2nd DIGITAL ASSETS CUSTODY SURVEY

conducted July 07/2020

TANGANY

RELIABLE WHITE-LABEL B2B CUSTODY SINCE 2018

Tangany provides custody and infrastructure services for digital assets on blockchain. Leverage our API or frontend solution to create your stunning blockchain-based business case.

More than 60,000 wallets under custody on Bitcoin, Ethereum, and Private Blockchains. Full support for all security tokens and smart contracts on Ethereum.

Our solution of warm and cold wallets is being used by 20 clients in all kinds of industries. Specialised services for financial institutions, tokenization projects, asset management and DeFi projects.

Supervised by the German Federal Financial Supervisory Authority (BaFin) as a crypto custody provider pursuant to Section 64y German Banking Act (Kreditwesengesetz).

DOWNLOAD NOW

OUR FREE PRODUCT PDF AT:

tangany.com/custody-survey

2nd DIGITAL ASSETS CUSTODY SURVEY

Dear reader,

Thank you for showing interest in our 2nd digital assets custody survey.

With this evaluation – which to our knowledge should be the most comprehensive study on digital asset custodians out there – we are once again looking to identify trends and challenges in the field of digital asset custodianship. Following up on our first survey, which was conducted at the end of 2019, we evaluated the given feedback and adjusted our questions slightly in order to maximize the output for our readers.

Despite being able to increase the number of participants by over 60 percent, we unfortunately did not achieve our initial goal of conducting a general "rating" of custodians. The wants and needs of the respective clients, and therefore also the requirements for services offered by their custodians, simply differ too much for such a rating at this point in time but may be done using assumptions at a later time. Furthermore, the differentiation between "pure-tech-providers" and "regulated or soon to be regulated custodians" (sometimes using tech from "pure-tech-providers") proved to be a challenging.

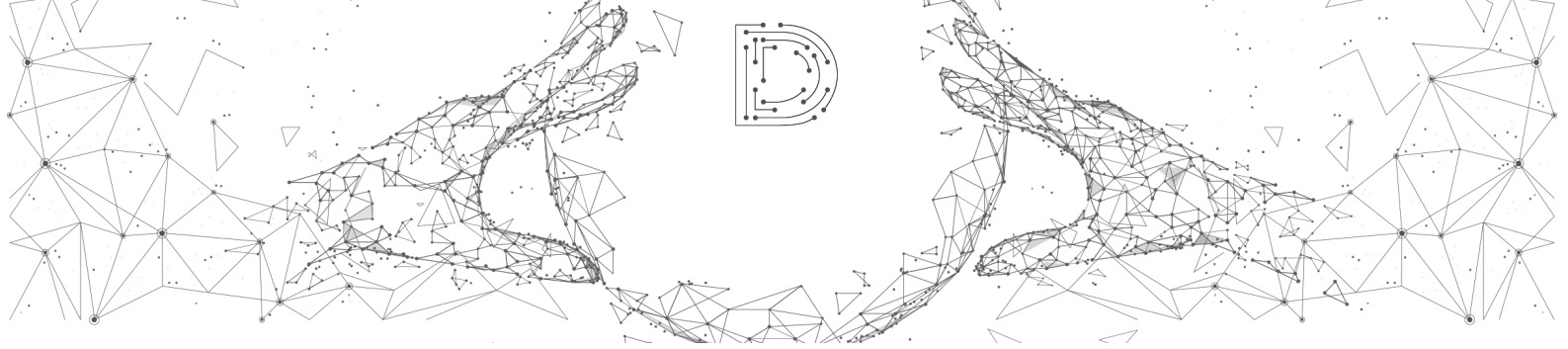
Nevertheless, we hope you enjoy the study which also includes expert contributions from Crypto Storage AG, RIDDLE&CODE and Trustology. We are happy these institutions took the chance to share their thoughts. If you have any further questions, are looking into digital asset custodianship for yourself or need a partner for the selection process or regulatory issues: Do not hesitate to contact us. We are happy to help.

Sincerely,

Dr. Sven Hildebrandt
CEO - DLC Distributed Ledger Consulting GmbH

Leander Schmidt
Research

Citlali Mora Catlett
Research



2nd DIGITAL ASSETS CUSTODY SURVEY

Content

1. Expert Contributions

In the first expert contribution, Dr. Lewin Boehnke from Crypto Storage AG discusses repeatable operations versus one-time auditing in the context of key ceremonies. Next, Jürgen Eckel from RIDDLE&CODE shares his thoughts on hardware security modules and multi-party computation and options of combining both. In the third article, Mark Hornsby from Trustology elaborates the Boneh-Lynn-Shacham signature scheme and discusses its impact on digital assets custody.

CRYPTO STORAGE

Key Ceremonies: Repeatable Operations vs. One-Time Auditing

Creating cryptographic secrets, which are used as private keys or as a “seed” to derive many keys, are critical, security-relevant operations in all digital asset handling, for both retail and institutional use. The key difference for retail use is that only the asset owner must feel assured of the integrity of the operation and that all elements involved have been subjected to the necessary controls and security considerations. E.g. the hardware wallet has not been manipulated, the procedure takes place in a closed room with shuttered windows and no cameras are in sight that could compromise the confidentiality of the recovery phrase without the owner noticing. From an operator's perspective in an institutional environment, security depends on the caution they and their coworkers both exercise; and the interplay of individual actions. The details vary greatly between different solutions: from on-chain multi-sig to the joint creation of keys and their separation through secret sharing schemes to separate partial individual key creations and their combination in MPC (multi-party computation).

The goal of overseeing and carefully auditing these actions is not to ensure the smooth functioning of the employed technologies or their parts. That comes in addition to it and is the point where proper review and certification of the technology is irreplaceable. Battle-tested hardware and software, and their relevant certifications (e.g. FIPS 140-2, NIST SP800-90) are invaluable and absolutely warranted to ensure a high degree of security.

The need for careful deliberation in defining a “key ceremony”, with checklists and recordings, is the operational element. A typical key ceremony exposes secrets. In the worst case, this would be 12 or 24 words of a mnemonic seed, as one might be familiar with from retail hardware wallets. More sophisticated solutions might only expose secrets that are “wrapped” and then “shared”. This means that they have been encrypted with a key provided by the operator that is exposed in multiple parts to a specific operator, and it might not display on a screen but may be exported directly to an attached storage device, or any combination of these or other elements.

A good script, supported by the relevant features of the infrastructure, indeed allows for a sane ceremony. This good script, and its faithful execution, results in the need for a one-time auditable event. The event and its audit should be so thorough that it withstands scrutiny even in the presence of adulterating factors. What if a laptop or storage medium is later found to be of questionable origin (Craig Wright's “demonstration” of being Satoshi Nakamoto in front of Gavin Andresen comes to mind), or an employee and participant in the ceremony is found to be unreliable? Which CISO or CRO will be happy to operate at the mercy of the previous one? Do not trust, verify! Key ceremonies are delicate operations.

Why is this necessary in the first place, and is there an alternative? A ceremony has two main objectives: first, to ensure that the cryptographic secrets created are sound and have the

intended level of security (i.e. can only be used given certain conditions or approvals), and second, to create a backup of the secrets while maintaining the intended security level. For some solutions – especially those based on Shamir's Secret Sharing – both of these goals are actually achieved using the same process. However, for solutions – especially those based on Hardware Security Modules (HSMs) – the first objective is met through the creation of keys in a HSM, with access control measures in or near the HSM, while the second objective is achieved through the way in which the "master key" data is exported.

The second objective can also be met by certifiable hardware, in a way that secrets are never exposed, not even in a wrapped or shared way. Instead, a backup is exported so that it is only recoverable by other identical devices. In such cases, backups become readily usable, redundant deployments of the HSM, and the objectives, key generation, and backup creation are all secured by the technology, not by the operations. The hardware certification and review that are critically necessary for the employed hardware – regardless of the remaining operations – fully supersede the need for an audit of the interaction.

A third objective frequently mentioned is interoperability, or the ability to recover keys from the backup without the same kind of infrastructure that is used for operations. Any kind of recovery that has the slightest chance of exposing secrets though strictly mandates moving assets off of those keys, rendering it "not worse" than recovering them from a redundant deployment of the same infrastructure.

If the technology is prevented from exposing secrets from the very start, wrapped or not, shared or not, then there is no need for a ceremony script and an audit of its faithful execution. The only purpose of the ceremony script is to oversee that the exposing of secrets and the creation of the backup were done carefully and without deliberately or accidentally exposing or leaking sensitive information in an uncontrolled way. If it is possible for any

operator to interact with the keys at any time after their creation to verify their integrity inside the infrastructure, attested for by the infrastructure itself, then this greatly reduces the need for observing and auditing the key creation. However, great care must be taken that the operators are aware what they must verify and when they must verify the key's integrity. If it eases operations, it is possible to "batch" the verification for many such secrets instead of verifying them on the fly. This operation is closest in nature and relevance to a conventional key ceremony. However, it is purely optional, can be repeated should any doubts arise, and (most importantly) can be done by each operator independently until he or she is satisfied, instead of forcing coordinated one-time events that lead to the need for an audit of the operation.

Dr. Lewin Boehnke

CTO AT CRYPTO STORAGE AG & HEAD OF RESEARCH
AT CRYPTO FINANCE AG

Dr. Lewin Boehnke has two roles within the Crypto Finance Group: Head of Research at Crypto Finance AG and CTO at Crypto Storage AG. He brings his technological experience and analytical perspective from his time as a theoretical and computational physicist to everything he does. He has worked on several projects since delving into crypto assets in 2011, including early mining and writing crypto trading bots. Dr. Boehnke holds a PhD in Theoretical Physics from the University of Hamburg.

For more information or inquiries contact Crypto Storage AG at: **info@cryptostorage.ch**

Riddle & Code®
THE BLOCKCHAIN INTERFACE COMPANY

Hardware Security Modules vs. Secure Multi-Party Computation in Digital Asset Custody: The Drawback of Choosing Just One and What Happens When You Combine Them

The most critical component in a digital assets system is the wallet. The wallet holds the private keys required to access and manage digital assets, and has three main responsibilities towards various user groups:

- creating and safekeeping digital assets for drawing transactions,
- storing a history of relevant transactions, and
- generating and forwarding transactions to the respective currency network(s).

Various wallet solutions are on the market today, and each one has its own advantages and disadvantages. When it comes to wallets that are specifically designed for institutional use, they can be divided into two camps: those using secure multi-party computation (MPC) and those using hardware secure modules (HSMs). We believe that, while both have unique and relevant strengths, solutions of the future should cleverly combine both techniques. Here is why.

Different Solutions for Different Users

Non-institutional, individual, digital asset traders who do not trade via exchange platforms often rely on so-called hardware wallets. These hardware wallets (specialised USB dongles) are responsible for performing the required key generation, management and signing of transactions.

With hardware wallets, a trader can execute dozens of transactions per day with all the necessary security and reliability added. Yet, hardware wallets existing on today's market do not support automatic trading and rely on

human operations. And human operations are prone to error.

Digital exchanges often make use of the same wallet programs to manage their customer's/user's assets. The daily volume of digital currency transactions varies. These volumes can be very low for some exchanges, while others deal with medium- to high-transaction volumes. To provide more accessibility and liquidity, exchanges often centralise customer's assets in so-called hot wallets, from which all transactions either originate or depart. The advantage of these systems is that thousands of transactions per day can be carried out in dozens of digital currencies. This can be done in either an automated or, if necessary (depending on the total value of the transaction), a manual setup.

However, the disadvantage of these systems is a lack of security and transparency. Most major digital exchange breaches have been hot wallet breaches. In addition, the administration of digital currencies via classic databases and hot wallets also lacks regulatory suitability. The actual change of ownership is not documented in the Blockchain. Instead, it is stored and managed in classical databases by the exchanges for as long as the assets remain in custody.

If cold storage has operational vulnerabilities and a hot wallet comes with security flaws, then what should institutional-grade custodians do to modernize their approach to custody? Lately, different technologies have been implemented to fulfill requirements for institutional grade, audited and highly secure digital asset platforms. A growing number of custodians are turning to hardware security modules (HSMs) as part of their security architecture and techniques such as secure multi-party computation (MPC).

Are HSMs Enough to Provide Custody at an Institutional Level?

A hardware security module is a tamper-resistant physical device that is isolated from external systems and used to generate and secure digital keys. HSMs are bank-proof, can secure

authentication, encryption, and transaction signing and handle a large number of transactions at high speed.

Still, HSMs require physical access for deployment, maintenance and configuration. They do not support complex business logics, cannot secure cloud applications or scale without additional hardware. A single module can protect only a limited number of keys and deployment cannot be automated. HSMs can be used to achieve the necessary transaction throughput with thousands of signatures. But when it comes to being "compliant" with the requirements of the established financial industry and its regulators, using only HSMs is not sufficient. In addition, an HSM centralizes keys, which always adds a security risk. As such, HSMs are most suitable for high volume, low value transactions in traditional industries.

Independent systems are needed to ensure the ability to flexibly derive key addresses and to generate key pairs for the respective token. Being data compliant requires the anonymized linking of generated keys and key addresses to classic customer bank accounts, which an HSM is not capable of doing. All these "non-HSM"-driven functions require another approach and technology.

Secure Multi-Party Computation – Eliminating Single Point of Failure

Secure multi-party computation (MPC) is a subfield of cryptography that lets parties (or devices) cooperatively compute a function over their data without revealing it. The potential applications for MPC are huge, from data analytics, auction bidding and electronic voting to privacy preserving, data mining and key management.

When it comes to key management, the technology has clear benefits, such as:

- eliminating the need for trusted third parties to keep data safe,
- allowing users to keep data within their internal firewalls,
- alleviating users from having to compromise between data

usability and data privacy/security, and
- meeting regulatory compliance requirements for cross-border transfers.

With MPC, participants in the process have no information beyond what is required to execute their individual function, and keys can only be compromised if all machines are breached simultaneously. Applied to key management, MPC allows the use of cryptographic keys without ever having them in a single place, thereby eliminating the key as a single point of failure. By distributing keys without sharing any sensitive information among the parties, the transaction is partially signed. The parties know their output and nothing else.

Moreover, MPC-based key management solutions enable access to real-time tamper-proof audit logs, support flexible advanced authorization schemes and can run in any environment.

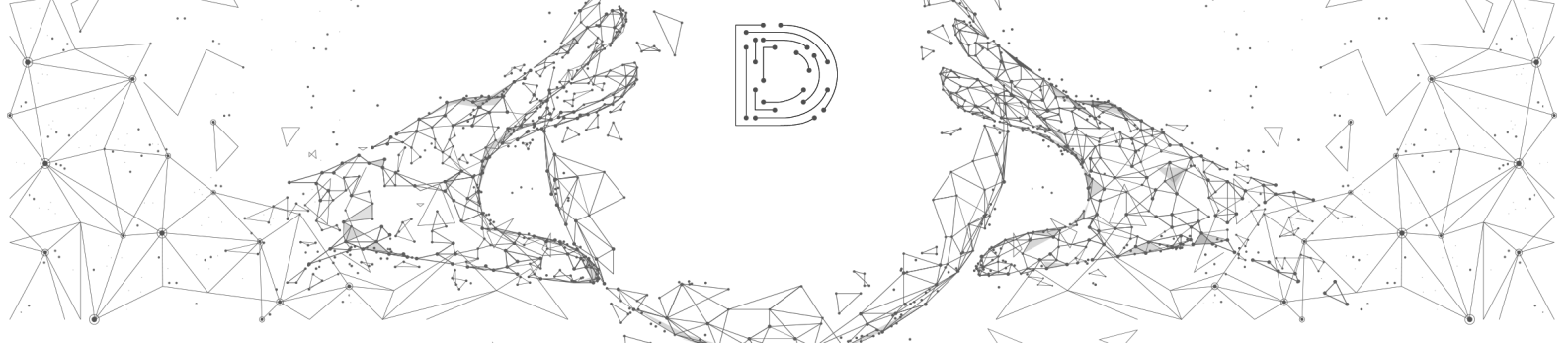
Yet, MPC also has its disadvantages. For starters, it lacks scalability. When real-time performance is required, MPC is not sufficiently practical. In case an increasing number of parties is required to sign a transaction, the computation becomes too complex and slow. For this reason, secure multi-party computation is most appropriate for highly confidential transactions with low volume and (probably) high value.

What Happens When You Combine Them?

There are two possible scenarios when combining these powerful mechanisms:

1. A solution that is flexible enough to allow switching of signing mechanisms according to the necessary requirements and use cases; or
2. A solution that combines the security strengths of MPC with the speed of HSMs.

However, either of these scenarios require business logic to identify appropriate use cases, coordination to execute correct signing processes and



confidential computing to protect sensitive information.

At RIDDLE&CODE, we have developed our own solution to enable this combination of signing techniques and have added the required orchestration and confidentiality. We named it the Policy Gateway. The Policy Gateway adds the flexibility of a custom business logic to the security of hardware. All operations are performed within the Trusted Execution Environment (TEE), which provides hardware-enforced code and data-in-use isolation.

The Policy Gateway performs and logs all processes preceding and following transaction authentication, achieving:

1. Full transparency and traceability of customers' segregated digital token accounts;
2. The possibility to reconcile accounts per customer, per token, etc.;
3. Regulatory criteria for transparency and compliance with "know your coin" (KYC) and "anti-money laundering" (AML) regulations;
4. Compliance with financial and crime regulations by ensuring that digital currency accounts have historically never been part of criminal transactions (blacklisting and token forensics);
5. Guaranteed compliance with the frameworks for the digital trade of token units and

6. Complete recording of all initiated and successfully processed transactions, the persons carrying them out, the place and time, the amount, the fees, and the accounts involved - for the purpose of logging, tracking, tracing, and real-time auditing.

By enhancing HSMs with secure multi-party computation, our solution is capable of orchestrating the best functionalities of the two mechanisms.

Jürgen Eckel

CIO AT RIDDLE&CODE GMBH

Jürgen Eckel manages the technology and development department at RIDDLE&CODE GmbH and oversees all stages of product planning and deployment. His passion for security and cryptography can be traced back to his university time when he explored secure microkernel design and formal systems.

Jürgen brings his technological expertise, the analytical perspective and the experience about shipping products from his background within the IT security sector. During this time, he was responsible for shipping various security products and content to customers to protect them against a wide range of cyberattacks.

Since joining RIDDLE&CODE, Jürgen has worked on several projects, including custody, energy trading, identity and lifecycle management solutions, as well as metadata DLT projects.

For more information or inquiries, contact RIDDLE&CODE GmbH: **office@riddleandcode.com** or visit our website: **https://www.riddleandcode.com/**

Trustology

Crypto Private Key Security and Threshold Signatures – is BLS Pure Magic for Custodians?

Multi-signature wallets have become the common standard for institutions managing digital assets as they enhance the security of assets over single key wallets. Until now this has been achieved at the protocol layer or through smart contracts, HSMs or MPC. But all of the current solutions have a range of limitations. With Ethereum's upgrade to ETH 2.0 and adopting the new Boneh-Lynn-Shacham (BLS) signature scheme, we now have a new interesting way to solve for this at the protocol layer in an extremely efficient manner through native cryptographic support for multisig. This is especially important as blockchains look to scale out and speed up.

We take a look at the evolving landscape of signature schemes and how that affects custody solutions in the market today when it comes to scalability (transaction size, complexity), centralization (n-of-m) and security (loss of private keys).

The Elliptic Curve Digital Signature Algorithm, ECDSA

ECDSA is everywhere, it is used multiple times a day, and has been vetted in the real world for decades. Although it is used by blockchains to verify identity, or to sign messages, it is also widely used beyond those applications. For instance, every time you use Google's search engines, or your browser verifies the security certificate of some website you visited, an elliptic curve algorithm is most probably being used.

One of the key reasons it is so commonly used is because it is efficient from an implementation point of view, where the public keys are a fraction of the size they were with previous RSA

technology. Another reason is that it has been around for a long time and is well tried and tested in real world applications. It is also been subject to abuse, if not properly implemented. One of the challenges is that it is necessary to put a random number into each signature and transmission and must never use the same random number twice or you risk exposure of the private keys placing your data at risk. This is where it becomes problematic, as implementers do not often understand the need for nonce (number used only once) or as it is otherwise known as the 'k value' to be used only once with that private key. This mistake was made by Sony in its Playstation III (PS3) where people were able to create their own software to run on the PS3, leading to millions of dollars of expense and lawsuits to remedy the security issue.

A second challenge is that you cannot combine signatures or keys and every signature has to be verified independently. With multisig transactions, this becomes especially taxing.

From a digital asset custodian's perspective, it is attractive because its use is so prevalent that any HSM purchased or hardware wallet is likely to provide support for ECDSA. The key challenge lies less in algorithm support but rather in terms of support for the specific curve that Bitcoin, Ethereum and numerous other Blockchains use. From a multi-party computation (MPC) perspective which has been in existence since the 1980s, there are algorithms out there to allow for MPC to be used to generate ECDSA-based signatures but this area of research and usage is much more recent driven by the increased popularity of Blockchain technology and digital assets over the last couple of years. Hence, from this perspective, it is less tried and tested and much more complex in terms of the cryptographic algorithms driving it.

Evolving Blockchains – ETH 2.0 and the Boneh-Lynn-Shacham (BLS) Signature Scheme

The Ethereum 2.0 upgrade, which is expected later in 2020, will revamp

Ethereum's design and make the consensus switch to proof of stake (PoS), which is anticipated to be a genuine game-changer for the Ethereum ecosystem. The upgrade will allow investors to earn passive income via staking while securing the Ethereum network. More importantly, it will introduce the new BLS signature scheme which will make it cheaper and safer to use.

The BLS signature scheme has been around since 2004 – yet another example of a widely used solution that is gaining adoption. Relying on pairing-friendly curves, its main improvement over ECDSA is that it supports signature aggregation, enabling secure multi-signature capabilities with a much lower memory requirement. That is, given a collection of signatures, anyone can produce a short signature that authenticates the entire collection. BLS is simple, efficient, deterministic and can be used in a variety of network protocols and systems to compress signatures or certificate chains. In essence, one could argue, through the use of signature aggregation, it is a form of MPC.

Use of BLS also enables efficient scaling as it requires far less data to be stored. Say there are 1,000 transactions in a block. Historically, it would have required one signature per transaction meaning a significant amount of storage space. With BLS, it now only requires one signature, but it will require one pairing for each transaction plus one per block to verify the validity of the block, i.e. less storage, but still a lot of computing power to verify.

Another major security advantage of BLS over ECDSA is that there is no randomness of numbers required as is the case with ECDSA. However, the BLS signature aggregation is insecure by itself due to the potential for a "rogue public-key attack". This is one downside of the signature scheme that can be defended against. The simple explanation to the rogue public-key attack is that the aggregation algorithm is actually an "addition" operation on the group field, and its reverse "subtraction" operation on the group field is easily available and trivial. The first, but not the only, defense against a rogue public-key attack is knowledge

of the secret key (KOSK) which requires one to check and make sure the owner of the public key has a matching secret key. This can be done by asking the owner to sign a simple message proving ownership of the provided public key. This proof need only be done once, if the public key is being reused, and everyone can then trust that the public key provided for each signature is owned by the party providing it.

A second downside to BLS is that it is significantly more expensive to calculate the verification of a signature and slower due to calculation requirements of the key pairing function. Hence, the building blocks of BLS are more expensive in terms of computing power, but cheaper in terms of storage in a block. But, as ETH is dropping PoW, the overall computing requirements will be lowered even though the BLS scheme is somewhat more expensive than ECDSA.

Making Private Keys Bullet-Proof - Encryption Schemes and Custody

BLS is already being used by Blockchains other than ETH 2.0, but it is unlikely to completely replace ECDSA as not every chain will likely adopt it. There is no need to, as each Blockchain leverages different signature schemes and signing methodologies depending on its purposes. For instance, Bitcoin is looking to soon implement Schnorr signatures as well as ECDSA.

Most current custodial solutions are best suited for ECDSA solutions, whether using MPC, hardware security modules (HSMs) or cold storage solutions. Before the popularity of Blockchain and digital assets, hardware solutions such as HSMs lacked support in providing implementation of signature schemes and curves like BLS to their hardware or secure software but this is beginning to change with increased institutional demand and adoption of digital assets. The only difference being that cold storage is now viewed as expensive, slow and non-scalable as it's offline — requiring users to load transactions to be signed by HSMs over a physical device such as a USB stick.

MPC is much more than just distributed ECDSA – yet most doing ETH / BTC

custody are very likely using distributed ECDSA. The application of MPC to ECDSA has only been developing over the last few years, and today it can be complex to safely implement coupled with vulnerabilities in the protocols that may exist and have yet to be discovered. Simplification of the implementation protocol put into practice by the end user can help to eliminate the risks of user error. Even if the math is sound, when put into practice additional risk vectors are often created, risks that newer untested implementations like MPC have perhaps not been hardened against.

Trustology is one of a handful of service providers using HSMs. But the devil is in the details. By re-signing transactions with our proprietary firmware running inside HSMs, we mitigate an important attack vector. Whilst the HSM may keep the wallet key safe, and even if other providers also use some form of end user hardware to authenticate transactions, hackers can still compromise the transaction if policy validation and re-signing is performed in software. It is this unique re-signing technology that enables us to easily adapt to signature schemes like BLS but also to different Blockchains and protocols.

Typically, keys are also stored by some digital asset custodians inside HSMs. This limits the number of keys to tens of thousands. It also means it is hard to quickly replace an HSM in case of failure or add a new HSM to scale out capacity. We have developed a fully stateless architecture on the other hand. Our wallet keys are only ever created and used by our firmware inside HSMs, but when not in use, they are encrypted, stored and backed up in the cloud. This means that our HSMs are in effect stateless, just like all of our cloud services. This allows us to operate a reliably fast and resilient service, capable of supporting a near infinite number of keys, with clusters of cloud and HSM resources spread across multiple regions, ready fpr seamless failover and scale out.

The Future is Quantum

Unfortunately, none of these encryp-

-tion algorithms are quantum computer resistant. As quantum computers become more powerful, all these encryption schemes will be broken. New post-quantum algorithms are already being tested, though, which one will become dominant is not yet clear. It is uncertain as to when this will become a real issue, but when the time comes,

we can quickly move to post-quantum algorithms. The world of cryptography is always moving, and the algorithms used are constantly changing as the technology evolves. For now, tried and trusted technologies with solid multi-party processes (multiple custodians) give the best of both worlds in terms of security and risk.

Mark Hornsby

CHIEF TECHNOLOGY OFFICER | TRUSTOLOGY

Mark is a dedicated technologist with extensive industry experience in top tier investment banks having worked at RBS, UBS, and Deutsche Bank.

For more information or inquiries contact Trustology at: **contact@trustology.io**

.

2. Management Summary

The field of digital asset custody is still in its infancy. Neither agreed terminology nor common pricing strategies are in place yet. The cacophony of different approaches as well as lacking definitions make it extremely hard to produce meaningful comparable data sets.

While we are seeing the industry grow on a broad scale, there is still a high degree of uncertainty – especially when it comes to regulation. Therefore, the EU-wide regulatory approach ("Markets in Crypto Assets (MiCA)") is a step into the right direction. In light of the upcoming regulation on Security-Token in Germany (eWPG) it remains to be seen if Start-Ups will be able to get a "piece of the cake", or if established entities will be the ones benefitting from the already established functions and procedures.

Apart from the ongoing regulatory challenges, nearly every custodian is also improving its core product. For example, more and more custodians offer staking and baking services, and the amount of supported chains is rising. This can also be seen when looking at insurance: Not too long ago, few custodians were able to offer insurance. This has significantly improved and nowadays insurance for the assets held in custody is available at almost every custodian.

It can be concluded that the space of digital asset custody will undergo significant changes in the future and adoption will rise due to more regulatory certainty. We believe to see some consolidation in the future and are very much looking forward to be part of this journey.

#changeisgonnecome #digitalassets #bitcoin

3. General Information

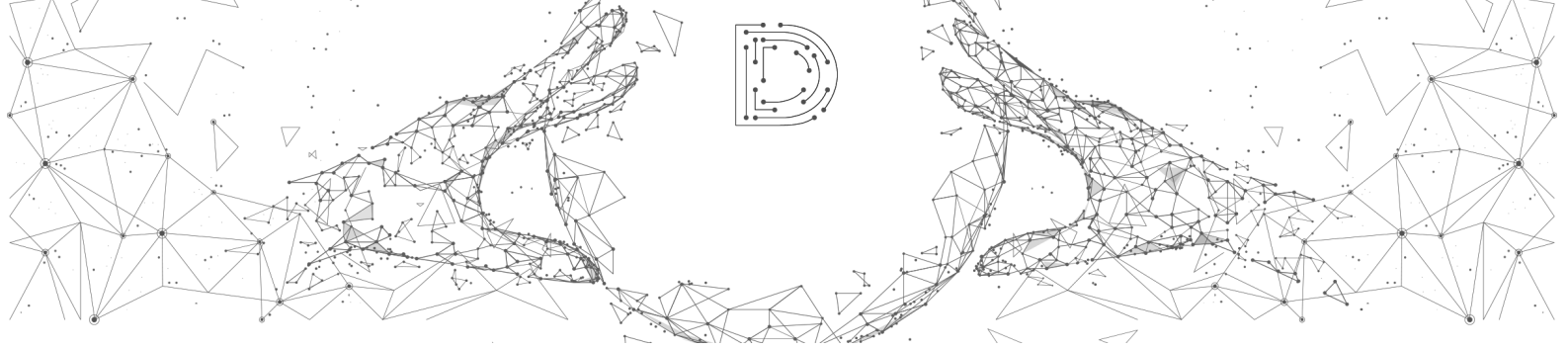
2.1 Aim of the Survey

As the field of digital asset custody is relatively new and less mature compared to other segments of the digital asset space, information on specialized custody providers and technical solutions offered is scarce. In combination with the high speed of (technical) development, clients looking for a professional digital asset custodian are not only faced with the difficulty of getting a good overview of the space in the first place, but find themselves confronted with the challenge of keeping up with constant change, which is complicated further due to terminology issues. At the same time, digital assets are becoming increasingly attractive for retail and institutional investors, which leads to a higher demand for professional service providers in the field of digital asset custody.

Taking into account the forementioned, Digital Assets Custody is conducting a semi-annual study, trying to reflect the current status of the ecosystem as well as reflecting on possible future developments.

2.2 Methodology and Participants

The survey included 33 questions (tick-box and free-text) and was conducted from the 17th of June until the 3rd of July, 2020. A total of 136 entities were invited to participate, of which 37 (27.21%) from 12 different countries submitted their replies – an increase of over 60% in participant numbers compared to the first survey conducted at the end of 2019.



The questions touched the following six areas:

- general information,
- tokens, private keys and transactions,
- fee structure,
- performance and available services,
- safety, and
- regulation.

After all responses were submitted, the data underwent a first "consistence" check and participants were contacted for clarification if "strange" appearing data was identified. After that, the data was evaluated and compared to the 2019 results.

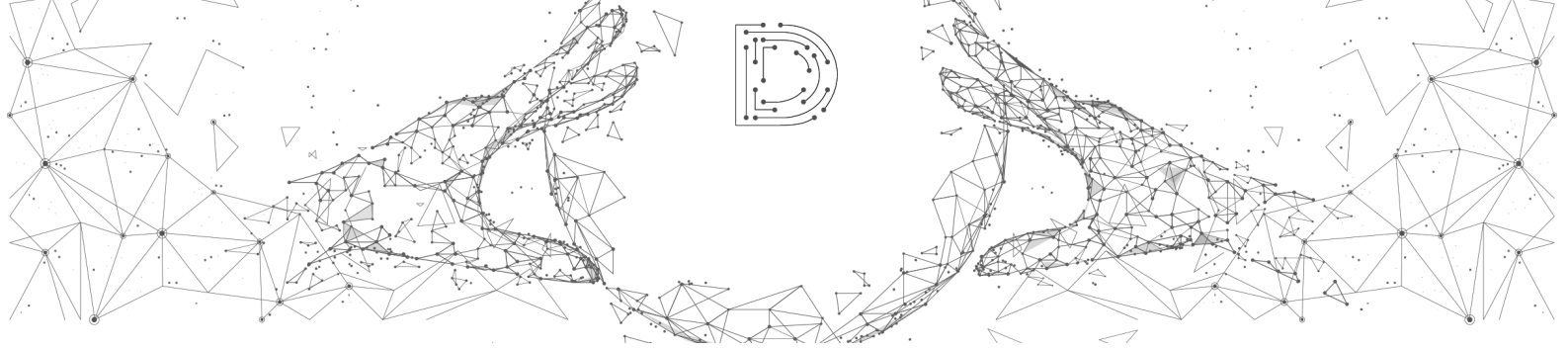
Participants of the 2nd Digital Assets Custody Survey

All participants of the survey had to indicate a categorization for their entity type. Participants could select from the following options:

- Custodian (centralized),
- Custodian (decentralized),
- Tech provider without license,
- Producer of technical devices, and
- Other.

How Does the Participant Compilation Look in Detail?

Over 40% of the participants of the 2nd Digital Assets Custody Survey indicated being either a centralized or decentralized *Custodian* for digital assets. At the same time, around 27% of the participants categorized themselves as *Tech Providers without a license*. Over 10% of the participants stated to be *Producer of technical devices*, roughly 22% answered "*Other*". Most participants of this category were either



traditional banks, service providers with a specialized digital asset custody department or tech platforms, who do not specifically produce a “device”, rather than a service.

4. Survey Results

3.1 General Information on Digital Asset Custodians

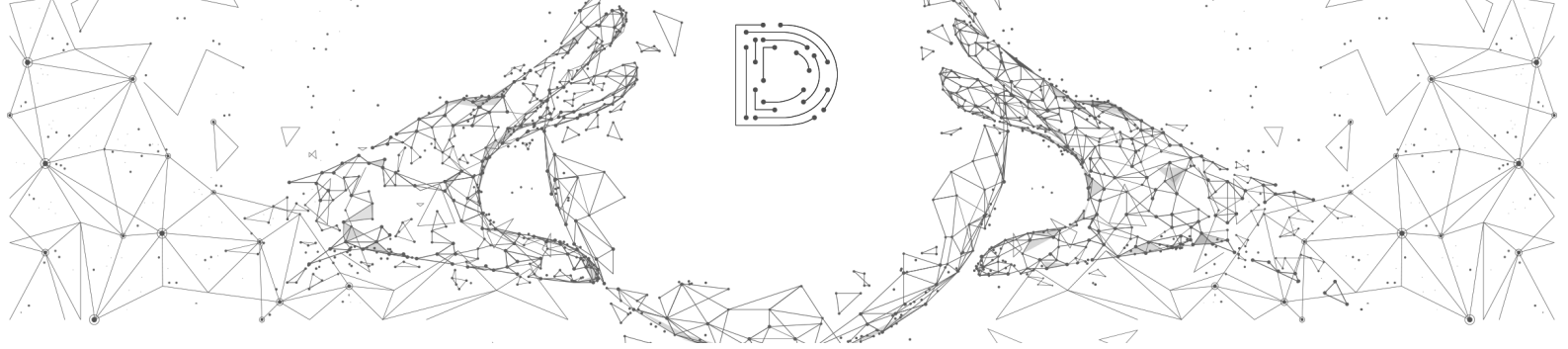
One might ask what the value added might be when it comes to taking a closer look at the "nitty-gritty" general information. We believe that general information can indeed deliver insights going beyond a mere account of quantitative data when this data is contextualized. For example, the location of headquarters might be an indicator for jurisdictions with a "fertile soil" for digital asset custodians, and the location of customers addressed indicates where digital asset adoption might be growing. Lastly, the manner in which target groups are constituted indicates which customer groups have currently the highest demands for digital assets custody.

This segment will include the following sub-topics:

- founding date,
- headquarter location,
- customer location, and
- target groups.

Founding Date

All survey participants were asked to indicate the founding date of their entity. 8.11% of the participants were founded before 2000. 2.7% indicated the time period 2001 to 2010, and the same percentage the year 2020 as their founding date. The number for the years before 2000 – which might sound strange due to "invention" of Bitcoin in 2009 – can be explained when taking a closer look at the participant compilation. All participants that indicated a founding date pre-2000 have a background in traditional banking and financial services, i.e. they were financial service providers before the upcoming of digital assets and later added digital asset custody to their service portfolio.



Most organizations that took part in the Second Digital Assets Custody Survey were founded after the year 2010, i.e. 89.19% of participants, with the majority (38%) in 2018.

Compared to the findings of our first survey, which was conducted at the end of the year 2019, the biggest change can be seen in the responses for the years 2011 to 2015 (2019: 21.74%, 2020: 13.51%), 2017 (2019: 17.39%, 2020: 21.62%) and 2018 (2019: 47.83%, 2020: 37.84%). Whereas, the change for the time period 2011 to 2015 is only a relative change not an absolute one, i.e. the number of responses for the category remained the same but the number of overall responses was higher than in the year 2019. When comparing the absolute values, one can see that the number of responses for the years 2017 (2019: 17.39%, 2020: 21.62%) and 2019 (2019: 8.70%, 2020: 10,81%) doubled.

A significant problem arose with the self-classification of the participants – as regulatory uncertainty looms, we have the feeling some of the participants we would have ranked in the "custodian" section did indeed indicate to be tech-providers, even when specifically asked about this issue. This also makes the data-evaluation difficult.

Headquarter Location

Participants were also asked to indicate the location of their headquarter. In the 2020 study, the most popular locations were Switzerland (29.73%), Germany (21.62%), the United States of America (13.51%), the United Kingdom (8.11%), Hongkong and Singapore (both 5.41%). In addition, Canada, Israel, Liechtenstein, Spain, France and Austria were also named as headquarter locations.

When comparing the responses for the most popular headquarter locations from the years 2019 and 2020, one can note that the relative value for Switzerland decreased from 39.13% to 29.73%. At the same time, the absolute value rose from nine to 11 responses. The relative value for Germany has risen from 17.39% to 21.62% while the

number of responses doubled. The relative and absolute values for the United States of America have also increased, from 8.7% to 13.51% respectively from two to five responses. The relative value for the United Kingdom decreased compared to the year 2019 from 13.04% to 8.11%, but the absolute value has remained constant. All other headquarter locations remain at under 10%.

Customer Location

The survey-participants were also asked about the location of their customers. The participants could choose from the following categories:

- the European Union,
- other European countries (non-EU members),
- the Middle East,
- Russia,
- East Asia (Japan, China, Korea, Taiwan, Hongkong, Macau),
- South and Southeast Asia (ASEAN),
- United States of America,
- Canada,
- Central and South America,
- Oceania (including Australia), and
- Africa (i.e. African Union).

An overall majority of participants in the 2020 survey indicated servicing customers from the *European Union* (94.59%). In addition, over half of the participants are also servicing customers from o*ther European countries* that are non-EU member states (67.57%). Interesting to note: Both companies that did reply not to offer any services to Europeans in 2020 did so in 2019, which might be a reaction to the regulatory changes.

Over half of the participants indicated servicing clients from the *Middle East* and *East Asia* (both: 56.76%), *Southeast Asia* and *Canada* (54.05%), and *Oceania* (51.35%). 45.95% of participants responded to service customers in the *United States of America* as well as *South and Central America*. Furthermore, *Russia* is serviced by 43.24% of all participants. The customer location that is less covered so far by custody providers is *Africa* with 40.54% of responses.

Although the degree of coverage varies between geographical locations, digital asset custody and tech providers in this space are present worldwide.

Target Groups

Survey participants were asked to indicate which target groups they serve.

The following categories were given to select of:

- (U)HNWIs,
- Asset managers,
- Exchanges,
- Traditional banks,
- Retail, and
- Others.

Taking a closer look at the responses, one can notice that the biggest target groups for digital asset custody services in the first half of 2020 are *Asset managers* with approximately 86.5% of all participants indicating this target group. This category is followed by *Exchanges* and *Traditional banks* (both with approximately 81%) as second most important target groups in 2020. About 50% of participants also stated to count *(U)HNWIs* to be part of their target group. The answers *Retail* (35.14%) and *Others* (37.84%) were only given by around 35 to 40% of the participants.

In 2019, a vast majority of participants indicated to service *Exchanges* as target group (91,3%). While *Traditional banks* (86.96%) and *Asset managers* (82.61%) followed closely as one of the most important target groups. *(U)HNWIs* were indicated as a target group by 65.22% of responses. *Retail* was given as a response in 43.48% of the answers. For the survey in the year 2019, the option *Other* as well as the number of undisclosed responses had a relative value of 0.

For both years, one can summarize that *Asset managers* (2019: 82.61%, 2020: 86.49%), *Exchanges* (2019: 91.30%, 2020: 81.08%), and *Traditional banks* (2019: 86.96%, 2020: 81.08%) continue to be the biggest target groups for digital asset custodians and custody service providers. Retail customers remain the smallest target group, measured by its response numbers. The relative number of participants stating to service (U)HNWIs has fallen since 2019 (2019: 65.22%, 2020: 51.35%). Still, (U)HNWIs are serviced by approximately 50% of the participants.

When comparing the responses for 2019 and 2020, one can notice that there is a small shift away from *Exchanges* as the main target group towards *Asset managers*. Whereby, the increase in responses indicating *Asset managers* as a target group is quite small with about four percentage points. At the same time, the decrease in the relative value for *Exchanges* is at around 10 percentage points. *Traditional banks* as a target group only had a small decrease in their relative value of about five to six percentage points. Furthermore, (U)HNWIs show a change of about 14 percentage points. While the relative value decreased compared to the responses of the year 2020, the absolute value increased by four responses. For retail customers, the value has decreased around eight percentage points compared to 2019. At the same time, the absolute value increased by three responses. The values for undisclosed responses are zero for 2019 and 2.7% for 2020.

3.2 Transaction Volume and Supported Token

This segment will include a summary of the responses regarding the following sub-topics:

- supported tokens,
- amount of assets under custody, and
- number of keys being managed.

Supported Token

Custody service providers were asked what type of tokens they support. Aiming for a comparison between the years 2019 and 2020, as well as beginning to build the foundation for mid-term time series analysis, a wide range of commercially available token were included as response possibilities.

For the year 2020, one can say that Ether and Bitcoin were supported by almost all survey participants with the former achieving a relative value of 97.3% and the latter of 94.59%. Bitcoin and Ether are both the most-known token and have the highest adoption rate. Thus, it is no wonder that they are supported by an overwhelming majority of custody providers.

Amount of Assets Under Custody

In the scope of the survey, participants were asked how many assets they hold under custody as of the 1st of January 2020 compared to one year earlier. The participants could indicate whether the amount had increased, decreased or remained at the same level. In addition, participants were asked for the absolute number of assets under their custody at the 1st of January 2020.

Over half of the participants indicated that the amount of assets under their custody had increased throughout the year (51.35%). No participant indicated a decrease in or constant number of assets. This could be interpreted as a sign for a positive trend

in regard to digital asset usage and custody demand. Still, due to the very high number of participants not wishing to disclose any information when asked about how the amount of assets has changed in the last year (48.65%), the data evaluation has to be interpretated carefully. Also, it has to be taken into account that providers of technical infrastructure cannot answer this question, as they most likely have no knowledge about the amounts stored, as they simply deliver the infrastructure. When just looking at the companies who stated to be a custodian or "other", 15 of the 23 reported an increased volume (65,22%).

Number of Keys Being Managed

Participants were asked to estimate how many keys they manage as part of their custody services. They could select from the following categories:

- 0 to 500,
- 501 to 2,500,
- 2,501 to 10,000,
- 10,001 to 50,000,
- 50,001 to 200,000, and
- Prefer not to say.

Sadly, as the value for *Prefer not to say* answers was very high with 27 answers, i.e. 70.27%, no reliable findings could be abstracted.

3.3 Fee Structure

In the fee structure segment, we were aiming to gain some "global" insights in the fee structure of custodians, which proved to be astonishingly difficult as the spectrum of answers was extremely diverse.

One-Time Setup Fee

When asked about a one-time setup fee, about 40% of the participants indicated having such a fee in place (40.54%). Around 30% did not ask for a one-time setup (29.73%). Furthermore, 8.11% indicated that their fee concept for one-time setup fees either depends on the client, token type or pricing model. 21.62% of participants did not disclose any information, i.e. indicated *Prefer not to say*.

Deposit Holding Fee

A deposit holding fee was indicated by almost 50% of the participants (48.65%). About 30% did not have such a fee in place (29.73%). The number of responses for both *Other* and *Not applicable* was 0%. Hence, the relative value of undisclosed answers, as in the case of one-time setup fees, was 21.62%.

Transaction Fee

A transaction fee is charged only by a fifth of the providers participating in the survey (24.32%) and 5.41% specified that the transaction fee is dependent of either clients, token or the pricing model. Whereas, around half of the participants indicated to not have a transaction fee in place (48.65%).There were no *Not applicable* answers as we would have suggested for the pure tech-providers for example, but 21.62% indicated *Prefer not to say* when asked about transaction fees. This is the same amount of responses as in the case of one-time setup and deposit holding fees.

3.4 Performance and Available Services

In this section, a summary of the responses regarding performance and available services will be presented.

When taking a detailed look at performance aspects, the transaction speed is essential – as digital assets usually have a high degree of volatility, time can be of essence. This aspect is especially of importance for clients that have to conduct a high number

of transactions on a regular basis and/or base their business on trading digital assets. Therefore, participants were asked to indicate their transaction speed for Bitcoin and Ether transactions.

In addition, to include a representative depiction of the services digital asset custodians offer, the participants were asked to state whether they offer crypto lending, staking (baking) and trading services. In case of a wide service offering, one could deduce that digital asset custodians are expanding their service portfolio to increase their unique selling point and further differentiate themselves from other providers in the space or that clients are demanding more holistic service offerings.

This segment will include the responses for the sub-topics:

- transaction speed for Bitcoin and Ethereum,
- all available services,
- crypto lending service availability,
- staking (baking) service availability, and
- trading service availability.

Transaction Speed of Bitcoin and Ethereum

All participants were asked how fast a standard transaction, i.e. withdrawal, for Bitcoin (BTC) and Ether (ETH) takes in seconds. The questions were further specified by differentiating between hot and cold wallet transactions.

Comparing average indications on transaction speed, Bitcoin hot wallets are faster than Ethereum hot wallets with the former taking on average three minutes 36 seconds and the later three minutes 48 seconds. Both have a similar average transaction speed and only differ in seconds.

When it comes to cold wallets, Bitcoin cold wallets are slower with 34 minutes and 42 seconds for a transaction than cold wallets for Ethereum with an average of 27 minutes 36 seconds. Again, both have very similar average transaction speeds.

One has to keep in mind that these values represent average transaction times. The indications varied from transactions being conducted almost immediately (0.1 seconds) to taking up to one hour for hot wallets and up to four hours in the case of cold wallets.

Moreover, the reliability of findings is not only limited due to variance in responses but further because of the high number of answers that could not be evaluated, i.e. empty answers, which are between 51% and 57%.

All Available Services

To provide a better overview of the different services entities in the digital asset custody ecosystem offer, participants were asked whether the following were part of their service portfolio:

- staking (baking) services,
- crypto lending services, and
- trading services.

When comparing all services to each other, one can note that the service mostly offered is digital asset trading with over half of participants (54.05%) providing such a service. It comes to no surprise that not all custodians answered these answers with a “yes”, as pure “tech providers” saw themselves as technology-providers, enabling their clients to offer trading services, but not offering those on their own. Considering all affirmative responses for services, trading services are the most common, followed by staking (baking) services, which are provided by around a third of the participants (35.14%) and crypto lending services, offered by almost a quarter of respondents (24.32%).

It was further inquired whether the different services were going to be offered in the future. The service with the highest response rate in this category was staking (baking) services with 46.54%. After which crypto lending is planned to be introduced into the service spectrum by approximately a third of the survey's participants (35.14%). Moreover, about a fifth is planning to incorporate trading services (18.92%).

There is a clear preference for trading services, regarding the services already being offered, could be explained by the attractiveness digital asset trading can have in regard to profit margins. At the same time, when it comes to future services, trading services are only planned by 18.92% of the participants, which is a much lower value than for staking and crypto lending services.

The popularity of staking (baking) services as a future service to be offered could be explained by the upcoming Ethereum 2.0 upgrade and the opportunity PoS protocols offer in regard to profit generation. Already 35.14% are offering staking services and another 40.54% are planning on offering it in the future. This might be the first signal for a continuing positive trend. This would need to be further evaluated with a larger sample size and longer time scope.

Crypto lending services are currently offered by 24.32% of the participants. This number will most probably rise in the future as 35.14% indicated to be planning an introduction of such services in their offering.

In the following pages, we will take a more detailed look at the different service offerings.

Crypto Lending Service Availability

When asked in regard to crypto lending services, around 25% of participants indicated to have such a service in place (24.32%). 32.43% negated this. At the same time, 35.14% of participants plan to introduce crypto lending services in the future.

When subsuming the responses for *Yes* and *Planned*, 59.46% of participants are likely to offer crypto lending services in the future. Thus, over half of the participants either have or are planning on having a crypto lending service in place.

The number of undisclosed answers was quite low with 8.11%.

Staking (Baking) Service Availability

In 2020, around 35% of participants indicated that they were offering staking (baking) services to their clients (35.14%). In addition, 40.54% indicated to plan on introducing staking services. Only around 19% indicated not offering such services now or in the future. The number of *Prefer not to say* answers was low with 5.41%. There were no *Not applicable* or empty answers given.

Drawing a comparison to 2019, one can see that the number of entities offering staking (baking) services has risen from 21.74% to 35.14%. The absolute value is almost three-times higher in 2020, while the relative value has increased by approximately 13 percentage points. The number of participants that indicated planning to introduce staking more than doubled in absolute numbers and is about 10 percentage points higher in regard to their relative numbers (2019: 30.43%, 2020: 40.54%).

In 2019, 17.39% of participants indicated to currently not offering staking services. This value increased in 2020 to 18.92%.

The values for answers not disclosing any information is higher for 2019 with 30.43% compared to 5.41% in 2020. Whereas, the high number of undisclosed answers results mainly from a high number of empty answers (26.09% in 2019). The number for *Prefer not to say* answers remained quite low and at the same level for 2019 and 2020. Thus, data validity for the year 2019 is not as high and the evaluation has to be interpreted carefully when abstracting general findings.

The increase in the number of participants either already offering staking (baking) services or planning on doing so in the future could be partly explained by the soon-coming Ethereum upgrade, which makes staking possible, and the high number of blockchain applications implemented on the Ethereum protocol.

Trading Service Availability

As stated previously, trading services enjoy a high degree of popularity - over half of the participants indicated to offer trading services in the year 2020 (54.05%). Additionally, almost 20% plan to introduce trading services in the future (18.92%).

On the one hand, 72.97% of participants indicated either already having a trading service in place or planning to do so in the future. On the other, 21.62% of participants do not offer any trading services at all.

The number of *Prefer not to say* answers was at a low 5.41%, i.e. two responses. There were no *Not applicable* or empty answers given. Thus, the value of undisclosed answers that could not be evaluated was low and data validity can be assumed.

Besides inquiring on the availability of trading services, participants were asked to provide further information on the trading services offered. When asked what transactions are offered, the following answer possibilities to select from were given:

- on-chain,
- off-chain,
- cross-chain, and
- other.

All participants that indicated not having a transaction service in place, planning on doing so in the future or not disclosing information, independently of whether they indicated a response in this category or not, were disregarded in the data evaluation

for reasons of consistency. Therefore, the sample size for this question was reduced to 20 participants instead of 37.

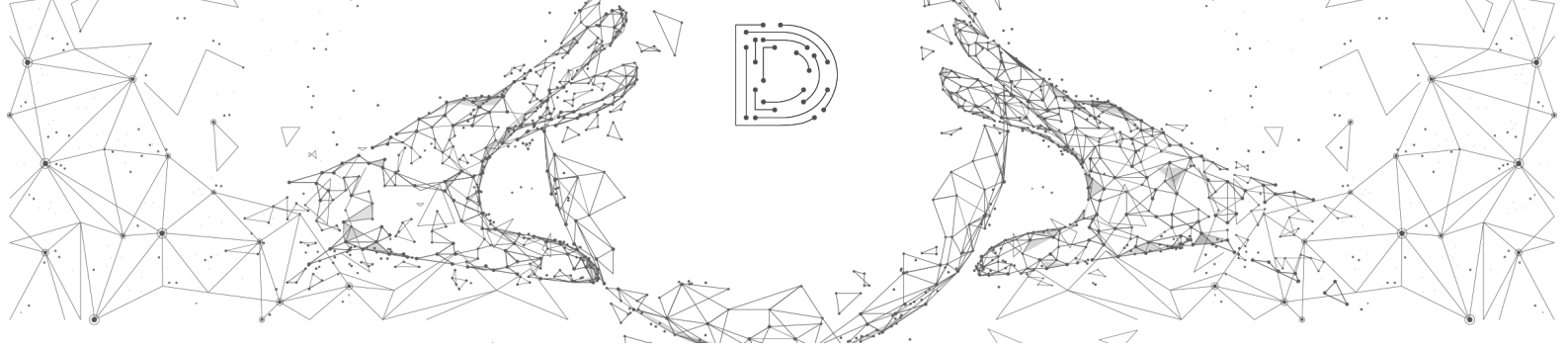
Of the 54.05% of participants currently offering a trading service, most opted for on-chain trading (70%). Comparing the different types of trading services offered, while on-chain transactions are the most popular ones off-chain and cross-chain transactions are offered by 30% of the participants. Moreover, 15% indicated to offer other forms of transactions, for example depending on the client's necessities.

While the findings give a peek into the different transaction setups available in the digital asset custody space, 20% of the participants did not disclose any information – additionally to the 49.95% of participants that do not currently offer any trading services. This is quite a high value, which makes quality data reliability and validity difficult in this case.

3.5 Safety

This section addresses aspects dealing primarily with questions on safety. Whereas, safety is understood not only as security and safety in a technical sense, i.e. ensuring that the system cannot be exploited and/or manipulated. Aspects that de facto increase individual security for custody clients, such as insurance coverage for assets, as well as aspects regarding regulatory safety, i.e. compliance like KYC and AML check procedures, were also incorporated into the questionnaire.

The deeper and more encompassing regulation becomes, the more compliance-related aspects and tasks arise. For this reason, services offering regulatory compliance but also utilizing on-chain analytic tools to avoid getting "tainted" tokens remain in high demand. All these, as well as insurance coverage and a suitable protocol in place in case a hack occurs assist with risk reduction in the area of digital asset custody.



This section presents information in regard to the following sub-topics:

- KYC and AML procedures,
- on-chain analytic tools,
- insurance of assets under custody, and
- experience with security hack attempts.

KYC and AML Processes

In regard to KYC and AML procedures, participants were asked if such procedures were in place, and in case they were, if they are conducted internally or by a 3rd party. Over 86% of participants indicated having KYC and AML procedures in place. In addition, 5% are planning on introducing this type of procedures. Thus, 91.59% of responses indicated either already having such procedures in place or planning on doing so. Only 2 entities did not have and are not planning on offering any KYC and AML procedures. As these entities act as "pure" tech-providers, the answers do not seem to be a concern, though.

The number of affirmative responses has risen compared to the year 2019; the relative value of those with KYC and AML procedures in place increased from 82.61% in 2019 to 86.49% in 2020. At the same time, the number of participants planning to introduce KYC and AML procedures has decreased in relative numbers (2019: 8.7%, 2020: 5.41%), while the absolute numbers remained the same. Further, the number of participants that indicated to not have KYC and AML procedures in place decreased by approximately three percentage points, as it was 8.7% in 2019 and 5.41% in 2020. The approximately 3%-points decrease is observable alongside no change in absolute numbers.

The relative value of undisclosed answers is very low for all data evaluations as it is beneath 6%.

When it comes to the question of who is conducting KYC and AML procedures, over half of the participants indicated combining an approach in which KYC and AML are conducted internally and with the help of 3rd parties (53.13%). At the same time, a quarter of participants indicated relying on internal processes for KYC and AML checks only. Those completely outsourcing KYC and AML procedures to 3rd parties, just made up to 18.75% of all participants – which seems still a fairly high number, given the fact KYC and AML procedures are one of the core aspects of custodianship.

Compared to the year 2019 responses, just a third indicated to let KYC and AML procedures be conducted internally and by 3rd parties (31.58%). This represents an increase from 2019 to 2020 of approximately 20 percentage points. At the same time, the absolute values tripled. Additionally, most custody providers indicated to rely on internal KYC and AML procedures in 2019 (52.63%). The number of these more than halved until 2020 to 25%, although the absolute numbers only decreased by two indications. A mere 10.53% opted to only employ 3rd parties in 2019. Thus, the number of participants that employed 3rd parties for KYC and AML procedures increased by around eight percentage points until the year 2020. The absolute number of responses tripled in the same time. Preferences seem to have changed.

All participants, that indicated not having KYC and AML procedures in place, planning to do so in the future or did not disclose any information in this regard, were excluded from the samples for 2019 and 2020. Therefore, the sample size was 19 for the year 2019 from 23 and 33 for the year 2020 from 37 participants.

On-Chain Analytic Tools

On-chain analytic tools are becoming a more and more common tool for investors, asset managers, funds, banks, exchanges, analysts, etc. They allow the analysis of metrics from Blockchain networks and assist in tailoring wealth management strategies, while at the same time help decrease systematic risks.

These types of tools are especially interesting for digital asset custody providers as they can be employed to screen token and other digital assets in regard to their provenance and help receive other on-chain information.

In the scope of the survey, participants were asked whether they employ on-chain analytics tools to prevent getting “dirty” coins from mixers or scams.

On-chain analytic tools are used to prevent receiving “tainted“ tokens from mixers or scams by 70.27% of all study participants. Only 13.51% of the participants did not choose to employ these.

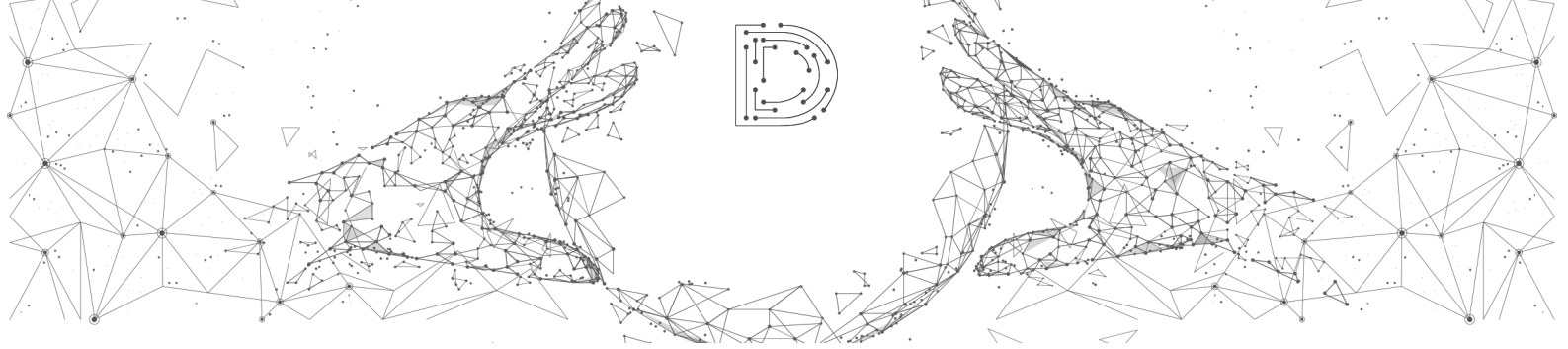
One has to note that from the 37 participants 16.22% chose to not disclose any information regarding their usage of on-chain analytic tools. Due to the high number of undisclosed responses, findings have to be taken into account with care and further surveys would be necessary for more reliable general findings.

One can clearly note that a majority of custodians choose to rely among others on on-chain analytic tools to avoid receiving illegitimate token.

Insurance of Assets Under Custody

In the scope of this survey, a special effort was made to include information on the insurance coverage of digital assets in custody. For this reason, we did not only ask participants to indicate whether they have any insurance coverage, but furthermore inquired on the size of their insurance cap and the amount of assets covered by the insurance.

We believe that the question of insurance has become an increasingly important matter in the space, especially for clients with a high number of digital assets in custody. In case of a security breach or any other issue leading to a token loss, custody customers are not as exposed when an insurance coverage is in place.



In regard to insurance coverage in 2020, one can summarize that a majority of custody providers and other entities in the space offering custody services have some form of insurance coverage in place. 70.27% of participants indicated to have some form of insurance setup. Only 5.41% of participants indicated to not have an insurance in place. Whereas, 13.51% stated that insurance coverage is planned but not available yet. Moreover, 10.81% did not want to disclose any information in 2020.

Compared to our findings in 2019, the relative number of custodians with insurance has risen by approximately 14 percentage points (2019: 56.52%, 2020: 70.27%). At the same time, the absolute numbers doubled in the same time period. This could be expected as 30.44% of participants in the 1st Digital Assets Custody Survey indicated to introduce insurance coverage in the future, while this number decreased to 13.51% in 2020. The absolute number of participants planning to introduce insurance did only decrease by 2 responses from 2019 to 2020. This decrease of around 16.5 percentage points could be explained by the high number of custody providers with insurance and especially those that have just introduced insurance coverage this year. The lower number of entities planning to introduce insurance coverage does not translate in non-insurance as still 70.27% indicated having insurance coverage. Instead it can be seen as a sign for a trend to add insurance coverage when offering digital assets custody. The relative value of those without any insurance has had a small decrease while the absolute number has remained the same for both years (2019: 8.7%, 2020: 5.41%).

It is important to note that about 4.35% of the 2019 and 10.81% of the 2020 participants did not want to disclose any information in regard to their insurance coverage.

The **insurance cap** and **insured amount** are both indicators to further explore the extent to which insurance coverage has been implemented. In addition, data on both can contribute valuable insights on whether insurance coverage is a differentiating characteristic between the different entities in the digital asset custody space.

When it comes to the insurance cap and the amount of assets under insurance, sadly, there is not enough qualitative data to abstract reliable findings. Due to a high number of entities not wanting to disclose information on their insurance cap, 73.08%, or the amount of insured assets, 80.77%, the validity of the data is too low to draw findings. Of those participants that indicated a response (70.27%), 26.92% gave further information on their insurance cap and 19.23% on the amount of assets covered by insurance. Of those that answered, 15.38% indicated that all assets are insured and 3.85% that only insure a bespoke amount of digital assets under custody.

All entities that did not indicate currently offering insurance with their custody services, i.e. either indicating no insurance, planning on introducing insurance or not disclosing any information, were not included in the data evaluation regarding insurance cap and the amount of insured assets. Thus, the sample population was reduced from 37 to 26 for both categories.

Experience With Security Hack Attempts

Participants were asked if they had any experienced attempts of internal or remote hacks in the past. This question was intended to give a better insight into the security challenges digital asset custodians are faced with.

Most participants indicated to not have experienced such an internal or remote hack so far (56.76%). Only in four cases a security hack was indicated to have occurred in the past (10.81%).

Moreover, the value of *Do not want to disclose* and empty responses is quite high with 21.62% for the former and 10.81% for the latter. The aggregated value for those not wanting to indicate a qualified response is 32.43%. This could be a result of the sensitive nature of the topic, and the potential security and reputation cost faced when this type of information becomes public knowledge.

Process in Case of an Effective Hack

When it comes to experiencing a security hack, either internal or remote, the process on how to handle it can be essential in determining the impact it will have. Thus, participants were asked to indicate the type of process with which they would react to a security hack. Participants could select between:

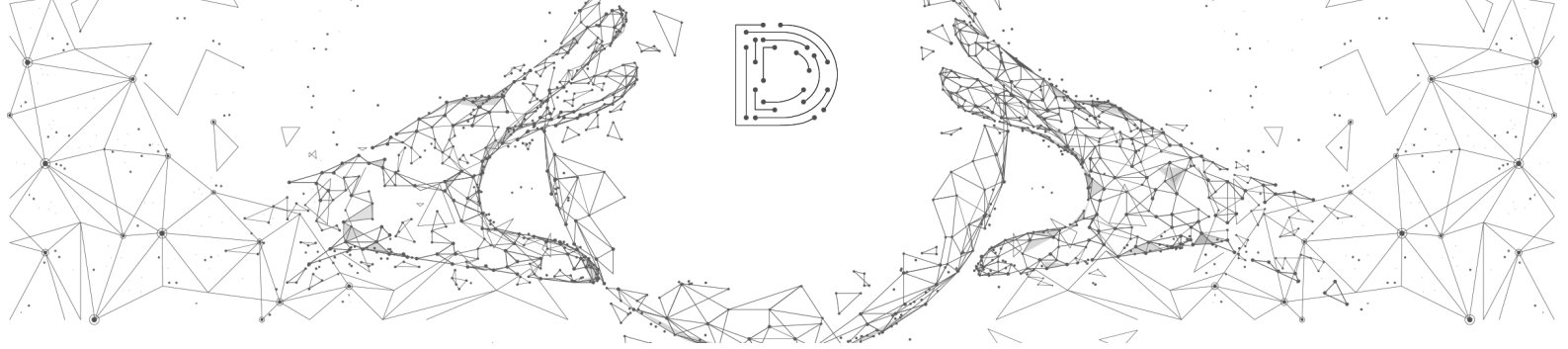
- we have a business continuity policy in place to handle everything,
- we have an emergency communication procedure in place,
- we freeze all external transactions, and
- we contact our partners and alert them.

Over half of the participants have some form of procedure in place for the case a security hack takes place (48.65%). Most of them have a business continuity policy and/or emergency communication procedure approach (43.24%). Another popular procedure is to contact partners and alert them of the security issue, with roughly one-quarter of participants indicating such a policy being in place (24.32%). Only 13.15% of participants freeze all external transactions as a reaction to a security hack.

The value for *Do not want to disclose* answers is very high with 40.54%. Additionally, the one for empty answers is quite high, too (10.81%). At the same time, 2.7% of participants indicated *Not applicable* as a response. All subsumed undisclosed answers make up to 51.35% of all answers.

3.6 Regulation

Regulation is of course a very important topic for digital asset custody providers. As the industry is still in its early days, new developments and technical advances challenge existing regulatory frameworks. Additionally, regulation continues to be very much a work-in-progress when it comes to Blockchain technology in general and



digital assets custody in specific. In the scope of this survey, a number of questions addressed regulation and regulatory insecurities of custodians in the space.

This section will thus delineate the main findings when it comes to regulatory issue areas, thus offering insights in regard to:

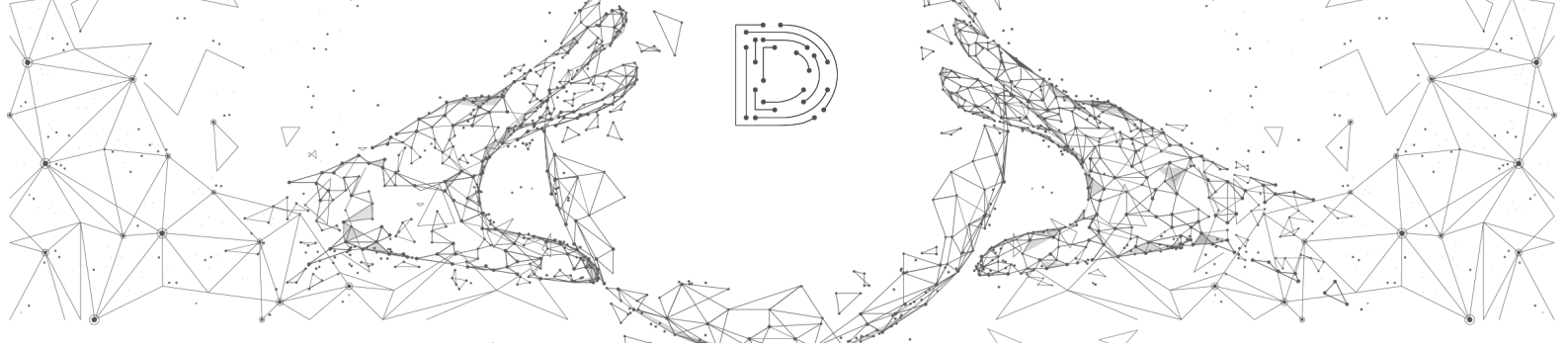
- regulation through financial authorities,
- involvement in industry groups, and
- regulatory issues.

Regulation Through Financial Authorities

An important avenue of regulation is regulation through financial authorities. Digital asset custody can be understood as part of the financial industry. As such, some jurisdictions have opted on addressing digital asset regulation by regulating custodians and other entities dealing with digital assets through existing supervisory financial authorities. Hence, there are a number of financial authorities supervising digital asset custody providers.

When asked if participants are supervised by a financial authority, i.e. regulated, almost 50% of participants indicated some form of regulation (45.95%). 43.24% indicated to not be regulated by any financial authority. The relative value of undisclosed answers was quite low in 2020 with 10.81% of responses.

Compared to the results from the 2019 survey, the relative value of those indicating to be regulated increased by approximately 15 percentage points from 30.43% to 45.95%. Hence, the absolute value more than doubled. The number of custody providers that are not regulated increased from 21.74% to 43.24%. Alongside the absolute number of responses more than tripled. The number of undisclosed answers decreased by 37 percentage points (2019: 47,83%, 2020: 10,81%). Thus, the observable change in the numbers of participants with and without regulation could be



explained by the large number of undisclosed responses in 2019, which drastically decreased in 2020.

In addition, participants, which indicated being regulated, were also asked to provide information on which financial authority supervises them. All participants that indicated to not be regulated or did not disclose any information were not included in the data evaluation. Therefore, the sample size for this category changed from 23 to 7 for 2019 and 37 to 17 for 2020.

In 2020, the most popular regulators were the German Federal Financial Supervisory Authority (BaFin) with 52.94% of participants being supervised by it, as well as the Swiss Financial Market Supervisory Authority (FINMA) and Self-Regulatory Organization (SRO) with 23.53%. Additionally, the Financial Market Authority in Liechtenstein (FINMA) supervises around 5.88% of the participants. The same number of participants indicated that their clients are regulated, and the same number of participants indicated to be unregulated spot exchanges.

The high number of entities regulated by the BaFin and Swiss FINMA could be a result of most participants being headquartered in Switzerland (almost 30%) and Germany (around 22%), as well as participants overwhelmingly servicing clients from the European Union (94.59%) and other European countries (67.57%). Furthermore, both countries have been progressing their regulatory framework for digital asset custody.

In 2019, the degree of diversification was higher, as the BaFin, Swiss FINMA and SRO, Liechtenstein's FINMA and the British Financial Conduct Authority were each indicated by 14.29% of participants. In addition, the same number of participants also indicated to be an unregulated spot exchange.

For the year 2020 there are no undisclosed answers. 2019, 14.29% of the answers were of an undisclosed nature, which only represents 1 response given.

Involvement in Industry Groups

Industry groups represent not only a forum to discuss developments and form industry-wide opinions and policy guidelines. In addition, they are also an opportunity to voice challenges and expectations towards regulatory agencies and government policies. For this reason, participants were asked if they are taking place in some type of industry body or working group.

Of all participants, 70.27% indicated to be involved in such an industry group, while 10.81% were not. The value for undisclosed responses is quite high with 18.92%. Therefore, all findings should be enjoyed with caution regarding data validity.

When inquired to specify the industry bodies participants are part of, the industry group with the highest membership number in the sample is the Crypto Valley Association (CVA) with 29.73%. Following are Global Digital Finance (GDF) and Bundesblock with 16.21%, the International Association of Trusted Blockchain Applications (INATBA) and International Token Standardization Association (ITSA), as well as the Hongkong FinTech Association and Bitcoin Association with each 10.81% and the Future of Finance and Swiss Blockchain Security with 8.11%. The Swiss Blockchain Federation (SBF) was only indicated by 5.41% of the participants. Moreover, 5.41% of responses named the Swiss Blockchain Federation (SBF). Furthermore, Berchain, the Asociación Española de Fintech e Insurtech (AEFI), Digital Chamber and the Blockchain Alliance all were indicated by 2.7% of the entities. The number of undisclosed answers amounts for 18.92% of all answers making data validity difficult.

The distribution of answers could be a reflection of where the entities are headquartered and the location of their customers.

Regulatory Issues

Participants were asked to elaborate on the biggest pain points when it comes to regulation, especially in regard to the European Union and its policies. When only

taking into account the aspects addressed by participants, the most relevant issue areas seem to be licensing and regulatory harmonization.

When it comes to licensing, passporting custody licenses and conceptualizing them based on functionality of digital assets instead of asset types were voiced.

In the area of regulatory harmonization, consistency across jurisdictions in the European Union, as well as regulatory harmonization for Security Token Offerings (STOs), a potential seal of compliance and the cohesion across jurisdictions, as well as the application and supervision of regulatory requirements were stated.

5. Appendix

5.1 Participants

AEGIS CUSTODY

BANK FRICK

VON DER HEYDT

Bitcoin Suisse

BitBox

BitGo

Bitwala

copper.co

CRYPTO STORAGE

curv

CUSTODIEX

CUSTODIGIT

Finoa

Fireblocks

GK8

Goldilock

Hex Trust

Kapilendo
Custodian AG

MAERKI BAUMANN & CO. AG
PRIVATBANK

METACO

Onchain custodian®

ONYZE


OSL
Custody


Riddle & Code


SEBA


dacs
Digital Asset Custody Services


securosys


SWISS CRYPTO VAULT
Hyper Secure Storage


SYGNUM

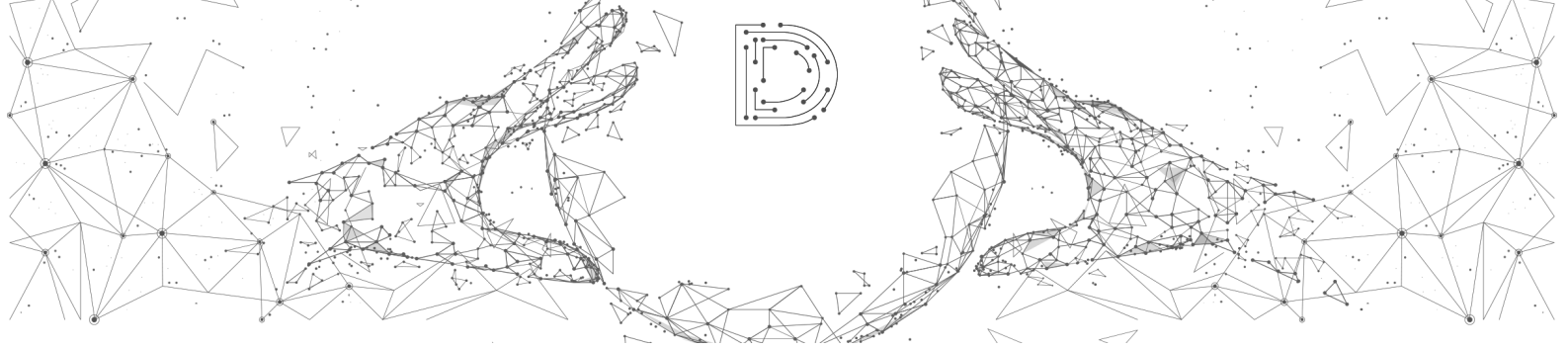

TANGANY


TAURUS


Trustology


upvest

5.2 Media partners



6. Final Note

In case you would like to take a look at the 1st Digital Assets Custody Survey's Executive Summary, get in touch with Digital Assets Custody by sending an email to inof@digital-assets-custody.com.

Digital Assets Custody (DAC) is a brand of DLC Distributed Ledger Consulting GmbH.

DAC operates the largest comparison platform for digital asset custodians on the Internet at www.digital-assets-custody.com. In addition, the company advises digital asset custodians and tech providers on regulatory issues and assists them in obtaining licenses. Furthermore, DAC supports established financial market participants within the framework of tender processes for digital asset custodians and the relevant hardware and software providers.

Get in touch:

DLC Distributed Ledger Consulting GmbH

Lange Reihe 73
20099 Hamburg, Germany

Phone: +49 40 88369187
Email: info@digital-assets-custody.com
Web: www.digital-assets-custody.com

DIGITALASSETS
CUSTODY