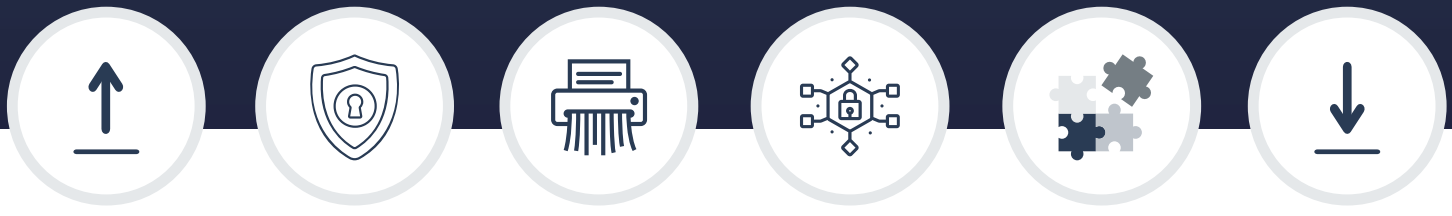
SOLLENSYS™

Making the World Safer, One Block at a Time

BLOCKCHAIN ARCHIVE SERVER™ (BAS)

For the Protection of Critical Infrastructure



INTRODUCING THE BLOCKCHAIN ARCHIVE SERVER™

for the Protection of Critical Infrastructure

MAKING THE WORLD SAFER, ONE BLOCK AT A TIME

Ransomware in the hands of cybercriminals is the leading threat to our way of life. Since 2016, Americans have experienced over 4,000 daily ransomware attacks (justice.gov), and as of October 1, 2021, The U.S. Department of Treasury warns that paying a ransom is now illegal under certain conditions (treasury.gov). As stated by officials from the Office of Foreign Assets Control, ransomware payments could be used to fund activities adverse to the national security and foreign policy objectives of the United States, and embolden cyber actors to engage in future attacks.

It's easy to say you would never give money to malicious hackers, but imagine your data and system access were suddenly gone. What would you do to get it all back?

Devastating Ripple Effects for Businesses
In a 2021 survey conducted by Cybereason of over 1,200 companies, 80% of those attacked experienced another breach soon after the first. While 46% got back access to their data, most of it was corrupted—rendering it useless at best and life-threatening at worst. In the same study, 60% of respondents experienced revenue loss, and 29% of respondents stated their companies were forced to cut jobs following a ransomware attack. As organizations implement proactive measures to mitigate the costs associated with a successful cyber attack, many have discovered massive holes in their approaches to data protection. The heavy consequences associated with a compromise of data integrity eventually force all victims of cyberattacks to rethink their defense strategy.

A Team Leading the Way in Data Security & Recovery
At Sollensys, we are a group of aerospace and mechanical engineers based on the Space Coast of Florida redefining and expanding the strength of distributive data technology. Our footprint spans government entities, healthcare, finance, supply chain management, aerospace, aviation, oceanography, and private industry. From consumer products to enterprise-class solutions, our unique approach creates revolutionary solutions to real-world problems.

By reimagining the use of current technology, we create a world with safeguarded infrastructure, fewer disruptions to industry, and protections for personal health, wealth, and well-being.

We believe you should NEVER:

1. Have cybercriminals hold your data hostage.
2. Pay a ransom to cybercriminals.
3. Experience revenue loss or employee reduction due to cyberattack.
4. Wait weeks for your system to be running again with your uncorrupted data.

Next-Generation Data Archive Vault
The sad truth is that as the threat landscape changes, the countermeasures and safeguards protecting against ransomware continually break down. This is why Sollensys created Sollensium and the Blockchain Archive Server™ (BAS) to create the essential (but missing) component of any cybersecurity arsenal. This system addresses the gap associated with archiving critical data, protecting it from attack, and facilitating the rapid restoration of guaranteed immutable assets.

Sollensium is the first Distributive Data Application that utilizes Sollensys' patent-pending Double Blockchain BAS to provide unparalleled archiving and data recovery following any cyber event, not just ransomware. Unlike any other data storage solution, Sollensium is designed to protect your data, and guarantee it is available and unchanged when you need it. In the following case study, we will discuss how.

sales@sollensys.com | 1 (866)-438-7657

Traditional Cloud Storage Creates False Sense of Security
As the risk of being impacted by ransomware grows, many businesses have turned to popular cloud storage to maintain backups of their sensitive files and data, trusting that this off-network storage will keep them safe from ransomware attacks. If this tactic worked we would not learn of constant cyberattacks against hospitals, school systems, oil pipelines, and government entities on the news.

Cloud storage accessed by computers on an infected network can provide cybercriminals with a single point of access to the organization's total collection of valuable files and documents. Even more alarming is that increasingly organized criminal groups can lurk in an infected network/IoT for months even before an attack. Hackers in 2019 spent an average of 95 days moving around inside business networks before launching their attacks (computerweekly.com).

Upon gaining access to a network, cybercriminals are now immediately looking for backups, encrypting the entirety of your "safe" cloud storage. Once attackers are in, the only way to potentially retrieve your data is to pay significant ransoms. With no guarantee these cybercriminals have even built a decryption process into their ransomware, you are potentially left with nothing, even after paying to get your data back.

REGARDLESS OF SIZE OR INDUSTRY, EVERY COMPANY IS AT RISK

No company is immune to cybercrime. The 2021 MSP Cybersecurity Threat Report states that 75% of companies infected with ransomware were running up-to-date endpoint protection. With the average cost of a data breach at $3.86 million according to Forbes, it is more important than ever to ensure business continuity and data integrity.

- Ransomware attackers are now targeting IT outsourcing services to gain access to all their clients. (Varonis, 2021)
- Attacks on healthcare cost more than any other industry at $408 per record. (HIPAA Journal, 2020)
- Since 2020, 1,681 higher education facilities have been affected by 84 ransomware attacks. (Emsisoft, 2021)
- According to a recent SBA survey, 88% of small business owners felt their business was vulnerable to a cyberattack. According to Datto, ransomware is the No. 1 threat to SMBs with 1 in 5 reporting they have fallen victim to a ransomware attack. A recent survey by National Cybersecurity Alliance shows that 10% of breached small businesses shut down in 2019.
- Extensive use of encryption was found to reduce the total cost of a data breach by $360,000 (SecurityIntelligence)
- Banks experienced a 520% increase in phishing and ransomware attempts between March and June of 2020. (American Banker, 2020)
- The top 5 states impacted by ransomware in Healthcare are: California, Texas, Georgia, Illinois, and Louisiana
- "A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death. A lawsuit says computer outages from a cyberattack led staff to miss troubling signs, resulting in the baby's death, allegations the hospital denies." https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116

sales@sollensys.com | 1 (866)-438-7657

Losses Extend Past The Cost of The Ransom

Cybercriminals target businesses large and small, demanding millions of dollars to restore network access and files in order to cause disruption throughout the free world. Without a safety net, ransomware can lock up your organization for months while your network infrastructure is rebuilt. Not only can ransomware be the downfall of an otherwise successful business, but being locked out of your system for even a few days can have drastic effects on your customers.

The Department of Health and Human Services (HHS) outlined a list of Best Practices for Preventing Business Disruption from Ransomware Attacks, which include:

- Requiring Multi-Factor Authentication
- Isolated Systems
- Filtered Network Traffic
- Strong Spam Filters
- Updated Software
- Anti-virus & Anti-Malware Programs
- **Secured Backups**

Sollensys Offers an Essential Solution

Blockchain technology is the most innovative security solution available for reliably maintaining data. It innately protects against malware, ransomware, and more traditional hacking attempts due to its immutable, unchangeable, and decentralized nature. With these properties in mind, it is easy to see how Blockchain can help companies across all industries as a “bolt-on” addition to any cybersecurity suite.

An Unbreakable Safety Net

The BAS is built on a unique Double Blockchain with two types of encryption algorithms: one holding your data and the other holding your unique identifier key to authorize data re-assembly. Alone, each Blockchain is nearly impossible to hack, but together a cybercriminal would have to hack both chains simultaneously.

Sollensys is not a storage solution. it is an immutable, unchangeable, and indestructible archive of your data built upon revolutionary new Double Blockchain technology. It allows you to fully recover from a cyber attack in a matter of hours, not days.

Significant Reduction in Damages

Cybercriminals typically set ransoms based on the size of their target organization, which can range from a few hundred to millions of dollars. Without a safety net to recover your systems, you could be subject to other financial damages as well. Costs can add up quickly for regulations and compliance issues, loss of revenue due to customer disruption, loss of intellectual property, file distortion from corrupted data, and loss of productivity during the recovery and reconstruction process—assuming recovery is even possible.

Safe, Fast, Unseen

Sollensys’ revolutionary Double Blockchain technology provides a quickly recoverable, immutable, unbreakable safety net. Your files, documents, photos, videos, and other sensitive materials are uploaded, shredded into millions of fragments, and secured. They effectively do not exist in a usable form for anyone without the correct authorization and the correct key to decode the information.

Even the Sollensys team cannot view or access your files in any way. This system is effective on or off-premise and quickly and easily integrates with existing cybersecurity and cloud-based solutions across all systems and file types, including video, which is a first for Blockchain.

sales@sollensys.com | 1 (866)-438-7657

TECH TALK

Encryption is at the center of Blockchain technology and protects your data from unauthorized access. Historically, encryption was only applied to messages, but now it touches every media type. While the most popular application of Blockchain is for digital cryptocurrency, Blockchain is actually a much more robust technology that can work as a standalone solution or addition to a comprehensive cybersecurity system.

Since Blockchain offers a superior method to store, secure, and transfer data, there is increasing demand to reimagine fundamental digital infrastructure using it. Following the success of Bitcoin, a plethora of other applications emerged to build on the capabilities of cryptographic technologies, including platforms like Ethereum, Hyperledger, and EOS. Of utmost importance is Blockchain's ability to provide guaranteed confidentiality and immutability to data owners. This is particularly useful in thwarting ransomware attacks. Owners can also get original (unmodified) data back for rapid system reconstitution if compromised.

The BAS Accommodates Your Current Security Architecture

We built the Blockchain Archive Server™ (BAS) to work with any pre-existing cybersecurity architecture to provide an infinitely scalable safety net for your data protection. Rather than starting with penetrable endpoints, Sollensys secures a copy of what hackers want to hold hostage and corrupt most … your digital intellectual property and operational data.

We ensure you NEVER have to pay a ransom by safeguarding an uncorrupted copy of your data that is virtually quantum in nature and cannot be altered. In fact, your assets don't physically exist until you download them, making Sollensys one of the most secure methods on the planet for storing your private assets.

The BAS is available for both Enterprise and Small Business environments with a physical (on-premises) and virtual (cloud customers with a tertiary archive) option, guaranteeing business sustainability and data assurance, regardless of operational size.

How It Works

The BAS performs all the 'heavy lifting' associated with aggregating, securing, and archiving your mission-critical data. It also facilitates the process when you need to get your secure and immutable data back.

The system utilizes two Blockchain networks: a Distributed File System Blockchain (DFS) which stores fragments of encrypted data across thousands of computers, and a Smart Contract Blockchain, which stores fragments of the private key that authorizes re-assembly.

First, your data is copied to the BAS, encrypted, fragmented, and distributed to a secure network we call Sollensium. Then the private key and hashes are distributed to a separate, secure Blockchain network. Finally, your private, encrypted key is used to reassemble your data upon request. Redundant backups and the Blockchain work together to protect both the physical security of your data and the integrity of the information held within.

The Distributive Data Ledger

Blockchain uses public-key cryptography and hashing algorithms to encrypt and index data on a ledger distributed across a network of different computers, called nodes. The encrypted files are fragmented into 256KB chunks and distributed across the Blockchain, with multiple copies of each fragment existing on the nodes geographically closest to your BAS.

When your data is secured and distributed across Sollensium, the effects of an attack against one computer cannot spread to the rest of the network because each new block is written based on the hash of the previous block. This creates an unbroken chain of time-stamped, encrypted data entries. Changing any time-stamped data would lead to a cascade of differences in the hash values, making it easy to identify unwanted changes. Blockchain 'immutability' means it is mathematically improbable for an adversary to access and alter your data ledger.

The private key and hash addresses to the data fragments are also encrypted, fragmented, and distributed out to nodes on the Smart Contract Blockchain to ensure that data fragments can only be called back and reassembled when authorized.

Smart Contracts

The proliferation of Blockchain-based Distributed File Systems (DFS) gives anonymity to hard drives of users around the globe who agree to store fragments of data on their computers. In addition to the many thousands of servers already participating, large digital infrastructure providers now host clusters of such nodes, further adding resilience to this network.

Smart Contracts exist as autonomous agents that live within the Blockchain and execute a specific task whenever called. In the case of data storage and archiving, the participant sending the data and the participants receiving and storing the data are the parties involved in the contract.

Smart Contracts simplify and automate transactions between participants that can range from purely financial (in the case of cryptocurrencies) or involve other assets such as data (customer, operational, supply chain, and patient). The agreement states that the receivers hold onto an encrypted chunk of "info" that the participant cannot see and that the sender can request at any time.

The Sollensys BAS empowers organizations to maintain complete control over their information. Once written to the ledger, the terms of the Smart Contract state that only the owner of the original data can gain access.

This guarantees your assets cannot be seen or tampered with by anyone else.

An attacker would have to control 51% of the global network in order to change the historical record, an impossible task given the thousands of independent assets distributed globally that share copies of that single unchangeable ledger.

Data Recovery

In the event you need to rapidly rebuild your infrastructure after a ransomware attack, a private encryption key unique to each account is provided to the owner of the Smart Contract. Once logged into your account, data fragments are recalled and reassembled using the custom hash addresses assigned to each. Private keys ensure that only authorized users in your organization have access to information. Without the credentials of the authorized user, it is impossible to download (or even see) your uploaded assets.

Everyone wants to know, "How fast can I recover my things?" Since the data fragments are copied across multiple nodes, downloading speeds are near the maximum bandwidth of your Internet connection with no additional cost for the download. Your protected data is available as quickly as your network speed allows.

SPECIFIC USE CASES

Blockchain provides the opportunity to improve data integrity, availability, and confidentiality in critical infrastructure sectors, including energy, transportation, and utilities. The security it provides for any organization will take their business continuity efforts to another level.

Here are a few examples of companies and institutions that learned about the devastating consequences of cyberattacks the hard way.

INDUSTRIAL AUTOMATION: Staying On Schedule Through An Attack

Even organizations that make up national critical infrastructures and key resources are not immune to ransomware. New viruses identified in early 2020 target industrial control systems and have the ability to kill critical software control processes before completely revoking system access in an instant.

In March 2019, a power and metals producer experienced an attack that disrupted their business process management system leading to:

- Multi-Site Shutdown
- Impaired Resource Management
- Manual Tracking of Large, Distributed Inventories
- Total Cost: $71 Million

As recently as May 2021, ransomware caused leadership at the Colonial Pipeline, the largest gasoline pipeline in the United States, to shut down operations due to the pervasiveness of the attack. This prompted organizations such as Precision Companies to adopt the BAS into their data backup strategy.

“The ability to avoid business interruption and ensure a safe archive of sensitive client data was more than worth the investment in the BAS.”
-- Jason Shye, Precision Companies.

IT SERVICE PROVIDERS: Protecting Managed Service Providers & Clients

MSPs are high-value targets for ransomware because once inside, attackers can often easily access other vulnerable targets hosted in adjacent environments. According to the FBI, cybercriminals frequently exploit vulnerabilities in tools used by MSPs, with four out of five MSPs targeted each year.

In late 2019, hackers infiltrated MSPs in Texas and Wisconsin, rendering 22 cities and towns and 400 dental practices incapable of:

- Providing Public Services & Documentation
- Accepting Online Payments
- Accessing Critical Applications
- Responding to Emails

Since MSPs often provide services for critical applications (like healthcare), it is imperative that they have all the necessary tools available for clients during a cyber attack. Therefore, MSPs around the world have begun to offer the BAS as a bolt-on to their existing backup products and strategies to ensure they best serve their clients at all times.

SPECIFIC USE CASES

RETAIL: Preserving Operations

Retail companies are a major target for ransomware attacks because cybercriminals understand how crucial it is for these organizations that provide consumer goods to maintain operational continuity. In late 2019, a commercial lumber wholesaler was locked out of its computer systems at both the store and corporate level, causing an inability to:

- Process Sales Transactions
- Check Product Prices & Inventory
- Access Historical Purchase Information
- Total Cost: $6 Million

Ransomware attacks are an increasingly prevalent danger for retail companies by grinding sales and support operations to a halt immediately and often taking weeks, if not months, to remediate. The crux of the problem is losing access to inventory data—shipping and receiving, sales, support, and admin functions all stop due to the inability to scan items or access records. This risk has led retailers such as Ashley Furniture to augment their existing cybersecurity protocols with the BAS.

“For the money I spent, to have that peace of mind in protecting my team and their livelihoods as well as my guests, it was absolutely a no-brainer.”
-- Chris Caprio, Ashley Furniture.

MUNICIPALITIES: Ensuring Critical Infrastructure

For three years, the strain of ransomware known as SamSam crippled over 200 critical municipal and medical networks across North America and the UK, including the cities of Atlanta and Newark, rendering these organizations unable to:

- Process Service Requests
- Access Billing Systems
- Conduct Medical Appointments & Treatments
- 200 Entities Affected
- Total Cost: $30 Million

IT leaders in municipalities constantly look to improve the operational resilience of their networks, especially in light of modern, sophisticated threats that paralyze critical network infrastructure. The BAS represents a peace-of-mind layer for these operators. In the event of a disruption, they are able to quickly recover operations and determine the most appropriate course of action for remediation.

EDUCATION: Staying On Schedule Through An Attack

Educational institutions are prime targets for attackers due to the willingness of these organizations to pay to avoid the unacceptable downtime resulting from ransomware disruption. In November 2019, a group of 28 schools in West Virginia suffered a ransomware attack that denied access for teachers and administrators to:

- Access Any File Stored on School Networks
- Access VOIP and Email Communication Systems
- Process Payroll and Vendor Invoice Payments
- Remediation Efforts Lasted 3+ Months

Ransomware attacks have led to schools starting weeks late and months of continued disruption as the entire administrative layer of the organization scrambled to repair and replace key data and reinstall operational software. The need to get up and running quickly makes the BAS a worthwhile investment as another layer of protection in the event of an attack.

sales@sollensys.com | 1 (866)-438-7657

Cybersecurity Built on the Brilliance of Blockchain Technology

Recent hacker methodology creates interesting challenges for infrastructure asset owners who are quickly discovering that traditional business continuity programs and system recovery methods may not provide the level of data assurance they really need. Contemporary cybersecurity countermeasures continue to be effective against some threats, but the consequences associated with compromised confidentiality of critical information become more and more severe with each passing day.

While the Blockchain Archive Server™ (BAS) cannot stop cybercriminals from attempting to compromise your data, we ensure you NEVER have to pay a ransom by safeguarding an uncorrupted copy of your data that is virtually quantum and cannot be altered. Trusting your critical data to Sollensium and the Blockchain Archive Server gives you one of the most secure methods on the planet for storing your private assets.

sales@sollensys.com | 1 (866)-438-7657

WORKS CITED

2020 Threat Report." Blackberry Home Page – Security Software & Services, Https://Www.Blackberry.Com/Us/En/Pdfviewer?File=/Content/Dam/Blackberry-Com/Asset/Enterprise/Pdf/Direct/2020-Threat-Report.Pdf. Accessed 28 Sept. 2020.

"Asymmetric Cryptography In Blockchains | Hacker Noon." Hacker Noon, https://hackernoon.com/asymmetric-cryptography-in-blockchains-d1a4c1654a71. Accessed 19 Sept. 2020.

"Blockchain - Public Key Cryptography - Tutorialspoint." RxJS, Ggplot2, Python Data Persistence, Caffe2, PyBrain, Python Data Access, H2O, Colab, Theano, Flutter, KNime, Mean.Js, Weka, Solidity, https://www.tutorialspoint.com/blockchain/blockchain_public_key_cryptography.html. Accessed 19 Sept. 2020.

Dudley, Renee. "Like Voldemort, Ransomware Is Too Scary to Be Named — ProPublica." ProPublica, https://www.propublica.org/article/like-voldemort- ransomware-is-too-scary-to-be-named. Accessed 28 Sept. 2020.

"The New Target That Enables Ransomware Hackers to Paralyze Dozens of Towns and Businesses at Once — ProPublica." ProPublica, https://www.propublica.org/article/the-new-target-that-enables-ransomware-hackers- to-paralyze-dozens-of-towns-and-businesses-at-once. Accessed 28 Sept. 2020.

"Ethereum Whitepaper | Ethereum.Org." Ethereum.Org, https://ethereum.org/en/whitepaper/. Accessed 22 Sept. 2020.

Gürsoy1, Gamze. "Using Ethereum Blockchain to Store and Query Pharmacogenomics Data via Smart Contracts | BMC Medical Genomics | Full Text." BMC Medical Genomics, 1AD, https://bmcmedgenomics.biomedcentral.com/articles/10.1186/s12920-020-00732-x.

"Introduction to Cryptography in Blockchain Technology - Crush Crypto." Crush Crypto, https://www.facebook.com/crushcrypto/, 20 Dec. 2018, https://crushcrypto.com/cryptography-in-blockchain/.

"IPFS - Content Addressed, Versioned, P2P File System." ArXiv.Org, https://arxiv.org/abs/1407.3561. Accessed 22 Sept. 2020.

"IPFS Gateway | Cloudflare Developer Docs." Developer Docs | Cloudflare Developer Docs, https://developers.cloudflare.com/distributed-web/ipfs-gateway. Accessed 19 Sept. 2020.

Kumar, Unique. "Can Blockchain Be the Antidote to Ransomware? | CIO." CIO, CIO, 17 Oct. 2019, https://www.cio.com/article/3446518/can-blockchain-be-the-antidote-to-ransomware.html.

"What Are Public and Private Keys?" Crypto Blog | Cryptocurrency & Trading Blog, https://blog.liquid.com/what-are-public-and-private-keys. Accessed 19 Sept. 2020.
"CheckPoint Live Cyber Threat Map" https://threatmap.checkpoint.com

"Lumber Liquidators Provides Information On Network Security Incident - Aug 27, 2019." Lumber Liquidators Investor Room, http://investors.llflooring.com/2019-08- 27-Lumber-Liquidators-Provides-Information-On-Network-Security-Incident. Accessed 28 Sept. 2020.

Massessi, Demiro. "Blockchain Public / Private Key Cryptography In A Nutshell | by Demiro Massessi | Coinmonks | Medium." Medium, Coinmonks, 15 Oct. 2018, https://medium.com/coinmonks/blockchain-public-private-key-cryptography-in-a- nutshell-b7776e475e7c.

Mearian, Lucas. "What's a Smart Contract (and How Does It Work)? | Computerworld." Computerworld, Computerworld, 29 July 2019, https://www.computerworld.com/article/3412140/whats-a-smart-contract-and-how-does-it-work.html

WORKS CITED

"Public Key Cryptography: What Is It? (Video) | Khan Academy." Khan Academy, https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/diffie-hellman-key-exchange-part-1. Accessed 19 Sept. 2020.
"Best Practices for Preventing Business Disruption from Ransomware Attacks" Department of Health and Human Services, https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf

Sullivan, Nick. "A (Relatively Easy To Understand) Primer on Elliptic Curve Cryptography." The Cloudflare Blog, The Cloudflare Blog, 24 Oct. 2013, https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve- cryptography/.

Tabora, Vince. "Using IPFS For Distributed File Storage Systems | by Vince Tabora | 0xCODE | Medium." Medium, 0xCODE, 22 June 2020, https://medium.com/0xcode/using-ipfs-for-distributed-file-storage-systems- 61226e07a6f.

"The Trade Secret: Firms That Promised High-Tech Ransomware Solutions Almost Always Just Pay the Hackers." ProPublica, 15 May 2019, https://features.propublica.org/ransomware/ransomware-attack-data-recovery- firms-paying-hackers/.

"Understanding Cryptography's Role in Blockchains | Comparitech." Comparitech, 10 Apr. 2019, https://www.comparitech.com/crypto/cryptography-blockchain/.

"What Is RSA Encryption and How Does It Work? | Comparitech." Comparitech, 10 Dec. 2018, https://www.comparitech.com/blog/information-security/rsa-encryption/.

"OFAC Advisory on Ransomware" US Department of Treasury, 2020. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf