Safety Agenda

Challenges and opportunities for the Netherlands on the cutting edge of safety and decentralized technology

Dutch Blockchain Coalition

DBC

connect and create

Pillar 1

Security measures against abuse and fraud in crypto-assets and blockchain

Pillar 2

Trust technologies for a safe and reliable digital society

www.dutchblockchaincoalition.org

Safety Agenda Dutch Blockchain Coalition

Challenges and opportunities for the Netherlands
on the cutting edge of safety and decentralized technologies

By

Dr Mark van Staalduinen
Nina Huijberts

Date

1 February 2023

Dutch Blockchain Coalition | Wilhelmina van Pruisenweg 35 | 2595 AN Den Haag
E info@dutchblockchaincoalition.org **| I** www.dutchblockchaincoalition.org

Table of Contents

SAFETY AGENDA DUTCH BLOCKCHAIN COALITION 5

Public-private partnership for decentralized technology and safety 5

Agenda pillars and items identified by triple helix activities 6

PILLAR 1: SECURITY MEASURES AGAINST ABUSE AND FRAUD IN CRYPTO-ASSETS AND BLOCKCHAIN 8

Problem statement 8

Implementation: Tackle the multi-stakeholder challenge 9

Innovation: Responsible data-driven security measures 10

Research: Deep understanding of blockchain risks and opportunities 12

PILLAR 2: TRUST TECHNOLOGIES FOR A SAFE AND RELIABLE DIGITAL SOCIETY 14

Problem statement 14

Implementation: Next level awareness and adoption through practical applications 15

Innovation: Test cases to discover full potential and limitations 16

Research: Deep understanding into large scale opportunities and risks 18

SUMMARY, RECOMMENDATIONS, AND WAY FORWARD 20

CONTRIBUTING ORGANIZATIONS 22

The Dutch Blockchain Coalition Safety Agenda identifies challenges and opportunities for the Netherlands on the cutting edge of safety and decentralized technology.

Pillar 1

Security measures against abuse and fraud in crypto-assets and blockchain

Pillar 2

Trust technologies for a safe and reliable digital society

SAFETY AGENDA DUTCH BLOCKCHAIN COALITION

Decentralized technologies such as blockchain and cryptography offer unprecedented opportunities for innovation for our society and business. Decentralized cryptography can ensure data integrity in crucial chains and contribute to secure data accessibility and exchange. This allows citizens, the business community and the government to benefit from the possibilities and opportunities that decentralized technology offers us. At the same time, these key-enabling technologies entail unknown risks. This is a fact that must be thoughtfully addressed to create a digital society where innovation is fostered, and risks are under control. This security agenda of Dutch Blockchain Coalition (DBC) articulates the identified risks and opportunities, including future actions to de-risk the adoption of blockchain and other decentralized technologies.

Public-private partnership for decentralized technology and safety

DBC's safety theme establishes a national public-private partnership to stimulate activities at the cutting-edge of safety and decentralized technology. Together with stakeholders from the government, the business community and knowledge institutions, this triple helix partnership is working on the safety agenda that jointly addresses the identified challenges and requirements. This agenda gives direction to activities to exchange and develop knowledge, to experiment and test new ideas, and encourages projects to achieve accelerated results that make the Netherlands safer and strengthen its economic position.

To understand the safety problem, it is important to understand the technology dynamics in the existing global market. Technology is the main driver of innovation and social change, realizing impact after adoption and practical use of those technologies. For this agenda is focused on decentralized technologies such as blockchain, crypto-assets and secure multi-party computation. Safety risks often only become apparent in or after the adoption phase, where it is complicated to make technological adjustments to implement security measures. That is why security and privacy by design is important to minimize risks at an early stage. Unfortunately, in today's technology-led world, where time to market is paramount, those security and privacy design principles are being reviewed often as an afterthought.

Agenda pillars and items identified by triple helix activities

The safety agenda presents a series of high-level ecosystem challenges and requirements. If a single organization can fulfill the outcome in isolation, then it is not considered an ecosystem challenge and does not fit in the agenda. Agenda items are identified in three phases of technology readiness: Research (TRL 1-4), Innovation (TRL 5-7), and Implementation (TRL 8-9). To manage the risks and opportunities that these three phases present, they are assessed synchronously to exploit the linkages between them. The implementation of technology usually results in new innovation and research requirements, and those results lead to new implementation opportunities. In each iteration, more details emerge, causing the ecosystem to mature step by step.

Input for the agenda pillars and items is collected during a series of expert consultations and discussions:

- Roundtables of Partners for International Business on Blockchain with focus on Financial Crime in period July 2020 to June 2022[1];
- DBC Conference on 28 June 2022 break-out session Safety;
- First expert session on 25 August to review different action items on the two pillars;
- Second expert session on 28 September focused on Safety in Blockchain;
- Third expert session on 30 November focused on Safety with Blockchain.

As a result of the first iterations and validation during the August session, the agenda is focused on two pillars:

1. Security measures against abuse and fraud in crypto-assets and blockchain (Safety in Blockchain)

[1] https://cflw.com/2021/11/11/report/ - Position Paper - Combat Financial Crimes in the Era of Emergent Technologies

2. Trust technologies for a safe and reliable digital society (Safety with Blockchain)

These two pillars have been selected because they address:

- Urgent and significant societal problems,
- Recognition of challenges by problem owners and solution providers,
- Translation into practical solutions at an early stage,
- Progress in solution translation through various initiatives.

The safety agenda is organized as follows. The two pillars including specific agenda items are presented and discussed in detail in the next two chapters. The safety agenda concludes with a summary and key recommendations for the future towards a secure and mature ecosystem with decentralized technology.

PILLAR 1: SECURITY MEASURES AGAINST ABUSE AND FRAUD IN CRYPTO-ASSETS AND BLOCKCHAIN

This pillar focuses on action items that contribute to a more secure and reliable blockchain ecosystem by developing effective measures to prevent or detect misuse and fraud. The safety problem in blockchain is not due to the technology or its innovative application, but when these technologies are used as facilitators for abuse or fraud. Therefore, security measures are encouraged that stimulate both innovation and improve safety.

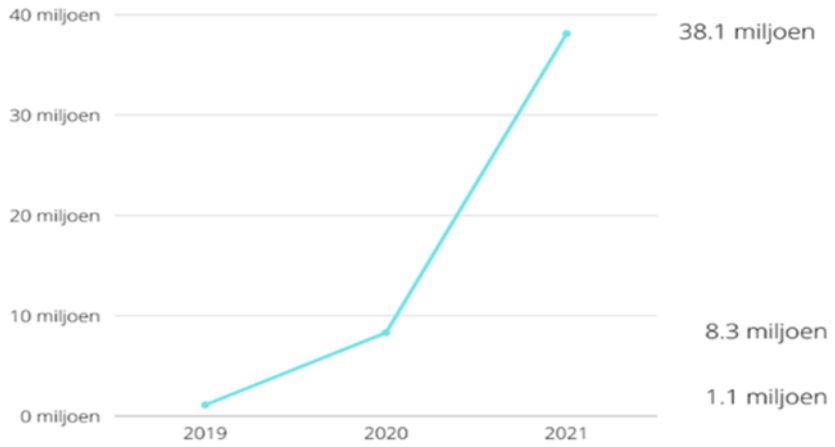


Figure 1. Increase in seized crypto assets from 2019 - 2021[2]

Problem statement

Initially, crypto-assets facilitated online drug trafficking, then became the payment method to decrypt the proceeds of ransomware attacks, and today crypto-assets are also used for serious organized crime, trafficking of child sexual abuse material, and terrorist financing. Thus, the use of crypto-assets to facilitate illicit activities and the subsequent laundering of these funds is becoming increasingly popular and emerging as an alternative to traditional fiat money, cash or virtual. This kind of misuse is also known as financial cybercrime.

It is essential to be able to investigate and prosecute illegal activities abusing blockchain. This is particularly important when using cryptocurrencies or crypto-assets as a means of payment for

[2] https://www.om.nl/actueel/nieuws/2022/02/24/intensievere-aanpak-criminele-geldstromen-wordt-voortgezet

illegal activities. By 2021, more than 10% of criminal funds seized by law enforcement was in cryptocurrencies[3] or related to crypto-assets. New investigative methods and working methods are needed, and they proved effective to detect misuse of various blockchain technologies, confiscate the profits, as Figure 1 illustrates, and thus frustrate criminal business models. In addition to investigative methods against abuse, it is important to implement preventive measures. Concrete examples of blockchain security measures are, for example, making smart contracts more reliable or getting a grip on the most important blockchain risks using practical checklists.

Implementation: Tackle the multi-stakeholder challenge

From law enforcement to regulators or crypto-asset service providers (CASPs), no single organization is responsible for the risks associated with crypto-assets. By its very nature, it requires a multi-stakeholder response to manage the risks involved within and over several organizations. For example, in most law enforcement agencies, crypto-assets are considered high-tech, as such a challenge is to have crypto-asset expertise and capabilities operational at all relevant units since crypto-assets facilitate different crime areas[4]. Specialized units for most crime areas are dispersed throughout the law enforcement agencies, making it challenging to designate a single unit to build crypto capacity. As a result, a networked organization model is needed to handle crypto-asset investigations within law enforcement.

In addition to organization-specific challenges, it is essential to work closely with the private sector. Information sharing and technological advancements are especially vital to CASPs, banks, crypto analytics firms, and the compliance industry. Due to the borderless nature of the internet, the challenge posed by crypto-assets is global in nature. Successful international cooperation requires building trust to enable information sharing to combat the international crimes related to crypto-assets. Therefore, the challenge lies in facilitating secure working models, methods, and good practices that may be internationally applied.

Since 2017, it has been widely accepted that crypto-assets are here to stay, thereby posing new risks to our society. As a result, various preventive measures have now been proposed by, for example, the Financial Action Task Force (FATF), the European Commission (EC) and the national authorities. Essential legislation is proposed by EC: Market in Crypto-Assets (MiCA)[5]. A second

[3] "Niet alle crypto is fout en crimineel, maar het valt zeker niet mee", Public Prosecution Service, Financieel Dagblad 10 October 2022
[4] https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas
[5] https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/

important measure is the Travel Rule[6], a concept that worked for Swift transactions but does not easily translate to crypto-asset transactions, as illustrated by Figure 2. Implementing this legislation is costly, so some jurisdictions are slower to enact this legislation, resulting in the sunrise problem where a counterparty might not yet be compliant. In addition, exchanges are required to store sensitive information about transactions, entailing another privacy risk. This remains a challenge—for example, cloud providers are not GDPR compliant by default.

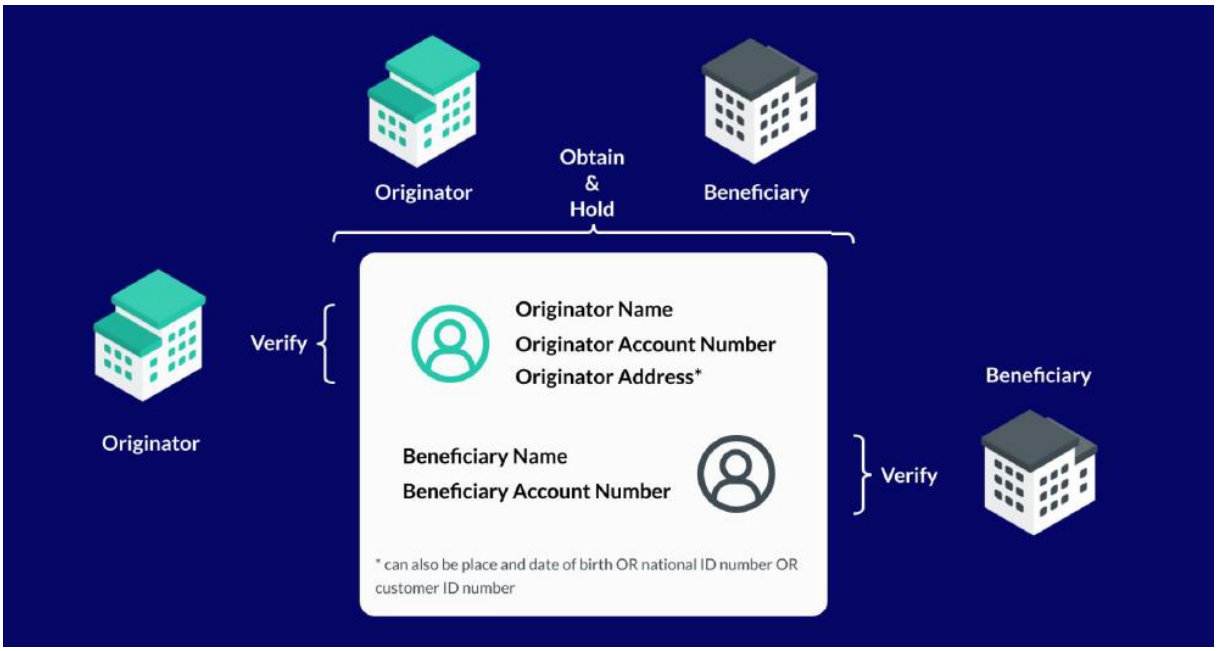


Figure 2. FATF Travel Rule Breakdown[7]

In the evolution of blockchain and crypto-assets, smart contracts have emerged as a common means of representing business logic. Smart contract code reviews should be performed to minimize the risks of (un)intentional coding issues, as several breaches have already been reported. It requires significant effort to build fundamental knowledge to understand different variants of crypto-assets and develop operational investigative techniques for investigators, policy makers and specialists. Good practices should be documented and maintained to address operational challenges such as freezing, seizing and confiscation of crypto-assets[8].

Innovation: Responsible data-driven security measures

IT investments over the past decade have ensured that data is captured at certain thresholds and stored in various databases, and applications. This creates significant opportunities for data-driven

[6] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html - See recommendation 16
[7] 21 Analytics presentation at DBC Expert Session 2 on 28 September 2022
[8] Seizing Virtual Assets Best practices and challenges - INTERPOL (law enforcement only)

security solutions. Terms such as data-driven or evidence-based policing are now widely recognized as a core direction for security innovation. A common data challenge is often the amount, it is too little or too much. Therefore, artificial intelligence (AI), data science, visualization and user-centric dashboards are needed to provide operational perspectives and strategic insights. In particular, such AI-based algorithms should detect money laundering and related financial crime activities. At the same time, there is a need for deeper understanding of the opportunities and risks of data-driven security measures.

Crypto-asset analytic tools are a core technology for tracing crypto transactions. The development of quantitative methods to understand the technical and socio-economic aspects of crypto-asset ecosystems are also required. In addition, there is a need to integrate intelligence on crypto, fiat, and cash transactions to obtain a holistic picture of money flows. To become scalable and repeatable, this cannot only be achieved with investigative dashboards, but requires automated workflows to make it possible.

Guidelines are needed to ensure the admissibility of digital evidence, covering the treatment of items such as "live" cash flow tracking and "dead" forensics on seized devices. Unhosted and hardware wallets present major challenges for investigations. Another major challenge with investigation supporting technologies is the predominant usage of black boxes and surveillance solutions, rather than responsible solutions adopting European principles as openness and transparency-by-design.

Data sovereignty is key. Access to the full dataset unleashes the potential of modern data science and analytics. While the capabilities of visual dashboards are limited, data literacy should become a core competency to realize a safer blockchain ecosystem based on domain knowledge, crypto-asset analytics built and data science know-how. Achieving data sovereignty will also require new data sharing models between public authorities and the private sector. Trust technologies based on such models must consider the balance between European values, such as the fundamental right to privacy, and the need for effective law enforcement in the digital age. Several solutions are discussed by way of the second pillar: safety with blockchain.

Within the established parameters, there is a need for innovative law enforcement interventions. It is impossible to arrest and prosecute every suspect. This is due to limited law enforcement capacity or jurisdictional issues where multiple countries are involved in the crime, making prosecution more difficult. It requires more applied research combining datasets, new de-anonymization techniques, and understanding of human factors to identify new interventions to disrupt or frustrate criminal

activity. Ultimately, this is not just the responsibility of law enforcement but a joint public-private responsibility.

Research: Deep understanding of blockchain risks and opportunities

New security and privacy challenges are being imposed by more recent decentralized and tokenization technologies such as DeFi, NFT, DAO, Web3 and Metaverse. These technologies are based on economic incentive schemes, as Figure 3 addresses, and more research is needed to thoroughly understand the risks associated with abuse and fraud, for example through wash trading with NFTs[9]. At the same time, research is also needed to understand the size and nature of abuse pertaining to traditional crypto assets such as Bitcoin and Ethereum[10]. Well-respected companies have reported lower abuse rates than that of fiat, which sounds implausible. This requires ongoing activities such as horizon scanning, global exchange of expertise. and sharing of good practices on technological innovation and the risks associated with them.

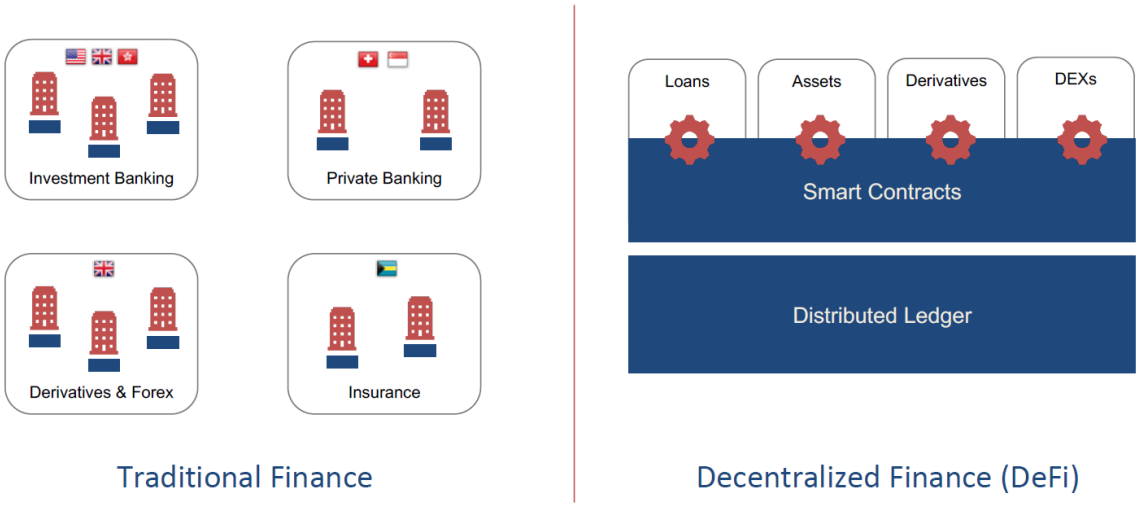


Figure 3. Conceptualization of Traditional Finance vs Decentralized Finance[11]

In the area of cryptocurrencies, two major trends should receive special attention: privacy coins and stablecoins. Privacy coins have built-in privacy measures that make it impossible to track the money on that blockchain. Within the Dark Web, Monero is the second most used crypto-asset after Bitcoin[12]. Stablecoins, on the other hand, have the distinguishing feature of tracking the USD rate, so they do not have the volatility of crypto assets such as Bitcoin. Research is needed to identify the

[9] https://cointelegraph.com/explained/what-are-wash-trading-and-money-laundering-in-nfts
[10] https://www.wodc.nl/actueel/nieuws/2022/11/08/bredere-blik-op-gebruik-virtuele-valuta-helpt-opsporing-criminele-gelden
[11] Ikna.io presentation at DBC Expert Session 2 on 28 September 2022
[12] https://www.coindesk.com/layer2/sinweek/2022/08/30/criminal-crypto-use-is-growing-but-thats-just-half-the-story/

weaknesses of stablecoins that can be exploited for attribution purposes in investigations. Tools that can link such private wallets to IP addresses are particularly interesting. Although a few industry parties reported such results, the levels of effectiveness and accuracy of their methods remain unclear.

New techniques are needed to address money laundering strategies based on well-known crypto-asset mixing or tumbling services, or more recent cross-ledger methodologies. The takedown of Bestmixer[13] by law enforcement has provided several relevant insights, including the fact that such mixing services are widespread. Cross-ledger methods are supported by so-called bridges[14] for Ethereum to make independent blockchains interoperable, for example by simply transferring funds from Ethereum to Solana to Avalanche. In practice, both money laundering strategies are designed to make follow the money techniques difficult, and research is needed to find vulnerabilities in such approaches that can be exploited for investigation.

Furthermore, layer-2 solutions such as the Lightning Network in Bitcoin or various types of Rollups in Ethereum are emerging that can circumvent scalability problems inherent to blockchain technologies. These solutions conduct most transactions off-chain and leave only limited on-chain transaction footprints. Since layer-2 solutions are also abused for illicit transactions and money laundering purposes, new strategies to follow the money across layers are needed.

[13] https://www.fiod.nl/the-fiod-and-the-public-prosecution-service-take-money-laundering-machine-for-cryptocurrencies-offline/
[14] https://ethereum.org/en/developers/docs/bridges/

PILLAR 2: TRUST TECHNOLOGIES FOR A SAFE AND RELIABLE DIGITAL SOCIETY

This pillar focuses on opportunities in developing a secure digital environment by harnessing distributed cryptographic opportunities referred to as trust technologies, such as multiparty computing (MPC), homomorphic encryption (HE), and blockchain technology.

Problem statement

Security and privacy are core conditions or fundamental rights in our digital society. It is a given that information sharing is an essential component for most safety and security measures. Since this seems to contradict with the requirement for privacy, several security measures have been deferred due to perceived privacy risks. However, new trust technologies enable ways to circumvent this constraint by transmitting insights without sharing the actual data[15], as illustrated by Figure 4.

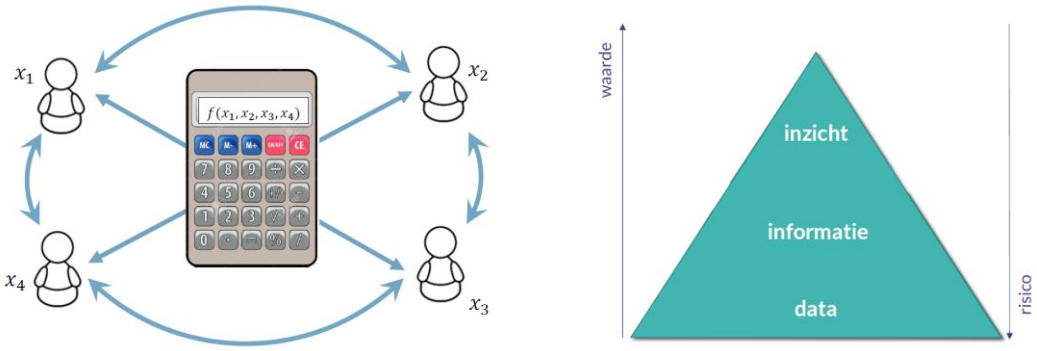


Figure 4. Trust Technologies as Multi-party Computation: share the insight not the data

By means of MPC, for example, parties can bring datasets together in a safe and privacy-responsible manner without explicitly sharing data or transactions. Insights, such as red flags, are only reported if there is a valid reason. Such approaches ensure the privacy of an individual or organization and minimize the risk of data breaches as well as the consequences of cyber-attacks.

In summary, trust technologies focus on collaborative, secure, and decentralized computation technologies whereby:

- Collaborative insight is obtained,

[15] https://www.tno.nl/en/newsroom/insights/2023/01/privacy-enhancing-technologies-practice/

- Underlying data is not revealed to the other parties,
- Privacy & Security by design: even participants do not see intermediate results.

Implementation: Next level awareness and adoption through practical applications

The potential for trust technologies in security applications with privacy by design has been proven in recent years by practical applications such as:

- Sharing information to fight financial crime[16]: Europol estimated the value of suspicious transactions at hundreds of billions of euros – equivalent to 1.3% of EU GDP. Global estimates are close to 3% of global GDP[17]. The problem faced is an unsustainable increase in the 'cost of compliance' e.g. total cost of financial crime compliance > $200 billion with significant year-over-year increases[18]. Collaboration in the field of data and information in KYC and transaction monitoring is therefore a must: "It takes a network to beat a network" ('waterbed effect', ie. money laundering does not stop at the border).
- SecureNed[19,20] combines cyber threat intelligence from more than 100 organizations on a weekly basis, enabling the National Cyber Security Center (NCSC) to create insights and dashboards without viewing the actual input data. This application has been in production since 2020.
- Human trafficking[21]: Combining data from human trafficking victims from various sources to resolve several issues, including to avoid unwanted interference between Police data and NGO's, while understanding full scope and nature of human trafficking.

Various applications are also being tested in domains such as health, mobility, and energy. Regardless of the domain, it's important to learn from those use cases as well, especially as pertaining to how the technologies are used. More potential security applications are being considered and discussed, and greater visibility of successful applications is required to increase awareness among decision makers and allow practical application of trust technologies to reach the next level.

While applications of trust technologies look promising, widespread adoption of these technologies has been slow. Time is a critical factor, especially for security purposes. Digital technologies are

[16] https://www.abnamro.com/clearing/en/news/tno-rabobank-and-abn-amro-are-working-on-privacy-friendly-data-analysis
[17] European Court of Auditors. EU efforts to fight money laundering in the banking sector are fragmented and implementation is insufficient
[18] LexisNexis True Cost of Financial Crime Compliance study Global report (June 2021)
[19] https://www.ncsc.nl/onderwerpen/securened
[20] https://rosemanlabs.com/blog/computable_1.html
[21] https://datasharingcoalition.eu/use-cases/improved-monitoring-of-human-trafficking-by-sharing-insights/

being brought to market at a rapid pace. It usually takes some time to understand the potential risks, let alone respond to these risks. DBC contributes to accelerating the pace of adoption by mobilizing the ecosystem and highlighting good practices.

Ultimately, trust technologies can achieve a paradigm shift by enabling different parties, such as from both public and private sectors, to collaborate on data without having to worry about security and privacy. This problem is not technical in nature, and neither can it be solved by a few parties working individually. Rather, it requires a joint effort from both the public and private sectors to work together in large-scale collaborative initiatives, like NICPET[22], etc., to attain critical mass through widespread adoption.

In this phase of adoption, it is more strategic to move forward rather than wait for all national and international stakeholders to come on board. Experimentation, testing, and deployment with a community of willing early adopters is key to keeping pace with technological developments. Public-private data partnerships have the potential to solve some of society's biggest challenges, but a holistic data governance framework is needed to build trust and address risk[23]. Trust technologies are therefore an important pillar under DBC's security theme.

When raising awareness and sharing good practices on how reliable technologies such as multiparty calculations contribute to compliance with the GDPR and its principles, it is important to identify several target groups. First, policy makers and decision makers, at whose level technical expertise is limited and understanding the potential of trust technologies can be difficult. Second, legal officers and consultants, including data processing officers, who often have solid legal backgrounds but lack the technical expertise to assess the potential and risks of trust technologies. In many cases, this skills deficit leads to the decision not to proceed further, to minimize risks. Third, technology providers should provide clearer and more transparent explanations to close the knowledge gap about how and why trust technologies work. In general, the knowledge gap poses a major impediment to faster adoption.

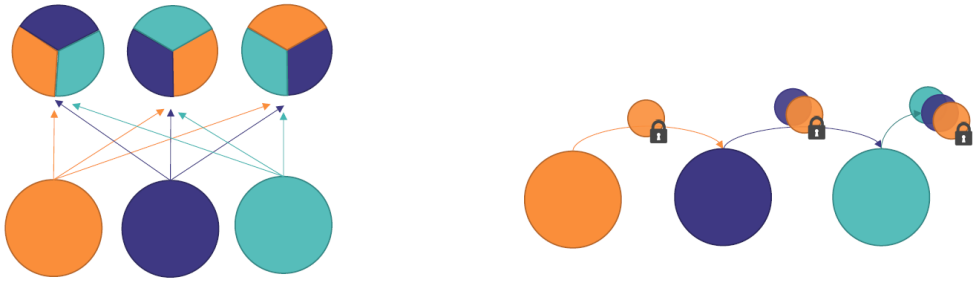
Innovation: Test cases to discover full potential and limitations

New technologies such as trust technologies are often seen as a panacea (solution to everything) but this perception is unrealistic. Nonetheless, trust technologies have the potential to achieve a

[22] https://www.linkedin.com/posts/freek-bomhof-894149_een-betere-overheid-houdt-ook-in-een-overheid-activity-6981549275411271681-zFjy/?trk=public_profile_like_view&originalSubdomain=nl
[23] https://www.mckinsey.com/capabilities/quantumblack/our-insights/collaborating-for-the-common-good

paradigm shift in how to deal with data security and privacy. For this reason, more use cases need to be tested and efforts need to be made to assess both its full potential and its limitations.

In practice, MPC applications based on fixed data conventions can be used in calculations, but there are more requirements for performing data analysis. For this reason, testing new use cases will explore different trust technologies for security applications and identify new requirements in trust technologies for a safe and secure financial system. More use cases need to be tested especially for AML, fraud-related, cyber intelligence, and collaboration features, while at the same time, implementation of proven applications need not be withheld.



Secret sharing

Homomorfe encryptie

Figure 5. Trust technologies collection is significant, so to select the right technology for the right problem.

The collection of trust technologies include but is not limited to secure MPC, federated learning, secret sharing, homomorphic encryption, zero-knowledge proofs, differential privacy, synthetic data and bloom filters. It requires deep cryptographic expertise to select the right technology for the problem at hand. This is a challenge for the application engineers who need to apply such technologies but lack deep cryptographic knowledge. This emphasizes the need to commoditize trust technologies to the point where they are used by default, as well as underlines the need for guidelines and support in implementing them.

To apply MPC, the datasets are encrypted by the sources before being delivered to the computation mechanism. It requires a purpose limited protocol on the computation to be performed and the results to be produced. A clear purpose limitation is required because it cannot be adjusted afterwards. At the same time, this constraint makes it hard to assess and review the obtained insight based on the actual data by going back to the source data. This is another reason why explainability is crucial.

A question to be resolved is whether a mechanism is needed and if it would be acceptable to go back to the actual data if necessitated by the computation and its obtained insight. For example, if the computation is designed to flag only when an illegal activity is detected, is it possible to go back to the data source and focus on a specific suspect? A fundamental discussion is needed about the need for privacy preservation if a red flag prompts an investigation into a particular suspect. For example, proportionality and data minimization can be cited if only suspicious data is disclosed and the rest remains encrypted.

Given the emphasis on purpose limitation, MPC technologies are especially suited for recurring cases, for example, when viewing daily produced and updated datasets. This poses challenges in regards to the scalability and interoperability of the application. If a different insight is needed at a later stage, it would be complicated to add, probably requiring changes in architecture and data flow that render scaling difficult. That's why initiatives like International Data Spaces Association[24] (IDSA) and GAIA-X[25] strive to achieve scalability and increase interoperability between vendors and providers, and why conducting such activities in the trust technologies space is so challenging.

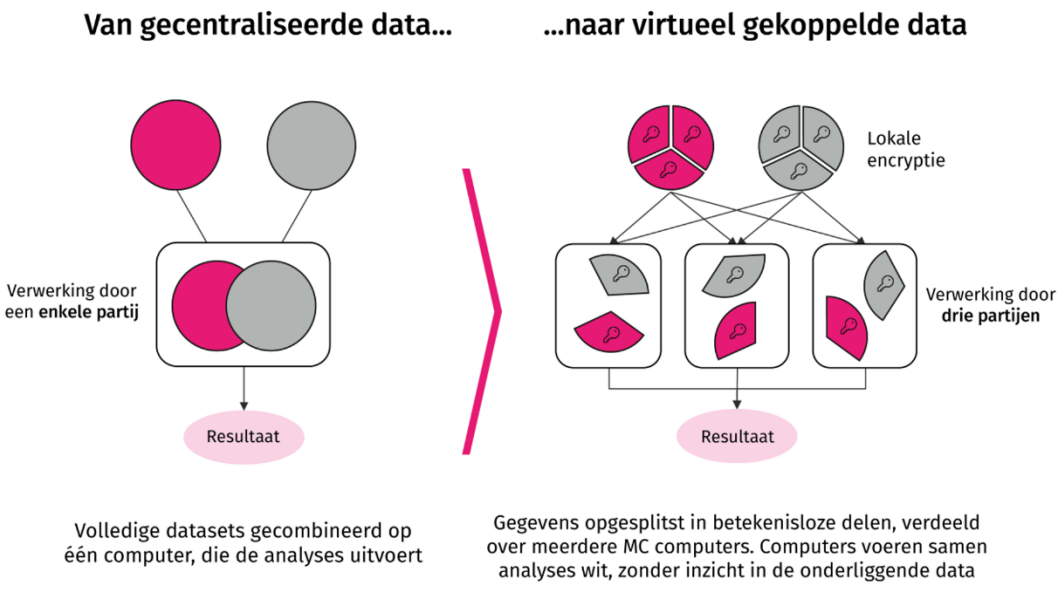


Figure 6. Advances in trust technologies enables data analytics with privacy by design

Research: Deep understanding into large scale opportunities and risks

Trust technologies are not yet accessible to all application engineers. To achieve widespread adoption, there is a need to make the technologies easy to use. To some extent, trust technologies

[24] https://internationaldataspaces.org - International Data Spaces
[25] https://gaia-x.eu - Gaia-X: A Federated Secure Data Infrastructure

should be incorporated into standard data processing frameworks where the data analysts can keep focusing on the data and not have to worry about privacy issues. Applied research is needed to develop a strategy that includes a methodology to make trust technology an integral commodity forming part of the internet and cloud infrastructures, so that security and privacy by design are implemented by default.

Existing trust technology applications have proven their worth for specific use cases. It is a challenge to deal with technical complexity, especially when solutions are scaled. This is not just a computational problem, because scaling also brings new security and stability risks, as experienced by the big data community. Data analytics based on small data sets can be easy, while processing larger data sets (multiple TBs) requires specific scalable infrastructures such as Kubernetes. Research is needed on the large-scale use of trust technologies, especially when implemented as infrastructure solutions.

The advantage of trust technologies is privacy by design, but such a benefit always comes with a cost, such as additional layers of encryption, necessitating more computation, and loss in flexibility. Research is needed to minimize those inefficiencies, and computational scalability is required, for example, to enable real-time processing, complex graph analysis, and AI model training.

Trust technologies operate within purpose constraints and so long as the data is properly provided. For example, a simple email address is often shared with or without capitalization, and in practice, it can be used to send email in any format. However, strict data format restrictions are required to match such values in the encrypted domain, which are beyond the capability of current data processing pipelines that mostly start with only a few data preparation operations. It is a research challenge to make trust technologies flexible enough to perform fuzzy matching, for example. Research is needed in areas such as speech recognition and image classification to endow them with security and privacy by design.

SUMMARY, RECOMMENDATIONS, AND WAY FORWARD

The safety agenda articulated a series of ecosystem challenges and requirements that the safety community cannot solve efficiently by one or two parties. Instead, solving these challenges requires collaboration through public-private partnerships to achieve a safer crypto-asset space as well as expedite adoption of trust technologies. All partners in this ecosystem may wish to consider the various agenda items and identify an area in which to contribute. The transition envisioned to de-risk decentralized technology and exploit its full potential requires the cooperation of every willing stakeholder. Table 1 presents a summary of the agenda items for pillar 1: Safety in Blockchain.

Table 1. Summary of key agenda items for pillar 1: Safety in Blockchain

Security measures against abuse and fraud in crypto-assets and blockchain
Tackle the multi-stakeholder challenge (Implementation) - Develop capacity building programs to make knowledge and expertise about crypto-assets and blockchain risks widely available and not just to a few specialists. - Develop a public, private and joint platform to actively share good practices in preventive (eg MiCA, Travel Rule, Smart Contract audits) and investigative techniques (Crypto-asset analytics). - Develop collaborative mechanisms within and across organizations (LEA, Regulator, CASPs, blockchain industry) in public-private settings on a national and international level.
Responsible data-driven security measures (Innovation) - Test data-driven preventive and investigative analytical techniques that adopt European principles as open and transparency by design instead of black boxes. - Test automated scalable and real-time workflows to become data-driven when monitoring suspicious transactions and risky entities. - Test and experiment with innovative and data-driven interventions to disrupt the criminal ecosystem rather than attempt to prosecute all criminals.
Deep understanding of blockchain risks and opportunities (Research) - Study pro-actively and using a structured approach together the scientific community new risks that may arise from DeFi, NFT, DAO, Web3 and Metaverse to be better prepared. - Study leads and find ways to investigate suspicious privacy and stablecoin transactions. - Study advanced money laundering strategies using crypto assets and find ways to track the money through crypto-asset mixers or staged money laundering techniques.

Table 2. presents a summary of the agenda items for the pillar Safety with Blockchain.

Table 2. Summary of key agenda items for pillar 2: Safety with Blockchain

Trust technologies for a safe and reliable digital society
Next level awareness and adoption through practical applications (Implementation) - Develop a communication strategy for practical and operational security applications with trust technologies to stimulate adoption by underlining that security and privacy can go hand in hand. - Develop capacity building programs for policy and decision makers to understand the potential and technology readiness of trust technologies. - Develop joint initiatives for data sharing with trust technologies by responsible authorities and data owners.
Test cases to discover full potential and limitations (Innovation) - Test more advanced use cases to discover the limits of new and existing trust technologies, without holding back the deployment potential. - Test approaches to make it easy and explainable to choose and deploy trust technologies to drive adoption by application engineers. - Test collaborative features and drive interoperability to make sharing and analytics on encrypted data more relevant and acceptable.
Deep understanding into large scale opportunities and risks (Research) - Study the approach to have trust technologies implemented by default, as security and privacy are fundamental rights. - Study the large-scale use of trust technologies with massive amounts of data and large number of users for security and privacy proofs. - Study next generation trust technologies capable of processing images, signals, and fuzzy inputs.

Going forward, DBC with its theme safety will provide the public-private platform for partners to meet, share and develop ideas into initiatives, taking project outcomes to the next level. This commitment will accelerate the necessary transition to make the Netherlands safer and strengthen its economic position.

CONTRIBUTING ORGANIZATIONS

The safety agenda is established with contributions by