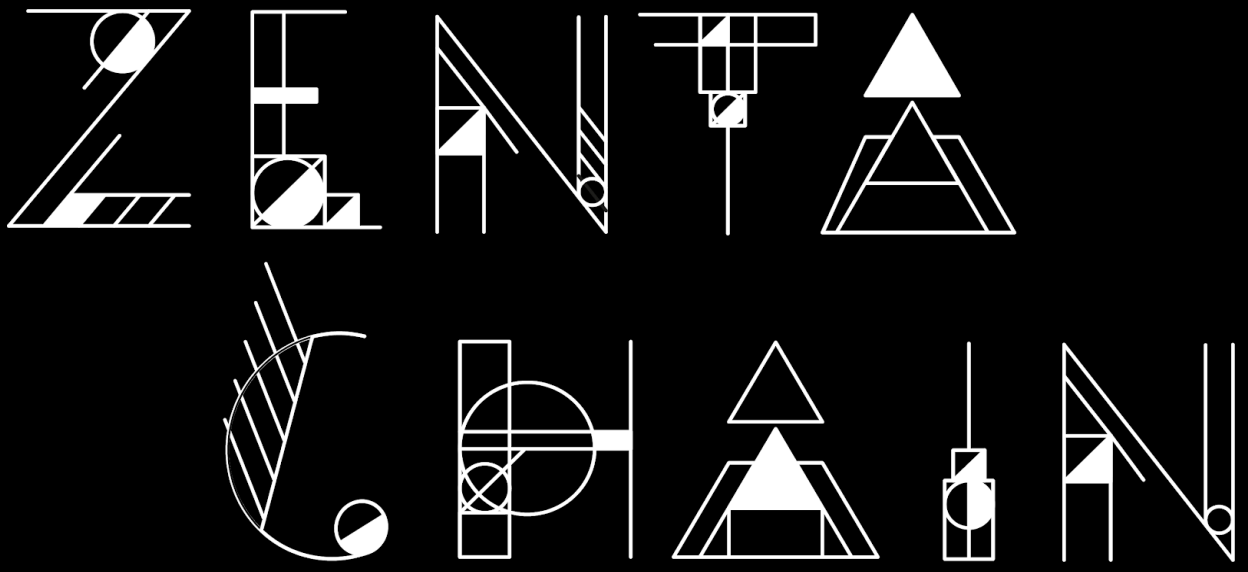


Whitepaper

“the future illuminates the potential of the present”

Version: 1.2

WHITEPAPER CONTRIBUTORS

Zentachain.io

SPECIAL THANKS TO Zentachain and friends!
E-mail:Team@zentachain.io

Engineered For Security, Anonymity & Offline Communication

Zentachain.io
(Dated:03.01.2020, Version 1.2)

Preface:

The digital revolution rewrote the world that we are in. We already live in a new version of our future. As Barbrook said in 2006: 'The importance of new technology is not for what it can do in the here and now, but for what more advanced models might be able to do one day. The present is understood as the future in embryo – and the future illuminates the potential of the present.' Digital transformation makes a larger contribution to our future. These days, humans depend on technology more than ever. Since the personal computer and more recently the smartphone got invented, it seems that almost the entire world has become interconnected. We cannot imagine a world without digital communications and interactions, social media, user-generated websites, and free online encyclopedias. The importance of the internet, the fibers that connect us all, keeps on growing. Now you have access to the world and also the world has access to you. Further digitalization can be considered as a positive because it transforms the whole way of working, making it more usable and efficient. It increased mobility and productivity and reduced the need for a dedicated workspace. But the digital revolution has a dark side as well, and that is exactly what Zentachain is going to protect against the companies who are saving your data files and document on a central server. Zentalk protects your contact history from large companies that can sell all this information because they have your message history. Cryptography allows Zentachain authenticated communication through untrusted channels as long as the secret keys are not exposed or located on a central platform. For Zentachain it is important to protect the information exchange over the internet and for decentralized storage of confidential data. Zentachain team works very precisely in communication and storage and is very careful about anonymity and encryption to bring them to the highest level of security. The main products are capable of encrypting data and host it on the user's own device. Zentalk is a hybrid decentralized messaging application without cloud storage. It has its own network called Zentamesh-network; this helps users communicate across themselves in a wide range of areas without internet access. Zentalk contains the Blake2 Algorithm. Zentachain will launch its own blockchain named under Zenta. We have designed Zenta blockchain to allow Offline communication on the Zentamesh network. Zentalk users can have Zentanode in the Zentamesh network to be rewarded with Zenta. Zentachain Labs is considering several options to build its Zenta blockchain on, among others: Cosmos (BPOS), Polkadot (Parachain & Blake2 & NPOS) and Ethereum (POW & POS). The ecosystem holds all necessary building blocks for creating and hosting scalable decentralized databases, distributed services, and Peer 2 Peer decentralized cloud storage.

CONTENTS

1. Problem
2. Vision
3. What makes Zentachain awesome?
4. Economics of Zenta
5. The problem worth solving
6. Data Hacks & Breaches
7. Privacy
8. Centralized messenger
9. Centralized Clouds
10. About Zentachain
11. Zentachain Ecosystem
12. Communication
13. Zentalk
14. Zentalk & Tor Network
15. Zentalk & Algorithm & Encryption
16. Cryptanalysis
17. Zentamesh Network & Zentanodes
18. Zentavault
19. Zentagate

1. Problem

- Need for secure interaction and digital data storage - owned by the initiators.
- Resolve the thread of unauthorized data access and manipulation of information streams.
- Protect against hackers - getting unauthorized access and stealing information, logging, harvesting and selling user data.
- Leverage the net neutrality for user information
- Ensure ownership of data, data security, and communication
- Ownership and security for cloud storage
- Every action made by a user on a device issued on a digital medium is potentially logged and stored in a database or on a file server. Likely this data is not properly encrypted or anonymized.
- Communications applications which are based on a server or a cloud.
- Data and communication history processes that are encrypted by large companies which are never have been encrypted or user has to start a function in the application manually to run the encryption.
- Applications that spy on each other to get rights in the programs so that they can access user data and information.

2. Vision

Zentachain is a decentral ecosystem built for net neutral data- and transactions interchange and data storage. The ecosystem is maintained by its users and immune against several forms of cyber attacks and hacking. Next to that, viable solutions for security and data ownership problems are present. Zentachain is an open-source project. Zentachain aims to become the missing gap between decentralized mesh network cloud services such as IPFS (https://ipfs.io) and dynamic routing and addressing protocols such as DNS and HTTPS. This comes down to the fact that Zentachain Labs will upgrade the IPFS peer-to-peer hypermedia protocol with state-of-the-art blockchain technology and its own mesh-network which is called Zentameshnet.

The web will not only become ultra-secure, decentralized and permanent, but it will also become faster and more clear. Zentachain will enable the ability to address large amounts of data with IPFS, and place the immutable, permanent IPFS links onto the Zenta ledger by using a blockchain transaction. This timestamps and secures content, without having to put the data on Zenta itself. Zentachain brings the freedom and independent spirit of the communication at full force and a low cost. The ecosystem will help deliver content in a way that can allow users to save considerable money and information.

High latency networks are a real barrier of entry to the developing world, Zentachain provides resilient access to data, independence of low latency or connectivity to the backbone. Zentachain is to truly decentral, without any exception and will design the ecosystem in such a way that it never keeps track of its users and will never save IP-address or any personal information. By design, the ecosystem simply doesn't have this information nor can link transactions to a certain user or identity.

The vision of Zentachain is largely based and focused on communication. Zentachain also uses extreme encryption of data and communication the multiple encryptions are applied. Zentalk will not only be a communication application as you know today. Zentachain aims at it and knows that the time has come to communicate in a strong range offline to offline. When paying for the so-called free apps with your data and information, Zentachain does not require any personal information from the user unlike today's communications and apps. Zentachain pays the user with their own cryptocurrency Zenta which is supporting the network.

Security & Business

Zentacore holds all business logic in the ecosystem. It houses offline communication - governing and consensus models - Zentameshnet governing. Zentacore will use one of the Blockchain technology such as NPOS, BPOS, DPOS, or Blake2. Zentachain will drastically improve the scalability by utilizing this kind of technology and blockchain. Zentachain has a witness mechanism partitioning of data in the network. To solve the centralization problem, each person holding shares votes, resulting in n-bit representatives (usually n=101), the value of n is decided by the number of nodes on the blockchain. The larger the number of nodes, the larger the value of=n, and the: n node representatives share the same rights.

3. What makes Zentachain awesome?

Zentachain enables users to communicate and store data with Zentalk & Zentavault within the ecosystem. All the running decentralized Apps will be anonymous and secure, there will be no record of users or linked transactions to prove and demonstrate the capabilities of Zentachain, the team introduces a decentralized ultra-secure messenger.

Zentalk

Zentalk is a highly secure hybrid encryption, decentralized and peer-to-peer messenger. Next to great usability, under the hood, you'll find state-of-the-art encryption with AES-256, Diffie-Helman, RSA and El-Gamal security. Zentalk is decentralized, it has no server point. Zentachain guarantees full anonymity and offline communication between the sender and receiver using Zentanodes inclusive hashing function Blake2 and the Tor-network.

Zentavault

Zentavault is a high-throughput encrypted and distributed file vault (encrypted storage) and transfer service. Unlike regular data storage systems, Zentavault will store nothing on the user's device. Zentavault acts as an encryption delivery tool, with the ability to encrypt and dynamically distribute content securely onto the InterPlanetary File System (IPFS). IPFS is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files. In some ways, IPFS is similar to the World Wide Web, but IPFS could be seen as a single BitTorrent swarm, exchanging objects within one Git repository.

Zentagate

„The Gateway to Zentamesh Network“
Zentachain takes security and anonymity very serious. We designed Zentachain in such a way that it is running on its own private Zentamesh network. Zentagate connects the ecosystem to use Zentamesh networks such as the Internet. Zentagate provides additional encryption by AES and anti-hack layer, to ensure the user is connected and protected safely. Next to gatekeeping and safe-unsafe network relaying, we plan on implementing a decentralized name service as well. Zentagate will run this service - enabling routing and rerouting data and transactions in and out the Zentamesh network with the Zentanodes which will allow the user to stay connected without having internet access.

4. Economics of Zenta

Zenta Distribution:
Chain Name: ZENTA
Symbol: ZENTA
Algorithm: DPOS, BPOS, BLAKE2, NPOS (Not Official)
Total Supply: 260.514.201
Softcap: $3.000.000
Hardcap: $10.000.000
Number of Zenta for sale: 60% - 156,308,520

5. The problem worth solving

More and more people are concerned about the issue of privacy in an age in which everything we do is virtually recorded somewhere in a computer system and communicated through some electronic means. Need for secure interaction and digital data storage - there has always been a danger that the initiator may be subject to unauthorized data access and manipulation of information streams, but this threat is expanding day by day. Hackers can now attack you from numerous countries, different regions and multiple locations simultaneously. If that’s not bad enough, there are also multi-billion dollar corporations that have made a lucrative business out of logging, harvesting and selling your data.

They sell your location history, messages, photos, documents, and even the profiles they created on you. Everything about you is up for auction to any corrupt and malicious organizations throughout the world who want this data. Some telcos may harvest on user data and actions. Regardless if they are regulated, and shouldn’t do that, you can never be sure that they are doing or not. Perhaps one day they might use this data for so-called "educational purposes".

It is very likely that this data isn't properly encrypted or anonymized. Services offered by social media companies and messaging applications advertise themselves as a "free service" that does not cost the consumer any money. Instead, these companies are enticing regular people to put all of their data and content online to be stored and sold to malicious organizations that are known to be manipulative. This means that you pay through data instead of paying monthly fees for the service.

6. Data Hacks & Breaches

The number of internet users is rapidly growing (from 1.36 billion in 2007 to 3.57 billion in 2017, an increase of over 2 billion users in the last 10 years). It is observable how our daily lives are becoming more virtualized, and our feelings, thoughts and personal information are making their way into the online world, making them vulnerable to thieves.

We have come to a point in time when everything and everyone can become a target. From personal attacks executed via phishing, ClickJacking, social engineering and other similar techniques to large scale infiltrations in centralized corporate databases which potentially give hackers access to large amounts of personal information. Although the former can, in most cases, be avoided by conscientious use of safe browsing practices, what worries us the most is the latter, because of the sheer scope of affected data and the fact that, in this case, the security of our personal information is completely out of our own hands.

7. Privacy

In the past two decades, mostly due to the impact the internet has had on our everyday lives, the question of preserving an individual's right to privacy has broadened from our physical to our digital environment. The famous quote "Knowledge is Power" evolved to "Data is Power" in today's world, as we continue giving our personal information into proverbial "gold-mines" that attract not just hackers and ill-intentioned individuals, but also companies and conglomerates seemingly operating completely by the law. On one hand, we are being targeted, for our identities, our credit card numbers, digital assets, etc., while on the other, we ourselves are handing over our information in exchange for more comfortable user experience. Although measures, like Europe's General Data Protection Regulation (GDPR), are being implemented to protect the users, their influence and level of execution still raise a lot of questions.

Weak and powerless country administrations have allowed for dubious practices by companies who gather their users' data, effectively giving them free reigns to handle our information at their complete discretion. We have already mentioned some of the most recent privacy affairs in the Data Breaches chapter of this Whitepaper. These and other similar incidents seem to either sadly fade into oblivion without proper repercussions and reactions from the wider public, or they sometimes create an atmosphere of paranoia and distrust which is detrimental to our interpersonal communication. This is why, it is imperative that we become aware of our privacy rights and look for new ideas like blockchain, as solutions to the burning privacy issues. Blockchain provides the tools users need to be fully in control of the means of their personal data distribution. It allows for higher degrees of anonymity (some even enable complete anonymity) and deployment of different encryption methods to safeguard that data. It gets rid of the vulnerable centralized databases and is immune to data tampering and manipulation. Ultimately, it presents itself as a platform with tremendous potential for re-establishing trust lost by unscrupulous cash-grabbing behavior exhibited by the world's leading businesses.

8. Centralized Messenger

As the presence of the Internet in our daily lives grew, so did the need for more efficient, more widespread means of online communication. Subsequent decades brought forth progress and the emergence of popular messaging apps like AIM, ICQ, and PowW which started incorporating more advanced features including private messages, multi-user groups, and file sharing.

In recent times the increase in popularity of messenger apps has correlated directly with the increase in smartphone usage. Desktop apps have been replaced by their mobile counterparts, enabling for more instant, on-the-go means of communication. The user base has grown exponentially, with leading service providers like WhatsApp, Facebook, Messenger, and WeChat individually amassing over 1 billion monthly active users.

However, today's messenger systems are far from being flawless. Recent events have raised serious questions about the issues of privacy. Facebook (owner of the two most popular messaging platforms) has been hit with indictments over selling user data for use in political purposes and the most popular messaging app in blockchain space. Telegram has agreed to disclose its users' data to "the relevant authorities" if it receives a court order. This is an issue related directly to the centralized architecture of existing messenger apps. Such an architecture enables the app owners to use, manipulate and restrict content, leaving its users vulnerable to potentially serious privacy breaches.

Today's messengers seemingly attempt to solve this by implementing end-to-end encryption solutions, but again, these close sourced implementations raise questions about the quality and actual levels of encryption. Another weakness of today's messenger apps is it's vulnerability to SIM swap attacks. As most apps require a phone number to register, hackers can potentially gain access to their user's messenger content by convincing the carrier to switch the victim's number to a SIM card they own.

9. Centralized Clouds

Centralized clouds are services that enable storing data on remote servers and access to that data via the internet. They are either free to use or require a monthly fee which is usually based on the length of the contract and storage capacity. Centralized clouds work by utilizing virtualized data centers which can be linked to the user via a web interface. User uploads their files over the internet which then gets stored on data servers.

They can be accessed only by providing a unique ID which then triggers metadata assembly allowing the user to view, edit, transfer or synchronize the files. To ensure uninterrupted data retrievability and integrity, the files should be stored on more than one server. There are different types of centralized cloud storages:

Public Cloud Storage - is a shared resource environment in which the client is charged only for the resources being used and the service provider is responsible for the cloud infrastructure maintenance. Private Cloud Storage - is usually an on-premise service used by a single client/organization and maintained by the service provider. Hybrid Cloud Storage - is a combination of public and private cloud storage which enables the flexibility of storing sensitive and publicly accessible information on different cloud types. It is obvious why centralized clouds have gained popularity in recent times.

The increased demand for data mobility and accessibility is causing users to switch over from their physical counterparts like HDDs and USB flash drives. However, in spite of a step in the right direction, centralized could services still have their problems. Firstly, the client is not the data owner. The centralized server architecture puts the client's data into the hands of the service providers and also makes it vulnerable to data breach hacks as well as DDoS attacks which interrupt the continuity of data access. Public Cloud services are especially exposed to attacks because of their resource sharing component which allows for malicious intrusions via one of the cloud's clients.

Laws and regulations are another major concern, with data security and privacy being susceptible to the ever-changing rules set by different governments of the world. For smaller organizations looking to employ complex data onto the cloud, the cost can be a serious issue, as large bandwidth requirements might prove to be financially unviable.

10. About Zentachain

Zentachain presents viable solutions to these problems. Open source, content that is not stored on centralized servers and integration of technologies like Zentameshnet, Hyperborea, and Tor-network for an increased level of security, clearly shows the benefits of using apps developed on this platform. Zentachain looks forward to safeguarding customers' data with fully secure data protection - ecosystem, against breaches and all kinds of cyber-attacks! Today, every service that people use is understood to be a confidential source of information for retailers and organizations to receive targeted consumer advertising. Zentachain's goal is to provide people and companies a way to remain secure, without the fear of eavesdrop, spying, or retrieving their data. Zentachain pledges to never keep any metadata on our customers and will not save your IP address, your email, or phone number. Nothing will be required in service use, except our App Zentalk which includes Zentawallet with a layer 2 to protecting payment between receiver and sender. As with all our services, Zentachain will have no information about your identity, the region in which you live, or any personal data about you. Zentachain does not care about these personal effects because our only goal is to provide world-class services that will give the consumer absolute anonymity, security, and privacy. Another important aspect of Zentachain is to provide offline communication via the decentralized Zentalk App(Provides communication without internet). Zentalk will have quantum resistance with multiple cryptography encryptions.

11. Zentachain Ecosystem

Zentachain ecosystem has multiple solutions, decentralized applications to keep its own value high and to protect the user in its own blockchain and Zenta will be used as a reward for people who are hosting of Zentanodes. The owners of Zentanode will be rewarded monthly and this is necessary for the network Zentameshnet to be successful. It is the same as a mining system but more energy-efficient and user-friendly. Zentalk is here for modern communications with multiple communication encryption capabilities. Zentavault is a decentralized IPFS cloud storage application that can store data in an encrypted and secure manner and it is the second application of Zentachain.

- **Anti-inflation**

Zentachain is an anti-inflation system and decentralized network which is built with deep privacy protection. Today, most communication applications and cloud storage systems have identified their main vision as acquiring user data and much more. Zentachain is different, it rewards the user and supporter of Zentalk and Zentavult. Zentachain will never be able to live with user data and information, but with products and a communication system that focuses entirely on privacy and a highly efficient own blockchain.

- **Zenta Reward**

Zentachain will reward all Zentanode holders on the network each month. There will be no difficulty in the network and Zenta's rewards will be fixed. All a user needs to do is to run Zentanode. If a user disconnects, Zentanode will no longer be rewarded with Zenta, which means that the user must run Zentanode permanently.

- **Zentanode**

Zentachain will have its nodes called Zentanodes. Zentanodes is no different than a node, a device or a data point in the Zentamesh network. Zentanodes will be for sale only on our official homepage. Zentanodes have been created to have a long-range of offline communications. All incomes from the Zentanodes will be used to support the Zenta Blockchain.

- **Zentalk**

Zentalk is an ultra-secure, hybrid and encrypted decentralized peer-to-peer (P2P) messenger application. Zentalk decentralized application will be not come out first as a free and fully public open-source Application.

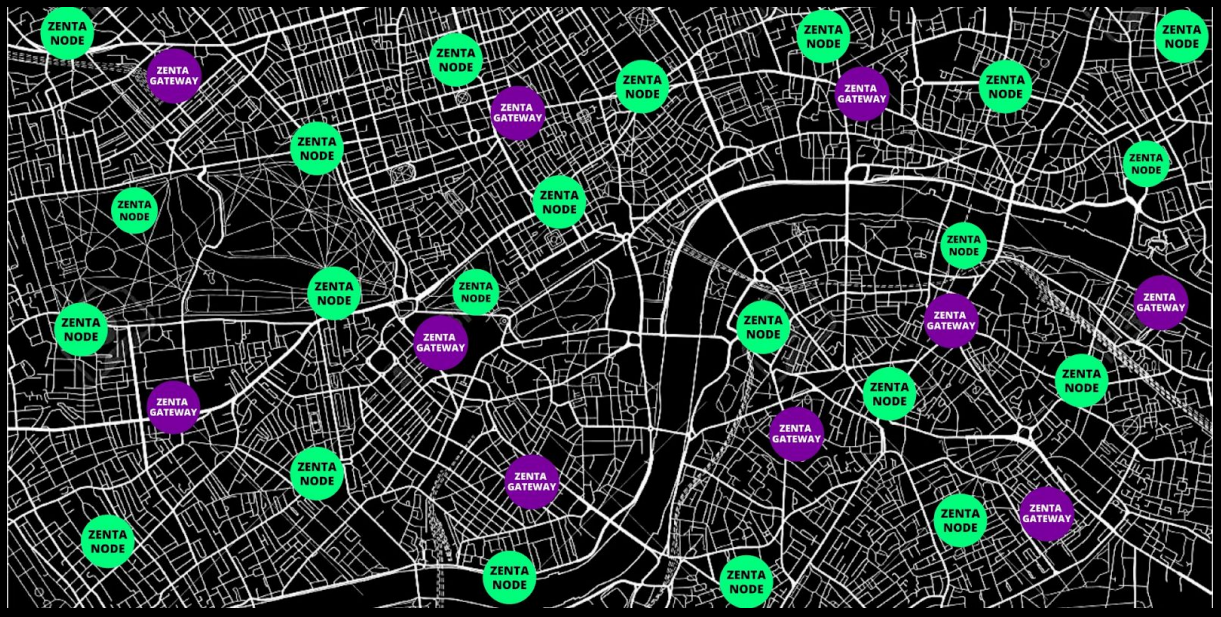
- **Zentavault**

Zentavault requires no monthly usage fees, instead, there is only a small transaction fee to upload data. Zentavault is a file-encrypting and distribution tool.

12. Communication

Communication means that two or more people can easily talk and communicate with each other. Communication on a technological platform was first achieved by telephones. And phones have gone down in history as a major technological advancement, but the speed of technology has increased day by day and today there are countless sources of communication. In the early days, telephones were able to maintain privacy and freedom, but the development of technology has shortened the time it takes. Because the communication and conversation between the two people began to be listened to by others. Therefore, the privacy of people began to disappear. However, as new technologies are emerging day by day, people's freedom and confidentiality are being tried to be re-protected, but this has not been fully achieved. Because today all conversations and correspondence are being followed in some way. And unfortunately, this is not the case when we are talking on the phone or with any communication device, even though we think that our conversations are only hidden between us and the other person.

13. Zentalk



Zentalk is an ultra-secure, hybrid and encrypted decentralized peer-to-peer (P2P) messenger application.

Zentalk achieves its privacy and security through the integration of Zentamesh-networking technologies. Zentamesh Networking (Zentameshnet) is known as one of the safest and most reliable variations of networking available. Zentamesh Network technology is powerful, has excellent load distribution, and contains zero central administration.

The Zentamesh-network is a network topology in which each node relays data for the network. Zentachain implements .cjdns- nodes an encrypted IPv6 network using public-key cryptography for address allocation and a distributed hash table for routing. No need configuration and it solves many security and scalability issues that plague existing networks. All Zentamesh nodes cooperate in the distribution of data in the network. Each device using Zentalk acts as a node in the Zentameshed network. These nodes have the unique ability to interconnect with each other in a distributed fashion.

Zentamesh network relay messages using either a flooding technique or a routing technique. With routing, the message moves along the road, jumping from one Zentanode to another until it reaches its destination. To ensure the availability of all routes, the network allows continuous connections using self-healing algorithms, such as Shortest Path Bridging, and corrupted or defective routes reconfigure itself. Self-healing allows a routing-based network to operate when a Zentanode breaks down or when a connection becomes unreliable. As a result, the network is absolutely reliable, as there is often more than one path between a source and a destination in the Zentanetwork. Although mostly used in wireless situations, this concept can be also applied to wired networks and software interaction.

An example of the common meshed network technology, if you register a new Zentanode in your house like a new light bulb, the device pairs with the control center through a self-configured meshed network. Common mesh networks are typically wireless but Zentameshnet is the blockchain-based network topology and less infrastructure.

Zentalk provides technological privacy, this means only highly encrypted Metadata is shortly kept and afterward automatically unrecoverably removed. This is achieved through the integration of the Zentamesh network and its architecture. Zentalk sends and tunnels all messages and data through the Zentamesh network. This ensures that any messages shared between the sender and recipient being the highest levels of their privacy.

In the Zentamesh network, each Zentanode is connected to one or more than one node. When multiple Zentanodes are interconnected, this is known as a fully Zentameshed network. When a message is sent from Zentalk and the data is sent through the Zentamesh network, it passes from one Zentanode to the next until the message has reached the desired recipient. Thanks to the design of the nodes in the Zentamesh network, we do not know which node sends or receives which

message. This remains anonym for the communication between the sender and the recipient. Zentalk users will not be rewarded by transferring just a single message. All Zentanode holders will be rewarded with the Zenta. This means that you must own a Zentanode and run it continuously; It is also very energy efficient and friendly. Zentalk is a highly secure encrypted messenger and every message in and outside on the network has been designed so that the user of Zentalk can't make any mistakes for his privacy. Zentalk will also not leave a gap open which could make users vulnerable to attack or hacking the users. Zentalk will use different types of encryption because some encryptions are vulnerable we will only use the ones that are really secure for Zentalk. Each encryption will have its own role and all the encryptions we use will be listed in the whitepaper. Zentalk will use encryptions that are really secure against quantum computer attacks.

Zentalk Features:

- Zentalk does not require Google Play services
- Personal information: No
- Having a Server/Cloud Server: No
- IP-Addresses are protected: Yes with the Tor-Network
- Messages Stored on a Server: Never
- Messages are encrypted on own device: Yes
- Data are encrypted on own devices: Yes
- Recovering user Account: No
- Backup: No
- Offline (using without Internet): Yes
- Google Tracker: No
- Supports Data: Yes
- Phone number: No
- E-mail: No
- Register: No
- Protects from men in the middle attack: Yes
- Group Chat: Yes
- Key-Sharing: Yes
- Sharing News: Yes
- Zentawallet: No first/Later Yes Chat & Pay (Only: Bitcoin, Ethereum, Zenta)
- Bitcoin Payment over Zentamesh network: Yes
- Bitcoin Payment with Tor Routing: Yes
- Zenta Rewards: Yes (Hosting Zentanode)
- Hash-Algorithms: BLAKE2b
- Hybrid Encryption: Yes (RSA, AES, DHKE, EL-Gamal)
- Block Cipher Encryption: 128 Bit
- Key Size: 256 Bit
- RSS: Yes
- API: Yes
- Private Nodes: Yes

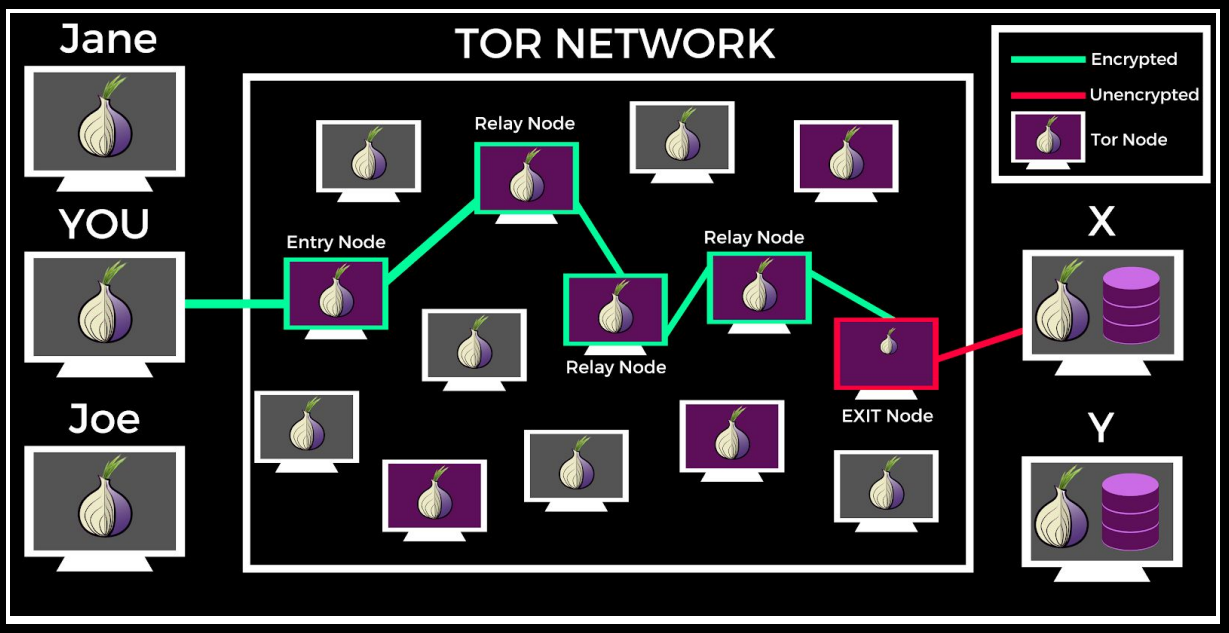
- Private Gateway: Yes
- Zentanodes Encrypted: Yes
- Onion-Share: Yes
- Quantum resistance: Yes
- Self-destruct after being read: Yes
- One-Way hashed Password Signature: Yes
- Stop Over Tracking by other Apps
- Using without having a SIM-Card: Yes
- Zentalk users within Bluetooth or Wi-fi range can communicate with other users and other users via Zentanode, even if they do not have access to the Internet.

Many features will continue to be added in the future.

14. Zentalk & Tor Network

Tor is a free and open-source software used to provide anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router". Tor directs over a free volunteer network of more than 7000 relays to hide a user's Internet traffic and location from anyone doing network surveillance or traffic analysis. Using Tor makes it more difficult to track user's Internet activity: this includes "visits to Websites, online posts, instant messages, and other communication forms". However, Internet Service Providers (ISPs) in various countries around the world are often warned by their governments to prevent users from accessing Tor. As a result, Tor bridges were developed to enable users to connect to the Tor network in countries where such access is blocked. By keeping some of the bridge relays secret, users can evade Internet censorship that relies upon blocking public Tor relays. Tor does not prevent an online service when it is being accessed through Tor. Tor protects a user's privacy but does not hide the fact that someone is using Tor. But, the bridges hide the fact that a person uses Tor. Tor's purpose is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored. When a user runs Tor, online data collectors won't be able to perform traffic analysis and gather data on user's internet habits such as Google Ads. So, surveillance organizations like the NSA won't be able to observe users. Tor encrypts the data, multiple times and sends it through a virtual circuit comprising successive, including the destination IP address, randomly selected Tor relays. Therefore, while developing the Zentalk messenger application, we have taken the privacy and freedom of the user into consideration. Zentalk guarantees full anonymity of communication thanks to Tor protocol. Users easily turn Zentalk on and off without installing a second VPN provider or Orbot.

Tor-Network



15. Zentalk & Algorithm & Encryption

Cryptography

Cryptography or cryptology is the application and examination of some techniques for secure communication between third parties, called aggressors. More generally, encryption is about creating and analyzing protocols that prevent third parties from reading private messages from individuals. Various aspects of information security like data confidentiality, data integrity, authentication are important to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, communication science. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

History of Encryption

Circa 600 BC: The ancient Spartans use a device called a scytale to send secret messages during battles. This consists of a leather strap wrapped around a wooden rod. The letters on the leather strip are meaningless when it's unwrapped, and only if the recipient has the correctly sized rod does the message make sense.

Circa 60 BC: Julius Caesar invents a password that changes characters in three places: A, D, B, E, and so on.

1553: Giovan Battista Bellaso envisions the first cipher to use -an agreed- proper encryption keyword that the recipient needs to know if he or she wants to decode the message.

1854: Charles Wheatstone invents the Playfair Cipher, which encrypts pairs of letters instead of single ones and is, therefore, harder to crack.

1917: An American, Edward Hebern, invents an electro-mechanical machine in which the key is embedded in a rotating disc. It's the first example of a rotor machine. It encodes a substitution table that is changed every time a new character is typed.

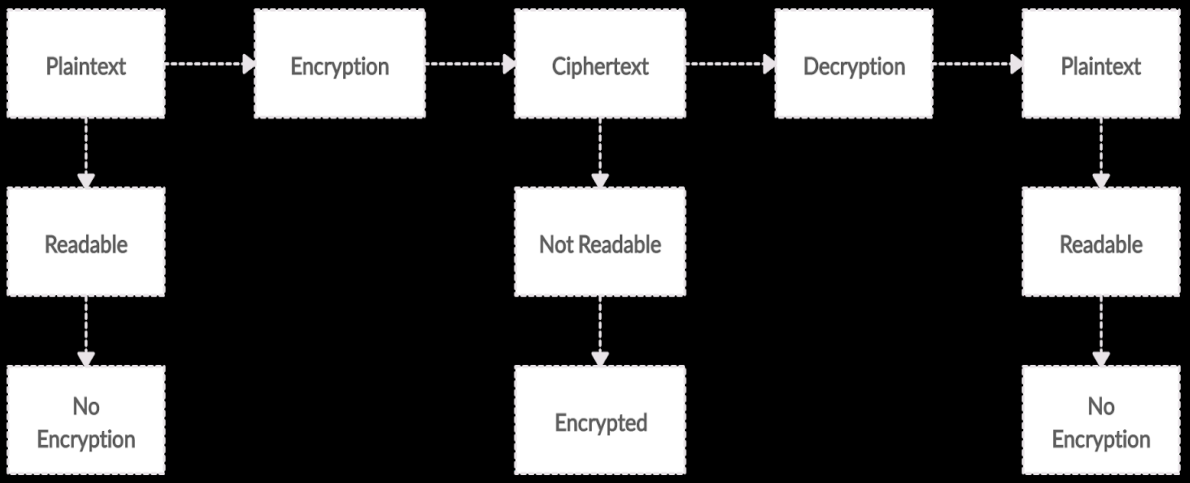
1918: German engineer Arthur Scherbius invented the Enigma machine for commercial use. It uses a few more than a rotor used by Hebern's machine. The German army, who knew the genius, began to use it to send encrypted transmissions.

1932: Polish cryptographer Marian Rejewski discovers how Enigma works. In 1939, Poland shared this information with the French and British intelligence services, allowing cryptographers like Alan Turing to figure out how to crack the key, which changes daily. It proved to be very important in winning World War II.

1945: Claude E. Shannon of Bell Labs publishes an article called "A mathematical theory of cryptography". It's the starting point of modern cryptography.

Early 1970s: IBM forms a 'crypto group', which designs a block cipher to protect the company's customers' data. In 1973, the US adopts it as a national standard - the Data Encryption Standard, or DES. It remains in use until it's cracked in 1997.

2000: DES is replaced by the Advanced Encryption Standard, or AES, which is found through a competition open to the public. Today, AES is available royalty-free worldwide and is approved for use in classified US government information.

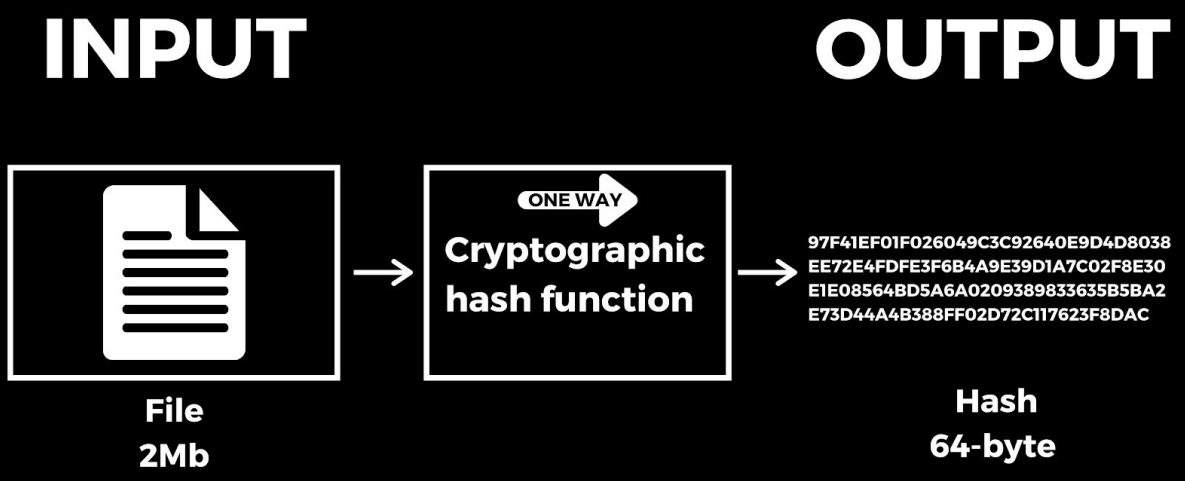


Hash Functions

Hash functions are the building blocks for modern cryptography. A hash function is a cryptographic algorithm that is used to transform large random size data to small fixed-size data. The data output of the hash algorithm is called hash value or digest. The basic operation of hash functions does not need any key and operate in a one-way manner. One-way operation means that it is not possible to calculate the input from a specific output.

- The values returned by a hash function are called hash values.
- A cryptographic hash function allows one to easily verify that some input data maps to a given hash value.
- Hash function is any function that can be used to map data of arbitrary size to data of fixed size.
- If the input data is unknown, it is difficult to reconstruct it by knowing the stored hash value.
- Hash functions do not have a key.
- For long-term security, 256 bits or more are recommended.
- SHA-1 has serious vulnerabilities and should not be used if possible.
- The SHA-2 algorithms have not yet been broken, but they work according to the same principle as SHA-1.
- The SHA256/512 Blake2b hash function and some others are considered safe. (They have quantum resistance for the next 20-30 Years)

Hashing-Function



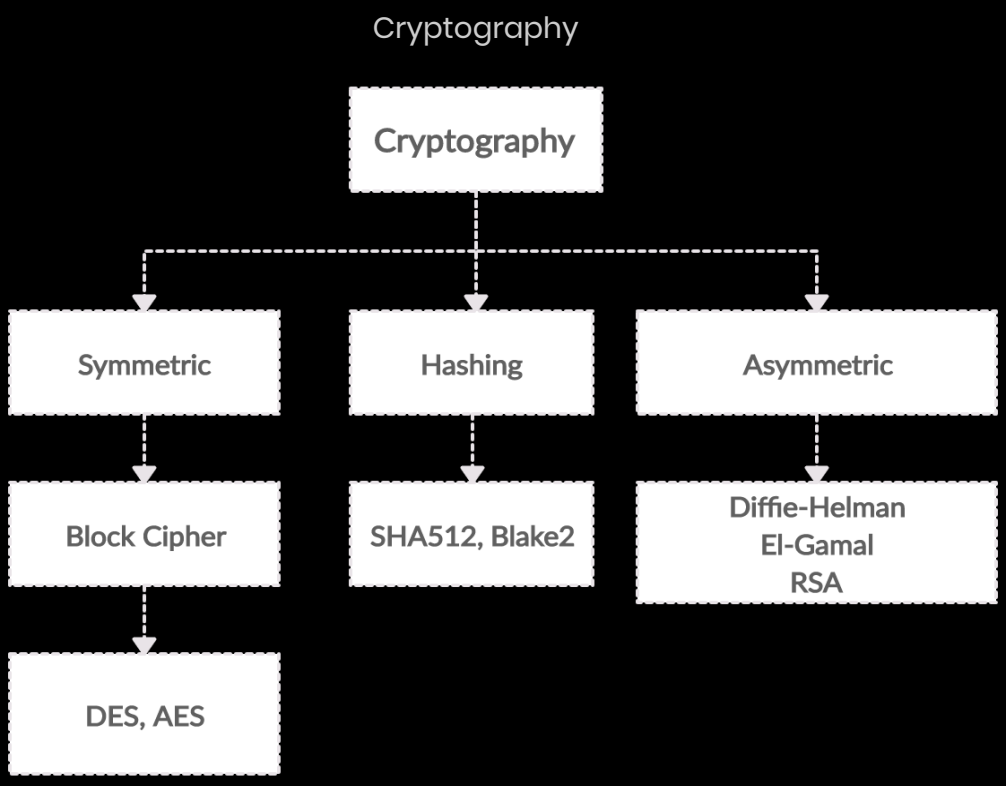
Encryption

Encryption is the method by which a text or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.

Encryption is widely used on the internet to protect user-information being sent between a browser and a server, including passwords and other personal information that should remain private. Organizations and individuals also commonly use encryption to protect sensitive data stored on computers, servers and mobile devices such as phones or tablets.

How encryption works

Encryption uses algorithms to scramble your information. And then the message is transmitted to the receiving party, who is able to decode the message with a key. There are many types of algorithms, which all involve different ways of scrambling and then decrypting information. Today's widely used encryption algorithms fall into three parts: Hash Functions, symmetric, asymmetric.



Block Cipher

A block cipher takes a block of plaintext bits and generates a block of ciphertext bits, generally of the same size. The size of the block is fixed in the given scheme. The choice of block size does not directly affect the strength of the encryption scheme. The strength of cipher depends on the key length.

Block Cipher Schemes:

- There is a vast number of block ciphers schemes that are in use. Many of them are publicly known. The most popular and prominent block ciphers are listed below.

- Triple DES - It is a variant scheme based on repeated DES applications. It is still a respected block cipher, but it is less efficient than the faster block ciphers available.

- Advanced Encryption Standard (AES) - It is a relatively new block cipher based on the encryption algorithm Rijndael that won the AES design competition.

- IDEA - It is a sufficiently strong block cipher with a block size of 64 and a key size of 128 bits. A number of applications use IDEA encryption, including early

versions of Pretty Good Privacy (PGP) protocol. The use of the IDEA program is limited due to patent issues.

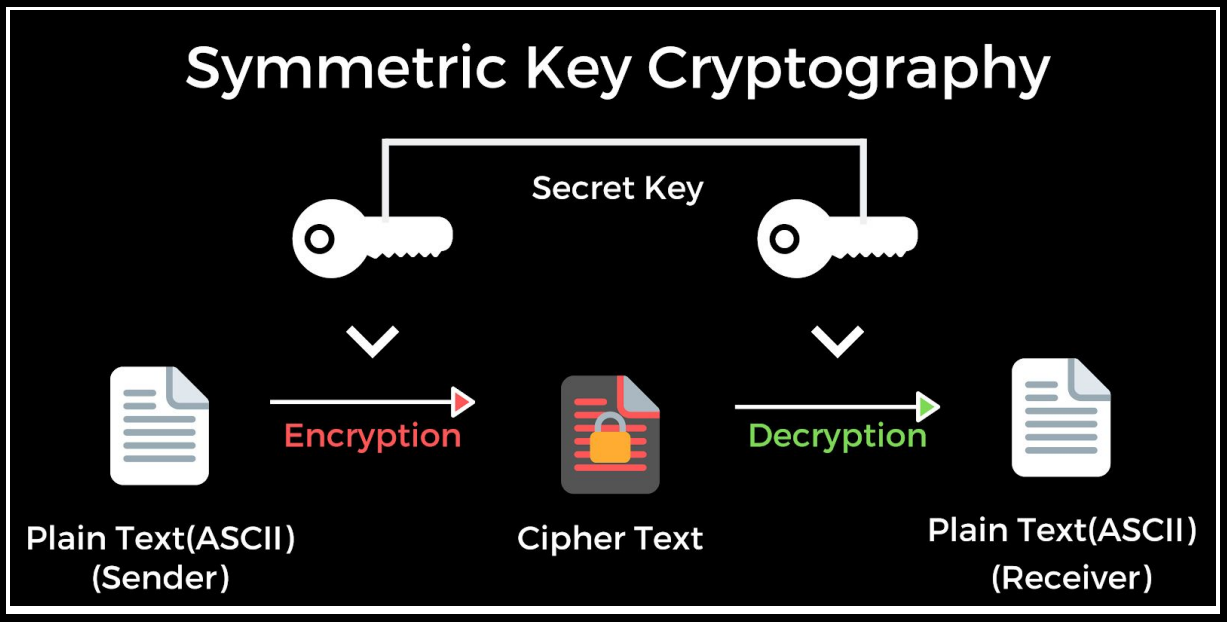
- Twofish - This scheme of block cipher uses a block size of 128 bits and a key of variable length. It was one of the AES finalists. It is based on the earlier block cipher Blowfish with a block size of 64 bits.

- Serpent - A block cipher with a block size of 128 bits and key lengths of 128, 192, and 256 bits, which was also an AES competition finalist. It is slower but has a more secure design than other block ciphers.

Symmetric Encryption

Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. This encryption method differs from asymmetric encryption where a pair of keys, one public and one private, are used to encrypt and decrypt messages. AES (Advanced Encryption Standard) is one of the most used symmetric encryption algorithms.

Symmetric Encryption



AES Encryption

The most commonly used symmetric algorithm is the AES (Advanced Encryption Standard), which was originally known as Rijndael. This is the standard set by the U.S. National Institute of Standards and Technology in 2001 for the encryption of electronic data announced in U.S. FIPS PUB 197. This standard supersedes DES,

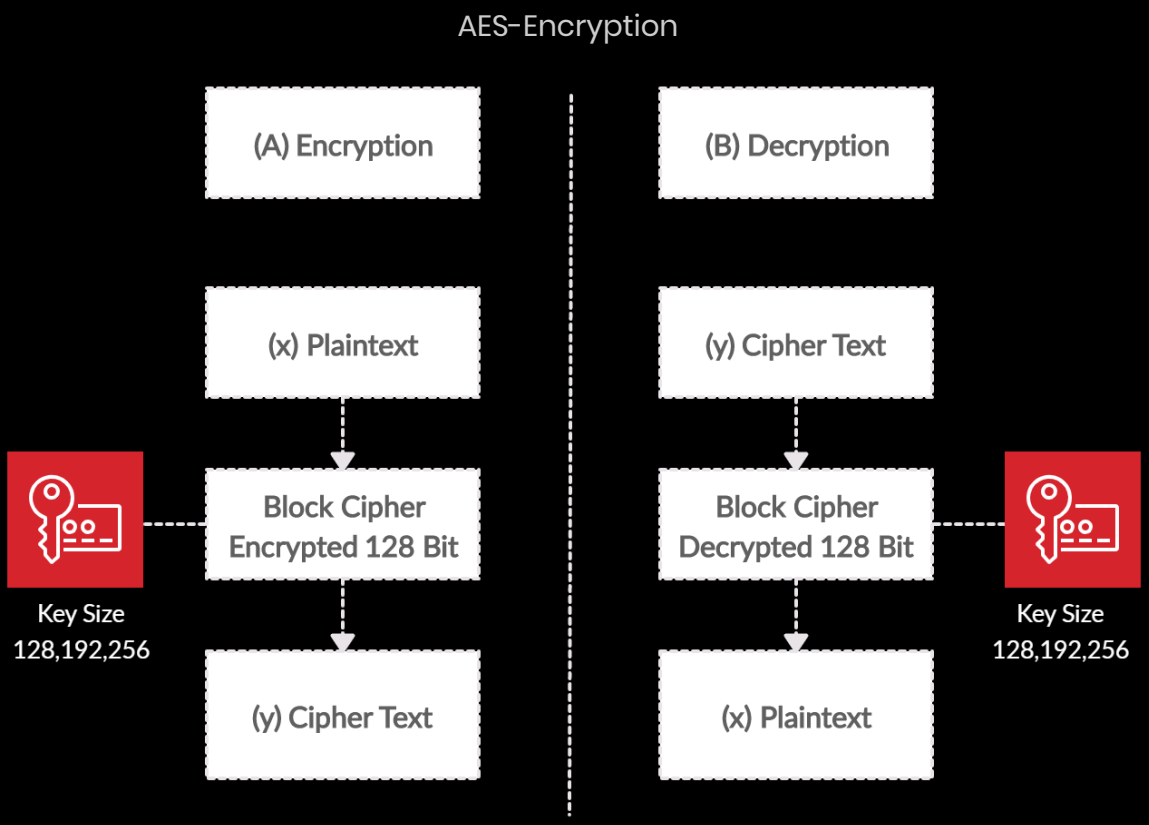
which had been in use since 1977. The AES cipher has a block size of 128 bits but can have three different key lengths as shown with:

- AES - 128 Bit - (K)
- AES - 192 Bit - (K)
- AES - 256 Bit - (K)

Rounding(R) numbers based on the key lengths:

- 128 Bit = 10 (R)
- 192 Bit = 12 (R)
- 256 Bit = 14 (R)

1. To date, there are no attacks on AES encryption.
2. AES can be implemented very efficiently in software and hardware.
3. It offers very good long-term security against brute force attacks.
4. AES has been intensively studied since the late 1990s
5. In practice, there is no reason for multiple encryptions with AES(DES today needs multi-key encryption called also as a TDES or 3DES).
6. The same secret key is used for encryption and decryption.
7. Alice and Bob both have the same cryptographic capabilities because they both have the same key, so any actions Alice can perform (such as encrypting and decrypting) can also be performed by Bob and vice versa.
8. More number of rounds provide a more secure system. But at the same time, more rounds mean the inefficient slow encryption and decryption processes.
9. Stronger and faster than 3DES.
10. Software implementable in C and Java.



The Key exchange problem with AES

The symmetric key must be exchanged between (A)Alice and (B)Bob over a secure channel. Therefore, the key can not be sent directly over a normal connection which would be the most convenient way and a different form of transmission is required. Even for medium-sized networks, such as a company with 1000 employees, more than 2 million keys are needed, which have to be generated and exchanged via a secure channel.

- In E-commerce applications, it is often important to prove that Alice really sent a certain message such as ordering a Zentanode.
- If we only use symmetric cryptography and Alice later changes her mind about the purchase, she can always claim that Bob (the seller) mistakenly created the order. Preventing this is called non-refoulment and can be achieved with asymmetric cryptography(RSA, El-Gamal, DHKE).

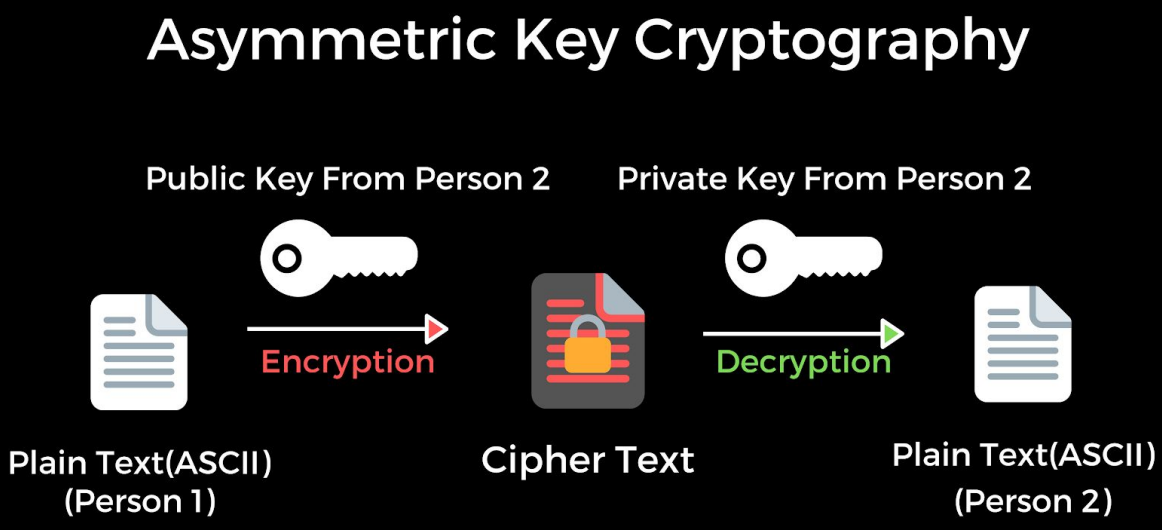
Asymmetric Encryption

Asymmetric cryptography, also known as public-key cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. The RSA encryption algorithm is the most widely used public-key algorithm, partly because both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This feature provides not only confidentiality but also a method to ensure the integrity,

reliability, and incalculability of electronic communications and data through the use of digital signatures.

- Asymmetric cryptography a very desirable tool for many security applications today.
- Asymmetric cryptography is dealt with in the workshop series Public-Key Cryptography (PKC).
- There are asymmetric algorithms which are also based on one-way functions.
- Families with disposable functions are of particular interests: Hash-based and code-based.
- Asymmetric algorithms provide opportunities where symmetric algorithms do not allow key exchange, especially through unsafe channels and digital signatures.
- Since about 2005, there has been much interest in asymmetric procedures in the “scientific” research.
- A major motivation for interest in these methods is that there have so far no attacks on asymmetric algorithms based on quantum computers.
- It is much slower than algorithms like AES or 3DES (TDES). This is because of very high computational effort required by RSA (and all other asymmetric algorithms).

Asymmetric



Rivest–Shamir–Adleman Encryption (RSA)

RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem". The acronym RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977.

A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but only someone with knowledge of the prime numbers can decode the message. Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem remains an open question. There are currently no published methods to defeat the system if a large enough key is used.

Encryption and Decryption RSA

To encrypt a plaintext M using an RSA public key we simply represent the plaintext as a number between 0 and N-1 and then compute the ciphertext C as:

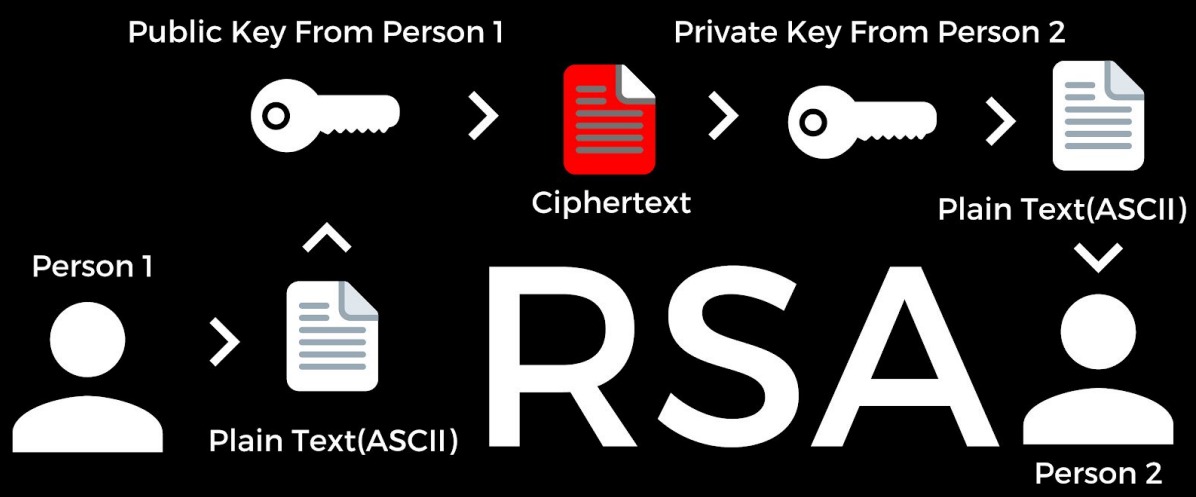
$C = Me \bmod N$

Decryption RSA:

To decrypt a ciphertext C using an RSA public key we simply compute the plaintext M as:

$M = Cd \bmod N$

RSA-Encryption



Diffie-Hellman

The Diffie-Hellman algorithm is one of the earliest known asymmetric key implementations and it is mostly used for key exchange. Although symmetric key algorithms are fast and secure, key exchange is always a problem. We have to figure out a way to get the private key to all systems. The Diffie-Hellman algorithm helps with this. The Diffie-Hellman algorithm will be used to establish a secure communication channel. This channel is used by the systems to exchange a private key. This private key is then used to do symmetric encryption between the two systems. That is why we are using the DH-Key-Pairs exchange. Diffie–Hellman algorithm is vulnerable to a man-in-the-middle attack.

Diffie-Hellman groups are used to define the length of the base prime numbers that are used during the key-exchange process. There are three types of Diffie-Hellman groups, as follows:

1. This is the least secure group and it provides only 768 bits of keying strength.
2. This group is set to a medium level, at 1024 bits of keying strength. Diffie-Hellman group.
3. This group is set to the highest level, at 2048 bits of keying strength.

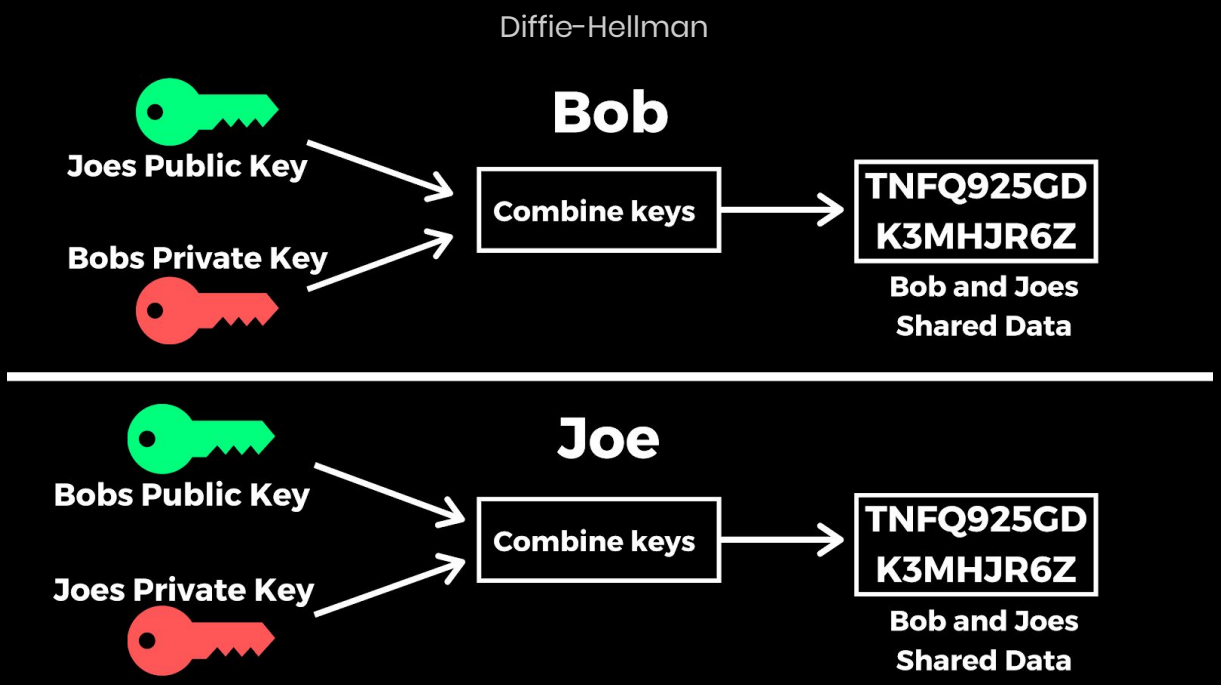
Diffie-Hellman Protocol

- For the Diffie-Hellman protocol in the prime number p should be at least 2048 bits to ensure long-term security.
- The Diffie-Hellman protocol is a widely used method for key exchange. It is based on cyclic groups.

Diffie-Hellman Hybrid Systems

Hybrid session key systems are similar to the Diffie-Hellman systems except that instead of going through the multiple steps to develop a session key the following occurs.

1. Party A simply generates a session key, encrypts it with Party B's public key, and sends the encrypted message to Party B.
2. Party B then decrypts the message with his or her private key, inputs the session key into his or her single-key software or telephone, and begins the conversation or data transfer in the faster temporary, single-key mode.
3. The actual process of selecting the temporary, random session key is invisible to the users because it occurs in the mathematical algorithm contained in the encryption software each uses.



El-Gamal

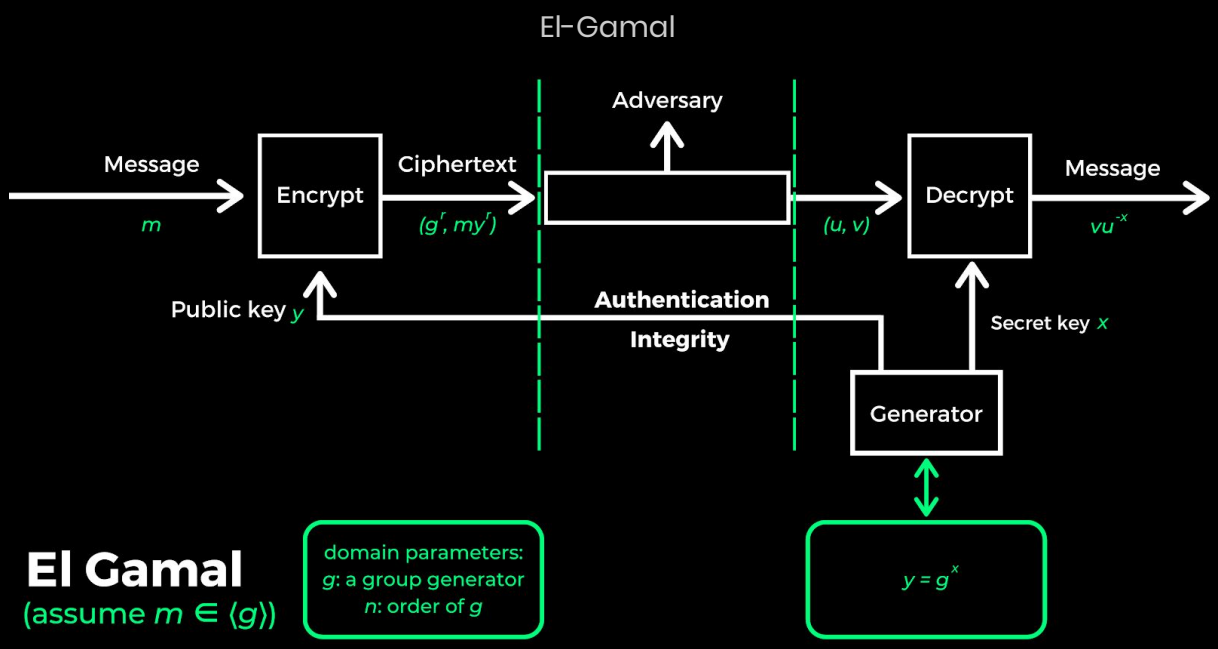
El-Gamal encryption is a public-key cryptosystem. It uses asymmetric key encryption for communicating between two parties and encrypting the message. Elgamal algorithm was invented by Taher El-Gamal which is based on Discrete Logarithm Problem and Diffie Hellman key exchange. El-Gamal is a probabilistic encryption method the encryption of two identical messages results in different cipher rates.

- El-Gamal has the disadvantage of having ciphertext twice the size of the plaintext.

- Each time when the same plaintext is encrypted it gives a different ciphertext.
- El-Gamal can be used for encryption as well as digital signature.
- El-Gamal is based on cyclic groups.
- For El-Gamal encryption, the prime number p should be at least 2048 bits.

El-Gamal Protocol

- Unlike the DHKE, no trusted third party is required to select the prime number and primitive element.
- The construction phase is only carried out once by the parties.
- The encryption phase and the decryption phase are executed with each message exchange.
- Alice only needs to send one message, while the Diffie-Hellman-based protocol requires two messages to be sent.



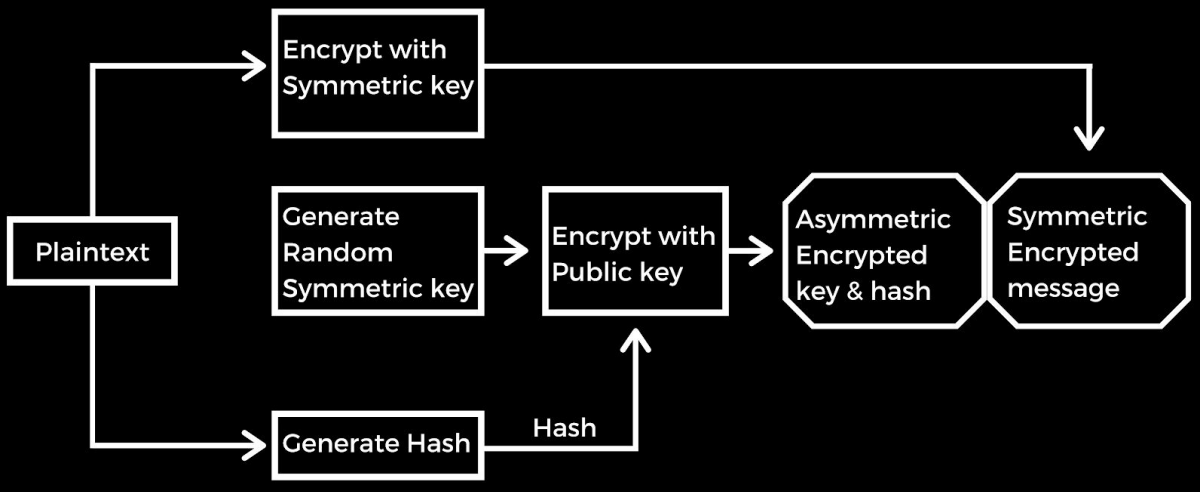
Hybrid Encryption

Hybrid encryption is a mode of encryption that merges two or more encryption systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively are speed and security. Hybrid encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure. A hybrid encryption scheme is one that blends the convenience of an asymmetric

encryption scheme with the effectiveness of a symmetric encryption scheme. The combination of encryption methods has various advantages.

- Users then have the ability to communicate through hybrid encryption.
- Asymmetric encryption can slow down the encryption process, but with the simultaneous use of symmetric encryption, both forms of encryption are enhanced.
- The result is the added security of the transmittal process along with overall improved system performance.
- Increased computational complexity, cryptographic goals such as confidentiality, integrity, and authenticity can be achieved by using hybrid cryptographic approaches.

Hybrid Encryption



SHA-256

SHA-256 is one of the sequential hash functions of SHA-1 (collectively called SHA-2) and is the most powerful of the available ones. SHA-256 is not much more complex to code than SHA-1 and has not yet been compromised in any way. The 256-bit key makes it a good partner-function for AES. SHA-256 is a function that takes an input of random size and produces an output of a fixed size.

In addition, SHA-256 has quite good technical parameters:

- Block size indicator: 64 Bytes.
- Maximum allowed message length: 33 Bytes.
- Characteristics of the message digest size: 32 Bytes.
- The standard word size: 4 Bytes.
- Internal position length parameter: 32 Bytes.
- The number of iterations in one cycle: 64.
- The speed achieved by the Protocol (MiB/s): approximately 140.

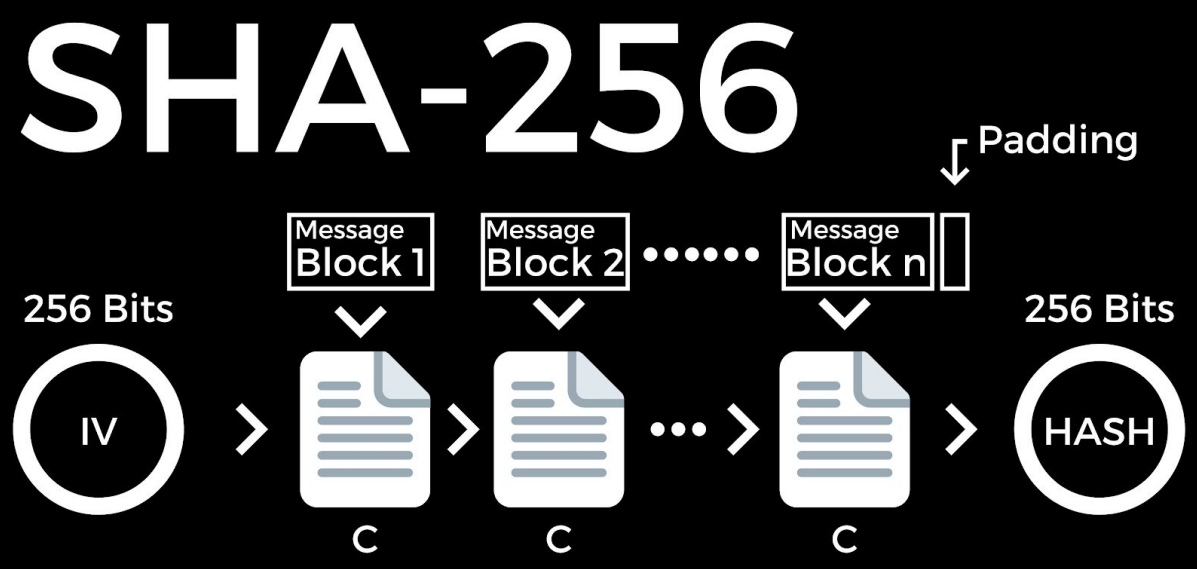
The SHA-256 hash function is utilized within the Bitcoin network in two main ways:

- Mining
- Creation of Bitcoin addresses

More importantly:
Over time, cyberattacks increase significantly as the cost of computer processing power decreases. By 2025, this will make the current digital signature-less secure than it is today. For this reason, the algorithm selection will be an important decision. This is necessary because temporary short-term upgrades can simply compromise its security. No hashing algorithm is able to maintain a high level of security for even a decade.

This does not mean that cryptographers will sit idly by while waiting for a problem. The Sha-2 successor, known as SHA-3, has already been completed. When the time comes to make that transition, the online technology industry will be able to use SHA-3 as its next choice. But, perhaps, by that time there will be a completely different algorithm.

It takes years to research and test new cryptographic standards before you can start developing software to support them. It is only when we are one step ahead that we can talk about one or another level of security.



Blake2

The BLAKE2 cryptographic hash function was designed by Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O'Hearn, and Christian Winnerlein.

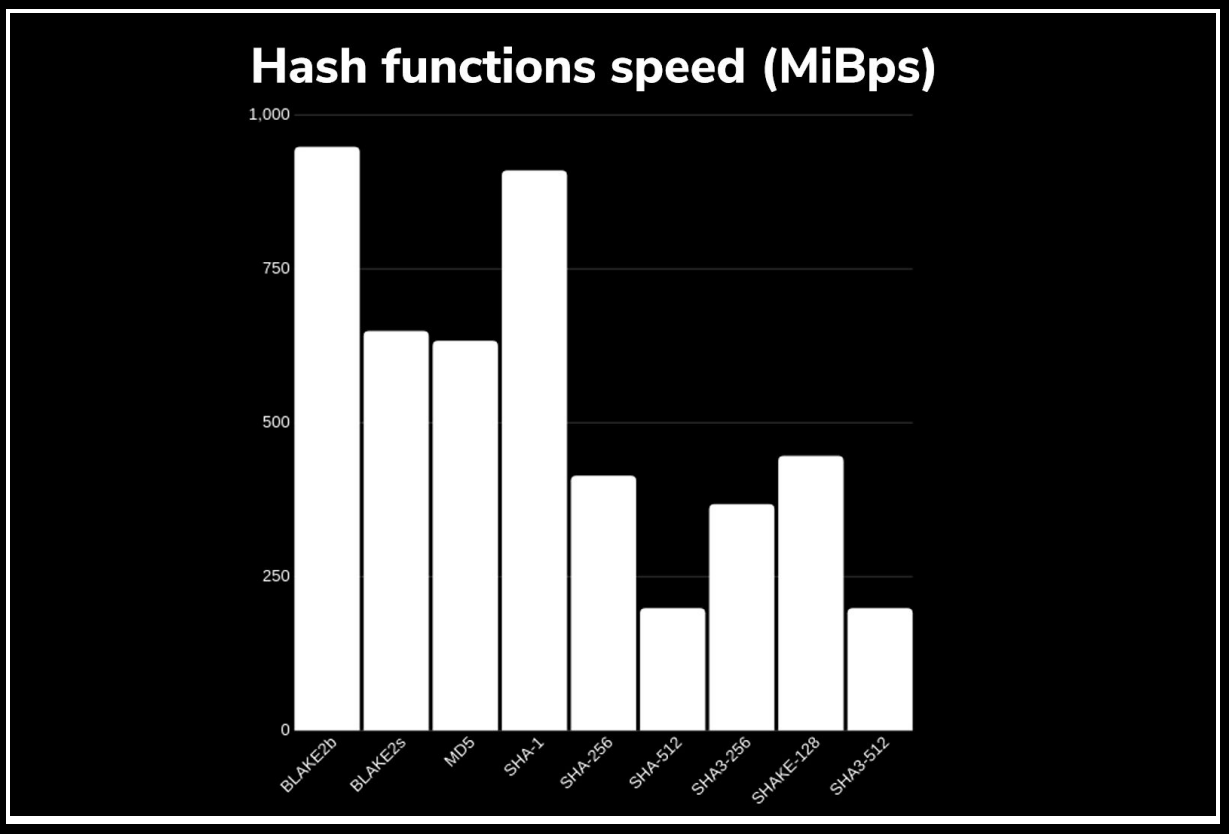
BLAKE2 is a cryptographic hash function faster than MD5, SHA-1, SHA-2, and SHA-3, yet it is at least as secure as the latest standard SHA-3. BLAKE2 has been adopted by many projects due to its high speed, security, and simplicity.

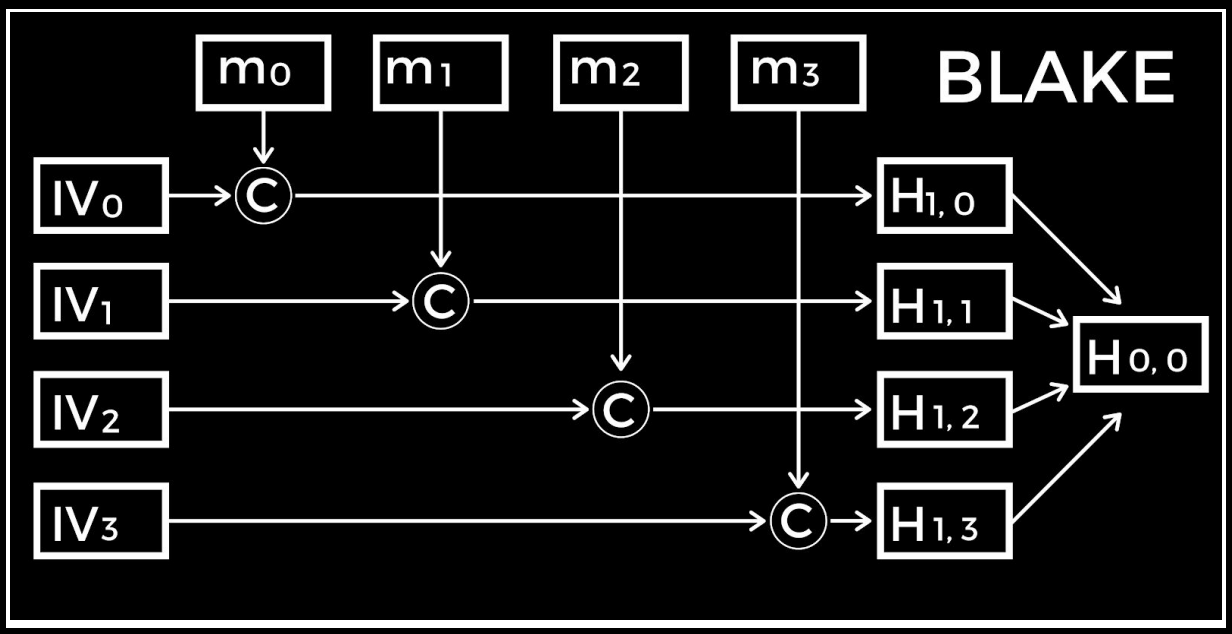
BLAKE2 comes in two flavors: BLAKE2b (or just BLAKE2) is optimized for 64-bit platforms—including NEON-enabled ARMs—and produces digests of any size between 1 and 64 bytes BLAKE2s is optimized for 8- to 32-bit platforms and produces digests of any size between 1 and 32 bytes.

The performance of BLAKE2 is much faster than BLAKE, mainly due to its reduced number of rounds. On long messages, the BLAKE2b and BLAKE2s versions are expected to be approximately 25% and 29% faster, ignoring any savings from the absence of constants, optimized rotations, or little-endian conversion. The parallel versions BLAKE2bp and BLAKE2sp are expected to be 4 and 8 times faster than BLAKE2b and BLAKE2s on long messages when implemented with multiple threads on a CPU with 4 or more cores (as most desktop and server processors: AMD FX-8150, Intel Core i5-2400S, etc.). Parallel hashing also benefits from advanced CPU technologies, as previously observed.

Figure 1: Speed comparison of various popular hash functions, taken from eBACS's "sandy" measurements. SHA-3 and BLAKE2 have no known security issues. SHA-1,

MD5, SHA256, and SHA-512 are susceptible to length-extension. SHA-1 and MD5 are vulnerable to collisions. MD5 is vulnerable to chosen-prefix collisions.





Example parameter block of BLAKE2b. We take as an example an instance of BLAKE2b with • 64-byte digests, that is, with parameter digest length set to 40, • a 256-bit key, that is, with the parameter key length set to 20, • a salt set to the all-55 string, • a personalization set to the all-ee string. BLAKE2b hashes data sequentially, thus tree parameters are set to the value specified for the sequential mode:

fanout and maximal depth are set to 01, leaf maximal length is set to 00000000, node offset is set to 0000000000000000, node depth and inner hash length are set to 00. The parameter block for this instance of BLAKE2b is: 40200101 00000000 00000000 00000000 00000000 00000000 00000000 00000000 55555555 55555555 55555555 55555555

Example parameter block of BLAKE2s. We take as an example an instance of BLAKE2s with • 32-byte digests, that is, with parameter digest length set to 20, • no key, that is, with the parameter key length set to 00, • no salt, and no personalization, that is, with all respective bytes set NULL. BLAKE2s hashes data sequentially, thus tree parameters are set to the value specified for the sequential mode: fanout and maximal depth are set to 01, leaf maximal length is set to 00000000, node offset is set to 0000000000000000, node depth and inner hash length are set to 00. The parameter block for this instance of BLAKE2s is: 20000101 00000000 00000000 00000000 00000000 00000000 00000000 00000000

Structure & Terminology:

```
+-------------+-----------------+-----------------+
|             | BLAKE2b         | BLAKE2s         |
+-------------+-----------------+-----------------+
| Bits in word | w  = 64         | w  = 32         |
| Rounds in F  | r  = 12         | r  = 10         |
| Block bytes  | bb = 128        | bb = 64         |
| Hash bytes   | 1 <= nn <= 64   | 1 <= nn <= 32   |
| Key bytes    | 0 <= kk <= 64   | 0 <= kk <= 32   |
| Input bytes  | 0 <= ll < 2**128 | 0 <= ll < 2**64 |
+-------------+-----------------+-----------------+
| G Rotation   | (R1, R2, R3, R4) | (R1, R2, R3, R4) |
|  constants   | (32, 24, 16, 63) | (16, 12,  8,  7) |
+-------------+-----------------+-----------------+
```

Blake2b sizing of the bytes:

```
const (
   // The blocksize of BLAKE2b in bytes.
   BlockSize = 128
   // The hash size of BLAKE2b-512 in bytes.
   Size = 64
   // The hash size of BLAKE2b-384 in bytes.
   Size384 = 48
   // The hash size of BLAKE2b-256 in bytes.
   Size256 = 32
);
```

Results of the Encryptions:

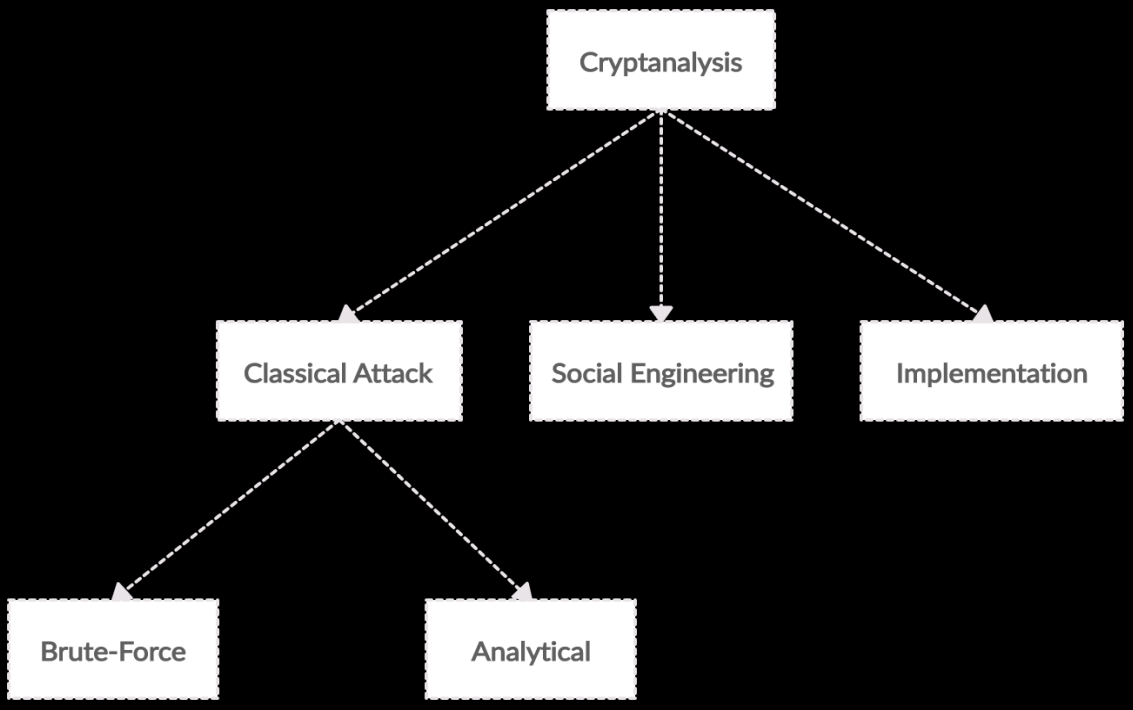
We have added all these encryption mechanisms, algorithms, and this multi-component encryption separately. We have also written the hash function needed to use it, because all data and IP addresses in Zentameshnet, Zentalk and Zentavult are very secure, well protected and perform at a high level we wanted to present you. More importantly, other encryption methods can no longer be used because the encryption mechanisms have been decrypted today and there is a lack of strength of the bits. Also, some encryption algorithms have a lack of speed and performance for some applications it is absolutely important to use the right encryption and hashes for applications. The Diffie Hellman key exchange indicates a weakness against an attack by a middle man attacks because it passing over the unsafe channel. The El-Gamal encryption and decryption phase takes place with each message being exchanged, but the Diffie-Hellman protocol requires two messages, so that A person only needs to send one message, and the encryption and decryption phase is performed as each message changes.

Hybrid encryption is an encryption mode that combines two or more encryption systems. Since Zentalk uses this encryption system as well, we named it Zentalk hybrid messaging application. Because it has to secure different encryptions in and outside the network for the system to work by itself and not have to access a third cloud-based memory and El-Gamal is pretty good as a digital solution for signatures. The encryption hash function BLAKE2 is often used because it is faster than other hash functions and is more suitable for decentralized applications, so we decided to use Blake2. A major issue with AES is that, as a symmetric algorithm, it requires that both the encryptor and the decryptor use the same key. This gives rise to a crucial key management issue – how can that all-important secret key be distributed to perhaps hundreds of recipients around the world without running a huge risk of it being carelessly or deliberately compromised somewhere along the way? The answer and solution are to combine symmetric and asymmetric encryption and to use the strengths of AES and RSA together. It is important also to use a strong bit strength of both encryptions. The SHA-256 hash functions are currently strong enough to use in our Zentanode Algorithm and are the best option for AES encryption, but due to the power of quantum computers, they may need a future update and again the bits need to be strong enough.

16. Cryptanalysis

Cryptanalysis is the study of methods for obtaining the meaning of encrypted information, typically without access to secret information. Typically, this involves knowing how the system works and finding a secret key. Cryptanalysis is also referred to as code breaking or cracking the code. (Brute-Force) The ciphertext is generally the easiest part of a cryptosystem to obtain and, therefore, is an important part of cryptanalysis. Depending on what information is available and what type of cipher is being analyzed, cryptanalysts can follow one or more attack models to crack a cipher. A cryptographic solution must be secure even if the attacker or a third-party user knows all the details of the cryptosystem, with the exception of the key. In particular, the procedure must be also secure even if the

attacker knows the encryption and decryption algorithm and the algorithm must also be secure against analytical attacks. An attacker will always exploit the weakest point of a crypto procedure. A large key room alone is no guarantee that the cipher is secure enough. For example, it may have mathematical weaknesses.



- **Classical Attack**

In classical cryptanalysis, there are various targets that an attacker can pursue. The two most common situations are those in which the attacker wants to calculate either the plaintext x or the key k for a given cipher rate y. In the full key search, the cipher is regarded as a black box, while in the case of analytical attacks, the internal structure of the encryption process is exploited.

- **Brute-Force Attack**

Brute-force attacks run the encryption algorithm for all possible cases of the keys until a match is found.

- **Analytical Attack**

Analytical attacks are those attacks that focus on breaking the cryptosystem by analyzing the internal structure of the encryption algorithm.

- **Social Engineering Attack**

Social Engineering Attack is Manipulation - interpersonal influences (such as fake accounts) are exploited to obtain the crypto keys. Phishing attacks are the best-known representatives of the social engineering attacking.

Example: "Good morning, I am X from the IT department. We need your password for an urgent security update."

An attacker looks for the weakest link in the chain to overcome the cryptosystem. Therefore, powerful cryptographic algorithms that resist classical cryptanalysis alone are not sufficient, and social engineering and application attacks should be prevented.

- **Implementation Attack**

Implementation attacks such as side-channel analysis can be used to obtain a secret key. They are relevant in cases where the attacker can obtain physical access to the cryptosystem.

How many Key-Sizes bits do we need?

The key lengths for symmetric and asymmetric procedures differ dramatically. Example a symmetric algorithm with a 128-bit key offers approximately the same security as RSA with 3072 bits (RSA is one of the most popular asymmetric methods).

Attack time using full key search for the symmetric algorithms:

- It takes a few hours or a few days to break 64-Bit.
- 128 Bit Long-term: it is breakable with a quantum computer.
- 256 Bit Long-terms: it is not breakable with quantum computers.

What do we need for secure systems?

A security system protects assets such as data, money or buildings. Cryptographic algorithms often play a central and decentral role in securing digital systems.

Rules of a secure-systems & key lengths of symmetric algorithms:

1. The breaking will be more expensive than the value being protected.
2. The protective values and security objectives should be defined initially.
3. Use only crypto algorithms (i.s. symmetric and asymmetric ciphers and hash functions) or protocols that have long been publicly known and extensively analyzed.

4. It takes many years to break 128 Bits unless the attacker has quantum computers.
5. 256 Bit: Safe against attacks with quantum computers.
6. Key lengths of AES-Encryption 128, 192 and 256 bits for several decades secure against brute force attacks.
7. We need RSA or the DHKE Protocol is a must to exchange the keys in an unsafe channel connection. As soon as the symmetric key has been decrypted, both parties (A) & (B) can use it for symmetric encryption and decryption of messages.
8. Encrypt data with symmetric or asymmetric algorithms like RSA, El-Gamal or 3DES.

17. The Zentamesh Network & Zentanodes

Understanding Nodes

The ideas of nodes were popularized with the adoption of packet-switching theory and the concept of distributed networks. In this context, nodes were gateways that could receive, store and send information along different routes through a distributed network. Each node was given an equal standing within the network, meaning that the loss of any one node wouldn't hurt the network.

Why is Zentameshnet better?

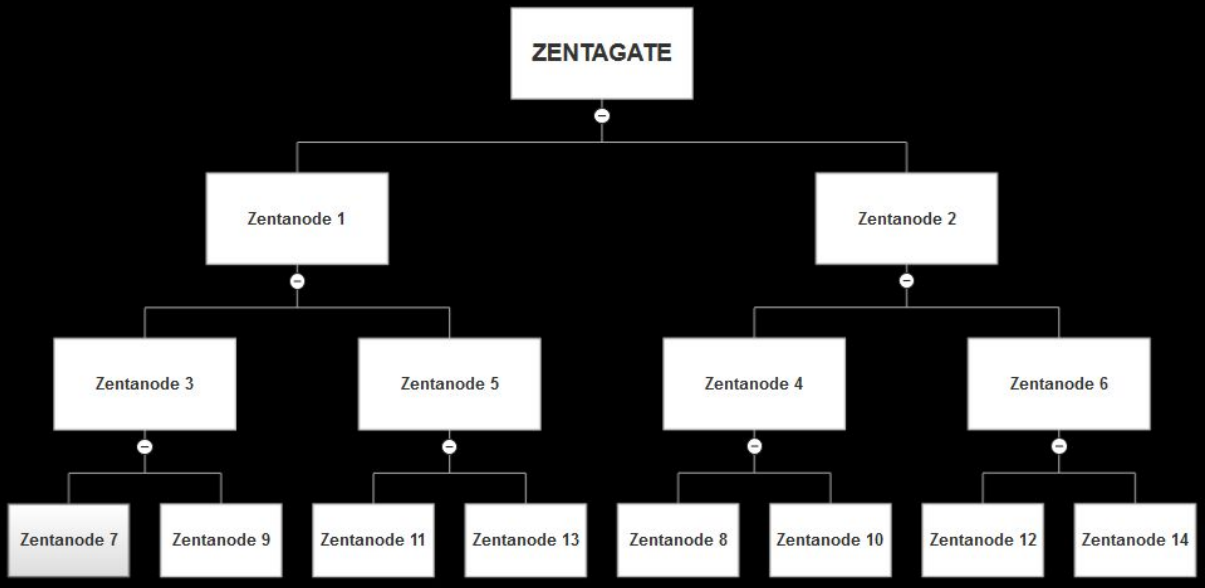
The Zentameshnet has self-healing properties that contribute to the ability to achieve censorship resistance. Self-healing means if a node connection is blocked or disabled, the mesh network can patch and rerouted around the lost node. The data is redirected and the network is still functional. Meshed networks can be applied to both wired and wireless networks, as well as Zentalk will establish a meshed WLAN (Wireless Local Access Network). This MWLAN can be achieved thanks to the use of a Zentanode Meshed WiFi. This will be required for offline communications over Zentalk.

This means that a Zentanode owner can establish and share an internet connection, and also communicate with devices that do not have internet access (offline-offline). This can be done even if there is little or no infrastructure at all. Zentanode owners will be rewarded with Zenta. Nodes are active network components like cell phones, routers, switches, bridges, and gateways.

Each Zentanode in a network is a connection point. This can either be a redistribution point or an endpoint in the data transfer. It has the feature to discover, process, and forward transmissions to other network nodes. A network node has at least two, usually more connections to other network elements.

Every Zentanode in Zentameshnet can also act as their Gateway to grow Zentamesh network. The user is also to be able to close his network with a pin code to connect with his only own Zentanodes. Every Zentanodes will have its own Id.

The role of a Zentanode will be connected with a device that is running Zentalk messenger dApp on a mobile phone, tablet or a computer.



11 Reasons for using Zentamesh technology:

1. Network stability

The data in the (wireless) mesh network can be transmitted over other Zentanodes, even if one or some of the Zentanodes are faulty or defective, and the data is routed through other Zentanodes in the ecosystem.

2. High bandwidth

Zentamesh networks are designed to follow the most optimal (dynamic) routes, allowing a higher bandwidth. With the increase in the number of nodes and the number of possible paths, the overall bandwidth is greatly increased.

3. Safety and Security

Compared with the single-hop mechanism of WLAN, the multi-hop mechanism of the Zentamesh network determines that the user communication needs to go through several Zentanodes.

4. Range of the Zentanodes

- The more Zentanode users, the larger and faster your wireless Zentamesh network.
- The range of a single Zentanode is up 25-50 Km at this time without having internet access(More Nodes = More Range).
- User of Zentanode is able to there run the Zentanode as also an own user gateway.
- Without Zentanode, the range will be about 100 meters via Wi-fi connection.

5. Data transfer through Zentameshnet

- In the Zentameshnet network first will be only possible to transfer data and files of a maximum of 15 Mb over the Wifi & BLE Connection.
- With an Internet connection, up to 150 Mb, the download speed will be 17.88/ second.

6. Zentanode Hash(H) & Encryption(E)

- AES(E), RSA(E), Hybrid(E)
- Zentanode Hash-Algorithms: SHA-256
- SLL

7. Operating Frequencies:

- Europe - 868MHz
- US, Canada & Mexico - 902MHz
- Latin America & SE-Asia - 922MHz

8. Available networks:

- IEEE 802.11,(Wifi) Bluetooth, LTE, 4G, 5G

9. The Wifi Connection

- They rely on the same WiFi standards (802.11a, b, and g) already in place for most wireless networks.
- Deep sleep: Yes

10. Bluetooth

- Low Energy

11. Zentagateway

- AES 128

18. Zentavault

Zentavault is the second dApp to be released from Zentachain application pipeline. Zentavault is a high throughput dApp, which is designed to be a highly encrypted and distributed storage service. This service will be hosted on the Zentachain platform. ZentaChain's dApps will never rely on centralized systems and will absolutely never have any backup databases for users' metadata. By doing so, Zentavault will keep privacy, anonymity and commercial performance at a high level.

Zentavault requires no monthly usage fees, instead, there is only a small transaction fee to upload data. Zentavault is a file-encrypting and distribution tool. Users will have full control to encrypt, store, and share content the way they choose. With Zentavault, you can ensure your data is encrypted and embedded permanently onto the InterPlanetary File System, also referred to as IPFS. It is a tailored network that allows for content to be embedded and shared using an associative memory strategy. When content is on IPFS, it is assigned a unique identifier, known as a cryptographic hash or hash Id. This can be used to locate the user's data or share it between two parties. Once your content is embedded onto IPFS, a hash Id is assigned to the file allowing a way to find or share content with others. By employing peer-to-peer hypermedia protocol technologies such as IPFS, Zentavault is able to achieve a more expeditious, protected and accessible file storage and transfer service.

IPFS (InterPlanetary File System)

The modern internet, though it is one of the breakthrough technologies of our age, has shown to have limitations since its inception in the 1990s. As technological advances progress, more and more tech is shown to be in need of either upgrading or even complete conceptual reimagining. Such is the case with the HTTP protocol.

In recent times we have seen an increased demand for solutions that would address the issues of privacy, security, and speed, the areas in which the HTTP protocol hasn't shown to be "up to the task", so to speak. Fortunately, IPFS has been put forward as an idea that provides solutions to these problems.

How does it work?

We can look at it in the terms of a BitTorrent swarm but with the ability to store and track file versions over time. Unlike the HTTP which works by mapping the resources via location-based IP addresses, IPFS uses a content-addressed system. This decentralized system stores files across peers and enables access to them via a cryptographic hash on a file that is used as the address. This means that the user becomes the client and the host at the same time.

It is made possible by the Merkle DAG (Directed Acyclic Graphs) data architecture and ensures immutability and content versioning on IPFS. Because of their similar structures, IPFS is a perfect fit for blockchain integration. It goes a bit further than that, though, solving blockchain's nagging issue of data storage and together with blockchain creates a solution for storing, encrypting, and sharing large data and files. Although still in its infancy, IPFS has all the tools to become the successor to HTTP and usher in a new era of the World Wide Web.

IPFS Identities

Nodes are identified by a NodeId, the cryptographic hash3 of a public-key, created with S/ Kademlia's static crypto puzzle. Nodes store their public and private keys (encrypted with a passphrase). Users are free to initiate a "new" node ID during each launch but lose some of the acquired network advantages, it is recommended that the nodes remain the same.

IPFS Network

IPFS nodes communicate regularly with hundreds of other nodes in the network, across the wide internet. The IPFS network stack features:

- Transport: IPFS can use any transport protocol, and is best suited for WebRTC Data Channels (for browser connectivity) or uTP(LEDBAT).
- Reliability: IPFS can provide reliability if underlying networks do not provide it, using uTP (LEDBAT) or SCTP.
- Connectivity: IPFS also uses ICE NAT traversal techniques.
- Integrity: optionally checks the integrity of messages using a hash checksum.
- Authenticity: optionally checks the authenticity of messages using HMAC with the sender's public key.

IPFS Routing

For routing, IPFS uses Distributed Sloppy Hash Tables based on S/Kademlia and Coral. Its purpose is to:

1. Announce data being added to the nodes

2. Locate data requested by specific nodes

Data equal lesser than 1KB in size is stored directly on the DHT. For data larger than 1KB, DHT stores references, which are the NoodeIds of peers who can serve the block.

Objects Merkle DAG

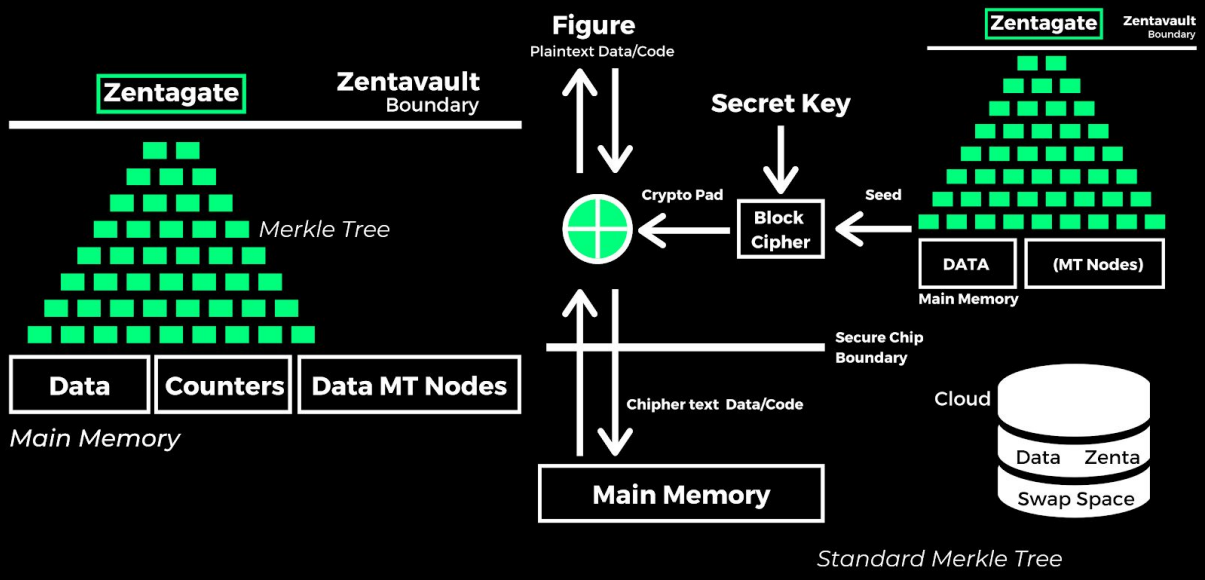
Merkle DAG (Merkle Directed Acyclic Graph) is used to keep the order of object files in the InterPlanetary File System. Merkle DAG allows Files to become linked to each other by their unique cryptographic hash, which is known as a hashId. The hashId (object) includes all hashId object links. Merkle DAG gives IPFS useful properties such as:

- Content safeguard: Merkle DAG insurers the security, safety and integrity of all content on IPFS If any object that stored or hosted on IPFS has been tampered with or otherwise corrupted, Merkle DAG changes the root hash automatically. This shows the changes made to the File.

- Anti-duplication for efficiency(It does not store the same data twice): All objects holding content on IPFS is sorted through, duplicated objects are recognized then deleted. This ensures that content isn't stored multiple times on IPFS.

- Content addressing: All content is able to be located by identifying the unique hashId or multi hash including links.

19. Zentagate



Standard Merkle Tree

Using Address Independent Seed Encryption

The goal of memory encryption is to ensure that all data and code stored outside the secure processor boundary is in an unintelligible form, not revealing anything about the actual values stored. The figure illustrates how this is achieved in counter mode encryption. When a block is being written back to memory, a seed is encrypted using a block cipher (e.g. AES) and a secret key, known only to the processor.

The encrypted seed is called a cryptographic pad, and this pad is combined with the plaintext block via a bit-wise XOR operation to generate the ciphertext of the block before the block can be written to memory. Likewise, when a ciphertext block is fetched from memory, the same seed is encrypted to generate the same pad that was used to encrypt the block. When the block arrives on-chip, another bitwise XOR with the pad restores the block to its original plaintext form. Mathematically, if P is the plaintext, C is the ciphertext, E is the block cipher function, and K is the secret key, the encryption performs C = P EK(Seed). By XORing both sides with EK(Seed), the decryption yields the plaintext P = C EK(Seed).

IPFS Files

IPFS also defines a set of objects for modeling a versioned file-system on top of the Merkle DAG. This object model is similar to Git's:

1. lock: a variable-size block of data.
2. list: a collection of blocks or other lists.
3. tree: a collection of blocks, lists, or other trees.
4. commit: a snapshot in the version history of a tree.

Why do we need IPFS?

- **Bandwidth**

Only being able to access data from one central location can have disadvantages. Imagine you want to share a file with a room full of people. You would then upload that file to a central server that is probably located somewhere far away from you (the backbone of the internet) and be routed over several servers on the way. The other people would then access this file by again connecting to this far away server and retrieving the file.

Especially with big files like pictures and videos, this can lead to a lot of bandwidth being used for sharing that file with a room full of people that are probably all connected to the same local area network as you are. With IPFS that file can be served directly by all the computers in the room that have the file through the local area network and thus use a lot less bandwidth because the detour to the central server is no longer needed. This becomes particularly important when looking at the cost of connection speed that is decreasing much slower than the cost of storage. If this trend continues, users will be able to store a lot more data and thus will increase their use of the network. But with the bandwidth not improving at the same pace, the connection speed will appear to get slower and slower. Security also increases — DDoS attacks, for example, wouldn't work, since they rely on attacking a central distribution system, which IPFS doesn't have. Speed is another factor that increases. In a distributed web, every node that requests something, requests it to the node closest to him, instead of to a single, central location.

- **Latency**

A related problem is latency. As the speed of light is constant and cannot be changed, the only way of reducing latency is serving the data from a point that is closer to the user. That is why the big cloud service providers now started offering storage locations by region. IPFS aims to reduce the distance to the computer that serves the requested data if possible.

- **Being Offline**

A lot of the services we use every day heavily rely on only the works that we do online. If you want to work collaboratively on a document with other people in the same room or want to transfer data from your phone to your laptop you are mostly only able to do that if you are connected to the central servers of the backbone of the internet. If there are bandwidth or infrastructure problems like congestion, ISP outage or datacenter problems you are not able to use these services anymore. IPFS hopes to change that by letting you connect to other peers directly without needing to connect to these central servers.

- **Censoring**

Access to data or services can be censored or restricted a lot easier if everything is stored and run on central servers compared to a P2P network. One example of this is when the government of Egypt cut all access to the Internet during the Arab spring in 2011 to prevent the organization of and restrict communication between the protesters. Through being connected P2P, IPFS hopes to make this form of censorship impossible.

- **Permanence**

Everyone has encountered an Error 404 before. This means that the required content could not be found because it was deleted or moved. This can be a huge problem if you want to link to this content for example because it is essential for the content you are providing. In general, it would be beneficial for society if most of the knowledge that is accumulated in the web would stay accessible and not be deleted because someone purposely or accidentally shut down some websites. With IPFS you are able to save and host some version of the linked content yourself and that way ensures that this content will always be available to users even though the original hosts no longer host it. The idea is to create a permanent network where no content is lost because all content is hosted by many people.

- **Security**

As the numerous hacks in recent years have shown, thinking only about the security in the communication between servers and clients is not sufficient. IPFS aims to protect the data itself through enhanced methods of authentication and encryption.

- **Self-Certified Filesystems - SFS**

No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security on a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use. We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal key management. While other file systems need key management to map file names to encryption keys, SFS file names effectively contain public keys, making them self-certifying pathnames. Key management in SFS occurs outside of the file system, in whatever procedure users choose to generate file names. The Self-certifying File System (SFS) addresses the issue of key management in cryptographic file-systems and proposes separating key management from file system security.

Servers have a public key and clients use the server public key to authenticate the server and establish a secure communication channel. To allow clients to authenticate servers on the spot without even having heard of them before, SFS introduces the concept of a `` self-certifying pathname ."

A self-certifying pathname contains the hash of the public-key of the server so that the client can verify that he is actually talking to the legitimate server. Once the client has verified the server a secure channel is established and the actual file access takes place. Remote SFS file systems are accessed through the /sfs mount point. An SFS pathname obeys the following syntax: /sfs/ location:hostid/real/pathname, where `` location" is the name (IP address or DNS Name) of the server exporting the file system and `` hostid" is the hash of a string containing the server's public key and some other information. SFS does not care about how the pathname has been obtained by the user; a user can eventually obtain host Id's using an existing PKI (Public Key Infrastructure). On the other hand, once a self-certifying pathname for the files he is interested in has been obtained, users do not need to remember any key.

This is used to implement the IPNS name system for IPFS. It allows us to generate an address for a remote filesystem, where the user can verify the validity of the address. SFS introduced a technique for building Self-Certified Filesystems: addressing remote filesystems using the following scheme:

/sfs/<Location>:<HostID>
where Location is the server network address, and:
HostID = hash(public_key || Location)
Thus the name of an SFS file system certifies its server.

It is designed to function as the web already functions, as you can read above. Instead of a special link that only certain programs understand, or a file to download other files, IPFS is designed to work with common links that work in the browser, and you don't need to install special software. IPFS can use any network architecture and any kind of file can be used as a DAG. This feature is called IPLD (InterPlanetary Linked Data).

Zentachain takes the right that everything written in the whitepaper is based on the knowledge of Zentachain and no one is allowed to copy and manipulate a text or images and then spread false information about Zentachain. Zentachain allows distribution only as an original file with the original text, images and contents. The responsibility for the Whitepaper lies with Zentachain.io. As Zentachain, we reserve the right to update Zentachain Lab constantly in order to keep up with the rapidly-developing technology.

REFERENCES

Adnan Abdul-Aziz Gutub, Farhan Abdul-Aziz Khan, Hybrid Crypto Hardware Utilizing Symmetric-Key & Public-Key Cryptosystems, 2012 International Conference on Advanced Computer Science.

Shankar Dhakar, Ravi & Kumar Gupta, Amit & Sharma, Prashant, Modified RSA Encryption Algorithm (MREA), 2012 2nd International Conference on Advanced Computing and Communication Technologies(ACCT), pp. 426-429, 2012.

Nishtha Mathur and Rajesh Bansode, AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection, Procedia Computer Science 79, pp. 1036 – 1043, Elsevier, 2016.

Koorosh Goodarzi, Abbas Karimi, Cloud Computing Security by Integrating Classical Encryption, Procedia Computer Science 42, pp. 320 – 326, Elsevier, 2014.

Shilpi Gupta and Jaya Sharma, A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman, 2012 International Conference on Computational Intelligence and Computing Research, IEEE, 2012.

R. Rizk, Y. Alkady, Two-phase hybrid cryptography algorithm for wireless sensor networks, Journal of Electrical Systems and Information Technology Vol 2, Issue 3, pp. 296-313, 2015.

Koorosh Goodarzi, Abbas Karimi, Cloud Computing Security by Integrating Classical Encryption, Procedia Computer Science 42, pp. 320 – 326, Elsevier, 2014.

M. Indra Sena Reddy and A.P. Siva Kumar, Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm, Procedia Computer Science 85, pp. 62-69, Elsevier, 2016.

Wang Rui; Chen Ju; Duan Guangwen, 'A k-RSA algorithm,' Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.21,24, 27-29 May 2011.

Liang Wang, Yonggui Zhang, A New Personal Information Protection Approach Based on RSA Cryptography, IEEE, 2011.

Christof Paar, Jan Pelzl, "Understanding Cryptography", SpringerVerlag Berlin Heidelberg, pp. 3-9, 30-31, 2010.

Assad Ibraheem Khyoon," Modification on the Algorithm of RSA Cryptography System" 2006.

Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, Implementation of Text Encryption using Elliptic Curve Cryptography, Procedia Computer Science 54, pp. 73-82, Elsevier, 2015.

Diffie: Whitfield Diffie and Martin Hellman, “New Directions in Cryptography", IEEE Transactions on Information Theory, Nov 1976.

Vitalik Buterin. Ethereum 2.0 mauve paper. 2016

Polkadot:
https://polkadot.network/PolkaDotPaper.pdf

Cosmos:
https://cosmos.network/cosmos-whitepaper.pdf

ABCI:
https://github.com/tendermint/abci

Bitcoin:
https://bitcoin.org/bitcoin.pdf

BitShares:
https://bitshares.org/technology/delegated-proof-of-stake-consensus

Computer Networks:
https://digitalescobar.wpcomstaging.com/wp-content/uploads/2018/12/DigitalEscobar.com-Computer-Networks-A-Systems-Approach-by-Larry-L.-Peterson-Bruce-S.-Davie-.pdf

AES Encryption:
https://townsendsecurity.com/sites/default/files/AES_Introduction.pdf

Blake2:
https://blake2.net/

Hybrid Encryption Algorithm:
https://pdfs.semanticscholar.org/d518/9533fd596a5cbc39864d21a5ef4e0156359d.pdf

A hybrid encryption algorithm based on RSA and Diffie-Hellman:
https://ieeexplore.ieee.org/document/6510190

IPFS:
https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf

A Review on Hybrid Encryption in Cloud Computing:
https://www.semanticscholar.org/paper/A-Review-on-Hybrid-Encryption-in-Cloud-Computing-Kumar-Badal/ad6ba7c05455b4b1416e19b52aa42ec050a5dd74

Ietf.org:
https://en.wikipedia.org/wiki/History_of_cryptography

Diffie–Hellman:
https://www.math.brown.edu/~jhs/MathCrypto/SampleSections.pdf

Crypho Security Whitepaper:
https://www.crypho.com/downloads/crypho_security_whitepaper.pdf

On the Security of ElGamal Based Encryption:
https://www.researchgate.net/publication/221010812_On_the_Security_of_ElGamal_Based_Encryption

Descriptions of SHA-256, SHA-384, and SHA-512:
http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf