CATENA
for a smarter blockchain

C_Chain – Frequently Asked Questions

As a base blockchain technology, C_Chain can be integrated into any software and thus offers flexible use in a wide variety of applications. This makes them easier to manage and secures them over the long term. On a more technical level, C_Chain is characterized by a clear and unique architecture. In the following, the most frequently asked questions about the architecture of the C_Chain ecosystem will be addressed in order to dispel doubts and to highlight the advantages of C_Chain compared to classic blockchain solutions.

Content

Centralized architecture

Does the centralization of the CCM create a "single point of failure"?
Does the centralization give the CCM absolute data sovereignty and can thus exercise control over the data at will?
Doesn't the centralization of the CCM cause a large attack vector focused on the CCM and thus a high risk?
Would a failure of the CCM, for example by taking the associated server out of operation, paralyze the entire system?

Using parallel chains

Are the chains for protection linked?
How is data integrity ensured even though not all data is cryptographically linked in a central chain?
What happens if a chain is to be deleted in the system?

Other questions

Is C_Chain just an encrypted database?
Why does C_Chain use a CryptID instead of simple public keys for identification?
What are the advantages of C_Chain?
What if the CCM's key were compromised?

CATENA
for a smarter blockchain

Centralized architecture

Does the centralization of the CCM create a "single point of failure"?

No. Chains can be replicated as often as required in C_Chain, i.e. they can be saved locally by different users. Even if the individual blocks are booked from a central point, the verification is carried out by several distributed agents. In principle, every participant in the system has the option of checking the correctness of individual blocks at any time. Loss of data in the event of a total crash is avoided through backups and the possibility of local replication of blocks and chains at the users' premises. A planned, new storage architecture will enable a global distribution and backup of the data, which means data loss can be almost completely ruled out.

Does the centralization give the CCM absolute data sovereignty and can thus exercise control over the data at will?

No. The data is always signed twice, once by the sender and once by the CCM, which makes attempted fraud impossible. The content of individual bookings can be encrypted end-to-end. This is optional and offers users another way of ensuring full control over the data. By using encryption, only involved parties can access the protected data. So not even the CCM can get to details of the exchanged data. Because of this and the double signatures, the CCM has no way of cheating or falsifying data.

C_Chain follows the "Security by Design" scheme and guarantees absolute data security as standard. With various configuration options, rights can be assigned and the visibility of the chains can be set individually.

Data sovereignty is guaranteed by implementing GDPR conformity in a later update (see GDPR concept).

Doesn't the centralization of the CCM cause a large attack vector focused on the CCM and thus pose a high risk?

No. To break the integrity of the data, the keys used would have to be obtained. The keys of the CCM are secured in the Microsoft Key-Vault and data security is guaranteed by Microsoft based on TPM. Various key rotations also reduce vulnerability. For example, there is no “master key” that could bring down the entire system. Additional security measures are implemented at the chain and individual block level. As with other blockchain solutions, C_Chain adheres to the current standards.

Would a failure of the CCM, for example by taking the associated server out of operation, paralyze the entire system?

No. The CCM runs in Kubernetes clusters distributed across several data centers and thus already consists of many servers and not just one. These clusters are operated in Microsoft Azure and can optionally also be hosted by other cloud providers at the same time. To additionally guarantee the security of the data, they will be replicated and secured globally in the future.

The system is not yet live. As soon as it goes live, the Kubernetes cluster will be deployed first, followed by a model for global replication of the data.

Using parallel chains

Are the different chains linked for additional protection?

No. That would contradict the core idea of the C_Chain for various reasons. Linking the chains would significantly worsen performance and increase the vulnerability of the entire system (see next point). One of the core arguments for C_Chain and against classic blockchains is the ability to use of any number of chains, depending on the requirements of the respective use-case. This not only increases the performance and efficiency of the system, but also guarantees perfect scalability.

How is data integrity ensured even though not all data is cryptographically linked in a central chain?

All security and integrity rules that apply to chains in any single chain blockchain solution also apply to a multi-chain system. One advantage of multiple chains is that in the unlikely event that individual chains are compromised, the system is never affected as a whole.

There are also classic blockchains, such as Ethereum, that use multiple chains. Since an attack by unknown hackers in 2016 who managed to steal several million dollars in the form of tokens, Ethereum has split the so far only chain into two (Ethereum - DAO event).

What happens if a chain is to be deleted in the system?

Since the deletion of chains contradicts the general blockchain principles, there is currently no way of doing this with C_Chain. A deletion strategy for the purpose of GDPR conformity is already being developed and will follow in a later update (see GDPR concept).

CATENA
for a smarter blockchain

Other questions

Is C_Chain just an encrypted database?

No. As can be seen above with the questions about centralization and the use of chain structures in the booking of the system, C_Chain is a blockchain solution and not a classic database. Administrators can manipulate a database as required. With C_Chain, the so-called immutability property ensures that data cannot be changed.

Why does C_Chain use a CryptID instead of simple public keys for identification?

As an additional security measure, the CryptID also contains the signature of the public key by the owner of the key pair with the associated private key. This ensures that it is a valid key for which an actual user exists. This is a type of self-signed certificate that will be replaced by a qualified certificate in later versions.

What are the advantages of C_Chain?

Compared to other blockchain solutions, C_Chain impresses with its speed, efficiency and unlimited scalability. Due to its efficient operation, and the resulting low energy consumption, the costs for operation are very low. Thanks to its light infrastructure, C_Chain also ensures that it can be used in a wide variety of use-cases. The C_Chain software development kit comes libraries for important functionality such as encryption or digital signatures, so that developers can concentrate fully on the application and implement it in a very short time.

What if the CCM's key were compromised?

In the unlikely event that the CCM's key is compromised, it will be invalidated immediately. The CCM then generates a new key with which all blocks that are still based on the compromised key are re-signed. The old key pair is no longer used in any context and signatures with this key are no longer accepted.