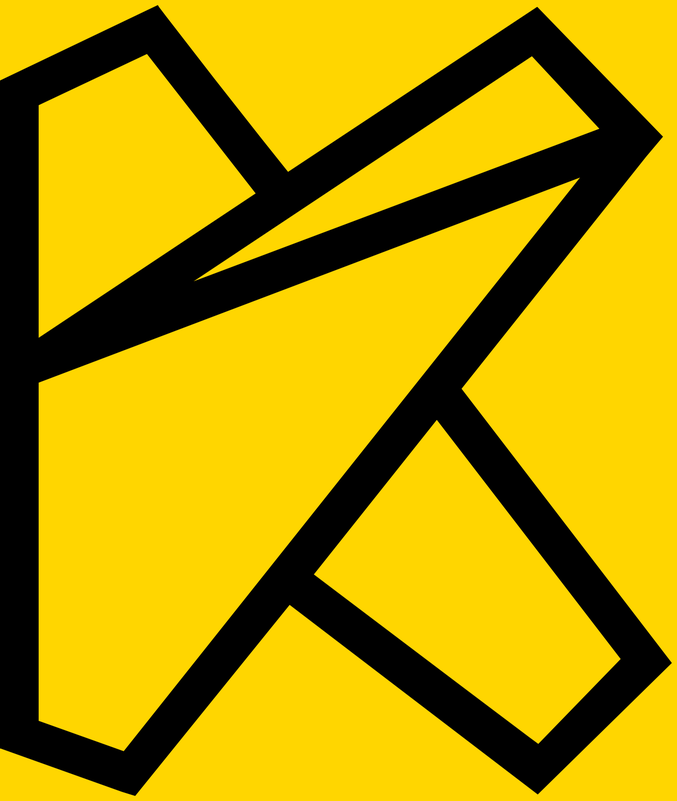
KEPLER

THE KEPLER PRIVACY PLATFORM

LITEPAPER

KEPLER.NETWORK



CONTENTS

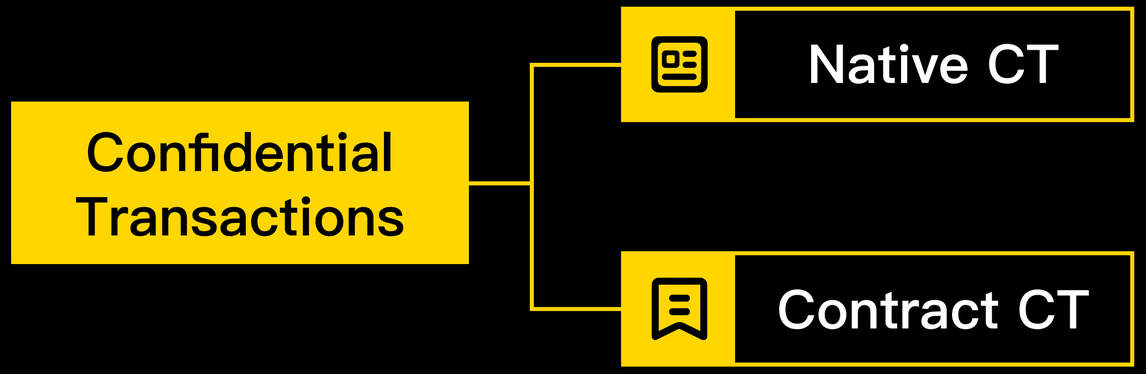
1 Privacy Protection on Blockchain

- Confidential Transactions (CT)
- Confidential Assets (CA)

Confidential Transactions (CT)

A few years ago, Bitcoin was considered to be anonymous. However, it has been found that the association between Bitcoin addresses and real users may be revealed through multiple channels, such as exchanges, offline payments, OTC transactions and some individuals or organizations that conduct data mining. Today, Bitcoin is more widely considered to be pseudonymous.

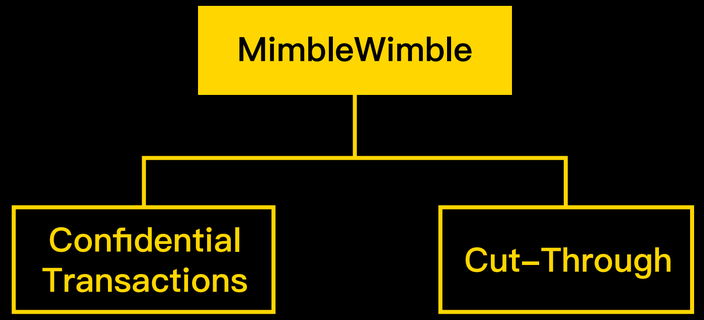
Similar to Bitcoin, the on-chain data of the majority of public blockchains is open. Privacy protection has recently gained more importance in the blockchain industry, and researchers are constantly exploring privacy protection solutions. At present, privacy protection solutions can be divided into two categories: one is **the confidential transactions native on the blockchain (hereinafter referred to as the native CT)**; the other is **the confidential transactions implemented by smart contracts (hereinafter referred to as the contract CT)**.



Native CT

Since the birth of Bitcoin, native CT technologies have been continuously improved, from early CoinJoin and Ring signature to zk–SNARK and MimbleWimble. Among the above technologies, MimbleWimble is simple, easy to use and efficient, it combines privacy protection and capacity scalability.

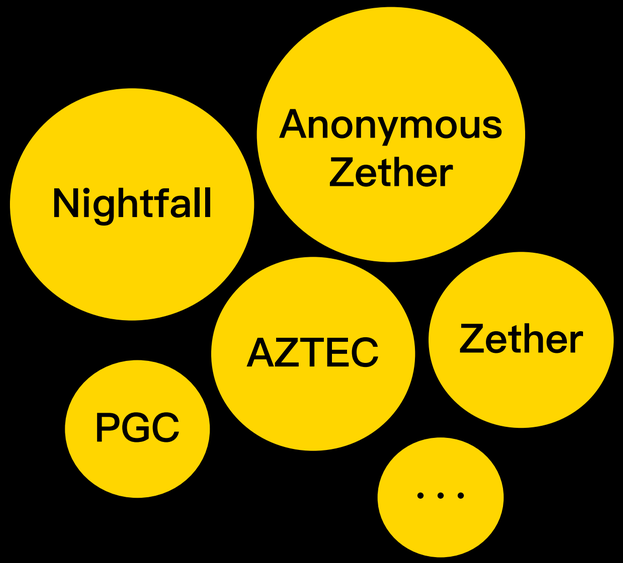
With the launch of Beam and Grin based on MimbleWimble protocol in January 2019, MimbleWimble has become a research hotspot. MimbleWimble contains two important concepts: **Confidential Transactions** and **Cut–Through**. Confidential transactions adopt Pedersen Commitment to hide the address and amount of transactions, and cut–through breaks the correspondence between the inputs and outputs of transactions, further confusing the relationship between the transaction participants.



Contract CT

Contract CT solutions include **AZTEC**, **Nightfall**, **Zether**, **Anonymous Zether**, **PGC**, etc. These implement native CT solutions (such as zk–SNARK, MimbleWimble) in smart contracts. A common problem with these contract CT schemes is the high gas cost, which of some schemes is even close to the total gas limit of the Ethereum block (about 8M).

If the problem of high gas cost is not solved, contract CT schemes are difficult to apply in practice. To this end, the Ethereum community proposed EIP–1109, proposing to reduce the gas of all precompiled contracts. However, the EIP needs to be applied to Ethereum through a hard fork, which may not be realized in a short time.

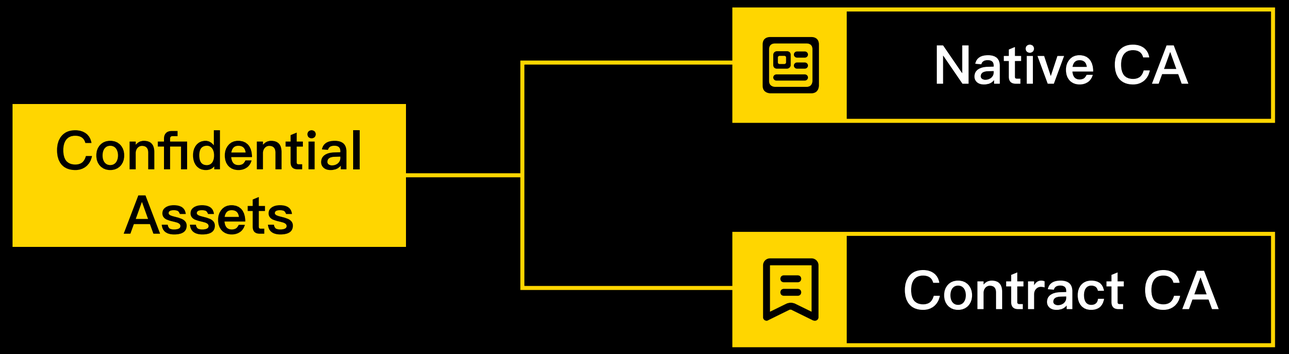


Confidential Assets (CA)

At present, many blockchain projects such as Monero, Zcash, Sero, Beam and Grin, have been able to implement native CT schemes. There are some issues with their design, which means that only the transaction amount can be hidden while the asset type cannot be hidden. For instance, one user conducts a confidential transaction on Grin, the network participants do not know the transaction amount, but can undoubtedly determine that Grin coins are being sent.

In reality, users usually have multiple asset types (such as different kinds of cryptocurrency, securities or other assets). In the transaction process, users also do not want to expose the asset type in addition to the transaction amount. To be better applied in practice, blockchain privacy technologies must address that user requirement. Therefore, researchers at Blockstream proposed to study a technology called Confidential Assets that can hide both transaction amount and asset types.

Similar to CT solutions, the CA solutions can be divided into two categories: one is **the confidential assets native on the blockchain (hereinafter referred to as the native CA)**; the other is **the confidential assets implemented by smart contracts (hereinafter referred to as the contract CA)**.



Native CA

Blockstream released the CA feature in its Elements blockchain platform in 2017. Elements' CA solution is based on Bitcoin system, and although the amount and asset type cannot be seen by blockchain viewers, the addresses of senders and receivers can still be seen.

In June 2019, Beam announced that it would extend the roadmap –– adding support for CA feature. Beam planned to work in two directions: 1. Bridges to Bitcoin, Ethereum and eventually other blockchains: allow locking assets on Bitcoin or other blockchains and issuing matching bAssets on Beam; 2. Allow 3rd parties to issue their tokens on Beam. Beam said it just had some initial thoughts at that moment and planned to refine and develop the scheme in the future.

Grin relies on the community governance model, and it is not controlled by any company, foundation or individual. About CA, there is only some discussion in Grin's forum, and whether Grin plans to support CA is not yet known.

Contract CA

The aforementioned contract CT schemes can also be used to implement the CA schemes, but some complex designs are required. Currently, most privacy projects based on smart contracts are designed to address the issue of how to hide transaction amount, and few projects claim to hide asset types. Besides, the gas cost is an issue that must be solved. Admittedly, contract CA technologies have a long way to go.

2 Why design Kepler

2

Why design Kepler

Blockchain technology has developed for a decade. The blockchain industry has experienced the rise and fall of many technologies or applications over the past decade, but the topic of privacy protection never goes out of date. Regardless of whether the blockchain technology is used in the financial field or DApps, users' privacy needs to be protected.

As mentioned above, the current CA technology has many problems, and the software development progress is very slow, which restricts the further development of the industry. Thus, Kepler proposed a MimbleWimble-based CA implementation that can hide transaction amounts, addresses and asset types, providing the strongest privacy of all solutions to date.

Besides, Kepler hopes to a CA platform where users can issue their confidential assets and conduct confidential transactions on demand, without having to develop a complete set of CA.

3 What is Kepler

What is Kepler

Kepler is the first implementation of the MimbleWimble-based CA project.
Things that make Kepler special include:

Users can issue and reissue their confidential assets. When the assets are issued, the asset type and max supply need to be disclosed.

When an asset is issued, the owner of the asset and the number of additional issues should be specified. The owner's signature is required to reissue the asset.

As the native coin of the system, Kepler is also a confidential asset and can be used to pay fees.

In addition to the native coin, other assets can be designated for payment of fees.

It has the privacy features of MimbleWimble, the sender addresses, receiver addresses and transaction amount can be hidden.

MimbleWimble's cut-through feature contributes to a smaller on-chain data of Kepler.

Kepler adopts the C31 mining algorithm which is ASIC friendly and can attract a large number of miners and mining equipment manufacturers to join the mining, thus ensures the safety of the system.

Implemented in rust language.

No ICO.

For a more in-depth review of the technology behind Kepler, take a look at "Confidential Assets" by Blockstream & "Confidential Assets on MimbleWimble" by Qtum.

4 Economic Model

Kepler's native coin is KMW, and all KMWs are generated through block rewards using PoW as consensus. KMW adopts the deflation model with a max supply of **2,138,639,000** and a genesis block reward (premine) of **42,000,000 KMWs**, which is about **2%** of the total. The initial block reward is **1000 KMWs**, and the average block interval is **60 seconds**. The block reward is cut in half every 2 years, which is equivalent to halving every **1048320** blocks. Detailed parameters are as follows:

KMW
Ticker symbol

2,138,639,000
Max Kepler Supply

2% as the genesis block reward
Premine

an average of **60** seconds
Block interval

1000 KMWs/block
Initial block reward

every **2** years,
or halving every **1048320** blocks
Block reward halving

4

According to the halving rule, after the 40th halving, the block reward will be less than (1 nano) KMW. At that time, the block reward will be directly set to 1 nano KMW, and the total mining rewards for a whole century will be only 0.052416 KMW.

Kepler adopts **the C31 mining algorithm**, and the miners get all the block reward.

As the native coin of the Kepler system, KMW can be used as fees for issuing, trading and destroying confidential assets. KMW can also be used as a confidential asset. Users need to lock a certain amount of their KMWs when issuing new confidential assets.

4

5 Future Work

5

Future Work

Kepler's first version of the CA feature will be released in Q2 2020. In the future, we will continue to improve and realize the following features:

- Asset type and supply can be hidden to achieve stronger privacy.
- Assets can be destroyed.
- Users can choose whether to hide the asset type and transaction amount.
- Support for non-interactive transactions. When senders initiate transactions, the receivers are allowed to be offline, which reduces the difficulty of trading operations.
- Support for setting lock_height on outputs.

KEPLER

https://twitter.com/Keplernetwork1
https://medium.com/@keplernetwork
discord.gg/CJpMCqZ
t.me/keplernetwork
https://bitcointalk.org/index.php?topic=5116576.0