WHAT IS THE SOLLENSYS BLOCKCHAIN ARCHIVE SERVER?

Sollensys®
DISTRIBUTIVE DATA

TABLE OF CONTENTS

Sollensys®
DISTRIBUTIVE DATA

WHAT IS THE SOLLENSYS BLOCKCHAIN ARCHIVE SERVER?

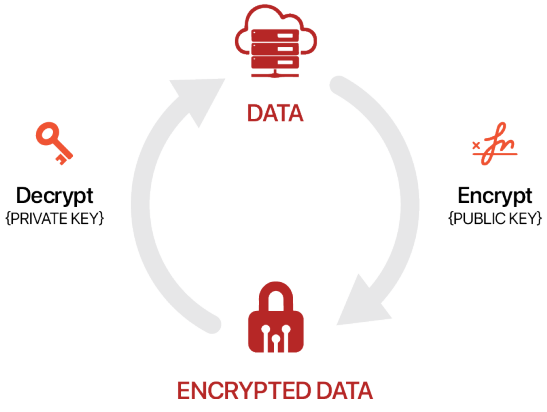
The Sollensys Blockchain Archive Server™ (BAS) is the first Distributive Data Application that utilizes Sollensy's patent pending double blockchain system to deliver unprecedented business continuity following a ransomware attack. This document is intended to provide business leaders with an introduction to the technologies that make up the BAS and describe how the BAS can ensure seamless data recovery in the event of a ransomware attack.

THE BASICS

Blockchain technology is at the center of the BAS. In the simplest terms Blockchain is a secure database. It encrypts and records data onto a ledger that is distributed across a network of many computers. While the most popular application of blockchain is arguably the Bitcoin cryptocurrency, Blockchain is actually a much more robust technology which is already being used to improve data integrity, availability, and confidentiality in the finance, supply chain and medical industries.

Data Encryption is at the center of Blockchain, so a basic knowledge of it is required to understand blockchain technology. Historically, encryption was only applied to messages, but now it touches every type of media including text, audio, video and images. Although there are many forms of encryption, we'll be focused on the two primarily used by blockchain:

PUBLIC KEY CRYPTOGRAPHY



HASHING ALGORITHMS

Input Text	Hash (10 Chars)
This is data .	e41a90bcb
This is data !	56b991289d
This is data ?	be57bdc201

Sollensys®
DISTRIBUTIVE DATA

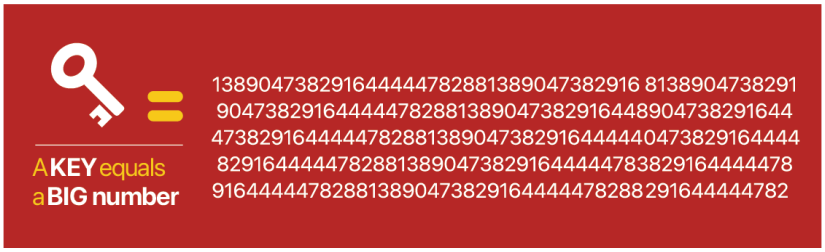
1. **Public Key Cryptography** uses a public key to convert data into random looking numbers that can only be decrypted with a paired private key. To better illustrate this, we'll use a real-world example. Say Alice and Bob want to send sensitive files to each other, but they need to make sure the information is secure. To do this, Alice and Bob will use Public-key Cryptography to generate two large prime numbers, called a key pair:

- A Public Key creates digital signatures on file requests.
- A Private Key then decrypts the files once received.

Trapdoor Function Example

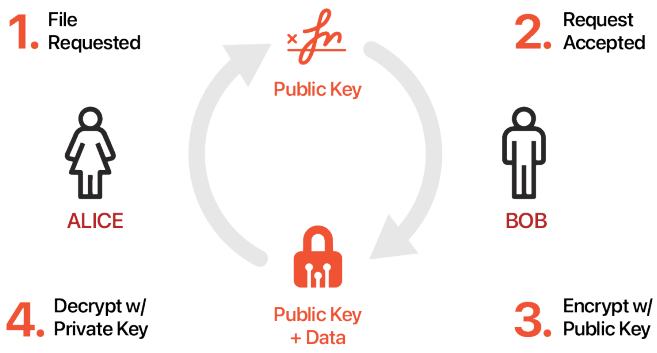
Input Text	Answer	Method	Difficulty
Solve 907 x 773	701,111	Multiplying	Easy
Find 2 prime numbers whose product is 701,111	907 x 773	Factoring	Hard

Alice and Bob's keys are generated simultaneously and are mathematically derived from each other with a function that is easy to perform in one direction (encryption), but difficult to undo (decryption). This structure is called a trapdoor function. In practice, it simply means Alice's public key can be derived from the private key, but not vice versa, making it safe to share the public key as a means of identification on the network without compromising the private key.



"the public key encrypts data, while the private key decrypts it."

Alice requests a file from Bob using her public key. Bob uses Alice's public key and the trapdoor function to convert the file into a string of random looking numbers and return them to Allice. Her private key is the only thing that can convert the jumble of numbers back into the original file.



Sollensys®
DISTRIBUTIVE DATA

Currently, there are several public key cryptography algorithms that are trusted by the security community, with notable examples being RSA and ECC.

It would take the strongest computer trillions of years to crack the private key

2. The Secure Hash Algorithm is the other major technology underlying Blockchain. One the most popular forms of this technology is 256-bit Secure Hash Algorithm (SHA-256). Although not technically encryption, the Secure Hash Algorithm is a one-way mathematical operation that takes data of any length and converts it into a 64-character code called a hash.

Input Text	Hash
BadPassword	AC606172c5011F97569A0AE344E7D 76D7B93EEE312839B44694CCEBC
badPassword	1AE74DD5F5D58CAAA60952C0F85F 49AAF40F83152E8950E68F52200AA
BadPassword	9003693D93220B28A03D3C1CAB20 B65A2E6BAFF3D4A2A651B713C461C

Hashing is a very useful tool when you want to verify that you possess a piece of information without showing or storing the information in its raw format. This is actually how most websites store your password— they don't. Rather, they store the 64-character hash of your password matched to your username from when you signed up. When you log-in, whatever you type in the password field is hashed and checked against that record. Hashing is much more secure since raw password data isn't stored, just 64 characters of mush. Since even the slightest change in the input will lead to a totally different hash, these algorithms are used as a means to create digital fingerprints in order to verify authenticity, ensure data haven't been corrupted, and as a means to index and address.

TECHNOLOGY SUMMARY

Public-key cryptography converts data along with an attached public key into random looking numbers that can only be decrypted with the paired private key.

Hashing algorithms convert any amount of data into a unique 64-character mush pile and is used for creating digital fingerprints for verifying and addressing.

Sollensys®
DISTRIBUTIVE DATA

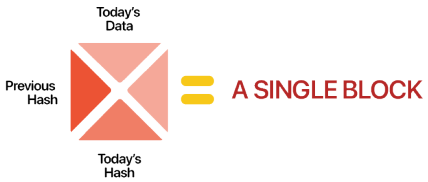
Ok, now that we have the core components, let's move on to how blockchain is used as a distributive data ledger.

THE DISTRIBUTIVE DATA LEDGER

As we've discussed, blockchain uses a combination of public-key cryptography to encrypt data and hashing algorithms to organize & index it on a ledger that is distributed across a network of many different computers, called nodes. Each new "block" is an entry in the ledger built of a piece of data secured with public key cryptography, the hash of the previous block, and its own hash.

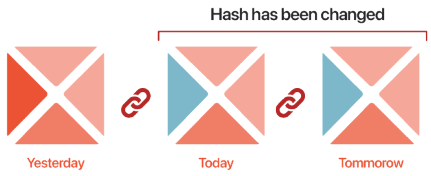
100% DATA FIDELITY

Since each block uses the hash of the previous in the creation of its own hash, every new block is tied to the previous block.



This creates an unbroken chain of time-stamped entries of encrypted data into the ledger. In the case of Alice and Bob this would mean that changing anything in any of the previous blocks or timestamped data would lead to a cascade of differences in the hash values, making it easy to identify an edit anywhere in the chain.

EASY TO IDENTIFY AN EDIT



In order to protect against tampering and ensure 100% data fidelity, the entire ledger is copied across many different nodes which must all agree on each new block before it's added. That way, the effects of an attack at one computer cannot spread to the rest of the network.

An attacker would have to control 51% of the network in order to change the historical record, an impossible task for all intents and purposes given thousands of independent machines distributed globally.

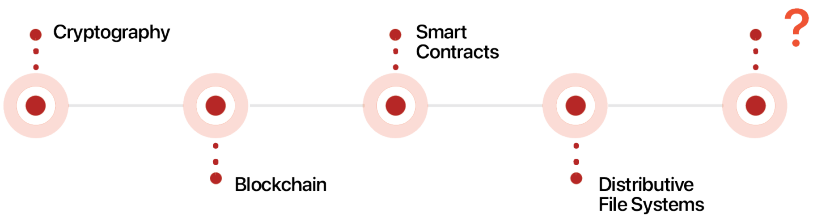
This gives blockchain the property of 'immutability'— it is virtually impervious to edits, except for additions of new blocks.

BLOCKCHAIN 2.0: SMART CONTRACTS & DISTRIBUTED FILES SYSTEMS

Following in the success of Bitcoin, a plethora of technologies have been developed to build on the capabilities and usefulness of the underlying cryptographic technologies, including platforms like Ethereum, Hyperledger, and EOS. Since blockchain offers a superior method to store, secure, and transfer data of all kinds, there is increasing demand to re-imagine fundamental digital infrastructure.

A natural extension of blockchain technology comes in the form of smart contracts that simplify and automate transactions and agreements of all kinds between participants. These transactions can be purely financial (in the case of cryptocurrencies) or can involve other assets such as data. These 'contracts' don't need to be fulfilled in the traditional sense. Rather, they exist as autonomous agents that live within the blockchain and execute a specific task whenever called. In the case of data storage, the participant sending the data and the participants receiving & storing the data are the parties in the smart contract. The agreement is simply that the receivers will hold onto an encrypted chunk of stuff that the sender can request at any time.

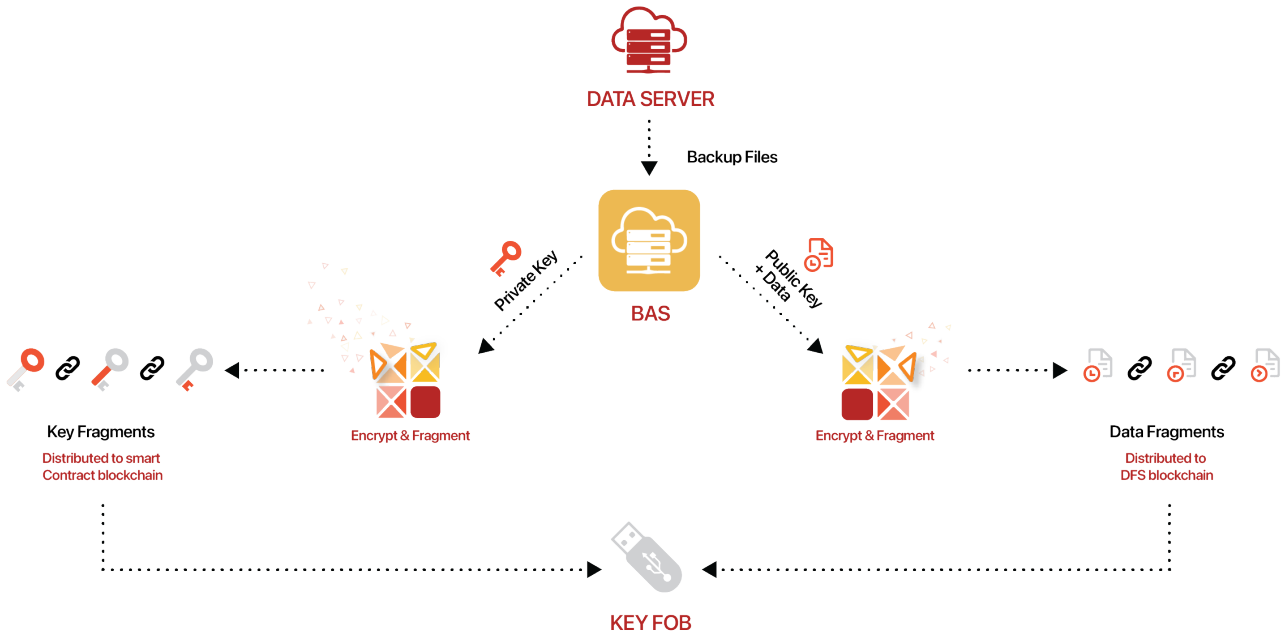
The ability to store data over a distributed network provides astounding resilience and data availability-- having no single point of failure, multiple copies, and hash fingerprints also leads to superior data fidelity and integrity, while the underlying encryption technologies ensure confidentiality of data stored on the chain. This has led to the proliferation of blockchain-based distributed file systems (DFS) -- basically abstract hard drives that exist across thousands of computers across the globe. In addition to the many thousands of servers already participating, large digital infrastructure providers such as Cloudflare have begun hosting clusters of such nodes to join in on the future of distributed computing, further adding resilience to the network.



Sollensys®
DISTRIBUTIVE DATA

HOW THE (BAS) WORKS

The BAS lives on premise as an 8TB server that acts as a staging point to prepare data for blockchain encryption. The system utilizes two blockchain networks in its operation: a distributed file system blockchain (DFS) which stores fragments of encrypted data across thousands of nodes and a smart contract blockchain which stores fragments of the private key that authorize re-assembly as well as the hash addresses to the data fragments.



DATA IS COPIED TO THE BAS, ENCRYPTED, FRAGMENTED, & DISTRIBUTED TO BLOCKCHAIN

These can be individual files or disk images that can be backed up as often as desired. The data is encrypted using public-key cryptography, ensuring confidentiality. The encrypted files are fragmented into 256KB chunks and distributed across many nodes on the DFS blockchain, with multiple copies of each fragment existing on the nodes geographically nearest to your BAS instance to ensure data integrity and availability.

THE PRIVATE KEY & HASHES ARE DISTRIBUTED TO A DIFFERENT BLOCKCHAIN

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.

A PHYSICAL KEY-FOB IS USED TO REASSEMBLE

A physical key-fob is used at the BAS terminal to automatically reassemble the private key, authorize data reconstitution, and call back the data fragments using the unique hash addresses assigned to each fragment. Since the data fragments are copied across multiple nodes, downloading tends to proceed near maximum bandwidth of your

internet connection, similar to downloading a torrent file: translation, data systems back and up and running quickly.

The use of physical keys ensures that only authorized users in your organization have access to the data, and no one else in the world. In the event your BAS instance is damaged or destroyed, a new server can be re-configured without any disruption to your data, provided you have at least one physical key.

WHERE DOES THE BAS FIT IN?

The BAS is a fail-safe contingency for data backups in the event of a ransomware attack. The purpose of the BAS is to ensure that critical data infrastructure can be restored quickly to ensure business continuity and increase the options available during the attack remediation process.

Many organizations rely on collaborative file sharing platforms such as Google Drive or SharePoint as a primary means of storing large amounts of company data due to the convenience of these tools. However, the convenience cuts both ways--these platforms are an attractive attack vector for bad actors. In fact, **59% of ransomware attacks involved data in the public cloud.** The BAS rectifies this risk by sitting invisibly in the background, backing up your organization's data regularly to ensure it's accessible.

Organizations who are already utilizing robust cybersecurity suites and backup protocols will be pleased to know that the BAS can work alongside any combination of technologies, further strengthening your company's data integrity and disaster preparedness strategies, without interfering with well-established processes and vendors.

WHERE THE BAS IS USED.

IT SERVICE PROVIDERS:
PROTECTING MANAGED SERVICE PROVIDERS & THEIR 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, cyber criminals frequently exploit vulnerabilities in tools used by MSPs, with 4 out of 5 MSPs targeted each year. In late 2019, hackers infiltrated MSPs in Texas and Wisconsin, rendering 22 cities & towns and 400 dental practices incapable of:

- Providing public services and documentation
- Accepting online payments
- Responding to emails

Since MSPs are often providing services for mission critical applications, it is imperative that they have all the tools available to them to help their clients in the inevitable event of a cyber-attack. This is why MSPs in the US and Canada have begun to offer the BAS as an add-on to their existing backup products and strategies to ensure they can best serve their clients during incidents.

RETAIL: PRESERVING OPERATIONS

Retail companies are targeted by ransomware because attackers understand how crucial it is for these organizations to maintain operational continuity. In late 2019, a large lumber wholesaler was locked out of its computer systems at both the store and corporate level, leading to an inability to:

- Process sales transactions
- Check product prices and inventory
- Access historical purchase information
- Cost: $6 million

Ransomware attacks are a clear and present danger for retail companies, 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 & 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 backup policies 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 MISSION CRITICAL INFRASTRUCTURE

For 3 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, Newark and a variety of medical centers, rendering these organizations unable to:

- Process service requests
- Access billing systems
- Conduct medical appointments and treatments
- Cost: $30 million across 200 entities

IT leaders in municipalities are constantly looking to improve the operational resilience of their networks, especially in light of modern, sophisticated threats that look to paralyze mission 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 so that they can determine the most appropriate course of action for remediation without being led by the nose by the attackers.

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 that results from ransomware disruption. In November 2019, a group of 28 schools in West Virginia suffered a ransomware attack which denied access to teachers and administrators to:

- All files stored on the schools' networks
- VOIP and email communication systems
- Payroll and vendor invoice payments
- Cost: Remediation efforts took 3+ months

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

INDUSTRIAL:
MINIMIZE CRITICAL SYSTEM DOWNTIME

No company is safe from ransomware, even the myriad quiet organizations that constitute the industrial sector. New ransomware strains identified in early 2020 target industrial control systems and have the ability to kill critical software control processes before it revokes system access. In March 2019, a power and metals producer experienced an attack which disrupted their business process management system leading to:

- Multi-site shutdown
- Impaired resource management
- Manual tracking of large, distributed inventories
- Cost: $71 million

Attackers know that the ability to cause maximum disruption leads to the highest chances of quick payment. The ability to disrupt OT assets makes ransomware particularly threatening to the industrial sector, especially because these companies hold vast amounts of sensitive data, both their clients' and their own. This has led to 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.

BIBLIOGRAPHY

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.htm . 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.

"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.

"**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.

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/.