, but these challenges are easily overcome and quickly replaced by benefits, which include:

- Better online user experiences for citizens.
- Increased public participation.
- Improved internal efficiency and productivity.
- Less burden on IT
- Better collaboration among departments.
- Reduced labor costs.

Government staff can think and act proactively on other strategic initiatives and no longer bound to a phone or service desk. For example, they can invest time streamlining procurement and approval processes, improving recruitment and hiring, and incorporating technology standards [3].

2.3 Digital Government Strategy 2020 transforming with equity

The Digital Government Strategy (DGS) should contain all the different objectives and initiatives to comprehensively advance to the digital transformation. The DGS is a dynamic and flexible map for digital transformation and innovation aiming at strengthening the relationship between citizens and the Government [4]. (See Fig. 2)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

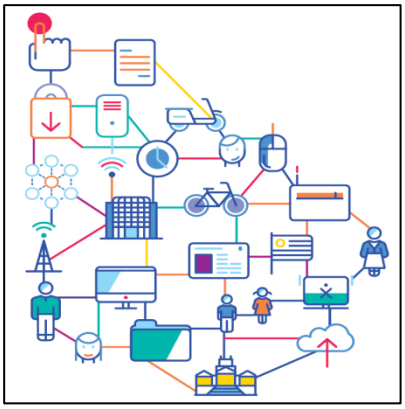

Fig. 2, Representation of the Digital Government Strategy

Digital government will help make public institutions more inclusive, effective, accountable, and transparent. However, against this backdrop of increasing digitization, there are substantial regional disparities. In many countries, the digital divide persists, or is even growing wider. At every stage of digital development, governments have to overcome barriers to success. These include both technical and cultural challenges that hinder collaboration within and between government organizations at local and national levels. The challenges also include financing and security issues. Government budgets are chronically constrained, so effective financing models need to be found for digital projects. Smaller projects, such as online license applications, with a clear revenue or cost-saving strategy and minimal upfront investment, are more likely to be successful.

Protecting the personal data and privacy of citizens is critical in digital government projects, because this is the key to user trust. Data protection is both a policy issue – e.g. the passing of privacy legislation – and a question of deploying the most advanced security technologies. Governments are more likely to be successful when they have a vision for future development, and can see money spent on digitization as an investment, rather than a cost. Governments with limited funds should consider making digital infrastructure a priority, and see digital transformation as a long-term growth strategy. Digital governments and societies will succeed in the long term when they set clear policies, invest in ICT infrastructure, adopt open platforms, and secure participation from both the public and private sectors [5].

Many technological agencies and companies help today's governments transition and transform their underlying processes, capabilities, and technologies to accelerate government innovation. The transition to digital government is supported by essential services of these companies which can provide built upon a strong foundation of IT governance [6]:

- Infrastructure services in a hybrid IT environment that leverages public cloud, private cloud, and dedicated IT infrastructure assets and security. The technological companies can provide market leading offerings and services to support any mix within a Hybrid IT environment.
- Application development with mobility services that provide users with seamless access to applications and data anytime, anywhere, and on multiple devices.
- Advanced data analytics that exploit growing stores of data to improve citizen services, operational efficiencies, and mission performance. (See Fig. 3)

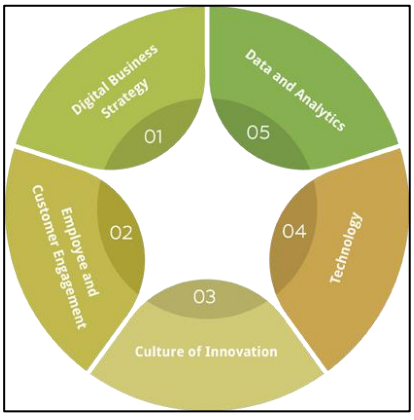

Fig. 3, Essential Elements of Digital Transformation

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

Digital transformation requires enabling the culture of innovation in the work environment, and includes changing the basic components of work, from its infrastructure, operating models, to marketing of services [7]. (See Fig. 4)

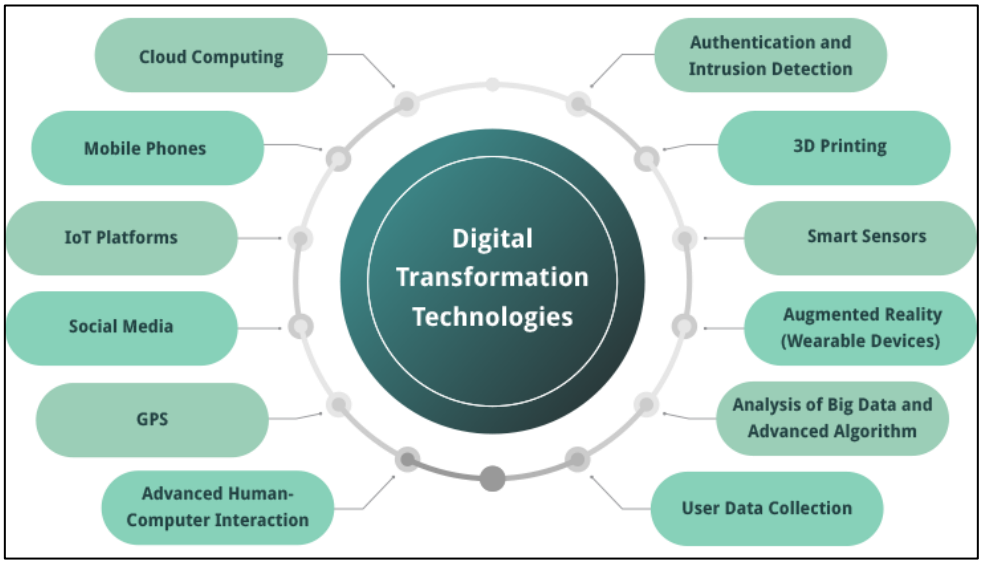

Fig. 4, Digital Transformation Techniques

III. Business Intelligence and Government Agencies

Information and communication technologies bring considerable benefits to government agencies, including better service delivery to citizens, improved interactions with business and industry, citizen empowerment through access to information, and more efficient government management. BI is able to support the decision-making processes and enhance operations. Experience shows that integrating BI into government agencies and public administration units can result in benefits:

- **Integrated data sources;** A data warehouse facilitates access to integrated data.
- **Classification;**Classification means structuring unclassified data and can be achieved using cluster analysis (a data mining technique).
- **Predictions;**Predictions and forecasts can be made using various mining techniques (e.g., regression analysis) that utilize data stored in the data warehouse.
- **Pervasive Analytics;**It is important to provide BI to administrative decision makers throughout the organization in order to support decision making.

The CAPMAS data warehouse environment is shown in Figure 5. The major components include the ETL (extract, transform, load (ETL)) server, Teradata data warehouse platform, and MicroStrategy Intelligence Server [8]. (See Fig. 5)

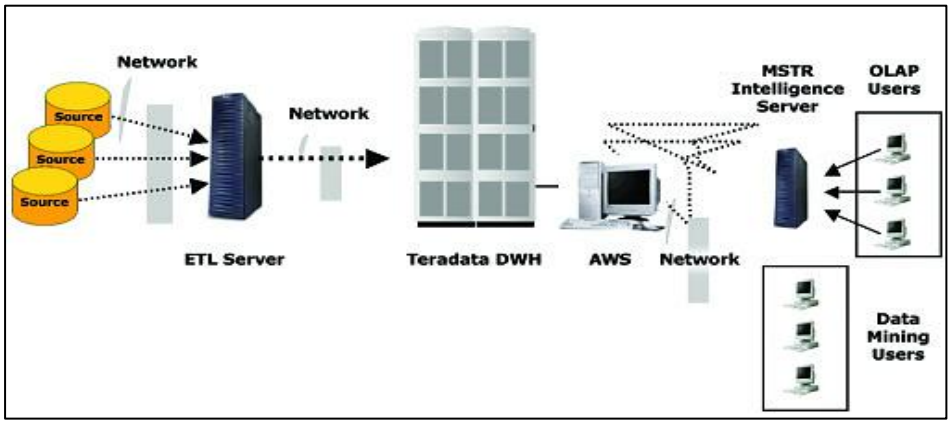

Fig. 5, Business Intelligence Systems Components

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

Fortunately, new technologies are emerging, improving the ability, speed and efficiency of the identity management systems, allowing companies to eliminate unnecessary processes and paperwork and improving the customer experience. Some of the most relevant are:

- **"Big data" Technologies,** including cloud computing and data processing engines, allow companies to have a centralized infrastructure able to gather, classify and store vast amounts of information.
- **Biometrics** improve the ability to validate, with a high level of certainty, a client's identity, allowing for automated onboarding and remote access to services. This technology enables automated recognition of users based on their physical (fingerprints, veins, iris) and/or behavioral characteristics (voice, keystroke and signature recognition). Valued at US$5 billion in 2010, the global biometrics market is growing at a CAGR of 18.5%, and is predicted to reach US$17 billion by the end of 2017.
- **AI and Machine Learning** are helping companies to identify complex patterns and relationships and use unstructured data sources to detect suspicious activities in a precise way.
- **Distributed ledger Technology** could be used to centralize identity attributes storage and sharing among different firms. This system could allow the sharing of some sensitive individual data (the ones the user chooses) across several entities without compromising private information.

IV. CYBER SECURITY AND CRITICAL INFRASTRUCTURE

Cybersecurity and Infrastructure Security Agency (CISA) as the nation's risk advisor, brings the partners in industry and the full power of the country government together to improve American cyber and infrastructure security. Since the beginning of the Coronavirus threat, also known as COVID-19, CISA has been monitoring the evolving virus closely, taking part in interagency and industry coordination calls, and working with critical infrastructure partners to prepare for possible disruptions to critical infrastructure. CISA continues to work closely with governmental partners to prepare the nation for possible impacts of a COVID-19 outbreak.

Functioning critical infrastructure is particularly important during the COVID-19 response for both public health and safety as well as community well-being. The guidance instructions is to support state, local, and industry partners in identifying the critical infrastructure sectors, and the essential workers needed to maintain the services and functions people depend on daily, as well as the ability to operate resiliently during the COVID-19 pandemic response. (See Fig. 6)

Fig. 6, Essential Critical Infrastructure Workers

Risk Management for Novel Coronavirus (COVID-19) provides executives a tool to help them think through physical, supply chain, and cybersecurity issues that may arise from the spread of COVID-19. On March 2020 released an alert reminding individuals to remain vigilant for scams related to COVID-19. Then on March 2020 too, released an alert encouraging organizations to adopt a heightened state of cybersecurity urging organizations to adopt a heightened state of cybersecurity when considering alternate workplace options for their employees. Remote work options—or telework—require an enterprise virtual private network (VPN) solution to connect employees to an organization's information technology (IT) network [9] and [10].

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

V. DIGITAL IDENTITY

Blockchain enables more secure management and storage of digital identities by providing unified, interoperable, and tamper-proof infrastructure with key benefits to enterprises, users, and IoT management systems.

- **For Companies;** Companies often collect sensitive information about their users and store them alongside less-sensitive routine business data. This creates new business risks with the rise of user privacy-centric regulations such as GDPR and the shifting industry focus to corporate IT responsibility.
- **For IoT Devices;** There are about 7 billion internet-connected devices. This number has been grown to 10 billion by 2020 and 22 billion by 2025. Interconnected internet of things (IoT) devices and objects must identify sensors, monitors, and devices, and manage access to sensitive and non-sensitive data in a secure manner.
- **For Individuals;** Identity is integral to a functioning society and economy. These data points are issued by centralized entities (governments) and are stored in centralized databases (central government servers). The inability to attain identification documentation jeopardizes a person's access to the financial system and in turn, limits their freedom.

Identification (or registration) is the process whereby an institution creates and/or records an individual's official identity. Often, though not always, this process includes issuing identity documents (IDs) or other tokens. Once an official identity exists and has been recorded, individuals can then authenticate or verify their identities using their unique identifiers or documents (See Fig. 7 for a common model of identification).

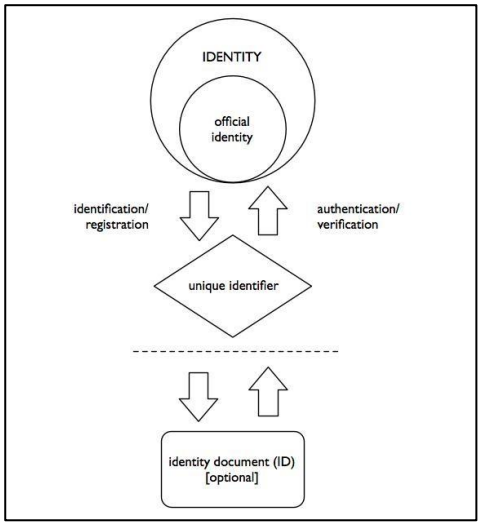

Fig. 7, Common Identification Model

Authentication refers to the process of answering the question "Is that person who he says he is?" Authentication occurs by verifying the credentials offered by an individual. Signing refers to process of attributing an identity to a specific transaction. An example of this would be a user appending his or her name to the end of an email agreeing to a transaction with another user [11].

5.1 Blockchain for Identity

Blockchain identity management systems could be used to eradicate current identity issues such as: Inaccessibility, Data insecurity, and Fraudulent identities.

- **Inaccessibility;** Approximately 1.1 billion people around the world have no proof of identity, and 45% of those without an identity are among the poorest 20% on the planet. Having an identity is crucial to gaining access to the existing financial system. Conversely, 60% of the 2.7 billion unbanked people already own mobile phones, which paves the way for blockchain-based mobile identity solutions which better suit the needs of vulnerable citizens.
- **Data Insecurity;** Large, centralized systems containing the personally identifiable information (PII) of millions of user accounts are incredibly appealing to hackers. A recent study shows that personally identifiable information is the most targeted data for breaches, comprising 97% of all breaches in 2018. Despite regulatory

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

legislation and enterprise efforts to increase cybersecurity, 2.8 billion consumer data records were exposed at an estimated cost of more than $654 billion in 2018.

- **Fraudulent Identities;** Users juggle various identities associated with their usernames across different websites. Furthermore, the weak link between digital and offline identities makes it relatively easy to create fake identities.

Due to the increasing sophistication of smartphones, advances in cryptography and the advent of blockchain technology, the tools to build new identity management systems become real and applicable.Blockchain can help in improving government initiatives processes in some ways as:

- **Improved Efficiency;** By enabling seamless access to information over a distributed database, Blockchain presents a perfect remedy to these problems.
- **Transparency;** When data is stored on a Blockchain, every stakeholder will have direct access. Moreover, it becomes virtually tamper-proof. This has two major implications. One, we as citizens have more visibility of the system. Two, it significantly brings down the risks of corruption, frauds, and scams.
- **Data Safety;** Blockchain distributes the data among participating nodes that can be located at different places across the globe, making data breach almost impossible. Moreover, using private keys, we are able to take control of our data and its privacy.
- **Cost Reduction;** Implementing blockchain in government would rule out the need for intermediary institutions and third-parties. Consequently, we would benefit from a significant reduction in the overall governance cost.

Despite the anticipated, and already realized, benefits of adopting blockchain for government, there are certain obstacles to the same. These issues have hindered the mainstreaming of the otherwise beneficial blockchain government initiatives. Some of the major issues in this respect include the following: Scalability, Risk of private-key theft and the consequent data breach, Lack of Blockchain awareness, and Social repercussions of decentralization [12].
Technological innovations have opened up new possibilities for creating, managing, and using identity systems. This includes biometrics, which can be defined as “any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual”. In addition to the commonly-used fingerprints, face prints and iris scans, recent years have seen an increasing range of such features used for identification, including voice prints, retinal scans, vein patterns, tongue prints, lip movements, ear patterns, gait, dynamic signature, DNA, brain waves (EEG) and even butt prints, with the latter two still at an experimental stage [13].
An individual’s primary and stable identification data comprises the identity contract. It can interact with other smart contracts and “uPort” identities. The controller contract is, in some sense, an overseer of the identity contract. Broadly put, it assigns and revokes the authorization of sign statements. Also, it is used to assign a new public key to the identity contract in case the host device is changed. Some of the primary benefits of this system are reduced costs, lower risk of data theft, and control over personal data. (See Fig. 8)

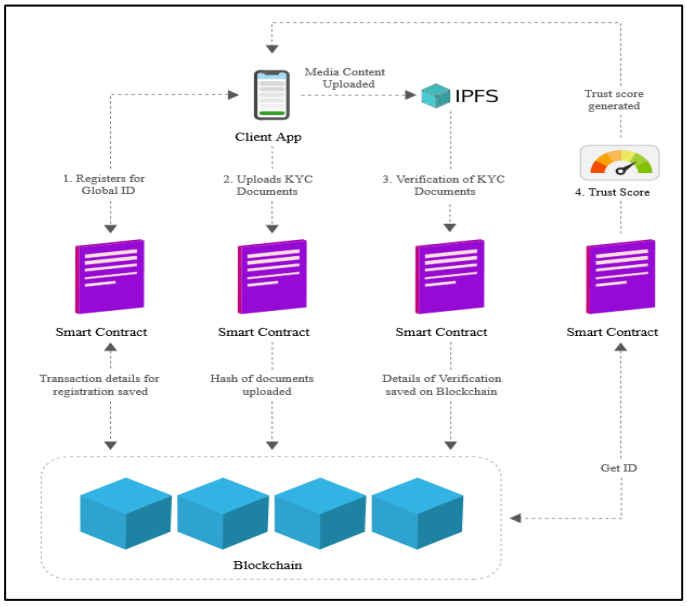

Fig. 8, Blockchain Identity Management

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

Blockchain enables an individual to verify that a product was sourced accurately and ethically. Documentation counterfeiting and fraud are also common among diplomas, certifications, and official identification. Blockchain records can transparently verify certifications, official legal documents, and coordinate record-keeping immutably, which prevents counterfeiting or fraud [14].

5.2 Blockchain inHealthcare and Life Sciences

Healthcare professionals and medical providers in fields including global public health, pharmacology, medicine, and health data are recognizing the advantages of Ethereum blockchain technology to streamline and secure medical data management, drug and medical device tracking, and more. The healthcare industry can greatly benefit from blockchain technology. Because of the inability to securely share data and the siloed management of medical records, patients spend precious time and resources seeking redundant medical care . In emergencies, physicians and other health professionals providing care may not have full visibility over a patient's medical history in which case they risk improper treatment.

In drug traceability, secure supply chain tracking is necessary to prevent the distribution of counterfeit or illicit drugs. Such risks may compromise the safety and success of treatment or lend to addiction and drug dependence. They also carry the risks of unknown side-effects, some of which may be fatal. In order to address illegal transport or unauthorized production of controlled substances, blockchain technology presents the opportunity to securely track, indicate chronology, and highlight identifying data (makeup and composition) of substances in an immutable record. Enterprise Ethereum provides smart contracts and systems interoperability that will revolutionize the industry.

Enterprise Ethereum enables secure data management, consent management, medical device and drug tracking, and other blockchain use cases. Enterprise Ethereum enables secure and structured data sharing among the medical community through decentralized databases. These structures work to protect patient data and privacy, allow doctors visibility over their patients' medical histories, and empower researchers to use shared data to propel scientific progress.Smart contracts on Enterprise Ethereum enable the introduction of micropayments to incentivize specific patient behavior. These contracts can be programmed to release rewards to patients for following a certain treatment plan or sharing their data for clinical research [15].

VI. CORONAVIRUS PANDEMIC

There is a national guidance that applies to most of counties all over the world in 2020 which people should follow the specific rules against that pandemic. The government has set out its plan to return life to as near normal as we can, for as many people as we can, as quickly and fairly as possible in order to safeguard livelihoods, but in a way that continues to protect our communities.

As many of our countries are facing unprecedented challenges from COVID-19 the strain on our governments is extreme. First steps have been to take proactive measures to protect people, and to adjust the timelines for all governmental organizations.

To get things started, governments should encourage people to share examples that may cover some of the following categories [16]:

- Citizen-led community responses, including neighborhood volunteer groups and neighborhood associations, clergy, teachers or others helping to inform the public on the risks and needed steps.
- Participatory disaster response strategies, including working with civil society and citizens.
- Building trust between government and citizens, including through strong communications and focusing on reaching vulnerable communities with the information they need.
- Transparency over forecasting models and data that are influencing government's strategies.
- Digital platforms or apps to keep citizens informed, enable public participation and/or offer open data; Digital tools to enable public participation.
- Digital and/or crowdsourced provision of public and government services.
- Protecting data rights and privacy as corporations help lead the response in many countries.
- Tackling misinformation and disinformation online.
- Publishing proactive information for affected communities, including economic and social support.

6.1 Digital Governmental Services in times of COVID-19 Pandemic crisis

We have seen the importance of adaptation to embrace the new normal. Changes in lifestyle have led to significant developments in digitalization through a modification of perspective at a very fast pace. From companies adapting home office policies and encouraging employees to work from home to businesses offering an extended range of digital services, opportunities to expand into the digital realm have never been so prominent. Many large-scale events have

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

converted to digital alternatives. From digital press conferences to the virtualization of meetings, an increased number of organizations have and will continue to adopt technologies that can help foster effective communication. Additionally, as working remotely becomes more necessary, both employers and employees will think of methods to enhance current processes.

At this moment the drive for innovation is undeniable. The current ecosystem has opened the doors to a range of possibilities and applications to help keep people informed, protected, and safe. Moreover, innovation is particularly imminent within technologies for Governments, which aim to provide advanced solutions for public services and policies. An important backbone of eGovernment Services is a protected individual digital vault, a place in the government's cloud where a person's documents are securely stored and can be retrieved and shared, at different levels, only by and with authorized individuals, companies or institutions. Anna has access to all her official documents by securely accessing her personal vault from her smartphone.

Anyone can schedule an appointment with a specialized doctor from her phone, have a video-appointment, share her past medical records with the doctor, and get an online prescription. A platform for online teaching is already in place. Anna can continue her classes, authenticate herself to take tests, and exchange paperwork with her school or university at any time from her home. Also, a digital form for authentication purposes is available via the app. When an authority officer asks for people's driver's license, she presents a QR code on her app. Once scanned, they can view Anna's driver's license and her personal details on their phones. Thus, no physical contact was necessary. A secure, convenient method for citizens and government authorities to authentication digital identity documents. (see Fig. 9)eServices make sure that even during difficult situations, government-citizen interactions in different sectors and situations are not brought to a standstill [17].

Fig. 9, QR code Authority

6.1.1 e-Governance Ecosystem

It is important to keep in mind that in order to build up an e-Governance ecosystem, appropriate policy frame- works and legislative bases need to be developed by the governments. Here are the primary registries and digitized functions of the government during covid-19:Civil registry, Business registry, Property registry, e-Customs, e-Taxation, Public finance management, Law enforcement and justice, and Unemployment insurance registry. Also, here are the enablers of secure e-governance: Data exchange infrastructure, e-ID, Data integrity, and Data privacy.

6.1.2 e-health

It includes: Hospital information system, e-Prescription, VR solutions for contactless healthcare, Drug shortage alert system, Auditable processing of sensitive data, and Rapid issuance of documents.

6.1.3 e-education

It includes: School management system, Digital content management, Students registry, Higher education and researchers information system.

6.1.4 Smart Mobility and City Planning

It includes: Location intelligence solutions, Connection platforms for health/trade facilities and logistics, Smart on-demand based public transportation platform, Road administration e-services, Public transport payment system, Smart pedestrian crossings, and Self-driving shuttle bus.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

6.1.5 Public Safety

It includes: Public-safety answering, point Catastrophe prevention, and Border services.

6.1.6 Cyber Security

It includes: Threat intelligence, Risk and threat assessment management, Cyber exercises and trainings, Cyber security information fusion and situation awareness, Preparedness procedures, Cyber security operational teams (CSIRT, CSOC), Digital forensics, and Cloud security [18].

6.2 Blockchain Technology and COVID-19

The COVID-19 coronavirus has impacted countries, communities and individuals in countless ways, from school closures to health-care insurance issues not to undermined loss of lives. As governments scramble to address these problems, different solutions based on blockchain technologies have sprung up to help deal with the worldwide health crisis.Therefore, the use of blockchain-enabled platforms can help prevent these pandemics by enabling early detection of epidemics, fast-tracking drug trials, and impact management of outbreaks and treatment. (See Fig. 10)

Fig. 10, COVID-19 coronavirus and Communication effect

With Blockchain we can share any transaction / information, real time, between relevant parties present as nodes in the chain, in a secure and immutable fashion. In this case, had there been a blockchain where WHO, Health Ministry of each country and may be even relevant nodal hospitals of each country, were connected, sharing real time information, about any new communicable disease, then the world might have woken up much earlier. We might have seen travel restrictions given sooner, quarantining policies set sooner and social distancing implemented faster. And may be fewer countries would have got impacted.

What every country is doing now fighting this pandemic, would have been restricted to fewer countries and in a much smaller scale. The usage of a Blockchain to share the information early on, might have saved the world a lot of pain. The world had not seen anything like COVID-19 pandemic before in the recent history. Today we need to take a hard look at the reporting infrastructure available for communicable diseases, both technology and regulations and improve upon that, such that we do not need to face another pandemic like this in the future. (See Fig. 11)

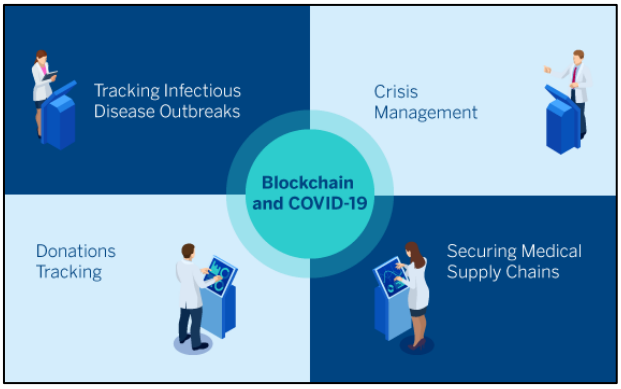

Fig. 11, Blockchain Applications in fighting COVID-19

6.2.1 Major Challenges of COVID-19

- How prepared the world's health systems are to respond to this outbreak.
- Tracking a huge population of infectious patients to stop epidemics.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

- Another is the immediate requirement for developing better diagnostics, vaccines, and targeted therapeutics.
- Misinformation and conspiracy theories spread through social media platforms.
- Various limitations while accessing the tools when required.
- No adequate measures to adopt in a crisis situation.

6.2.2 Donations Tracking

As trust is one of the major issues in donations, Blockchain has a solution for this issue. There has been a concern that the millions of dollars being donated for the public are not being put to use where needed. With the help of blockchain capabilities, donors can see where funds are most urgently required and can track their donations until they are provided with a verification that their contributions have been received to the victims. Blockchain would enable transparency for the general public to understand how their donations have been used and its progress.

6.2.3 Crisis Management

Blockchain could also manage crisis situation. It could instantly alert the public about the Coronavirus by global institutes like the World Health Organization (WHO) using smart contracts concept. (See Fig. 12)
Not only it can alert, but Blockchain could also enable to provide governments with recommendations about how to contain the virus. It could offer a secure platform where all the concerning authorities such as governments, medical professionals, media, health organizations, media, and others can update each other about the situation and prevent it from worsening further.

Fig. 12, Alerting the public about the Coronavirus using the Block chain technology

6.2.4 Securing Medical Supply Chains

The World Health Organization (WHO) is working with blockchain and other tech companies on a program to help convey data about the ongoing COVID-19 pandemic, named MiPasa. The program is a distributed ledger technology (DLT) that will hopefully help with early detection of the virus and identifying carriers and hotspots. MiPasa is built on top of Hyperledger Fabric in partnership with IBM, computer firm Oracle, enterprise blockchain platform HACERA and IT corporation Microsoft. It purports to be “fully private” and share information between need-to-know organizations like state authorities and health officials. (see Fig. 13)

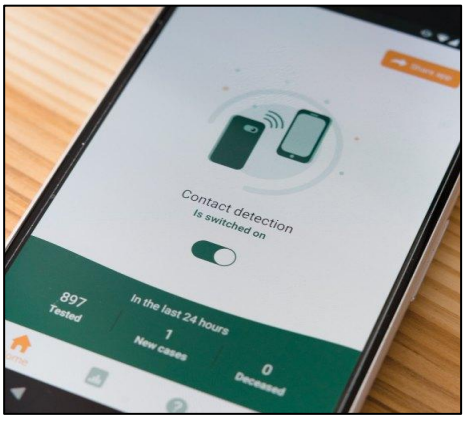

Fig.13, Blockchain for Tracking Public Health Data Surveillance

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

MiPasa cross-references siloed location data with health information. It promises to protect patient privacy and to help monitor local and global trends such as the virus that has now sent the world spiraling into chaos and uncertainty in recent weeks. The U.S., European, and Chinese Centers for Disease Control and Prevention, the Hong Kong Department of Health, the Government of Canada and China's National Health Commission have all worked with the project [19].

6.2.5 COVID-19 Crisis Recovery using Blockchain

The pandemic and the subsequent lockdown have had a negative impact on many industries and we expect a significant slowdown in technology spending, including blockchain. Before the pandemic, International Data Group Inc. (IDC's) Worldwide Blockchain Spending Guide had forecast European blockchain spending of $1.4 billion for 2020 and healthy growth of 58% CAGR to 2023. IDC now expects a number of changes in spending in 2020. Blockchain solutions will see a slight slowdown, with spending decreasing by around 8% in 2020 compared to the previous forecast. Nevertheless, there are some bright spots where blockchain is used to combat the effects of COVID-19 and aid in the recovery process. These innovative use cases can demonstrate the benefits of blockchain to a wider audience.

VII. E-VOTING USING BLOCKCHAIN

Politics, especially elections and voting, have been disrupted by the pandemic. The traditional political process puts politicians, voters, and all those involved in the related services at risk. The recent Wisconsin Democratic primary in the U.S. could have been avoided by using a secure blockchain voting mobile app, though while the proof of concept is there, no dominant solution from a prominent company has emerged from the many tests and pilots.

Smaller countries have made more rapid progress. Estonia remains the go-to example for electronic voting in Europe, but even this system has been criticized for its identity authentication method. Larger countries such as Germany, Finland, Ireland, and the Netherlands have run trials but have subsequently abandoned them. Blockchain technology can alleviate many of the security concerns that have plagued previous e-voting attempts. However, the biggest hurdle remains the general public's skepticism and mistrust of voting using digital technology [20].

An application of blockchain as a service to implement distributed electronic voting systems has been proposed in many countries. The proposed system is a novel electronic voting system based on blockchain that addresses some of the limitations in existing systems and evaluates some of the popular blockchain frameworks for the purpose of constructing a blockchain-based e-voting system. In particular, the potential of distributed ledger technologies through the description of a case study will be evaluated; namely, the process of an election, and the implementation of a blockchain-based application, which improves the security and decreases the cost of hosting a nationwide election.

The objective of such a scheme would be to provide a decentralized architecture to run and support a voting scheme that is open, fair, and independently verifiable. The proposed application is a potential new e-voting protocol that utilizes the blockchain as a transparent ballot box. The protocol has been designed to adhere to fundamental e-voting properties as well as offer a degree of decentralization and allow for the voter to change/update their vote (within the permissible voting period). It stimulates employees and students by saving time and effort from voting anywhere in the home or at work, especially the elderly, who put a lot of effort into voting, making electronic elections more comfortable than paper ones.

There are three countries used e-voting:

- **Italy:** The latest experiment of e-voting in Italy was in October 2017, during the referendum of Lombardy and Veneto to gain autonomy, and traditional polling stations were used in that occasion. However, the case was deeply controversial, because tallying procedures were abnormally slow, even more so than traditional ones, and this also raised suspicion of tampering. Moreover, the regions incurred significant expenses for the hardware, which was not reusable.
- **United States:**The Uniformed and Overseas Citizens Absentee Voting Act of 1986 requires states and territories to allow overseas military personnel and citizens to vote in federal elections. The Military and Overseas Voter Empowerment Act of 2009 amended this law to require delivery of ballots by at least one electronic means (email, fax, or web site). As of September 2016, submission of ballots is done by mail in 18 states; the other states and the District of Columbia allow submission by one or more of email, fax, or secure web site.
- **Hawaii:**Allows email voting by any permanent absentee voter who has not received a ballot within five days of an election Idaho allows email and fax voting in declared emergencies Utah allows email and fax voting for those with disabilities.

There are two countries used e-voting using block chain:

- **Sierra Leone:** Sierra Leone conducted a Blockchain-based voting system and became the first country to become so. Leonardo Gammar of Agora, stored votes in an immutable distributed ledger, thereby offering

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

instant access to the election results. Sierra Leone wished to create an environment of trust and transparency with the voters in a contentious election. By using blockchain as a means to record ballots and results immutably, the country created legitimacy in the election and reduce fall-out from opposition parties.

- **Russia:** Authorities of Moscow planned and launched a blockchain-based electronic voting system pilot project in June 2019. The project was carried out by partnering with the Moscow City Election Commission and Moscow Department of Information Technology (DIT). They provided the required support for the testing of the project. The blockchain-based system is not considered as a replacement for the regular voting system but represents another form of voting which the Muscovites used. The Russian Duma saved the results of e-voting with the help of Distributed Ledger Technology (DLT). This helped in enhancing transparency in elections and eliminating intermediaries in the electoral process [21].

Fig. 14 shows the proposed structure for the E-Voting system based on Blockchain Technology in sequence of six steps.

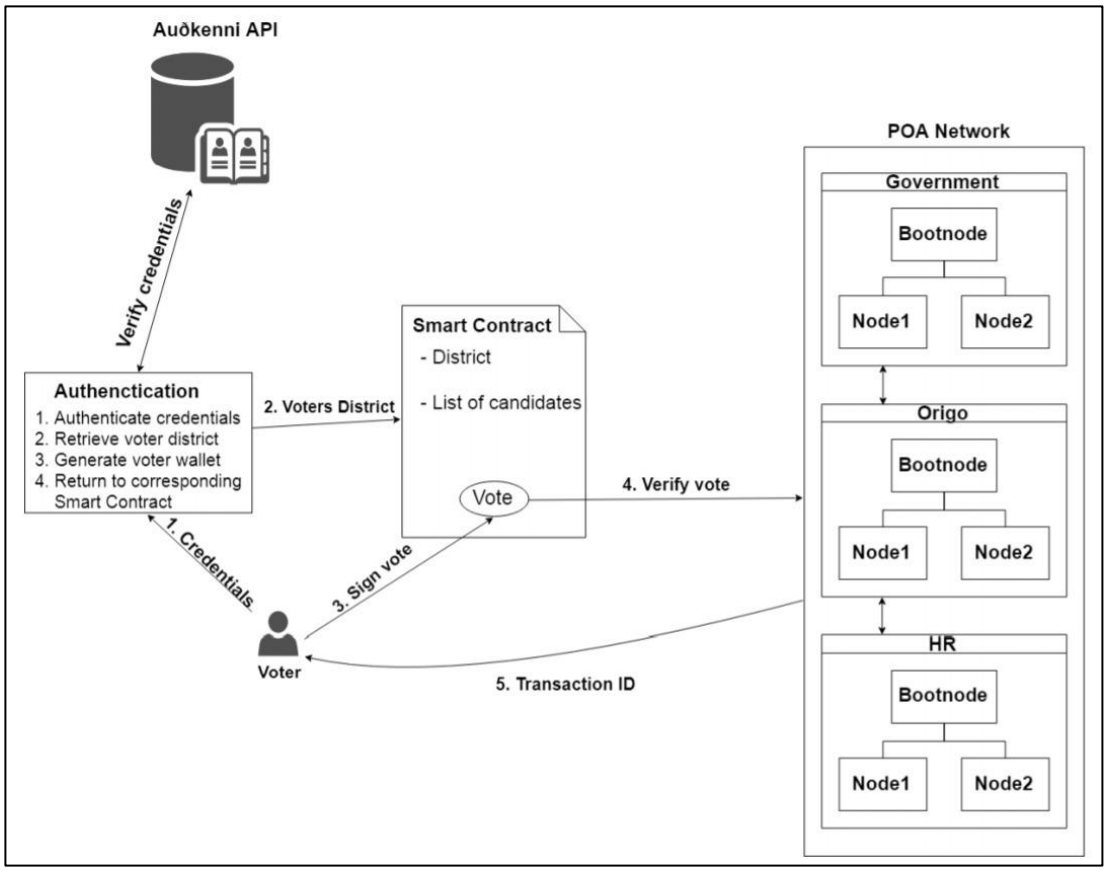

Fig. 14, Proposed Blockchain voting system

- **Step 1: Candidate's registration**
  Candidate can register on the blockchain enabled platform to receive the votes during elections. For registration, candidates need to submit PII (personally identifiable Information), that would be stored on the public blockchain(1). The candidate's information is accessible to every stakeholder involved in the system. The stored details on the blockchain could help voters to know about the candidates and their capabilities before voting. Once the candidate successfully gets registered on the platform, the private key would be generated, enabling candidates to check the number of votes in their account during elections.
- **Step 2: Voter's registration**
  To register on the platform, a voter would need to submit PIIs and proof of their citizenship. And, all these users' information stored in the IPFS(3). The information submitted by the voter would be verified through existing government-approved systems. If the documents are checked and found to be correct, then they are allowed to create their account on the system. After successfully signing up on the system, the private key would be generated and the public key will be saved on the blockchain after getting verified. Using the private key, the voter can cast vote during elections. All the information submitted by the voter is encrypted by the private key.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

Moreover, voters can view the candidate's profile to check his capabilities before casting a ballot. With no doubt, the critical aspect of democracy is the secret ballot; thus it is essential to maintain the anonymity of the voter's vote.

- **Step 3: Voting on Blockchain**
  On the election day, participating candidates can receive the votes in their account on the blockchain voting platform. At the time of elections, every voter needs to login to the platform by using the private key. And, if it's valid, then voter can cast the vote to their choice of candidate. The voter can encrypt their vote with the public key and send it to the Arbitration Server(2), ensuring the voter's anonymity. Meanwhile, the AR(2) is responsible for sending the voter's vote in the form of the voting token to the appropriate node. Each node would verify the transactions according to the regulations built in the Smart Contracts. The Smart Contracts would cross-verifying the votes received with the number of voter's voted in total against all candidates. Casting the ballot on the Blockchain involves sending the voting token to the candidate's account. When the voter logs in the system, they have the limited time period to send the vote to the candidate's account. If they are unable to send votes in the set time period, the smart contract would destroy the voting tokens. The vote stored on the blockchain is verifiable, immutable and transparent.

- **Step 4: Verifying the vote**
  The verification process of the voting depends on the type of elections. Some elections allow for short-term results and some do not. If the election allows for the short-term result, then one of the blockchain's nodes could be made publicly accessible. On the blockchain system, the voter could enter the public key and verify whether their vote was counted. If the election's organizers want to keep a secret result, the voter could only get a binary verification via the arbitration server. But, at the end of the election, the voter will be able to verify whether their vote was counted or not for the election. With blockchain, voters can track their vote and can verify if it ended up in the right candidate's account. Though voter's information is not tied to it, the voting history would be saved on the blockchain.

- **Step 5: Counting the votes**
  Voting could be transparent with the blockchain system as it makes easy to follow and evaluate votes in the real-time. Each voter can vote once for the candidate of their choice. And, the candidate who has the highest number of voting tokens in their account wins the election. For voters who abstained from voting, their voting tokens will be sent to an abstain account, ensuring their vote does not get misused. The counting of the ballots is so easy and can declare the winner of the election in the shortest span of time.

- **Step 6: Election's Results**
  Using the blockchain voting platform, the elections' result is instant. The pre-defined rules built in the smart contracts notify the stakeholders that voting has been closed along with the election results.

7.1 Advantage of E-voting using Blockchain

Voting is one of the most important ways of ensuring that fair and diplomatic decisions are being made. Without voting, people would not be able to have a say on certain decisions and proposed changes. However, there are certain flaws with the current voting system that blockchain can solve.

- **Transparency**
  We know that without transparency, people can become discouraged about the legitimacy of their votes and can lead to questions about tampering and falsified results. Transparency makes for a trustworthy democracy which then leads to more positive outcomes from the votes. This is why it is important that all records are accurate and kept safely. Blockchain and its decentralized ledger can bring about trust at every stage of the voting process. By using blockchain, votes can be tallied and stored on an immutable public ledger. This means that they can be tracked and counted while being visible to everyone. In turn, by allowing voters to see live records of the number of votes coming in, everyone will be able to see the legitimacy of the voting, making for a transparent and trustworthy voting system.

- **Security**
  One of the most important factors of voting is security. Currently, voting systems are very open to hacks. Without substantial security mechanisms in place, malicious actors can enter the system and alter the outcome. This is where blockchain comes in. The technology has the ability to introduce a seemingly unhackable system.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

All votes could be verified as soon as voting is finished to ensure they are all counted correctly. Without blockchain, this would have to be done by a central body overseeing the process. This causes many questions to arise about the trust of these central bodies. But with blockchain and its decentralized ledger system, there is no need for a potentially fallible or corruptible central body.

- **Anonymity**
  People want privacy when voting and don't always want others to know who or what they voted for. Blockchain allows for anonymity when voting. As with transactions on the blockchain, voters can use their private keys to keep themselves anonymous. They can then vote in the system without the worry of others knowing how they voted. Having the ability to guarantee anonymity might then encourage more people to take part in and use the voting system.

- **Processing time**
  Current voting systems often take time to collate and process answers. Often when voting stations are in different areas and offices are not all together, it can be difficult to gather all the information quickly and efficiently. This then leads to time and cost issues. But blockchain can transform all of this. Instead of having to wait for a large number of people to communicate manually, all organizers will be able to see the outcome instantly on the blockchain. Results can be gathered and processed quickly and straight after the voting has finished [22].

7.2 Concerns of E-voting Blockchain

- **Vulnerability to hacking**
  According to the Congressional Research Service of Election Reform and Electronic Voting Systems, vendors and election jurisdictions generally state that they do not transmit election results from precincts via the internet, but they may transmit them via a direct modem connection or Virtual Private Network (VPN). However, even this approach may be subject to attack via the internet, especially if encryption and verification are not sufficient. That is because telephone transmission systems are themselves increasingly connected to the internet and computers to which the receiving server may be connected, such as through a local area network (LAN), may have internet connections. So, using internet would be out of the question in case of Bangladesh where we continuously have history of suspicion over electoral fraud.
- **Voter verified paper audit trails**
  All fully-electronic (touch screen, DRE, internet)voting systems are subject to the limitations and risks of computer technology. This includes the inability to detect the presence of hardware and/or software that could be used, deliberately or inadvertently, to alter election outcomes. According to Rebecca Mercuri, PhD, president, Notable Software, democratic elections require independent verification that all balloting choices have been recorded as intended and vote totals have been reliably and indisputably created from the same material examined by the voters[23].

VIII. CONCLUSION

This paper has highlighted some of the main challenges in linking national ID and CRVS systems, and despite the ongoing global and regional initiatives are yielding improvements to both systems, there is still much to do especially in the time of pandemic. IDC believes that blockchain technology offers a great potential in many COVID- 19 impacted scenarios in the supply chain, transparency across multiple use cases, and the tracking of goods, and investments are expected to recover once the pandemic eases. The recovery will be bolstered by the European blockchain ecosystem, with the biggest players in the market working together with a variety of smaller, innovative companies [20].

Democracy depends on fair election's process, this paper introducing a blockchain based e-voting system as a case study during the pandemic time that provides trusted, secure, and fast voting system. The proposed system could fit to apply in any country, while putting into consideration the additional work to integrate with different laws and election system changes among various countries. Eventually, the system could be applied for different use cases and measurements can be taken to compare if the calculations hold, also, synchronization and consensus algorithms should be discussed and improved for better performance and security depending on the circumstances and the infrastructure of each country.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

ACKNOWLEDGMENTS

The authors would like to thank ***October 6 University (O6U), Egypt*** and ***Park University, USA*** for their support to introduce this research paper in a suitable view and as a useful material for researchers. The authors also would like to thank their colleagues who provided insight and expertise that greatly assisted the research.

REFERENCES

[1] Arnauld Bertrand, "How does digital government become better government?," EY Global Government & Public Sector Advisory Leader, 10 Apr 2019. [Online] Available: https://www.ey.com/en_gl/government-public-sector/how-does-digital-government-become-better-government

[2] Center of Excellence for CVRS Systems, "Knowledge Briefs on Gender and CRVS,"© 2020. [Online] Available: https://crvssystems.ca/news-and-events/knowledge-brief-series-gender-and-crvs-0

[3] Granicus, "What Is Digital Government Service?," last updates January 2020. [Online] Available: https://granicus.com/dictionary/digital-government-services/

[4] Uruguay's 2020 Digital Government Strategy, "Digital Government Strategy 2020: Transforming with equity," Agesic, Uruguay, 2020. [Online] Available: https://leadingdigitalgovs.org/...digital-goverments/...digital-goverments/.../ dgs_2020_0.pdf

[5] Huawei, "Digital Government, Intelligent Government," Industry Insights, last updates March 2020. [Online] Available: https://www.huawei.com/en/industry-insights/technology/digital-transformation/government

[6] UNISYS; Securing your Tomorrow, "Digital Government and Government Solutions," Copyright © Unisys 2020. [Online] Available: https://www.unisys.com/offerings/industry-solutions/public-sector-industry-solutions/digital-government

[7] Saudi Arabia Vision 2030, "Digital Transformation," Unified National Platform, GOV.SA, 2020. [Online] Available: https://www.my.gov.sa/wps/portal/snp/aboutksa/digitaltransformation

[8] Ahmed Elragal, "Egypt's Census Bureau Goes Digital," German University in Cairo, March 2011.[Online] Available: https://www.researchgate.net/publication/262711694_Egypt's_Census_Bureau_Goes_Digital

[9] Homeland Security; USA.gov, "DHS Responds:Coronavirus (COVID-19)," July 17, 2020. [Online] Available: https://www.dhs.gov/coronavirus/cybersecurity-and-critical-infrastructure

[10] Dinh C. Nguyen, Ming Ding, Pubudu N Pathirana, and Aruna Seneviratne, "Blockchain and AI-based Solutions to Combat Coronavirus (COVID-19)-like Epidemics: A Survey," April 2020, DOI: 10.36227/techrxiv.12121962. [Online] Available: https://www.researchgate.net/publication/340639639_Blockchain_and_AI-based_Solutions_to_Combat_Coronavirus_COVID-19-like_Epidemics_A_Survey

[11] Dani el Castro, "EXPLAINING INTERNATIONAL IT APPLICATION LEADERSHIP: Electronic Identification," The Information Technology and Innovation Foundation (ITIF), September 2011. [Online] Available: https://itif.org/publications/2011/09/15/explaining-international-it-application-leadership-electronic-identification

[12] Akash Takyar, "A Detailed Insight into Blockchain Government Initiatives," ©2020 LeewayHertz, USA.[Online] Available: https://www.leewayhertz.com/blockchain-government-public-sector-initiatives/

[13] David Allessie, Maciej Sobolewski, and Lorenzino Vaccari, "Blockchain for Digital Government: An assessment of pioneering implementations in public services," Joint Research Centre (JRC), EU Science Hub, The European Commission's science and knowledge service, 2019.[Online] Available: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-digital-government

[14] Joseph Lubin, "Blockchain in Supply Chain Management," CONSENSYS, Blockchain Use Cases, 2020 © CONSENSYS.[Online] Available: https://consensys.net/blockchain-use-cases/supply-chain-management/

[15] Joseph Lubin, "Blockchain in Healthcare and the Life Sciences," CONSENSYS, Blockchain Use Cases, 2020 © CONSENSYS. [Online] Available: https://consensys.net/blockchain-use-cases/healthcare-and-the-life-sciences/

[16] Open Government Partnership, "Collecting Open Government Approaches to COVID-19," © 2020 Open Government Partnership, May 12, 2020. [Online] Available: https://www.opengovpartnership.org/collecting-open-government-approaches-to-covid-19/

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

[17] VERIDOS, "A need for digital government services in times of COVID-19," Identity Solutions, © 2019. Veridos GmbH, Berlin, Germany.[Online] Available: https://www.veridos.com/en/topictrends/a-need-for-digital-government-services-in-times-of-covid-19.html
[18] ITL Estonia, "e-solutions from Estonia," Estonian ICT cluster,2020.[Online] Available: https://e-estoniax.com/
[19] Open Mind BBVA; Sharing Knowledge for a Better Future, "Blockchain Technology and COVID-19," BBVA Group, © Copyright 2020, 22 June 2020.[Online] Available: https://www.bbvaopenmind.com/en/technology/digital-world/blockchain-technology-and-covid-19/
[20] Radoslav Dragov, Carla La Croce, and Mohamed Hefny, "How Blockchain Can Help in the COVID-19 Crisis and Recovery," IDC: Analyze The Future, © 2020 IDC UK, May 4, 2020.[Online] Available: https://blog-idcuk.com/blockchain-help-in-the-covid-19-and-recovery/
[21] Jack Tatar, "How Blockchain Technology Can Change How We Vote," the Balance, Updated April 22, 2020. [Online] Available: https://www.thebalance.com/how-the-blockchain-will-change-how-we-vote-4012008
[22] Kevin Curran, "E-Voting on the Blockchain," The Journal of British Blockchain Association 1(2):1-6, December 2018, DOI: 10.31585/jbba-1-2-(3)2018. [Online] Available: https://www.researchgate.net/publication/329400689_E-Voting_on_the_Blockchain
[23] Branquinhoz, "Create a voting application prototype using Hyperledger Composer Playground Using blockchain to ensure voting fairness and security," AWVI.CO, IBM developerWorks, January 1, 2017. [Online] Available: https://awvi.co/2018/07/17/create-a-voting-application-prototype-using-hyperledger-composer-playground/
[24] Peter Garrett and Joshua Seidma, "EMR vs EHR – What is the Difference?," The office of the National Coordinator for the Health InformationTechnology,Health IT Buzz, Electronic Health & Medical Records,USA.gov, January 4, 2011. [Online] Available: https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference
[25] González López, Lucia. et al. 2013. "Civil Registration, Human Rights, and Social Protection in Asia and the Pacific." Asia Pacific Population Journal. Volume 29, No. 1.[Online] Available: https://www.un-ilibrary.org/population-and-demography/civil-registration-human-rights-and-social-protection-in-asia-and-the-pacific_ba046677-enhttps://btcmanager.com/us-authorities-blockchain-covid-19-critical-services/?q=/us-authorities-blockchain-covid-19-critical-services/&
[26] Hunter, Wendy. 2018. "Identity Documents, Welfare Enhancement, and Group Empowerment in the Global South, " The Journal of Development Studies. Volume 55, No. 3.[Online] Available: https://www.tandfonline.com/doi/pdf/10.1080/00220388.2018.1451637?needAccess=true&cookieSet=1
[27] Emerging Tech, "Blockchain Emerges as Useful Tool in Fight Against Coronavirus," © 2020 All rights reserved, e.Republic. [Online] Available: https://www.govtech.com/products/Blockchain-Emerges-as-Useful-Tool-in-Fight-Against-Coronavirus.html
[28] Mohua Sengupta, "Could Blockchain be the solution for surveillance and reporting of the Covid-19 pandemic?," Express Computer, Mar 31, 2020. [Online] Available: https://www.expresscomputer.in/blockchain/could-blockchain-be-the-solution-for-surveillance-and-reporting-of-the-covid-19-pandemic/51670/
[29] Gari Singh and Jonathan Levi, "MiPasa project and IBM Blockchain team on open data platform to support Covid-19 response," Blockchain Pulse: IBM Blockchain Blog, March 27, 2020. [Online] Available: https://www.ibm.com/blogs/blockchain/2020/03/mipasa-project-and-ibm-blockchain-team-on-open-data-platform-to-support-covid-19-response/
[30] Richard Brown, "Expert Blockchain Security Audits," Quantstamp; Leaders in Blockchain Security and Solutions," Last update April 2020. [Online] Available: https://www.ledgerinsights.com/us-homeland-security-lists-blockchain-as-covid-19-critical-service/
[31] Toshendra Kumar Sharma, "How Blockchain Can Solve Major challenges of COVID-19 Faced by Healthcare Sectors?," blockchain-council, 28 March, 2020. [Online] Available: https://www.blockchain-council.org/blockchain/how-blockchain-can-solve-major-challenges-of-covid-19-faced-by-healthcare-sectors/

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details