Thursday, 23 April, 2020

The Bridge

# How Crypto-Asset Wallets Work

# Introduction

A crypto-asset wallet is a tool that allows users to interact with blockchain networks. Such wallets can be classified into hot (online) and cold (offline) wallets. Hot wallets usually consist of software wallets, whereas cold wallets consist of hardware and paper wallets. For security purposes, multiple cryptographic methods are used to open wallets and transfer coins.

# How different types of encryption work

Encryption methods can be broadly divided into three categories: hash functions, symmetric encryption, and asymmetric encryption.

A hash function is any mathematical function that takes data of any length as input and maps it into a fixed-size string of values. Hash functions do not produce any decryption keys; therefore, these functions are one-way functions, making it almost impossible to decrypt the original input from the output.

As an example of this function, when a hash for the word “bitcoin” is created using a SHA256[1] algorithm, the string “6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b” is generated as output. The SHA256 algorithm will always produce the same hash output for the same input, a change as minor as capitalising initial letter in the input will change the output dramatically. Readers can try hashing their data here[link1].

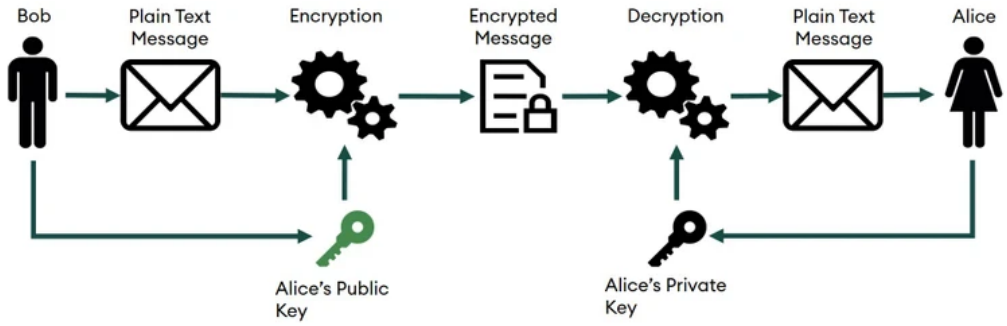
Symmetric encryption is a process that generates and uses a single key to encrypt and decrypt data. It is called symmetric c as the same key is used to perform both functions. As an example, a key that moves 3 alphabets forward for encryption and 3 alphabets backwards for decryption will easily decrypt the word *elwfrlq* to *bitcoin*.

Let us consider a scenario where Alice and Bob privately send messages to each other. To do this securely using a symmetric cryptography method, they will generate a single key and share it with each other. Bob (sender) will use that key to encrypt the message and send it to Alice. On receiving the message, Alice will use the same key to decrypt the message.

Asymmetric encryption or public-key encryption is a process that generates and uses a pair of related cryptographic keys, one public and one private, to encrypt and decrypt data and protect it from unauthorized access or use. The public key is simply the hashed output of the private key. (We invite readers to watch a very insightful video on public-key cryptography[link1]). As hash functions are one-way functions, it is impossible[2] to decipher private keys from public keys. A public key can be used by any person to encrypt a message so that it can only be deciphered by the intended recipient with their private key. A private key or secret key is shared only with the owner of the key.

Let us consider a scenario where Alice and Bob privately send messages to each other. To do this securely, using an asymmetric cryptography method, they will generate two pairs of private and public keys, of which one pair will be with Alice and the other will be with Bob. The public key is available for all to view, so both Alice and Bob can look at each other's public keys. However, the private key is kept as a secret by its owner. As shown in figure 1, to send a message to Alice, Bob will encrypt the message by using Alice's public key and then send it to Alice. On receiving the message, Alice can use her private key to decrypt Bob's message.

**Figure 1: How Asymmetric Cryptography Works**




Source: SEBA Research

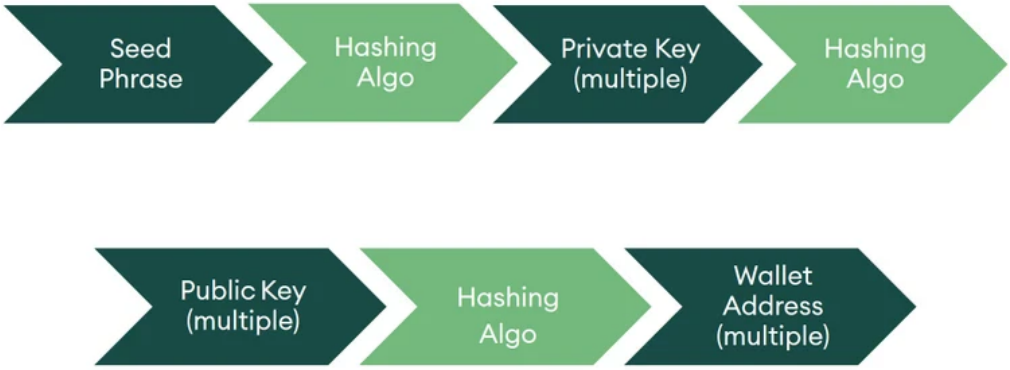
**How wallet encryption works**

Now that we know what asymmetric encryption is, we can further understand how blockchain wallets work. Whenever a person creates a crypto-asset wallet, the wallet randomly generates[3] a private key and a public key. The public key is then input into a hashing algorithm to create the wallet address of the account holder. Wallet addresses are generally 34-digit alphanumeric codes that function in the same manner as an email address. If someone intends to send cryptocurrency, such as bitcoin, to another person, they should know the receiver's wallet address. When the bitcoins are transferred between two parties, the coins never actually leave the blockchain but merely move from one address to another.

On the other hand, the private key is used to digitally sign[4] new transactions and provide access to the funds in the wallet; therefore, it should not be shared with anyone. In very simple terms, it is equivalent to your password or a PIN. For easier private key management, most modern wallets generate a seed phrase out of which the private keys can be recovered. Seed phrases are a list of words that store all the information needed to get access to the wallet. The process of using the seed phrase to recover funds is shown in figure 2. One can only move from the seed phrase towards the wallet addresses and not the other way round, due to the hash function's one-way nature. If the seed phrase is lost,

the funds are almost impossible to recover. It is best practice to store both your seed phrase and private keys offline in a safe location, as anybody who has the seed phrase or private keys can access and control the wallet.

**Figure 2: How Crypto-Asset Wallets Create Addresses Using Asymmetric Encryption**




Source: SEBA Research

## Types of crypto-asset wallets

There are many ways to classify a wallet. The two most common ways are based on the physical status and the operational structure of the wallet. Depending on their physical status, the majority of crypto-asset wallets can be classified as software, hardware, or paper wallets. Each type offers some advantages and disadvantages over the others (figure 3).

**Figure 3: Different Types of Crypto-Asset Wallets According to Physical Status**

| | Software Wallet | Hardware Wallet | Paper Wallet |
|---|---|---|---|
| **Advantages** | 1. Fast transactions<br>2. Easy to use | 1. Highly secure from hackers<br>2. Physically transferable | 1. Free of cost<br>2. Highly secure from hackers<br>3. Can create multiple copies |
| **Disadvantages** | 1. Least secure of all three types<br>2. Third party involvement (in case of exchange wallet) | 1. Cost of purchase<br>2. Low transaction | 1. Prone to physical damage and theft<br>2. Not user friendly |
| **Example** | Web wallets (Blockchain.com), desktop wallets (Exodus) or mobile wallets (MyCelium) | Ledger Nano S, Trezor and Keepkey | Paper |

Source: SEBA Research

In operational terms, wallets can be classified as either hot or cold. A hot wallet is a wallet that is connected to the internet. Most software wallets fall under the hot wallet category. These provide users with the ability to quickly transfer or exchange their funds; however, they are relatively more vulnerable to attacks (or being threatened by hackers) through the internet. On the other hand, cold wallets store the users' funds in a device that is not connected to the internet, making them more secure than hot wallets. Most hardware wallets and all paper wallets fall under this category.

# Conclusion

Crypto-asset wallets use multiple types of encryption techniques to keep user funds safe. As the cryptoverse has expanded, so have the types of wallets and their security. The users of crypto assets should clearly understand the importance of things such as seed phrases, private keys, and the hot and cold nature of wallets to make well-informed decisions about storing their funds.

[1] bitcoin = 6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b Bitcoin = b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4

[2] Formally speaking, it is almost impossible, as the likelihood to decipher private keys from public keys. The probability is 1 over 2128, or 1 chance in 340,282,366,920,938,463,463,374,607,431,768,211,456. (https://www.quora.com/How-does-a-supercomputer-decrypt-the-private-key-from-a-public-BTC-address-Is-that-worth-to-do)

[3] The wallet generates multiple pairs as a security measure; therefore, a wallet can have multiple pairs of private and public keys, but to keep it simple, we'll assume just one pair.

[4] Digital signature is a way of authenticating a transaction. To understand more, please click the following link. https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm

# Authors

**Yves Longchamp**
Head of Research
SEBA Bank AG

**Ujjwal Mehra**
Research Analyst
B&B Analytics Private Limited

**Saurabh Deshpande**
Research Analyst
B&B Analytics Private Limited

research@seba.swiss

# Disclaimer

No representation or warranty, either express or implied, is provided in relation to the accuracy, completeness or reliability of the information contained in this document, except with respect to information concerning SEBA. The information is not intended to be a complete statement or summary of the financial investments, markets or developments referred to in the document. SEBA does not undertake to update or keep current the information. Any statements contained in this document attributed to a third party represent SEBA's interpretation of the data, information and/or opinions provided by that third party either publicly or through a subscription service, and such use and interpretation have not been reviewed by the third party.

Any prices stated in this document are for information purposes only and do not represent valuations for individual investments. There is no representation that any transaction can or could have been effected at those prices, and any prices do not necessarily reflect SEBA's internal books and records or theoretical model-based valuations and may be based on certain assumptions. Different assumptions by SEBA or any other source may yield substantially different results.

Nothing in this document constitutes a representation that any investment strategy or investment is suitable or appropriate to an investor's individual circumstances or otherwise constitutes a personal recommendation. Investments involve risks, and investors should exercise prudence and their own judgment in making their investment decisions. Financial investments described in the document may not be eligible for sale in all jurisdictions or to certain categories of investors. Certain services and products are subject to legal restrictions and cannot be offered on an unrestricted basis to certain investors. Recipients are therefore asked to consult the restrictions relating to investments, products or services for further information. Furthermore, recipients may consult their legal/tax advisors should they require any clarifications. SEBA and any of its directors or employees may be entitled at any time to hold long or short positions in investments, carry out transactions involving relevant investments in the capacity of principal or agent, or provide any other services or have officers, who serve as directors, either to/for the issuer, the investment itself or to/for any company commercially or financially affiliated to such investment.

At any time, investment decisions (including whether to buy, sell or hold investments) made by SEBA and its employees may differ from or be contrary to the opinions expressed in SEBA research publications.

Some investments may not be readily realizable since the market is illiquid and therefore valuing the investment and identifying the risk to which you are exposed may be difficult to quantify. Investing in digital assets including cryptocurrencies as well as in futures and options is not suitable for every investor as there is a substantial risk of loss, and losses in excess of an initial investment may under certain circumstances occur. The value of any investment or income may go down as well as up, and investors may not get back the full amount invested. Past performance of an investment is no guarantee for its future performance. Additional information will be made available upon request. Some investments may be subject to sudden and large falls in value and on realization you may receive back less than you invested or may be required to pay more. Changes in foreign exchange rates may have an adverse effect on the price, value or income of an investment. Tax treatment depends on the individual circumstances and may be subject to change in the future.

SEBA does not provide legal or tax advice and makes no representations as to the tax treatment of assets or the investment returns thereon both in general or with reference to specific investor's circumstances and needs. We are of necessity unable to take into account the particular investment objectives, financial situation and needs of individual investors and we would recommend that you take financial and/or tax advice as to the implications (including tax) prior to investing. Neither SEBA nor any of its directors, employees or agents accepts any liability for any loss (including investment loss) or damage arising out of the use of all or any of the Information provided in the document.

This document may not be reproduced or copies circulated without prior authority of SEBA. Unless otherwise agreed in writing SEBA expressly prohibits the distribution and transfer of this document to third parties for any reason. SEBA accepts no liability whatsoever for any claims or lawsuits from any third parties arising from the use or distribution of this document.

Research will initiate, update and cease coverage solely at the discretion of SEBA. The information contained in this document is based on numerous assumptions. Different assumptions could result in materially different results. SEBA may use research input provided by analysts employed by its affiliate B&B Analytics Private Limited, Mumbai. The analyst(s) responsible for the preparation of this document may interact with trading desk personnel, sales personnel and other parties for the purpose of gathering, applying and interpreting market information The compensation of the analyst who prepared this document is determined exclusively by SEBA.

Austria: SEBA is not licensed to conduct banking and financial activities in Austria nor is SEBA supervised by the Austrian Financial Market Authority (Finanzmarktaufsicht), to which this document has not been submitted for approval. France: SEBA is not licensed to conduct banking and financial activities in France nor is SEBA supervised by French banking and financial authorities. Italy: SEBA is not licensed to conduct banking and financial activities in Italy nor is SEBA supervised by the Bank of Italy (Banca d'Italia) and the Italian Financial Markets Supervisory Authority (CONSOB - Commissione Nazionale per le Società e la Borsa), to which this document has not been submitted for approval. Germany: SEBA is not licensed to conduct banking and financial activities in Germany nor is SEBA supervised by the German Federal Financial Services Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht), to which this document has not been submitted for approval. Hong-Kong: SEBA is not licensed to conduct banking and financial activities in Hong-Kong nor is SEBA supervised by banking and financial authorities in Hong-Kong, to which this document has not been submitted for approval. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Hong-Kong where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not "professional investors" within the meaning of the Securities and Futures Ordinance (Chapter 571 of the Laws of Hong Kong) and any rules made thereunder (the "SFO"). Netherlands: This

publication has been produced by SEBA, which is not authorised to provide regulated services in the Netherlands. Portugal: SEBA is not licensed to conduct banking and financial activities in Portugal nor is SEBA supervised by the Portuguese regulators Bank of Portugal "Banco de Portugal" and Portuguese Securities Exchange Commission "Comissao do Mercado de Valores Mobiliarios". Singapore: SEBA is not licensed to conduct banking and financial activities in SIngapore nor is SEBA supervised by banking and financial authorities in Singapore, to which this document has not been submitted for approval. This document was provided to you as a result of a request received by SEBA from you and/or persons entitled to make the request on your behalf. Should you have received the document erroneously, SEBA asks that you kindly destroy/delete it and inform SEBA immediately. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Singapore where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not accredited investors, expert investors or institutional investors as defined in section 4A of the Securities and Futures Act (Cap. 289 of Singapore) ("SFA"). UK: This document has been prepared by SEBA Bank AG ("SEBA") in Switzerland. SEBA is a Swiss bank and securities dealer with its head office and legal domicile in Switzerland. It is authorized and regulated by the Swiss Financial Market Supervisory Authority (FINMA). This document is for your information only and is not intended as an offer, or a solicitation of an offer, to buy or sell any investment or other specific product.

SEBA is not an authorised person for purposes of the Financial Services and Markets Act (FSMA), and accordingly, any information if deemed a financial promotion is provided only to persons in the UK reasonably believed to be of a kind to whom promotions may be communicated by an unauthorised person pursuant to an exemption under the FSMA (Financial Promotion) Order 2005 (the "FPO"). Such persons include: (a) persons having professional experience in matters relating to investments ("Investment Professionals") and (b) high net worth bodies corporate, partnerships, unincorporated associations, trusts, etc. falling within Article 49 of the FPO ("High Net Worth Businesses"). High Net Worth Businesses include: (i) a corporation which has called-up share capital or net assets of at least £5 million or is a member of a group in which includes a company with called-up share capital or net assets of at least £5 million (but where the corporation has more than 20 shareholders or it is a subsidiary of a company with more than 20 shareholders, the £5 million share capital / net assets requirement is reduced to £500,000); (ii) a partnership or unincorporated association with net assets of at least £5 million and (iii) a trustee of a trust which has had gross assets (i.e. total assets held before deduction of any liabilities) of at least £10 million at any time within the year preceding the promotion. Any financial promotion information is available only to such persons, and persons of any other description in the UK may not rely on the information in it. Most of the protections provided by the UK regulatory system, and compensation under the UK Financial Services Compensation Scheme, will not be available.