THE STORY OF BITCOIN

Until about the 1970s, cryptography was mainly practiced in secret by military or spy agencies. However, that changed when two publications brought it into public awareness: the US government publication of the Data Encryption Standard (DES), a block cipher which became very widely used, and the first publicly available work on public-key cryptography, by Whitfield Diffie and Martin Hellman.

Diffie–Hellman key exchange:

Diffie–Hellman–Merkle key exchange was one of the first public-key protocols as conceived by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. DHM-key_ex is one of the earliest practical examples of public key exchange implemented within the field of cryptography. This is the earliest publicly known work that proposed the idea of a private key and a corresponding public key.

Although Diffie–Hellman key agreement itself is a non-authenticated key-agreement protocol, it provides the basis for a variety of authenticated protocols, and is used to provide forward secrecy in Transport Layer Security's ephemeral modes (referred to as EDH or DHE depending on the cipher suite).

Diffie–Hellman is used to secure a variety of Internet services. However, research published in October 2015 suggests that the parameters in use for many DH Internet applications at that time are not strong enough to prevent compromise by very well-funded attackers, such as the security services of some countries.

Digital Signatures:

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

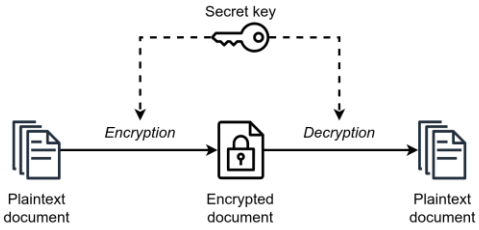
Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

In many digital communications, it is desirable to exchange an encrypted messages than plaintext to achieve confidentiality. In public key encryption scheme, a public (encryption) key of sender is available in open domain, and hence anyone can spoof his identity and send any encrypted message to the receiver.

This makes it essential for users employing Public Key Cryptography (PKC) for encryption to seek digital signatures along with encrypted data to be assured of message authentication and non-repudiation.

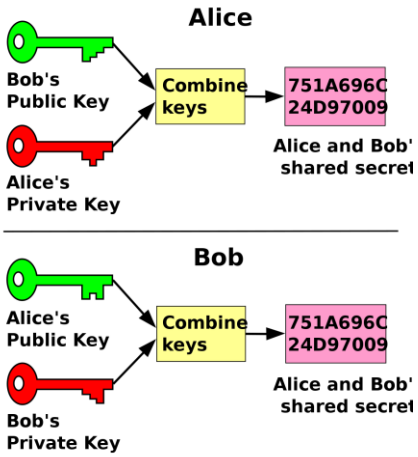
Symmetric and Asymmetric Key:

Symmetric key encryption uses the same key for encryption and decryption. This makes sharing the key difficult, as anyone who intercepts the message and sees the key can then decrypt your data.



This is why symmetric key encryption is generally used for encrypting data at rest. AES-256 is the most popular symmetric key encryption algorithm. It is used by AWS for encrypting data stored in hard disks (EBS volumes) and S3 buckets.

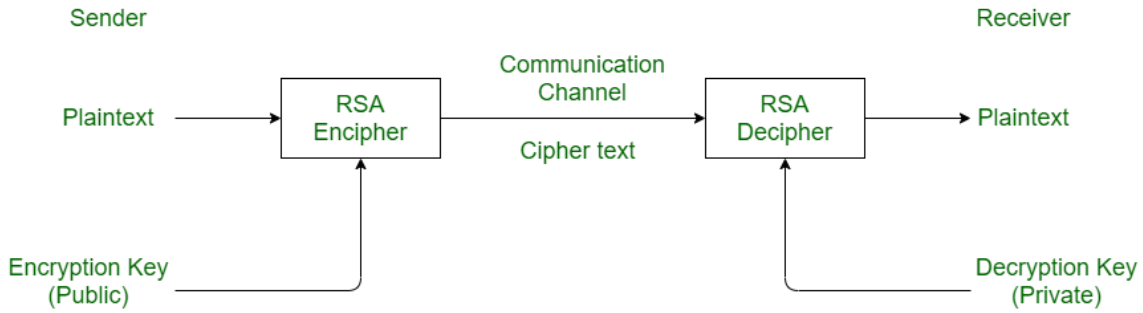
In asymmetric key encryption, one key is used to only encrypt the data (the public key) and another key is used to decrypt (the private key). Asymmetric key encryption is used when there are two or more parties involved in the transfer of data. This type of encryption is used for encrypting data in transit, that is encrypting data being sent between two or more systems. The most popular example of asymmetric key encryption is RSA.



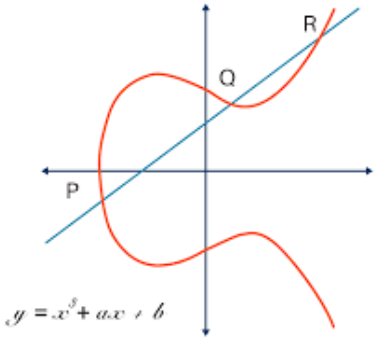
RSA

An implementation of public-key cryptography using **asymmetric** algorithms. **RSA** (**Rivest–Shamir–Adleman**) is a public-key cryptosystem, widely used for secure data transmission. The acronym "RSA" comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who publicly described the algorithm in 1977.

RSA is a relatively **slow** algorithm. Because of this, it is not commonly used to directly encrypt user data. More often, RSA is used to transmit shared keys for symmetric-key cryptography, which are then used for bulk encryption–decryption.



Elliptic-curve cryptography (ECC)

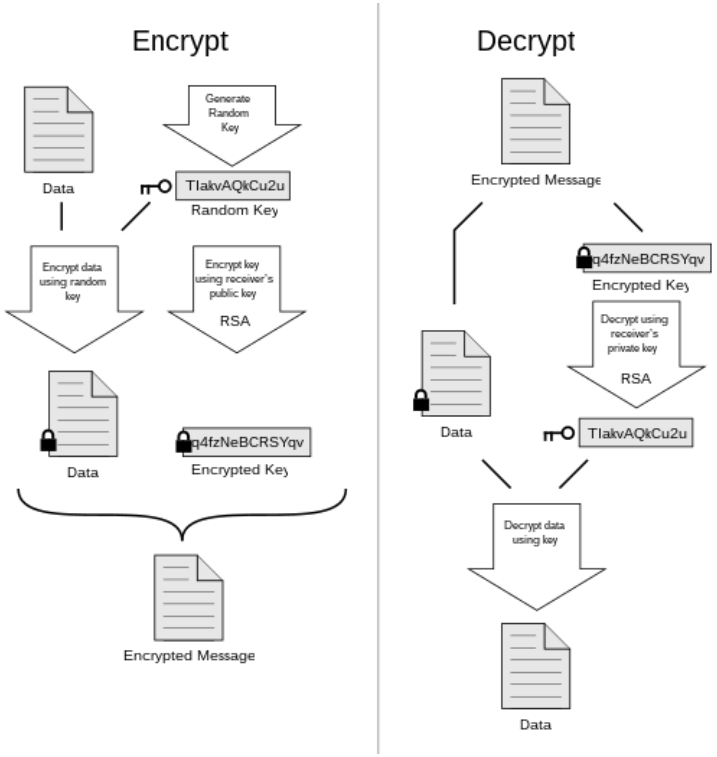


An approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.

Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme.

Shor's algorithm can be used to **break** elliptic curve cryptography by computing discrete logarithms on a hypothetical quantum computer. The latest quantum resource estimates for breaking a curve with a 256-bit modulus (128-bit security level) are 2330 qubits and 126 billion Toffoli gates. Satoshi Nakamoto **discouraged/hated** this form of encryption.

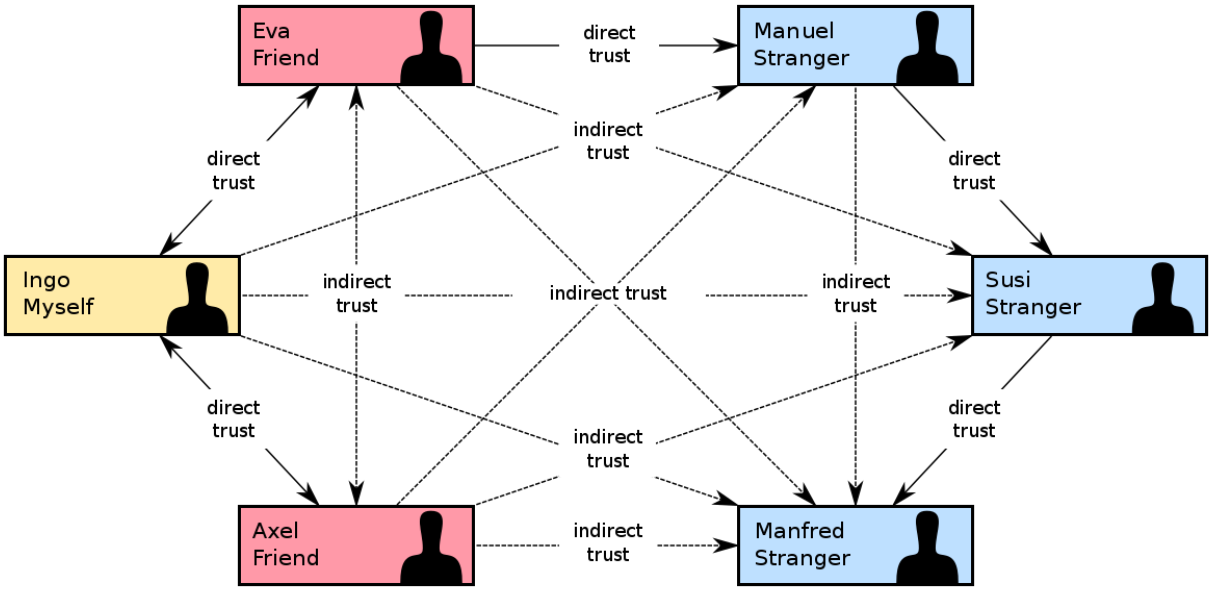
Pretty Good Privacy (PGP):



An encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. Phil Zimmermann developed PGP in 1991.

They follow the OpenPGP, an open standard of PGP encryption software, standard (RFC 4880) for encrypting and decrypting data. In 1991, he made it available (together with its source code) through public FTP for download, the first widely available program implementing public-key cryptography.

Web of Trust [Decentralized]:



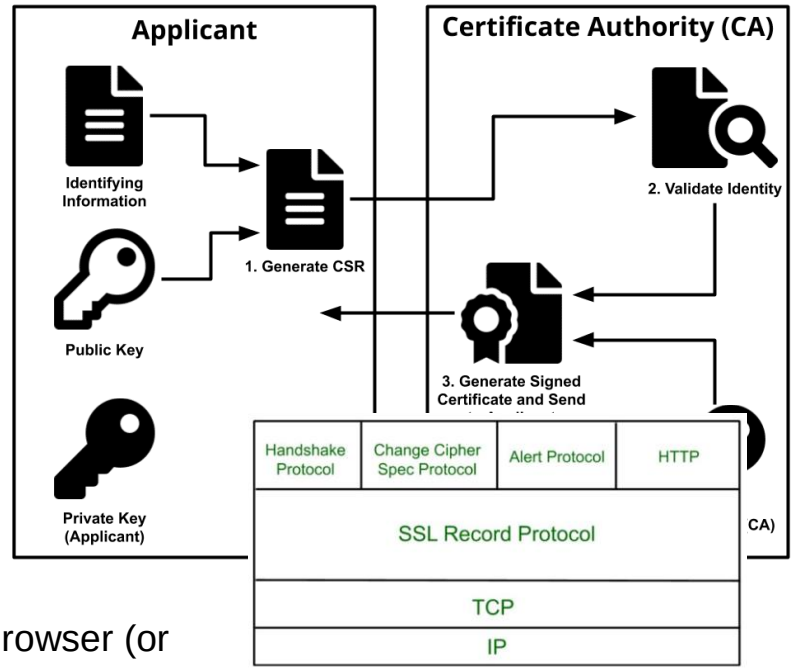
First put forth by Phil Zimmermann in **1992**. In cryptography, a **web of trust** is a concept used in OpenPGP-compatible systems to establish the authenticity of the binding between a public key and its owner. Its **decentralized** trust model is an alternative to the centralized trust model of a public key infrastructure (PKI), which relies exclusively on a certificate authority (or a hierarchy of such).

Certification authority (CA) [Centralised]:

In cryptography, a digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party, trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 or EMV standard.

One particularly common use for certificate authorities is to sign certificates used in HTTPS, the secure browsing protocol for the World

Wide Web. Another common use is in issuing identity cards by national governments for use in electronically signing documents. GeoTrust brand was the first CA to issue public domain-validated SSL certificates.



Secure Socket Layer:

SSL is standard technology for securing an internet connection by **encrypting** data sent between a website and a browser (or between two servers).

It consists of **IP address** and **Port Number**.

Secure Shell:

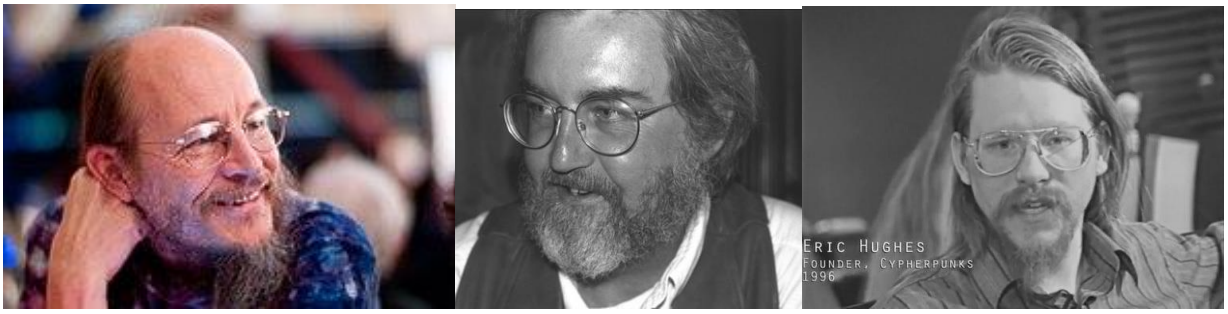
SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network. SSH also refers to the suite of utilities that implement the SSH protocol.

CypherPunk [1992]:

A **cypherpunk** is any individual advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change. Originally communicating through the Cypherpunks electronic mailing list, informal groups aimed to achieve privacy and

security through proactive use of cryptography. Cypherpunks have been engaged in an active movement since at least the late 1980s.

Founded by Eric Hughes, Timothy C. May, and John Gilmore.



The Cypherpunks mailing list was started in 1992, At its peak, it was a very active forum with technical discussions ranging over mathematics, cryptography, computer science, political and philosophical discussion, personal arguments and attacks, etc.

Main Principles:

- Privacy
- Anonymity
- Hiding the act of hiding:

  An important set of discussions concerns the use of cryptography in the presence of oppressive authorities.

Time Stamp Protocol

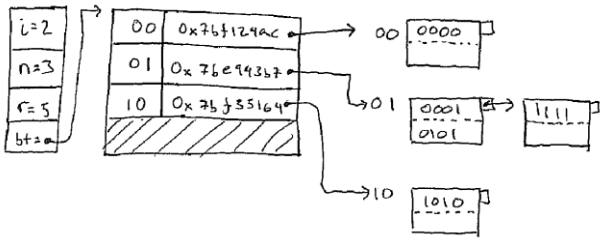
The Time-Stamp Protocol, or TSP is a cryptographic protocol for certifying timestamps using X.509 certificates and public key infrastructure. The timestamp is the signer's assertion that a piece of electronic data existed at or before a particular time. The protocol is defined in RFC 3161. One application of the protocol is to show that a digital signature was issued before a point in time, for example before the corresponding certificate was revoked.

HASHING :

Hashing is the process of transforming any given key or a string of characters into another value. This is usually represented by a shorter, fixed-length value or key that represents and makes it easier to find or employ the original string.

A hash function generates new values according to a mathematical hashing algorithm, known as a hash value or simply a hash. To prevent the conversion of hash back into the original key, a good hash always uses a one-way hashing algorithm.

- Secure Hash Algo 1 (SHA-1)
- Secure Hash Algo 2 (SHA-2)
- Secure Hash Algo 3 (SHA-3)
- Message Digest MD2
- Message Digest MD4
- Message Digest MD5



Once Message Digest is hashed, the signature is transformed into a shorter value called a message digest.
Secure Hash Algorithm (SHA) is a standard algorithm used to create a larger (160-bit) message digest. SHA-2 is used to create an even larger (224-bit) message digest.

POST - QUANTUM CRYPTOGRAPHY :

Post-quantum cryptography is the development of cryptographic systems for classical computers that can prevent attacks launched by quantum computers.
In the 1990s, after mathematician Peter Shor successfully demonstrated that a theoretical quantum computer could easily break the algorithm used for public key encryption (PKE), cryptographers around the world

began to explore what a post-quantum cryptography system would look like.
In contrast to the threat quantum computing poses to current public-key algorithms, most current symmetric cryptographic algorithms and hash functions are considered to be relatively secure against attacks by quantum computers. While the quantum Grover's algorithm does speed up attacks against symmetric ciphers, doubling the key size can effectively block these attacks.

Algorithms:

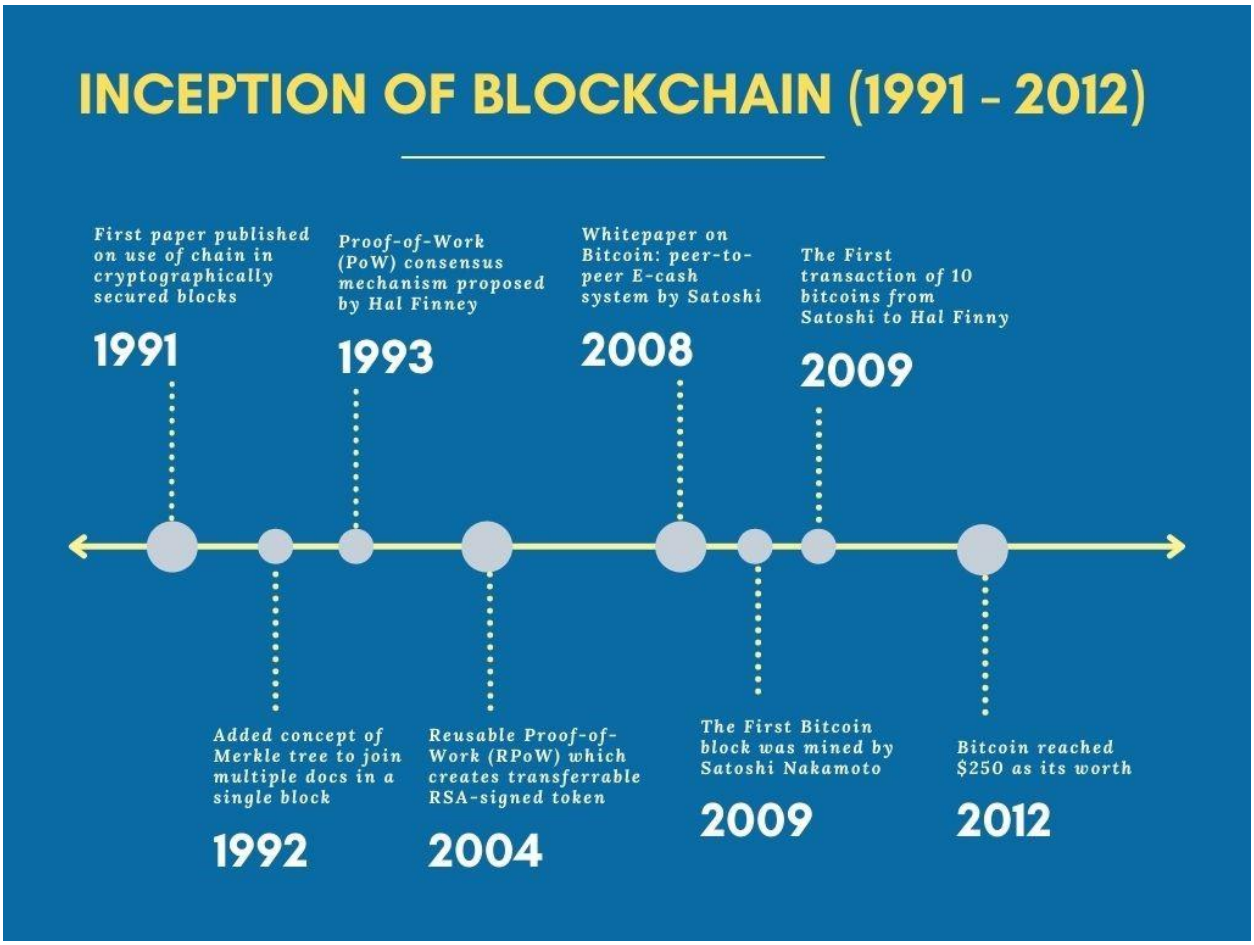
- Lattice based
- Multivariate
- Hash-based
- Symmetric key quantum resistance

Open Quantum Safe (**OQS**) project:

Started in late 2016 and has the goal of developing and prototyping quantum-resistant cryptography. It aims to integrate current post-quantum schemes in one library: **liboqs**

Bitcoin:

Nakamoto stated that work on the writing of the code for Bitcoin began in 2007. On 18 August 2008, he or a colleague registered the domain name bitcoin.org, and created a web site at that address. On 31 October, Nakamoto published a white paper on the cryptography mailing list at metzdowd.com describing a digital cryptocurrency, titled "Bitcoin: A Peer-to-Peer Electronic Cash System".



STANDARDS:

The Internet Engineering Task Force (IETF):
It is a standards organization for the Internet and is responsible for the technical standards that make up the Internet protocol suite (TCP/IP). It has no formal membership roster or requirements and all its participants are volunteers. Their work is usually funded by employers or other sponsors.

The IETF is organized into a large number of working groups and birds of a feather informal discussion groups, each dealing with a specific topic. The IETF operates in a bottom-up task creation mode, largely driven by these working groups.

Rough consensus is the primary basis for decision making. There are no formal voting procedures. Because the majority of the IETF's work is done via mailing lists, meeting attendance is not required for contributors.

The details of IETF operations have changed considerably as the organization has grown, but the basic mechanism remains publication of proposed specifications, development based on the proposals, review and independent testing by participants, and republication as a revised proposal, a draft proposal, or eventually as an Internet Standard.

The Internet Architecture Board (IAB) oversees the IETF's external relationships and relations with the RFC Editor. The IAB provides long-range technical direction for Internet development.

The IETF cooperates with the W3C, ISO/IEC, ITU, and other standards bodies.

European Telecommunications Standards Institute (ETSI):

It is an independent, non-profit, standardization organization in the field of information and communications. ETSI supports the development and testing of global technical standards for ICT-enabled systems, applications and services.
ETSI was set up in 1988 by the European Conference of Postal and Telecommunications Administrations (CEPT) following a proposal from the European Commission. ETSI is the officially recognized body with a responsibility for the standardization of Information and Communication Technologies (ICT).
ETSI develops standards in key global technologies such as: GSM, TETRA, 3G, 4G, 5G, DECT.

National Institute of Standards and Technology (NIST):

An agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness.

From 1901 to 1988, the agency was named the **National Bureau of Standards**.

In February 2014 NIST published the NIST Cybersecurity Framework that serves as voluntary guidance for organizations to manage and reduce cybersecurity risk.

It emphasizes the importance of implementing Zero-trust architecture which focuses on protecting resources over the network perimeter. ZTA utilizes zero trust principles which include the following to safeguard users' assets and resources.

- never trust, always verify
- assume breach
- least privileged access

Since ZTA holds no implicit trust to users within the network perimeter, authentication and authorization are performed before at every stage of a digital transaction. This reduces the risk of unauthorized access of resources.

Institute of Electrical and Electronics Engineers Standards Association (IEEE SA):

- **IEEE FOR WIFI - 802.11:**

  IEEE 802.11 is part of the IEEE 802 set of local area network (LAN) technical standards, and specifies the set of media access

control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) computer communication.

IEEE 802.11 uses various frequencies including, but not limited to, 2.4 GHz, 5 GHz, 6 GHz, and 60 GHz frequency bands. Although IEEE 802.11 specifications list channels that might be used, the radio frequency spectrum availability allowed varies significantly by regulatory domain.

802.11a uses the 5 GHz U-NII band which, for much of the world, offers at least 23 non-overlapping, 20-MHz-wide channels. This is an advantage over the 2.4-GHz, ISM-frequency band, which offers only three non-overlapping, 20-MHz-wide channels where other adjacent channels overlap (see: list of WLAN channels).

- **IEEE FOR BLUETOOTH - 802.15:**

IEEE 802.15 is a working group of the Institute of Electrical and Electronics Engineers (IEEE) IEEE 802 standards committee which specifies Wireless Specialty Networks (WSN) standards.

Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz, using a spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops/sec. The 2.4 GHz ISM band is available and unlicensed in most countries.

Bluetooth v4.0 is the most recent version of Bluetooth wireless technology. It includes a low energy feature that is the basis for Bluetooth Smart devices. A product bearing the Bluetooth Smart and Bluetooth Smart Ready logos must include Bluetooth v4.0, but must also meet additional criteria.

RFC :

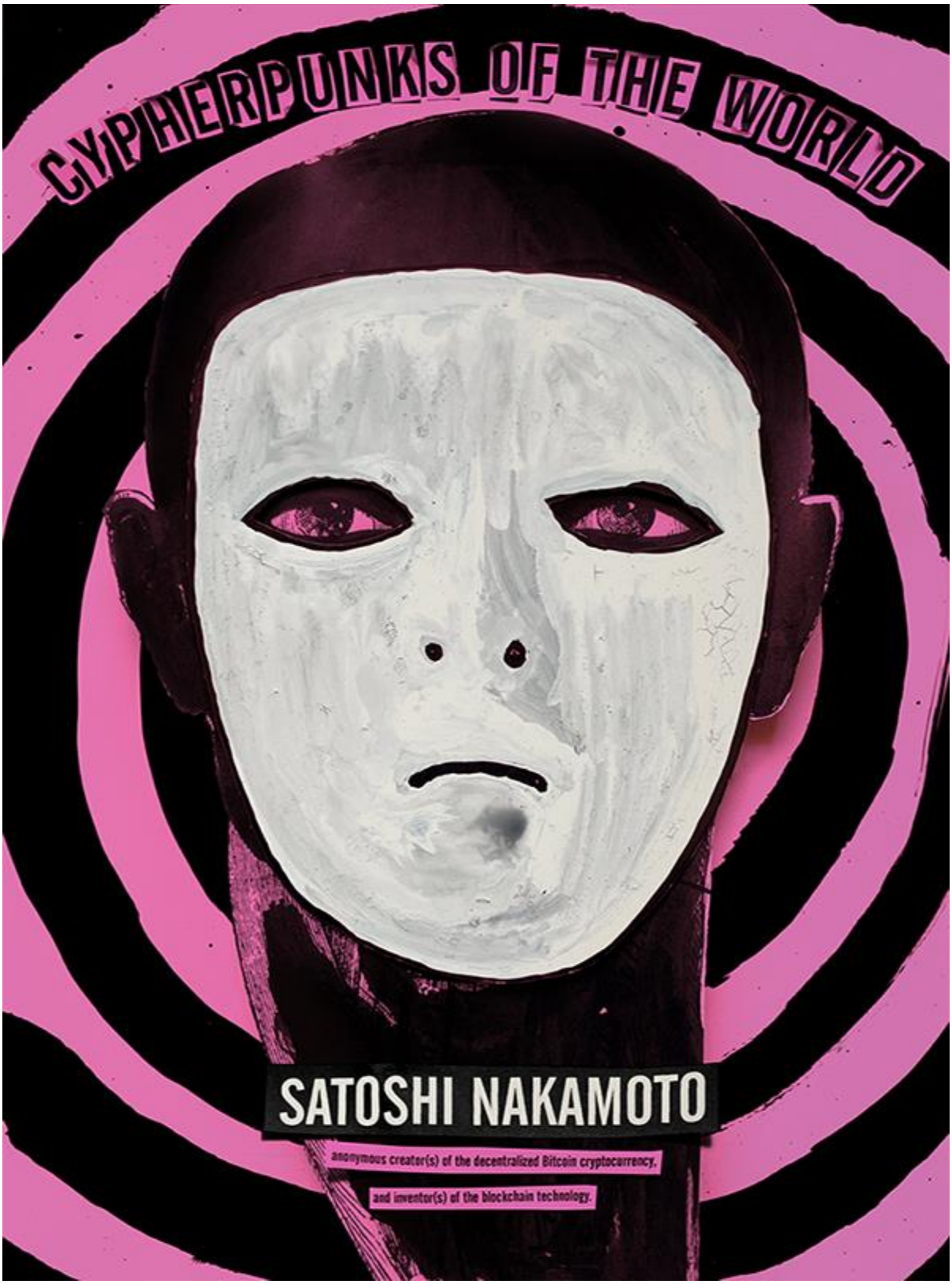
RFC documents contain technical specifications and organizational notes for the Internet.

RFCs produced by the IETF cover many aspects of computer networking. They describe the Internet's technical foundations, such as addressing, routing, and transport technologies. RFCs also specify protocols like TLS 1.3, QUIC, and WebRTC that are used to deliver services used by billions of people every day, such as real-time collaboration, email, and the domain name system.

The RFC Series includes documents produced by the IETF, the Internet Architecture Board (IAB), the Internet Research Task Force (IRTF), and independent submitters. All RFCs are published by the RFC Editor, which is the authoritative source for retrieving RFCs.

The first document in this series, RFC 1, was written in 1969. It was soon followed by others, including those that describe the core Internet Protocol (IP) still used in the Internet today. The collaborative process used to develop early RFCs remains an important part of the IETF spirit. Today, there are more than 9000 individually numbered documents in the series.

Speculations on the identity


CYPHERPUNKS OF THE WORLD
SATOSHI NAKAMOTO
anonymous creator(s) of the decentralized Bitcoin cryptocurrency,
and inventor(s) of the blockchain technology.

When translated from japanese, **Satoshi Nakamoto** literally means **“**The Clever/intelligent one who lives in the middle**”.** There are many widespread theories surrounding this sure shot obvious made-up name.

Hal Finney:

In 2004, Finney created the first reusable proof of work system before Bitcoin. In January 2009, Finney was the Bitcoin network's first transaction recipient. And received the first bitcoin transaction from bitcoin's creator Satoshi Nakamoto.

It is even widely believed that he is Satoshi Nakamoto who introduced Bitcoin transactions that could only take place between two persons. People believed that he hid behind the made-up name. Dorian Satoshi Nakamoto lived in (Temple City, California), adding to speculation that he may have been Bitcoin's creator. Finney denied that he was Satoshi Nakamoto. He may be worried about the backlash of the establishment. This is because the concept was a challenge to the US Dollar.

Nick Szabo:

Nick Szabo is a computer scientist and cryptographer who is known for his work on digital currency and smart contracts. Some people believe that Szabo is Satoshi Nakamoto, based on the similarities between his writing style and the Bitcoin white paper. However, Szabo has denied being Satoshi.

Craig Wright:

Craig Wright is a computer scientist and early contributor to the Bitcoin project.

Wright has asserted that he is the true identity of Satoshi Nakamoto, the pseudonym for Bitcoin's otherwise anonymous creator.

Despite his claims, most of the cryptocurrency community either rejects or remains highly skeptical of Craig Wright being Satoshi.

He has been a lecturer and researcher in computer science at Charles Sturt University, authored many articles, academic papers, and books, and has spoken publicly at conferences on IT, security, Bitcoin, and other topics relating to digital currency.

Wright currently works as chief scientist at nChain Inc., a blockchain research and development company.

Dorian Nakamoto:

Several similarities were claimed between Satoshi Nakamoto and Dorian Nakamoto. Dorian graduated in physics from California Polytechnic and worked on classified defense projects. Nakamoto said he was “no longer” involved with Bitcoin and that he had “turned it over” to other people. Dorian Nakamoto later denied and claimed that he had misunderstood the question and had nothing to do with Bitcoin.