MADANA

WHITE PAPER

MADANA is an open data analysis platform, preserving privacy by design. The blockchain-based ecosystem allows anyone to stay in control of their data while monetizing it in an anonymous way. MADANA aims to provide a GDPR compliant way for data processing, enabling new business models for future Apps and Services.

Table of Contents

Further, by authorizing and verifying the identity, confirm all this. Evidence of successful registration at the Pin Up casino will be the presence of a working account, which will store all information about the user. After that, the gamer will be able not only to play for money, but also, having made the first deposit, activate the welcome bonus package using a special promotional code. The main thing is to familiarize yourself in detail with the club's policy, as well as the conditions for using various gifts, both before registering at a Pin Up casino and when activating bonus rewards. Users will be able to acquire pleasant surprises by becoming a member of the loyalty program.

This white paper aims to provide a deeper insight
into the technology and business behind MADANA.
The tokenomics will be highlighted in a separate paper.

This paper is subject to change.
It will be amended from time to time to
include continuous feedback to questions received from the community and
further findings. Any amended versions of this paper will be published
on the MADANA website; only the most recent version of the
white paper published on the website is the relevant white paper.

For more information, visit www.madana.io or email info@madana.io.
White Paper Version 1.0 (June 2018)

EXECUTIVE SUMMARY

Abstract: The MADANA – Market for Data Analysis – ecosystem empowers everyone to participate in the data market with their own data, while simultaneously preserving their privacy. The PAX token enables anyone to buy data analysis results from a decentralized pool of information while rewarding data producers and plug-in providers for their contribution.

Individuals create significant amounts of data while using daily devices such as mobile phones, tablets, smart home devices, and computers. In most cases, data producers give up all rights of their data by agreeing to non-transparent terms and conditions. Data brokers sell this data to big corporations making substantial profits. The data producers are left without any control or profit. Currently, most of our data is stored in centralized servers, which are popular targets for hacker attacks, who gain access to sensitive information and leak it. The progress in global data protection policy is slow and the market for big data grows continuously. As the amount of breaches, leaks, and hacks is increasing severely, a new approach to handle data is needed. It is time to regain the control over our own digital identity.

MADANA is building an innovative data analysis market ecosystem based on the Lisk blockchain that allows data producers, data analysis buyers, and plug-in providers to become active in a fair, anonymous and privacy-protecting open data market. For the first time in history, decentralization is bringing transparency, balanced value distribution, and efficiency.

The MADANA ecosystem encompasses the following key elements:

- Client-sided data storage and easy to handle encryption framework to retake control of personal data
- Monetization of anonymous data contribution through PAX token
- An open, blockchain-based data analysis marketplace for everyone
- Monetization of analytics and data science skills through PAX token
- Reliable analytics of internal and external data for business purposes
- A decentralized, non-manipulatable pool of information

Utilizing state-of-the-art technologies and blending them intelligently into a new ecosystem enables various applications and scenarios in data-driven industries while prioritizing data security and data privacy.

Establishing the MADANA ecosystem will provide a durable basis for future expansion stages regarding market exploitation and increasing technological distinction. The business approach is long-term oriented and encloses key-partnerships in traditional industries and consulting companies as multipliers as well as technological differentiation. Thus, resulting in the fulfillment of MADANA's novel potentials like **Standardized Privacy Layer, Big Data Analysis Store, Background AI-training, Reputation Score, Data Privacy Certificate, Data Model Standardization, GDPR-Compliance and Cross Analytics of Sensitive Data.**

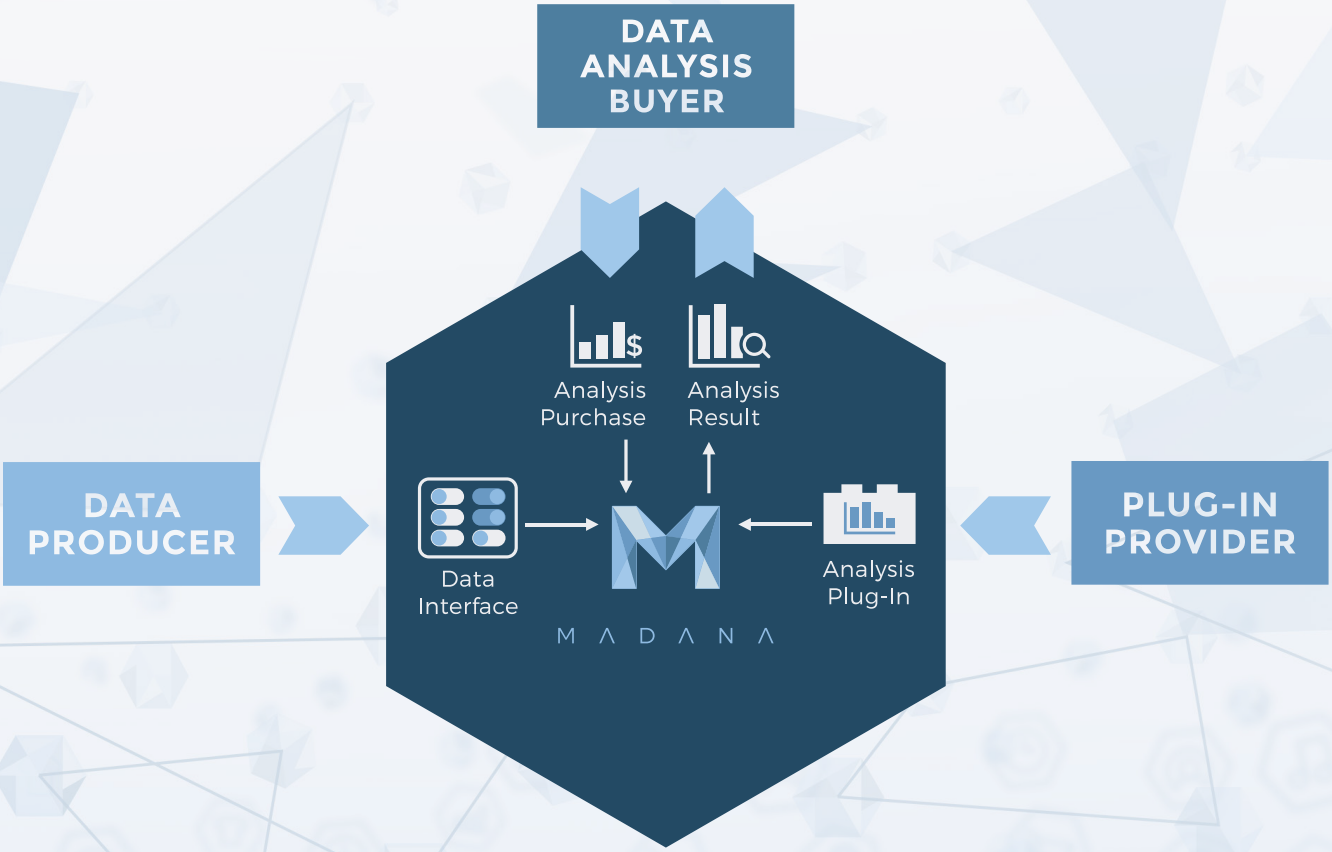


Figure 1 – MADANA Ecosystem

BACKGROUND

We are living in a world that is becoming more digitalized every day. Valuable information is created everywhere, and companies are pressured to utilize that information or risk falling behind their competition. In the world of free apps, many developers turned to the rising asset class, data, as their main source of income a long time ago. Information about us is gathered in many pieces, packaged, and then sold to the highest bidder. [1]

Most end-users do not realize how their privacy is being assaulted and abused. Beside the applications on our mobile devices and computers, a rising number of smart devices and company-owned sensors are also generating valuable data. But the monetization of this new asset is challenging. Data markets are complex, consisting of many different parties and above all, are designed to maximize the value by ignoring the privacy of the data producers.

„You already have zero privacy. Get over it.“

Scott G. McNealy,
CEO of Sun Microsystems Inc. (1999)

As for payments in Пин Ап casino, they are quite fast in comparison with other virtual gambling establishments. The maximum time becomes only two days. It all depends on the withdrawal method and the amount. In cases where it is not possible to make a deposit or withdrawal, the client can always contact the Pin Up casino technical support service.

Data Market Context

Data and analytics capabilities have made a leap forward in recent years. The volume of available data has grown exponentially, more sophisticated algorithms have been developed, and computational power and storage have steadily improved. The convergence of these trends is fueling rapid technology advances and business disruptions. Moreover, data and analytics are changing the basis of competition. Leading companies are using their capabilities not only to improve their main operations but to launch entirely new business models. Flows of data have created new infrastructures, businesses, politics, etc. The value of data is increasing as new methods and tools of data analysis are popularized. Furthermore, the extracted value is highly dependent on its ultimate use, and ecosystems are evolving to help companies capture that value.

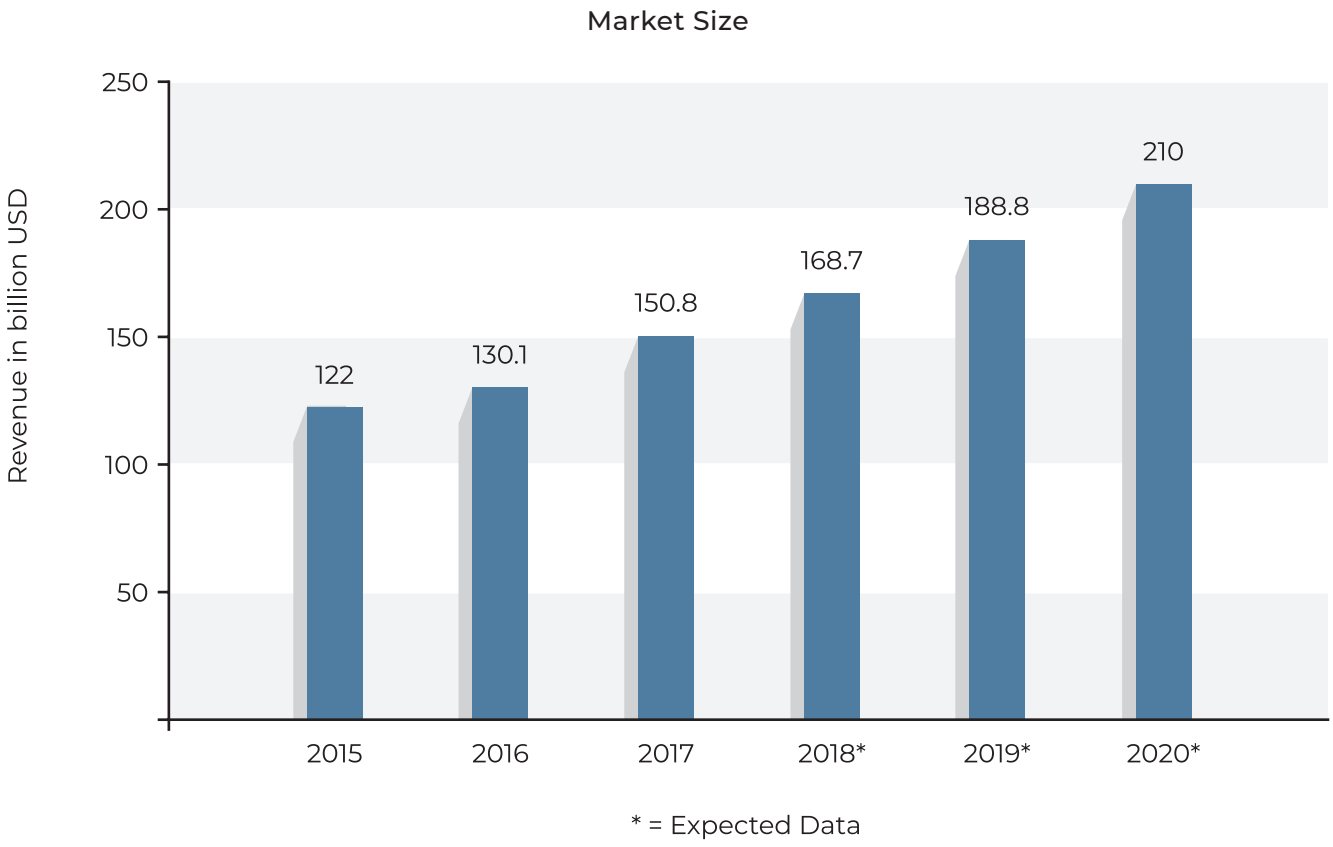


Figure 2 – Revenue from Big Data and Business Analytics worldwide from 2015 to 2020 (in billion USD) (based on [2])

[2] IDC (2017): IDC's Worldwide Semiannual Big Data and Analytics Spending Guide, [online]

The global data market size was predicted to grow from USD 9.7 billion in 2016 to more than USD 18.2 billion in 2018. The growth is directly connected with the world's data size expansion and with dynamic digital market growth.[3] According to E-marketer[4] , the global value will rise to over USD 375 billion by 2021. The knowledge about customers is essential for effectively tailoring products and services to customers' needs in the programmatic model.

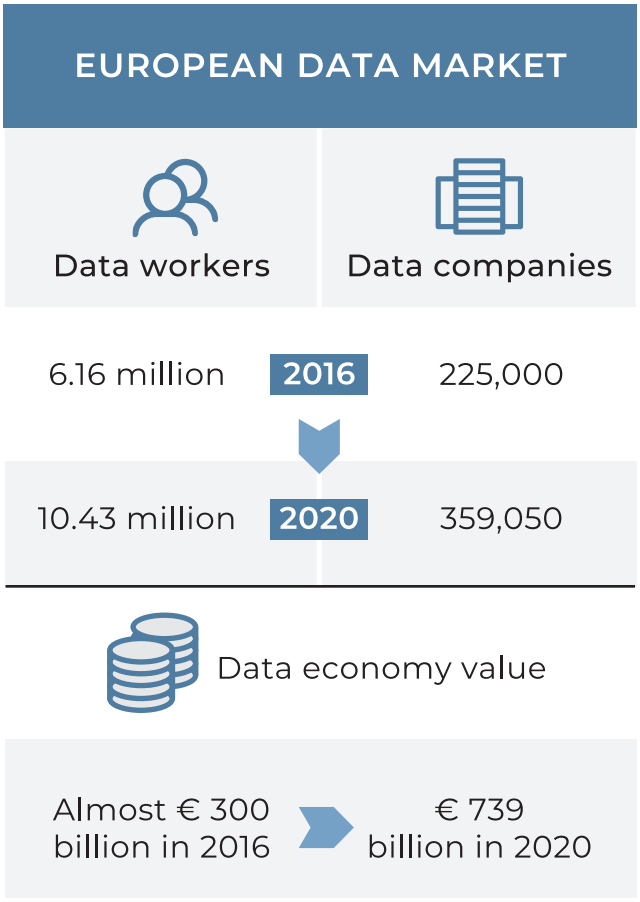


Figure 3 – European Data Market Supply (based on [5])

When it comes to Europe, the value of the **European data economy** was estimated at EUR 257 billion in 2014, or 1.85% of EU GDP. This increased to EUR 272 billion in 2015, or 1.87% of EU GDP (year-on-year growth of 5.6%)[5]. The European Commission (6) predicts that, if policy and legal framework conditions for the data economy are put in place in time, its value will increase to EUR 643 billion by 2020, representing 3.17% of the overall EU GDP. As shown in Figure 4, the top data markets for 2017 in Europe include the UK, Netherlands, France, Germany, and Denmark.

COUNTRY	DATA MARKET SIZE
UK	$ 1,285 m
Netherlands	$ 196 m
France	$ 181 m
Germany	$ 133.5 m
Denmark	$ 78.5 m

Figure 4 – Top 5 Largest Data Markets in Europe in 2017 (based on [3])

[3] OnAudience (2017): Global Data Market Size 2016-2018, [online]
[4] e-Marketer (2017): Worldwide Ad Spending: eMarketer's Updated Estimates and Forecast for 2016–2021, [online]
[5] European Commission (2017): Final results of the European Data Market study measuring the size and trends of the EU data economy, [online]
[6] IDC (2017): European Commission (2017): Building a European Data Economy, [online]

The data-driven transformation is spreading into every corner of the economy and society, ever-increasing amounts of data are generated by processes or machines based on emerging technologies, such as the Internet of Things (IoT). The new era of connectivity itself changes the way data can be accessed. The enormous diversity of data sources and types, and the rich opportunities for applying insights into this data in a variety of domains, including for public policy development, are only beginning to emerge. To benefit from these opportunities, both public and private players in the data analysis market need to have access to large and diverse datasets. The issues of access and sharing in relation to the data generated by these machines or processes are central to the emergence of a data economy and require careful assessment. [6]

In a new data-driven economy, a new set of rules and regulations are required for the market to operate efficiently and effectively. Currently, data is collected from different parts and then marketed through data brokers (fig 5). These data markets offer the service of combining data from different sources to generate new insights. This results in two major issues:

Data brokers are in the position to take the major cut. The earnings only partially go to data gatherers such as app developers and companies. End- users, the true data producers, get nothing, or a fraction of the value, in form of rebates or bonus programs.

Unfortunately, until now **data markets** are rarely designed to be open. Data is kept isolated within the market it belongs to. As a result, valuable information that could be generated across data markets is lost.

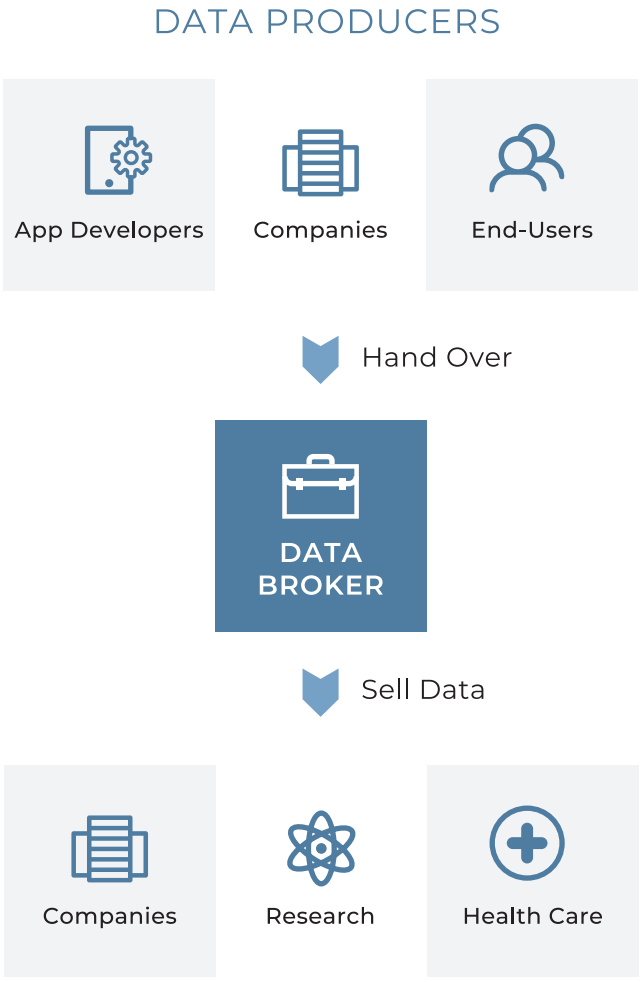


Figure 5 - Data Markets Today

[6] IDC (2017): European Commission (2017): Building a European Data Economy, [online]

Data Market Participants

Parallel to the rise of data markets, **data analytics** and data science industries are constantly and rapidly evolving, aiming to extract and process data into meaningful dedicated analyses.

Because the technologies underpinning **data science** are shifting rapidly, following trends in data science have been identified for 2018 [7, 8] :

- Continuing rise of open source
- Pioneer projects on decentralized ledger systems (dApps)
- Continuing growth in the field of visualization tools
- Consideration of infonomics
- Rising importance of the Chief Data Officer (CDO)
- Increasing focus on Data Governance
- Increasing use of AI for the analysis of unstructured data

Not only individual data producers face challenges in the big data industry, but also companies and developers need to cope with inefficiencies.

The first obstacle for companies are costs. Market research for companies requires the purchase of datasets, which then need to be processed, organized and formatted. In addition to the data acquisition costs, data scientists need to be hired. Average wages for data scientists are around USD 100,000 annually [9], while the costs for data analytics tools spread between USD 10,000 and USD 50,000 annually [10].

The next obstacle is that most datasets do not contain the exact data that is suitable for a more precise analysis. As a consequence, the analysis results are not as accurate as they could be. In a centralized data market, brokers bundle large bulks of data, which are usually not formatted for direct use and need to be disentangled and prepared for internal use. Companies cannot be sure if the data acquired is exclusive and of high quality, as the data market lacks transparency.

Opportunities for data scientists and developers as so-called plug-in providers to offer their skills and knowledge on any platform to a broad mass are increasing but in a slow and modest manner. Plug-in providers can rarely participate in the data market as freelancers and therefore cannot consistently develop their skills. The bigger barrier for small developers is data privacy regulations, which requires them to ensure data producers' privacy. The efforts necessary to fulfill the requirements make it impossible for data scientists to be profitable in an entrepreneurial way.

[7] Keith D. Foote (2017): Big Data Trends for 2018, [online]
[8] Dataspace (2018): State of the Analytics Market 2018, [online]
[9] Paysa.com (2018): Data Science Salaries, [online] (as of 05/02/2018)
[10] Softwareadvice.com (2018), [online]

Personal Data Privacy Today

Everyone has the right to the protection of personal data concerning him or her [...] The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.

[REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (2016) [11]]

In 2017 over 2.6 billion data records have been compromised globally ([12]). These data records are digital profiles of individuals and contain highly sensitive personal information. The internet does not forget, and data markets don't either. They hold information gathered years ago in many different places. This data combined with external data uncovers truths (or insights) about us, that not even we are aware of. This is called the **Digital You**. The Digital You is vulnerable as it is stored on central servers. The question of how your personal data should be protected is very complex and complicated.

It is mainly a technical problem. Data aggregators are tasked to have adequate security measures in place. But as a series of data hacks show, even the most established companies do not seem to be fully capable of ensuring data security. Besides their own precautions, users only have a few regulations in place to protect themselves. But a look at the EU politics shows how complicated data protection laws really are. The solution that the EU came up with after not bringing major changes since the 90s is the General Data Protection Regulation (GDPR). But already the above-mentioned citation shows how challenging it is:

Protection of privacy and enabling business in the digitalized world are two opposing matters needed to be balanced continuously. All attempts at data protection regulation are compromised in the end. Precise information is the most valuable, but also most private. Some of the most private and valuable data include financial information, health data, geolocation data and behavioral data. [13]

To solve this issue a technology-based solution is needed that is capable of protecting the data producer whilst still allowing all participants to reap the benefits of a data-driven society.

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council (2016): On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [online]

[12] Gemalto (2018): The Reality of Data Breaches, Data Records Compromised in 2017, [online]

[13] European Commission (2014): Towards a thriving data-driven economy, [online]

GDPR – A Possible Regulatory Approach

The EU General Data Protection Regulation (GDPR), ratified in 2016 and being enforced ever since the 25th May 2018, is replacing the Data Protection Directive 95/46/EC. It is designed to harmonize data privacy laws across Europe, protect and empower all EU citizens' data privacy, and reshape the way organizations around the world have to approach data privacy. Three GDPR key changes can be identified[14]:

INCREASED TERRITORIAL SCOPE

The jurisdiction of the GDPR will be extended. It now applies to all companies worldwide that process personal data of data producers, literally the data subjects, residing in the EU. Non-EU businesses processing the data of EU citizens will now also have to appoint a representative in the EU.

STRENGTHENED CONDITIONS FOR CONSENT

The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Clear and plain language must be used, and it must be as easy to withdraw consent as it is to give it. That means that companies will no longer be able to use long illegible terms and conditions full of legalese.

REFINED PENALTIES

Organizations can be fined up to 4% of annual global turnover or €20 Million (whichever is greater) as a maximum fine for the most serious infringements (e.g. not having sufficient customer consent to process data or violating the main principles of data protection of the GDPR). It applies to both controllers and processors (Clouds as well).

The GDPR could strengthen the rights of data producers by several measures[14]:

Figure 6 - GDPR Aspects (based on [14])

[14] EU GDPR Portal (2018): Home Page of EU GDPR, [online]

BREACH NOTIFICATION

Breach notification becomes mandatory for all controllers processing personal data. It must be done within 72 hours of first having become aware of the breach. Also, data controllers will be regularly required to notify their customers, the data subject, without delay.

RIGHT TO ACCESS

Right for data producers to obtain confirmation from the data controller as to whether or not personal data concerning them is being processed, where and for what purpose. The controller must provide a copy of the personal data, free of charge.

RIGHT TO BE FORGOTTEN

Data producers have the right to request the data controller to erase their personal data, cease further dissemination of the data, and potentially have third parties halt processing their data.

DATA PORTABILITY

The right for data producers to receive the personal data that concerns them, which they have previously provided in a commonly used format. The right to transmit that data to another controller.

RIGHT TO OBJECT

Under certain conditions, data producers have the right to object to the processing of personal data, in particular for marketing purposes. For example, if a data producer receives marketing emails based on personal data that the company has collected earlier, the data producer has the right to tell the company to stop sending marketing emails. Companies must comply with this request without incurring any costs for the data producer.

PRIVACY BY DESIGN

When new systems get designed, data protection will be taken into account from the beginning on. Data controllers are called to hold and process only the data that is absolutely necessary for the completion of their duties, as well as limiting the access to personal data for third party data processors.

The position of data producers may get significantly strengthened among powerful companies which collect more and more data for commercial purposes by the GDPR. It is one of many steps needed towards a digital world in which data producers have full sovereignty over their data.

Background Summary

GROWTH

The overall value of the European data economy grew from EUR 247 billion in 2013 to almost EUR 300 billion in 2016 [5]. European and global forecasts and predictions are commonly positive and enthusiastic. The amount of data produced puts pressure on companies in every sector, requiring them to participate in a race of data acquisition and utilization in order to achieve a competitive advantage.

PARTICIPANTS

Companies and data brokers are not the only participants in the data market anymore. Awareness among society, developers, data scientists and individual data producers is increasing rapidly, which makes them important participants in the data market. Considering the different needs and wants of the participants adds more complexity to the data market and makes it more challenging.

DATA PRIVACY

By moving through the digital world, everyone is leaving – mostly unknown – digital traces, that are being aggregated into a clear digital copy by a third party for commercial use. This so-called Digital You is becoming more valuable, as digital data privacy is set at the end of the line. Recent scandals regarding data privacy abuse have awakened politics and society. Regulations like the GDPR are trying to intensify the rights of data producers at the level of legislation.

With a high growth potential in the data markets and as the demanding responsibility towards a structured and balanced data world grows, it is clearly obvious to act now.

[5] European Commission (2017): Final results of the European Data Market study measuring the size and trends of the EU data economy, [online]

VISION

Digitization enters more and more aspects of our lives. Data-driven technologies and their applications are making our world more complex, and the speed at which it is changing is rapidly increasing. Our digital privacy is also subject to this change. It is not always easy for normal consumers to keep track of the different developments. In the meantime, our Digital You leaves data traces everywhere it goes, which often leads to a significant breeding ground for digital crime.

In order to prevent and guard our digital identities in the future, MADANA envisions, that through the use of upcoming technologies and methods a meaningful and social solution can be found. This solution is imaginable by utilizing and logically combining community-driven intelligence, secure encryption frameworks, decentralized applications, the latest data science methods, decentralization enabling technologies, as well as scientifically proven new information technologies and applicable game theory approaches. Balancing these elements in a savvy way has resulted in the creation of thought-provoking impulses and ideas:

- Providing the same access to data for everyone.
- Creating the world's open decentralized generic pool of information.
- Gathering innovative tools for data evaluation.

MADANA ultimately envisions that every single data producer – human or electronic device – is in full and transparent control of their generated data and the Digital You.

MADANA envisions a new data ecosystem approach, where data is the main resource benefitting all participants by being smartly used.

MADANA envisions a data ecosystem, which by itself is of self-regulatory nature driven by all its participants.

MADANA envisions that the world and societies will hugely benefit from a smart and fair applied data-driven ecosystem beyond the borders of various industries.

In order to reach the mentioned approaches and to realize the high- level visions a baseline for privacy- driven data handling must be set initially.

PRODUCT DESCRIPTION

MADANA –
MARKET FOR DATA ANALYSIS

The data market is currently dominated by enterprises who are buying big sets of data from third parties that are subject to different data protection laws. In known systems, these enterprises decide which data is available for sale. A problem with this is that all of the data is shared regardless of whether the data, or part of the data, contains information the originator does not want to share. Thus, the originator of data is exposed to an unnecessarily high risk of privacy violations.

MADANA is creating a new approach to provide a system implementing the method to eliminate the stated problems and to extend the data market with further advantages. The objective is achieved with a system which provides the following key aspects:

- A method for contributing data anonymously to a remote system while getting paid.
- Client-sided data storage and an easy to handle encryption framework to retake control of data in general.
- A method for contributing analytics skills while getting paid in exchange.
- An open data analysis marketplace for anyone.
- A decentralized pool of information.
- A method for getting analysis results of new and sensitive data.
- Trustworthiness through blockchain and smart contracts.

The most important advantage is that data producer's privacy is respected, no third parties are involved, and entry barriers are minimized. Thus, a new ecosystem can be established in which everybody can participate – through transparency, trust, and monetary benefits.

Ecosystem

MADANA proposes an open data analysis market ecosystem that will run on multiple smart contracts based on blockchain technology. It is MADANA's goal to allow data producers, data analysis buyers, and plug-in providers to participate in the data market in a fair, anonymous and privacy-protecting way.

The new data analysis market is achieved with a system which offers open access to analysis results based on various kinds of data from different sources while preserving the privacy of data producers by design.

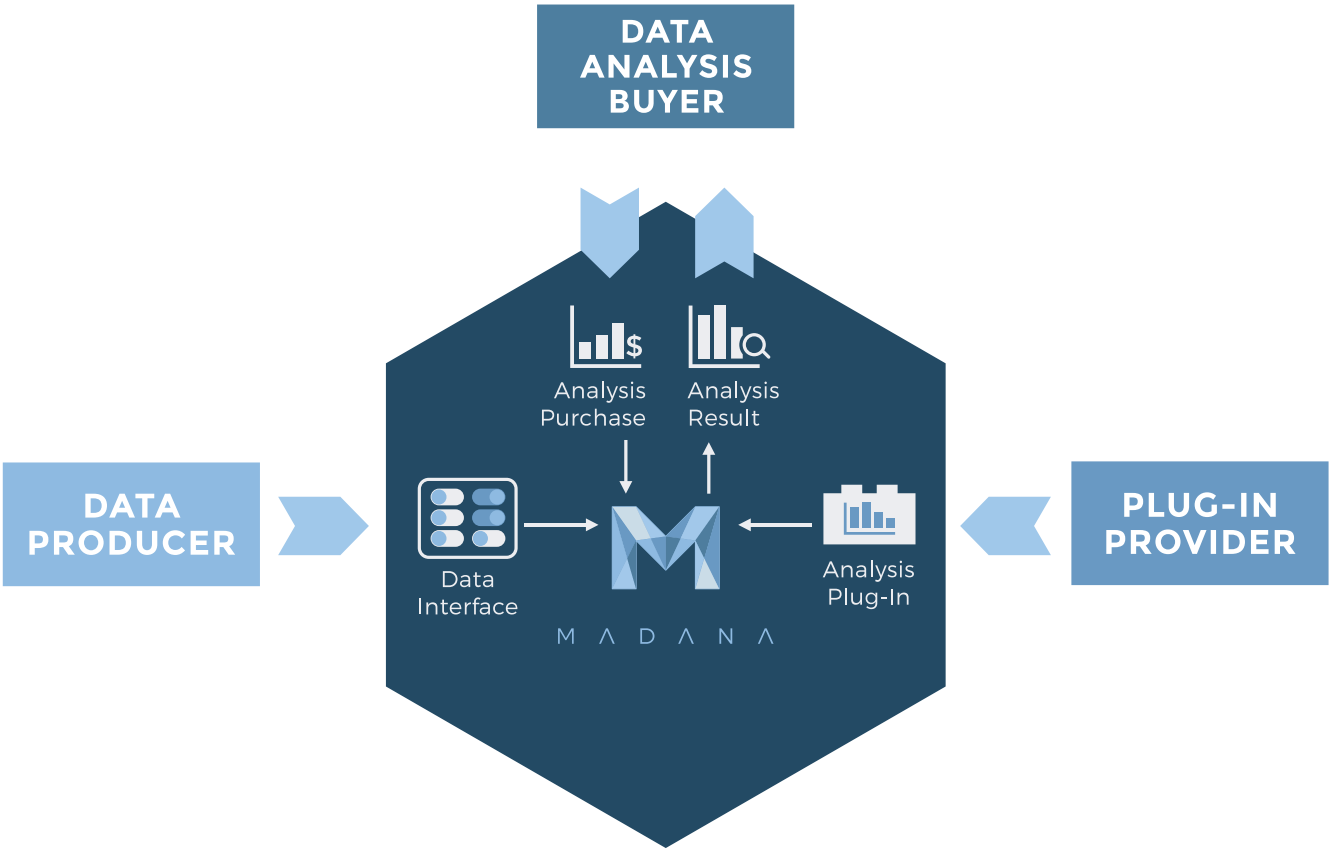


Figure 7 – MADANA Ecosystem

DATA PRODUCER

The system enables data producers to publish all kinds of data to a network and thus to participate in the data market with their own data. By platform design, data producers can monetize their data without giving up control over their data or compromising their privacy. Queries for data are processed on demand. Therefore, the data stays encrypted on the producing devices and can only be accessed if the user agrees to publish it when needed for analysis processing. Data will only be processed in secured environments and afterward deleted to minimize the risk of unwanted data breaches. The data analysis buyer never receives any raw datasets, only analysis results.

Creating the world's open decentralized pool of information

By uploading the data, the owner will be rewarded with MADANA's PAX token which will be automatically transferred through the underlying smart contract. No third parties involved.

Companies and public databases can act as data producers by making their existing or new data accessible through an API into the MADANA ecosystem.

Data producers can be:

- End-Users
- Data Collecting Devices
- Applications
- IoT Devices
- Companies
- Public databases

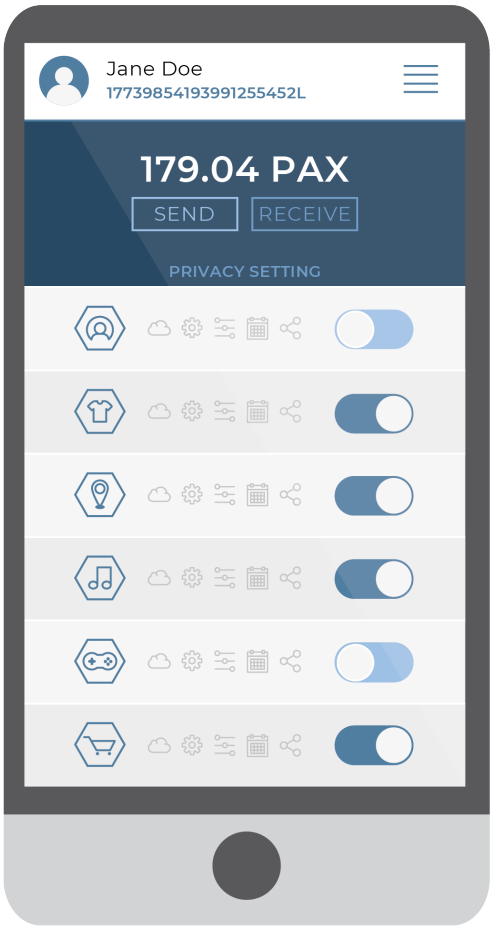


Figure 8 –
Mockup MADANA Mobile dApp Interface

DATA ANALYSIS BUYER

Anyone will be able to purchase custom analysis results on demand with optional cross-analytics insights from a continually growing pool of information, which will arise from encrypted data stored decentralized on data producers' side. Since plug-in providers will supply the MADANA platform with analysis schemes, data analysis buyer will have the possibility to choose the right analysis schemes for desired analysis results. Especially small enterprises who currently do not have access, or only limited, to the data market today can purchase specific analysis results to accelerate their business development. Since it is a defined goal for MADANA to populate the available data stock with a wide range of data, data analysis buyer will be able to request analysis results from different sources at one convenient touching point.

Providing the same access to data for everyone.

Data analysis buyers can be:

- Companies
- Institutions
- Market Research Institutions
- Every Data Analysis Professional
- Anyone

PLUG-IN PROVIDER

A plug-in provider in the MADANA ecosystem will be either an entity, which will contribute analysis schemes or integrate the MADANA privacy framework.

Plug-in providers contribute analysis schemes to the MADANA platform and can profit from their data analysis skills. Since the MADANA system protects the data producers' privacy and offers incentives for the data producers, a whole new pool of datasets – especially sensitive ones – will be available to the analysis schemes. Thus, new cross- analytics findings will unlock advanced value for the data buyers and therefore for science and society.

MADANA will provide a framework for specialists to develop analysis plug-ins which can be used within the MADANA platform by customers to process the various kinds of data.

By integrating the MADANA privacy framework in applications, app developers will secure the end-user's privacy and thus differentiate themselves from their competitors. Various possible differentiations based on privacy-focused applications are imaginable.

Every time a plug-in will be used, the creator earns a certain amount of PAX.

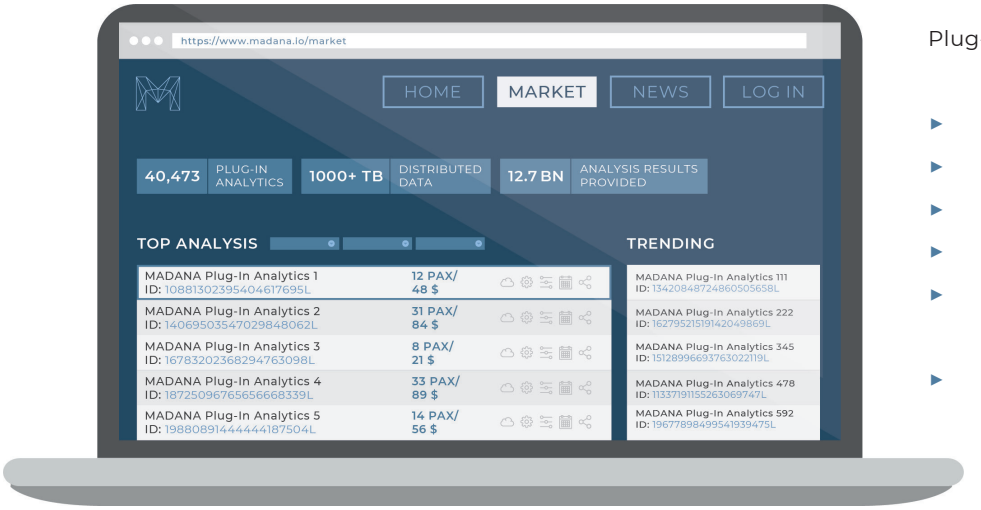


Figure 9 – MockUp MADANA WebView Interface

Plug-in providers can be:

- Freelancers
- Developers
- Data Scientists
- Analytics Companies
- Market Research Institutes
- Academic Institutions

Gathering innovative Tools for Data Evaluation and Analysis

PAX

PAX will be the essential token for the MADANA ecosystem and will be based on the Lisk Blockchain. To provide trust, process transparency and to handle rewards for the contributions, the MADANA platform will be running on the PAX token through smart contracts.

MADANA intends to implement an exchange service onto the system, to support a convenient usability for all participants.

Figure 10 – PAX Brand Logo

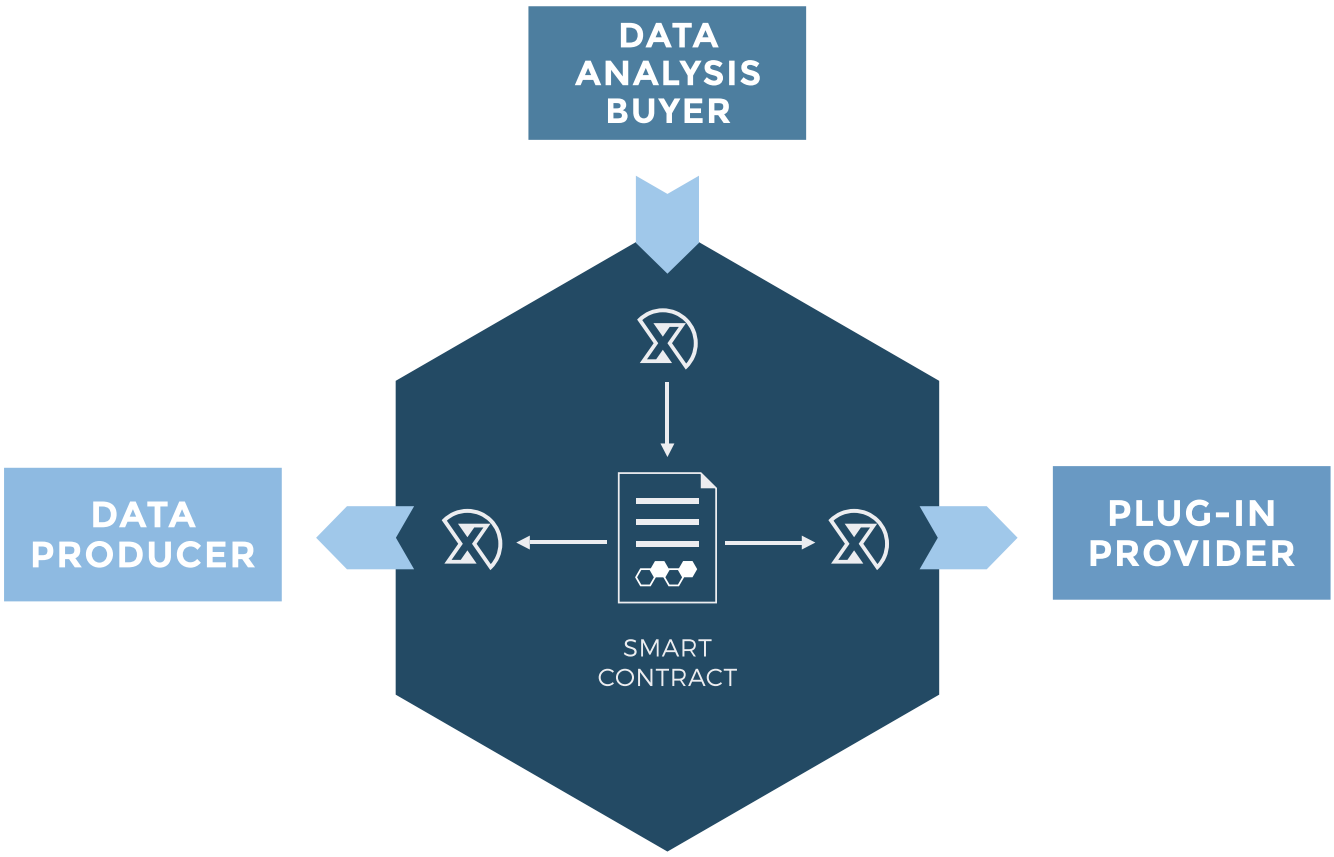


Figure 11 – Token Flow in the MADANA Ecosystem

Technical Details

This section provides a detailed description of the technical concepts, objectives, and processes of MADANA which are currently being developed. Additionally, it functions as an insight into the contents of the MADANA patent. Following the description of the eco-system's participants i.e. data producer, data buyer entities, and plug-in provider in the previous section, these will be referred to as entities. In some cases, the data buyer will also be referred to as the actor.

OVERVIEW

The product encompasses a method and a system for the protection of electronic data from origination up to data processing by third parties. With such a system, a data analysis buyer without knowing the identity of a data producer can provide funds in exchange for more unique insights.

EVERYONE IS A DATA PRODUCER

Everyone nowadays is a data producer. One example is the use of digital services such as apps, browsers or the use of social networks such as Facebook, Twitter, Instagram, and others. Every electronic device that helps people, such as temperature sensors in rooms, milling machines, pulse counters, etc., also generates electronic data that can be evaluated and is therefore valuable. However, in most cases data producers cannot freely determine how much data is collected. It is customary for the data producer to transfer the rights to their data to a service provider by agreeing to the service provider's (often non-transparent) terms and conditions in order to use the service. Large companies in particular collect and use this data for profit, without the data producer being able to control or participate in the profit. The data market is currently dominated by enterprises who are buying big sets of data from third parties that are subject to different laws of data protection. In previously known systems these enterprises decide which data is available for sale. A problem with this is that all of the data is shared, regardless of whether the data, or part of the data, contains information the originator doesn't want to share. Thus, the originator of this data is exposed to an unnecessarily high risk of privacy violations.

Acknowledged by many, these centralized data servers on which the data to be analyzed is stored are increasingly being attacked and data is being stolen by hackers. This poses an enormous danger, especially for data producers if personal data such as bank details, addresses, telephone numbers, etc., fall into the hands of unwanted parties.

USING DATA WHILE PRESERVING PRIVACY

It is therefore desirable to have an automated and modular system available which implements a procedure to eliminate the disadvantages mentioned above. The objective is to achieve this with a system which offers access to analysis results based on various kinds of data from different sources. The most important advantage of the product is that data producers' privacy will be respected, no third parties will be involved, and entry barriers and regulations will be minimized. Thus, a new ecosystem can be established where everybody can participate and profit.

THE PROCESS IN OVERVIEW

Upon requesting a data analysis result by the data analysis buyer, the system initializes a connection with the data producer and the request inherits a purpose that has been stated by the **Analysis Requesting Entity** (ARE). Based on the principles of asymmetric encryption, the data will only be accessible to the entity possessing the private key. The request for participation contains the public key of the **Analysis Processing Entity** (APE) and of the ARE for identification purposes. The unique public key of these instances can also be used by the system to aggregate even more information (e.g. what information has already been requested).

The raw data can only be accessed by the **Data Producing Entity** (DPE) so to speak the data producer and later on from the APE within a secured environment after DPE agreed to participate in the data retrieval. The latter process requires the DPE to transfer the data to the requesting entity (APE).

The data will only be used to create an analysis result based on various algorithms (the plug-ins) which are uploaded to the plug-in archive and have been validated. After processing the analysis, the APE will destroy itself along with all the inherited data. So, there is no way to disclose data based on the concept of the system.

If the ARE wants to use the data for any other purpose than stated, it has to initialize a new request and ask the data producer for approval. The concept of the system itself ensures that the above principles are met.

COMPLYING WITH THE GDPR

To illustrate MADANA's GDPR compliance this section focuses on some key clauses within the GDPR and addresses how MADANA achieves this.

Data subjects should be given notice when their data is being collected.

All data is stored client-side encrypted on the data producer's device, therefore the main system is not able to access the data without the approval of the originator. Moreover, the data producer has full control over what data the system collects on his or her device.

Data should only be used for the purpose stated and not for any other purposes.

When the Main System requires data for analysis, it sends a request to the data producer that contains the purpose for which the data is needed. After processing the data and building the analysis result the analysis instance destroys itself with all data that it inherits. If the Analysis requesting entity (ARE) wants to use the data for any other purpose than stated it has to initialize a new request and ask the user for approval.

Data should not be disclosed without the data subject's consent.

The raw data can only be accessed by the data producer and later on from the Analysis Processing Entity (APE) within a secure environment after the approval has been provided by the data producer itself.

Collected data should be kept secure from any potential abuses.

All data that is collected into the data producers' local data store. Only the originator has access to data. The data producer has to ensure that its private key is kept secret, so nobody can access the data storage without the users' consent.

Data subjects should be informed as to who is collecting their data.

Data producers are provided with an interface that notifies them whenever their data is being requested for analysis. This is necessary because before the data can be retrieved, it must be decrypted by the data producer. Every request for participation inherits the public key of the Analysis Requesting Entity, which can be used to identify the user in the system.

Data subjects should be allowed to access their data and make corrections to any inaccurate data.

Based on the data collecting interface there will be an interface for data producers to access their data along with possibilities to view / edit / delete their data.

Data subjects should have a method available to them to hold data collectors accountable for not following the above principles

The concept of the system itself ensures that the above principles are met. Beyond that, a rating system will be embedded in which all participants can evaluate each other to mark faulty suspects.

USING THE LISK BLOCKCHAIN

Written in JavaScript, the Lisk blockchain application platform allows for the deployment of custom sidechains that are secured by the mainchain. In contrast to traditional decentralized application platforms like Ethereum, Lisk sidechains allow for tailored blockchain architecture and logic to satisfy a variety of developer needs and give them the control to customize the blockchain configuration to fit the envisioned functionality of the application. To make this process as accessible as possible to developers, Lisk provides tools under their **Sidechain Development Kit** (SDK) for simple construction, deployment, and management of a given blockchain application.

MADANA will pioneer the field of deploying a sidechain on the Lisk platform and will be the first major ICO and blockchain application on it. Once the registration of sidechains is implemented, MADANA will register the name and all associated information for the future MADANA sidechain on the Lisk Blockchain. Shortly after, the team will begin building and testing on the test network.

Interoperability between different sidechains through the Lisk mainchain will allow other blockchain applications to interact with the MADANA sidechain and utilize MADANAs' platform as a **'privacy backbone'** for their needs. This is crucial because the MADANA network can grow organically along with the Lisk sidechain network as more and more entrepreneurs could leverage the possibilities MADANA want to demonstrate with its blockchain application on Lisk.

DETAILED DESCRIPTION OF THE PRODUCT

This section provides a detailed description of how the components within the system are working together to fulfill the demands stated in the process overview above.

DISCLAIMER

The product will be described more in-depth with reference to accompanying drawings. These drawings will show, by way of illustration, specific exemplary embodiments by which the product may be designed and implemented. Nevertheless, the product may be represented in many different forms and should not be construed as limited to the realizations set herein. These embodiments are provided so that this description will be thorough and complete, fully conveying the scope of the product to those skilled in the art. Among other things, the future product may be embodied as methods or devices. It may also take the form of an entire hardware embodiment, an entire software embodiment or an embodiment combining software and hardware aspects. The following detailed description is, therefore, not to be taken in a limiting sense.

DEFINITIONS

Data is generally understood to mean information, (numerical) values or formulated findings that have been obtained through measurement, observation, etc. According to the product, data is all electronically recorded information that applies to an object or event. When data is processed, data is defined as characters (or symbols) that represent information and serve the purpose of processing. Data protection law essentially refers to personal data, i.e. information about natural persons, such as gender, date of birth or place of residence.

A **data producer** can be a natural person who enters information about themselves, such as their clothing sizes when shopping online. A data producer may be a legal person or a community of persons. The data producer can also be a machine that either generates data itself by executing instructions or contains sensors that record the temperature of a room, for example.

A **third party** is any person or instance that is not represented as a data producer. For example, it is often a platform (Facebook, Twitter, Google+, etc.) that users can only use by agreeing that certain rights to their data are transferred to the platform (third party). Any broker who transfers data from one provider to a buyer and receives the data is a third party. A direct purchaser of user data is also a third party in this sense.

A **user device** can include any electronic application that has an input and an output or interface to process the data. The user device may also include any type of data processing device capable of receiving and transmitting data over a network. For example, the user device can be a computer, a mobile phone, a laptop, a tablet, a server, a smart-watch or any combination of these devices. The user device is there to record the data of a data producer. In the case of a smart IoT device as data producer, the data producer could also directly be the device.

DATA STORAGE PROCESS

One part of the product to be developed will be an application which will run on a device **[10]**. This is the data collecting part of the system: The application gains access to data sources and can trigger storage processes. A device in this case may be any computing device which is capable of receiving and transmitting a message over a network. The category of “device” may include smartphones, handheld computers, IoT devices, wearable computing devices, tablets, desktop computers, servers or any device combining one or more of the preceding devices.

The main objective of the data collecting part of the system are two software interfaces: a data-viewing interface and a connection interface. These interfaces will be open-source and can be implemented into every kind of application. To ensure the integrity of all participating processes, all executed code must be signed off by a certificate authority of the Main System (fig. 15). This is done implementing scripts that use a cryptographic hash to validate the authenticity and integrity of the code. The hash is used to verify that the code has not been modified and that the correct version is available. If this is not the case, the proceedings will be suspended.

These interfaces are used to encrypt and save different types of data that the application is generating and update the meta-information that is stored on the Main System. The application itself has to trigger events that activate the start of the processes that follow.

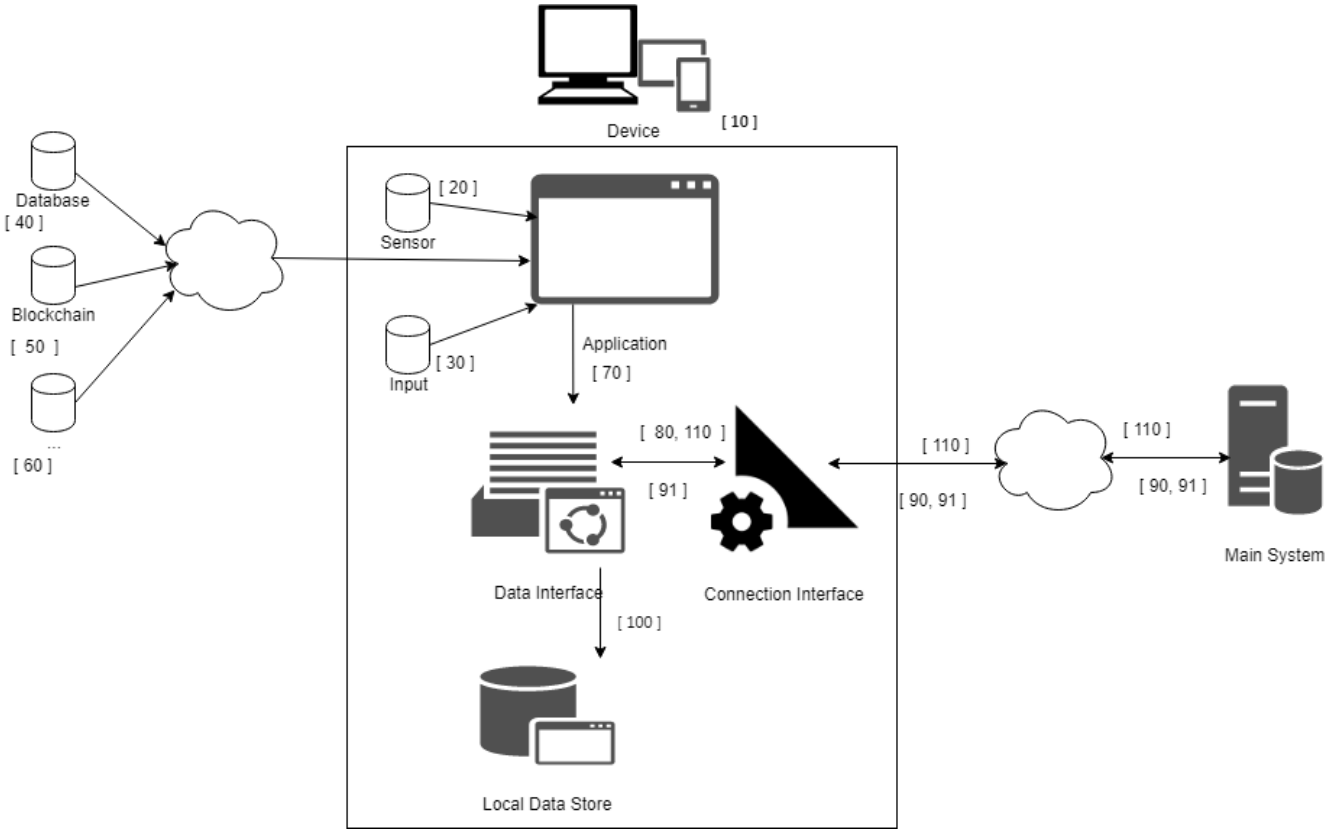


Figure 12 – Generating Data – It depicts an example of a system for collection of various kinds of data which is later used by a remote system for further processing.

An application can generate different types of data that can later on be used in the product's processes. As pictured in **[20 - 30]**, data can come from direct user input by interacting with the device or from the device's sensors or peripherals. Data can also be fetched from external sources, like for instance a database, APIs or other sources **[40 - 60]**. The processes involved in generating or fetching data within the application is not part of the product.

After the application gains access to its data sources, it can trigger the data interface to initialize a new storage process **[70]**. The data interface automatically triggers the connection interface **[80]** and authenticates the user and the application against the Main System **[90]**. The communication of these units takes place independently of the executing system via a network interface based on TCP/IP. The connection itself is secured via TLS, using Diffie-Hellman authentication methods. The Diffie-Hellman method (DHE) or Diffie-Hellman key exchange is a protocol for the key agreement. It enables two communication partners to agree on a shared secret over a public, unsecure line, which only they know and a potential third party, as an eavesdropper, cannot calculate. The agreed key is then used to encrypt the data to be transferred symmetrically. This so-called forward secrecy can be achieved by using DHE-RSA or DHE-DSA for example. To increase the security of the connection, ciphering methods based on elliptical curves can be used in ECDHE-RSA or ECDHE-ECDSA to establish a perfect forward secrecy.

Once the Main System authenticates the data producer, it responds with a data model **[91]** that will be redirected to the data interface **[91]** and used by it to restructure data before it will be saved.

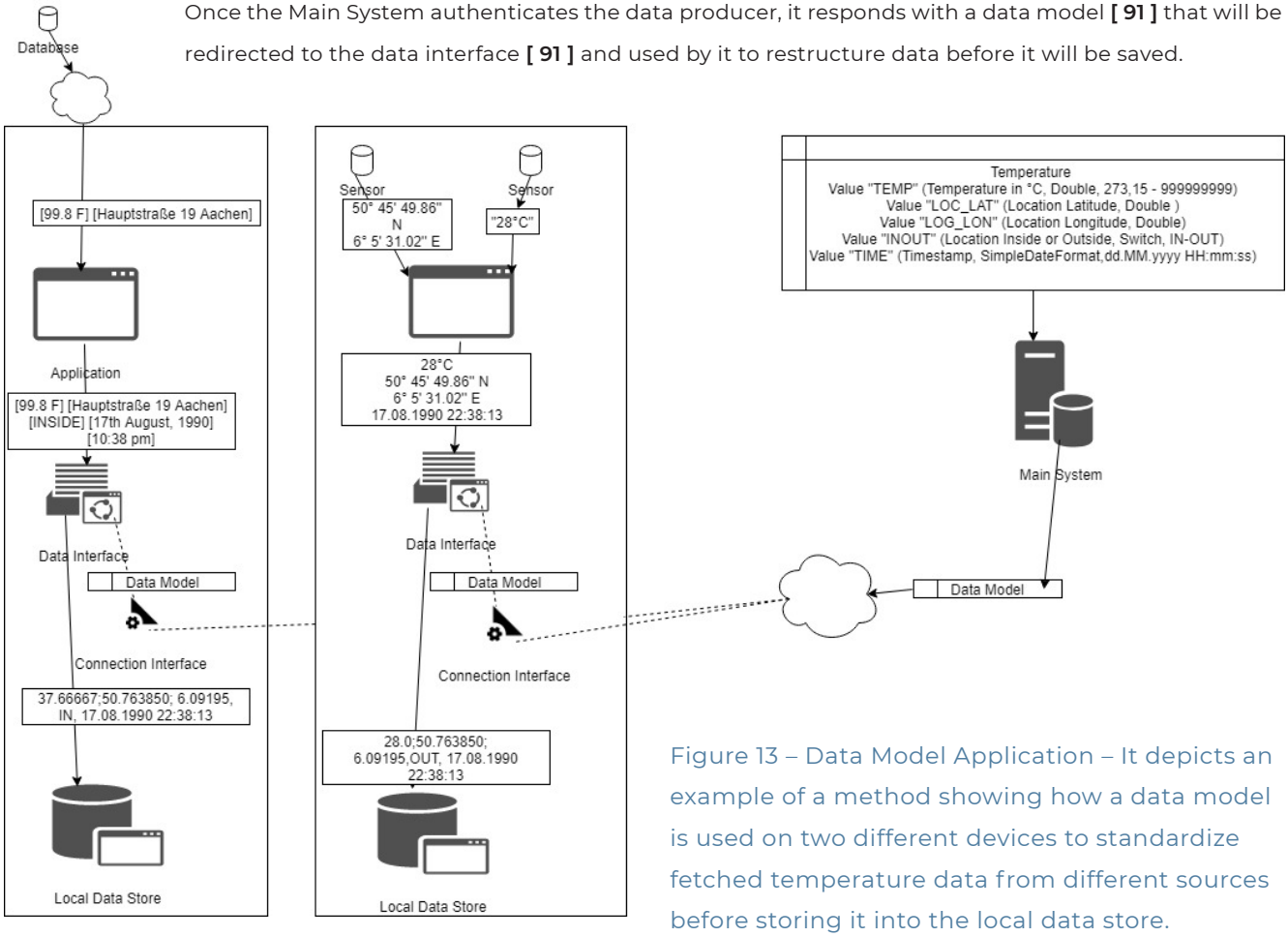


Figure 13 – Data Model Application – It depicts an example of a method showing how a data model is used on two different devices to standardize fetched temperature data from different sources before storing it into the local data store.

These data models are deployed to the data-interfaces participating in the system to define an inter-application standard for every kind of data. The data model is used within the data normalization process and plays a key role. It defines how values should be stored in the local data store and is used to identify rule violations, thus establishing a consistent level of quality and consistency. It enforces specific units, length and a structure on the stored data, making it possible to analyze the data. Only if the data is accurate, reliable, and formatted consistently, further processing will be possible. The application itself has to ensure that the con-signed data meets the requirements of the model. If the data doesn't meet these requirements, the data-interface won't accept the data and it won't be processed further. The normalization process builds on the interpretation of the data before the data is put into the local data store. The standardization process then reformats the data and creates a consistent data representation with fixed and discrete columns based on the data model. The advantage of standardization is that the conformity of the data guarantees simpler and more secure processing of the data. Moreover, all data models are provided in such a way that they comply with industry standards or other common conventions.

Once the data is validated in reference to the data model, the data-interface establishes a connection to the local data store and will ask for the data producers' encryption key, which is typically stored on the device protected by a password. The data-interface then encrypts the data and saves it **[100]**. The local data store is therefore an encrypted storage unit in which data is stored consistently, efficiently and permanently. Nevertheless, the data interface allows the connected application to delete, store, retrieve and modify information from the database that is based on globally valid data models.

When data has been successfully stored into the local data store, the data interface proceeds to trigger the connection interface and notifies the Main System **[110]** about the type of data and how many data-sets have been stored. This will allow the Main System to know which devices to connect to when a data buyer requests an analysis that needs specific data types.

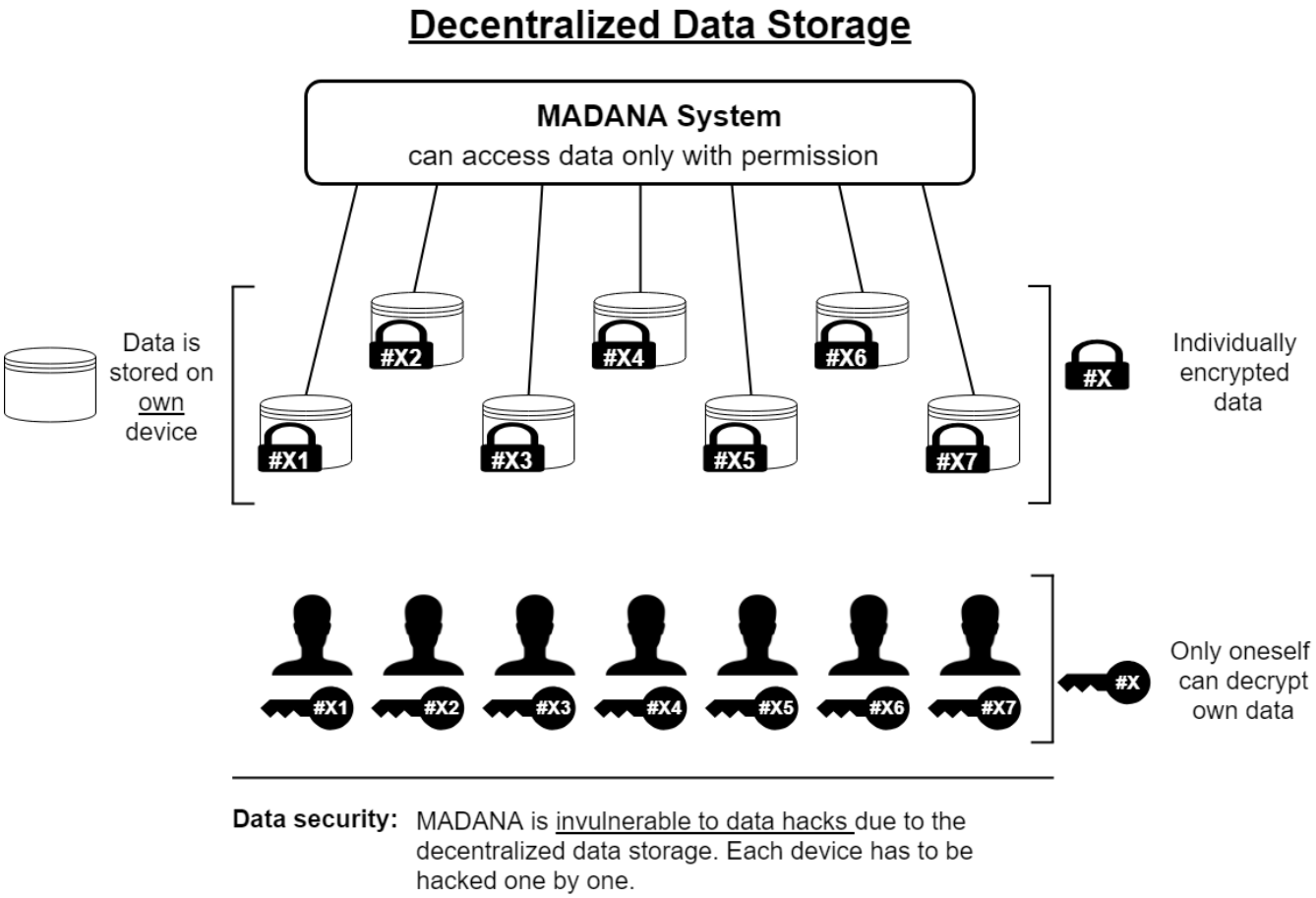
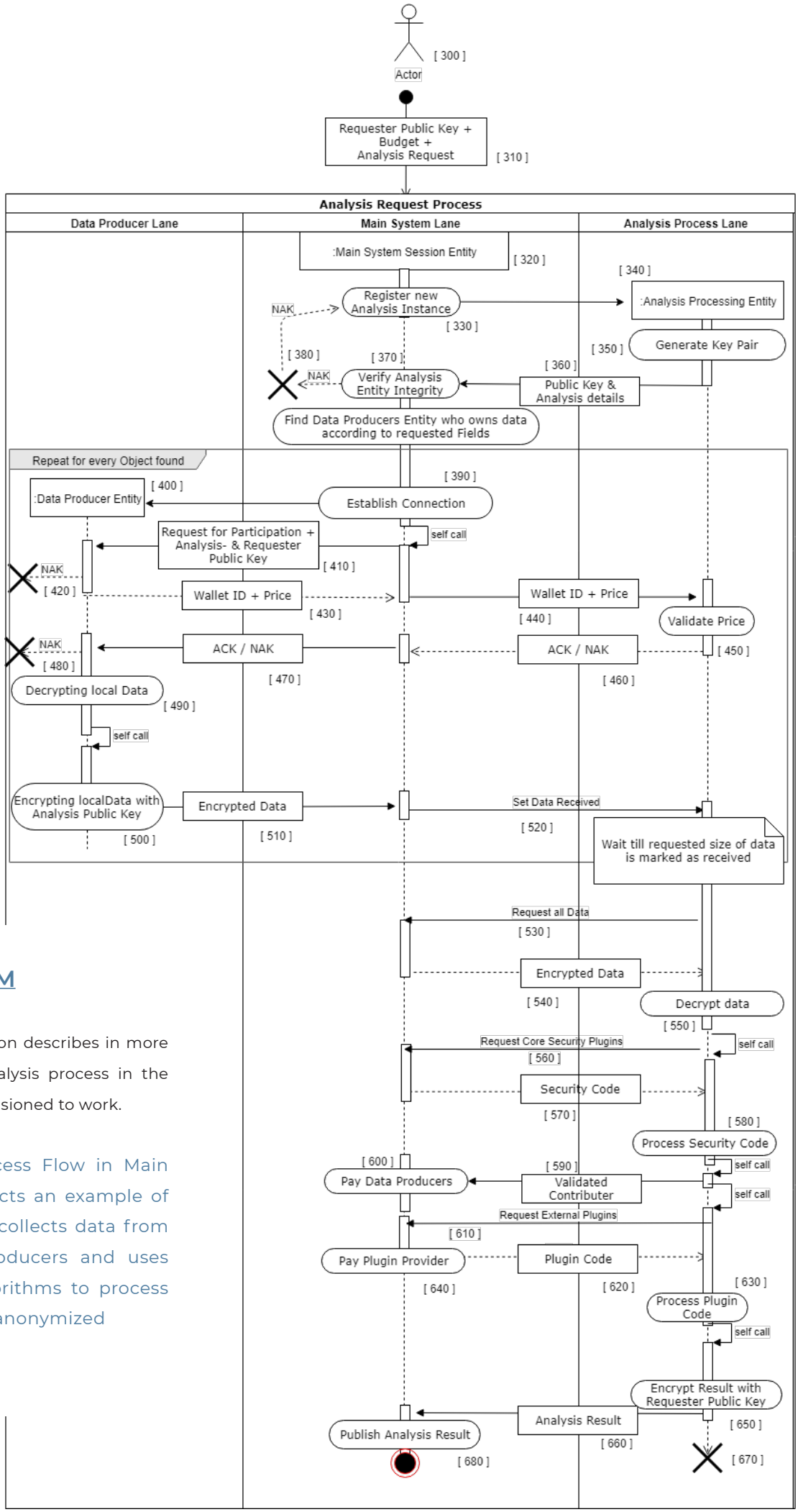


Figure 14 – Decentralized Data Storage

MAIN SYSTEM

The following section describes in more detail how the analysis process in the Main System is envisioned to work.

Figure 15 – Process Flow in Main System – It depicts an example of a system which collects data from various data producers and uses contributed algorithms to process data and create anonymized analyses.



ANALYSIS REQUESTING PHASE

The process is initialized by the ARE **[300]** which functions as the actor in the system. First of all, the actor has to register itself within the system and create a first key pair. The private key of the first key pair (henceforth mentioned as first private key) is used to access all encrypted information that will be gained over time when requesting new analyses. If the actor wants to request a new analysis, a purpose must be declared in reference to the global data model. The actor now may choose which information will be retrieved for the analysis process from data producers. Moreover, the actor can choose from plug-ins uploaded by third party developers to further process and aggregate the data for the requested analysis. The system now predicts the budget needed based on the external price, previously processed analyses, and current demand, while being dependent on the number of available data producers. If the actor agrees to the stated price, all information including the public key of the requesting entity is transferred to the Main System **[310]**.

After the request is accepted and the payment has been received, a new thread, hereafter mentioned as Main System Session Entity (MSSE) **[320]**, is generated and will take care of further processing. MSSE registers this information **[330]** and the Main System uses it to select a node from a network of connected nodes by using a suitable scheduling procedure, such as the round robin, and another instance called the APE **[340]**. A node in this case is an electronic device in a telecommunications network that actively connects to the Main System via a communication channel in order to perform certain tasks as instructed.

An APE is a stand-alone application, which is located on a separate physical unit to the Main System. It is essential for the product that the separate physical unit has a secure execution environment, i.e. a trusted execution environment (TEE) (e.g. from AMD, Intel), and supports it. The trusted execution environment provides a secure and trusted runtime environment for applications. The TEE can exist in isolation on a separate processor, directly on the main processor of a computer system, or in a chip of a multiprocessor system. The secure execution environment provides end-to-end protection by supporting protected execution of authorized code, data protection, integrity, confidentiality and restricted data access rights. Thus, this secured execution environment provides a suitable hardware environment for processing and analyzing data. It enables secure data storage and processing while protecting against software attacks that attempt to interfere with the application and gain unauthorized access to the data producers' data.

The TEE is a hardware-backed security environment running parallel to the operating system used when application requirements, like these from the APE, justify the work involved. It separates the trusted application (APE) by hardware from the main operating system and ensures the secure storage and processing of data. The TEE also offers a higher level of protection against software attacks that aim to interfere with the application to get access to the inherited data. Once a connection is established between the MSSE and the APE, the latter generates a second key pair at **[350]** which will later on be used for data encryption/decryption. The public key of the second key pair is sent to the Main System **[360]** together with integrity information, such as the signature of the running application and information about the TEE. This information is used by the Main System in order to check the integrity of the APE **[370]**. If the integrity is insufficient, the Main System selects another node from the network based on the defined scheduling procedure and validates the integrity information as described above. This process is repeated until a suitable node is found **[380]**. Once the integrity of the APE is approved the initialization stage is successfully completed.

The MSSE now proceeds and searches in its connected data storage system for the corresponding data producers according to the specified data model. In the previous procedural steps, the amount of data or data records is recorded as

metadata by the Main System from all data producers as soon as new data is generated or collected. Noticeable to say, since the metadata may also contain sensitive information, this process can and may be discarded in reference to the types of data based on the data models and the inherited metadata. For this, each data producer will define the actions taken by the Main System after being notified.

ANALYSIS REQUESTING AND RETRIEVAL PROCESS

As described in **[100]**, different types of data are stored client-side encrypted on the data producers' device, therefore the Main System is not able to access the data without their approval. Furthermore, the Main System, as a third party, cannot and must not have access to the data in order to comply with the data protection guidelines.

After having chosen the data producer entities, or DPEs, the MSSE establishes a connection **[390]** to all the relevant ones **[400]** based on the data required. Consequently, the APE sends the public key of the second key pair and the request for participation originated by the actor (ARE) to the Main System, which forwards it to the data producer **[410]**. This message also inherits a purpose that has been stated by the actor and significant information about the requesting entity itself **[300]** for identification purposes. The unique public key fingerprint can be forwarded to the Main System to aggregate even more information (e.g. what information has already been requested). Either the DPE now declines the participation in the analysis request which eliminates the DPE **[420]** process for the instance, or it returns its wallet ID and the required price to the MSSE **[430]**. After receiving the wallet ID and price, the MSSE forwards this information to the APE **[440]**. The APE now validates if the DPE's data, depending on its claimed price and the requesters budget, should be used for the analyzing process **[450]**. In reference to the result, the APE returns an acknowledged or not-acknowledged command (NAK) **[460]** to the MSSE which forwards it **[470]** to the DPE. If the DPE receives a NAK (Not-Acknowledged) the process ends **[480]**, otherwise if the DPE receives an ACK (Acknowledged), the DPE can access the data (therefore decrypting the local stored data **[490]**).

Finally, the data is encrypted with the public key of the second key pair (also called the second public key) **[500]**. Next, the DPE sends the encrypted data to the MSSE **[510]**, returning a response code to the APE indicating whether the data from the DPE has been successfully received by the MSSE **[520]**. Upon receiving this information, the data requesting stage for this DPE has ended.

ANALYSIS PROCESSING PHASE

The APE now checks if the number and type of data-sets sent to the MSSE matches what was requested. Depending on the whether the request is fulfilled, the APE either goes back to the idle state to wait for more data or starts processing the analysis. The processing stage begins with a request-for-data command which is sent from the APE to the MSSE **[530]**. The MSSE now returns all the necessary encrypted datasets **[540]** which are later on decrypted by the APE with its private key **[550]**. Because the analysis process runs within the trusted execution environment and the keys have been generated on runtime, only the selected analysis process **[340]**, has access to the original raw data of the data producers.

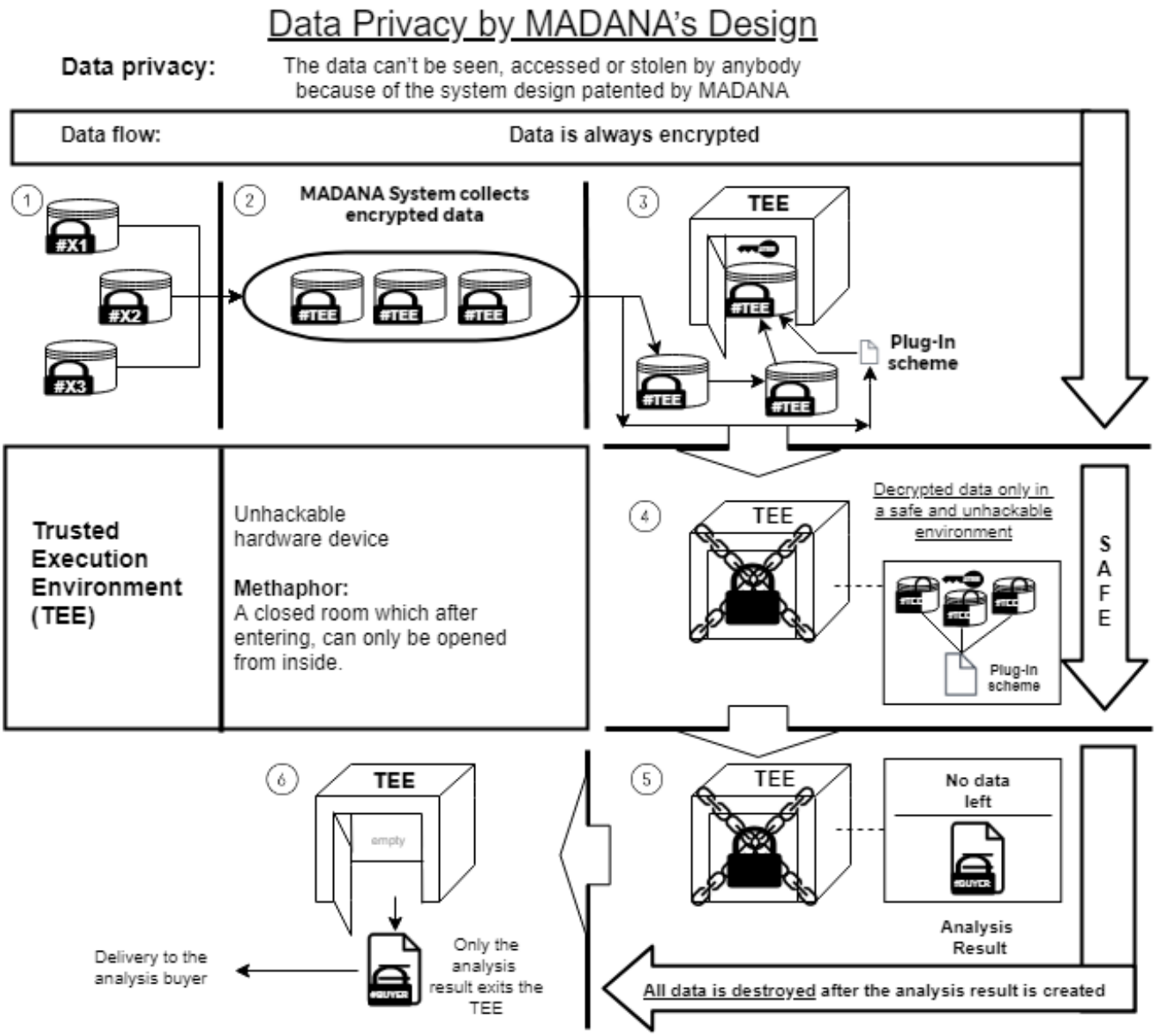


Figure 16 - Brief Overview of Data Process Flow

PAYMENT PHASE

The applied payment transaction is based on microtransactions on the blockchain and is automatically executed by the Main System. Payment of the participating data producers and plug-in providers is based on smart contracts. Smart contracts are code that is stored, verified and executed in a blockchain. Because these programs are run on a blockchain, they have unique properties compared to other program types. For example, they are transparent and interruption-proof for all parties involved. The program itself is recorded in the blockchain and enables the storage and transfer of tokens, whereby no other instance can interfere in the process.

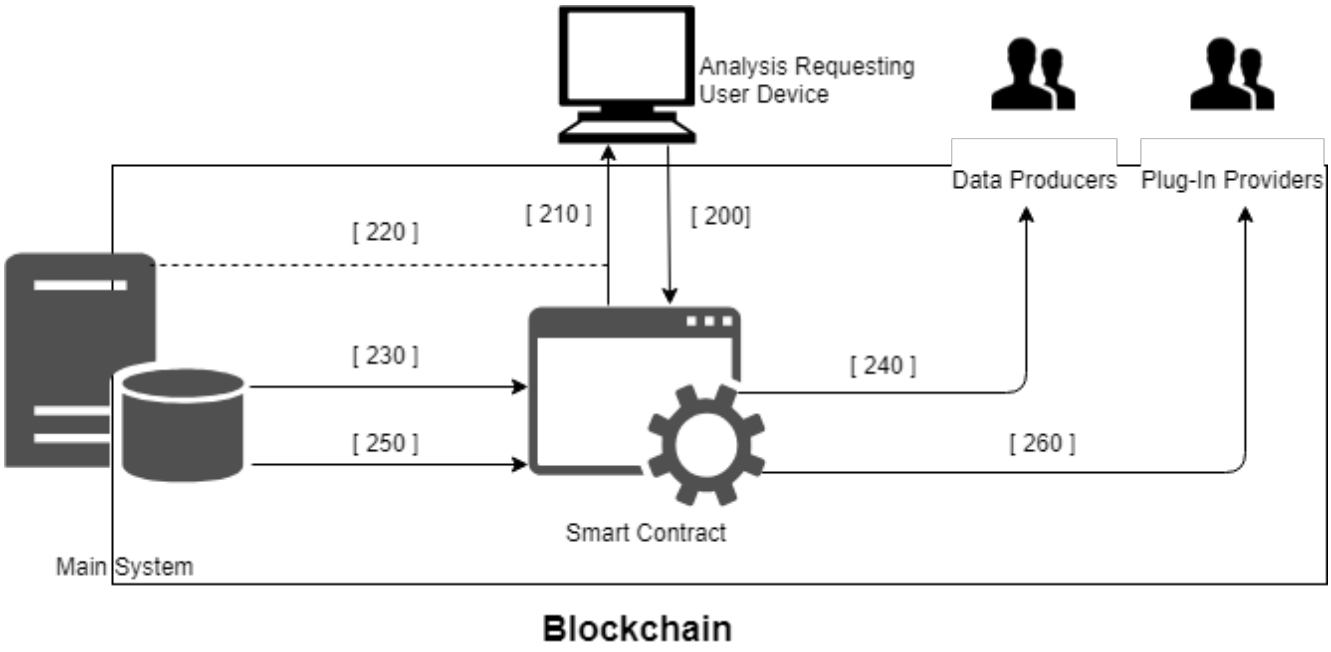


Figure 17 – Payment – It depicts an example of a system which uses microtransactions based on blockchain technology and smart contracts to pay data originators and plug-in providers for contributing to a system.

As pictured in **[200]** in Fig. 17 and in **[310]** in Fig. 15, with every new analysis request the actor automatically calls a specific method in the smart contract. The smart contract creates a unique identifier which is stored on the blockchain and read by the Main System **[210]**. After the MSSE received the analysis request in **[310]**, the MSSE waits until the block with the payment for the analysis requesting entity has been processed by the network **[220]**. This will indicate to the Main System that the budget required to pay all parties involved is now deposited. All validated contributors **[590]** are consequently handed over by the APE to the MSSE and the payment is initialized by the MSSE **[600]**. Following this, the wallet ID's of all validated contributors and the prices for their data will be transmitted to the smart contract by calling the payment function in the smart contract and handing over the previously fetched identifier **[230]**. It's important to define that the MSSE, as the owner of the smart contract, is the only instance able to call this function, thus no manipulation can occur. The smart contract now iterates through all received entries and uses the previously stored budget **[200]** to make microtransactions and pay the data producers **[240]**. Subsequently, the “pay plug-in providers” function in the MSSE **[640]** is triggered, and so all wallet IDs of the plug-in providers are transmitted to the smart contract **[250]**. The remaining budget is used to pay the plug-in providers **[260]**. Therefore, this innovative system provides a method to overcome the disadvantages of current systems and allows access to analysis results based on different types of data from different sources. All while preserving the privacy of data producers and protecting the data itself from unauthorized access. The system aims at complying with all the GDRP guidelines while offering the opportunity to fairly compensate participants for sharing their data for the analysis results.

EXPANSION STAGES

The former description of the platform is not the final target version but should rather be understood as the first publicly available version. Various blockchain-based technologies are currently developing at a rapid pace. Thus, the long-term goal of MADANA is to develop a completely decentralized platform and to replace the still central components with decentralized or distributed ones. Many of the currently available decentralized alternatives are relatively new technologies which could not yet be validated and tested effectively in productive environments. Therefore, these will only be adopted in the further course of development if it can be guaranteed that neither security, performance nor scalability of the platform could be negatively affected.

To develop a platform that can also be used and integrated outside the blockchain space for industrial purposes, we'll focus on building a stable platform that solves the problems mentioned above. Moreover, it is a big priority to build a close platform community and to align it with the effective requirements of the users instead of defining a long-term orientation of the platform that is unchangeable. Nevertheless, the following describes a listing of optional or further technical components which are currently planned to be embedded into the product after a complete evaluation.

Advanced Node Utilization

MADANA will first use its Lisk sidechain to process analysis result purchases via smart contracts. This allows for immutable, private and unbiased participation on the platform and distributes the funds automatically without anyone being able to intervene. Further utilization of nodes in the network is also possible in terms of democratic data model voting, offering processing power for the analysis process entity and managing the work distribution for this task.

Democratic Data Model Voting

One of the key elements of a working data analysis platform like MADANA are data models, which are standardized across the network. These standard data models will be created and distributed by the MADANA Main System in the first iteration of the platform but are supposed to be expanded to a democratic solution by letting participants provide new data models which are democratically chosen to be added.

Nodes as Analysis Executer

It is envisioned to give participants the opportunity to take part in the analysis process by offering processing power. Meeting hardware and software requirements, a node can claim a job through a smart contract and would deliver the analysis result. The software that MADANA wants to provide for that case will ensure that the node owner does not tamper with the process. To further incentivize the node owner to process the analysis fast and properly, he would need to make a deposit which the smart contract releases after the successful execution of the analysis process. Such a node would have the responsibility to provide enough processing power for the analysis and would earn PAX when it delivers.

Decentralization of the Main System

In the first version of the platform, the Main System will be a cloud application. However, the first step after evaluation will be to switch this over to a decentralized system. The advantage of starting with an application running in the cloud is that it can be accessed at any time by different devices, whether stationary or mobile. Further, it is proportionally easy to deploy new updates to the central server which will be essential in the first versions of the platform. Decentralized applications have the advantage of being particularly secure and reliable and also data manipulation by unauthorized persons can be overcome. To eliminate this single point of failure in the cloud, one of the first goals in the expansion stages will be to decentralize all modules of the Main System as fast as possible.

Distributed Result Validation

One future potential of MADANA is the implementation of a distributed network of APEs. By meeting specific requirements of software and hardware, volunteering entities can host the analysis process and get PAX tokens as a reward. An important question is how MADANA could ensure that the APE returns the correct and desired result which has been requested by the inquirer. The answer is, by validating the signature of the code to be executed. This will ensure that only the desired code will be executed.

Moreover, it is conceivable to go one step further and execute the analysis process simultaneously on an odd number of previously validated nodes and then compare the respective results with each other afterward. The described process would rule out whether an analysis that is faulty for undetermined reasons would be sent back to the requesting entity. Corrupt APEs could be quickly detected in the network and marked, which would have a positive effect on the quality of the analyses. The approach of distributed analysis processing would per se be vulnerable to adoption by a majority of corrupt APEs but should be interceptable by the other security measures implemented in the system.

Backup Strategy

Data is continuously collected and stored in the datastore by the data producer. Consequently, the datastore could become so large over a longer period of time that the storage capacities of the respective device could be significantly occupied by MADANA's service. This includes devices with relatively small capacity, such as mobile phones. As a result, it will be absolutely necessary to be able to store the data on an external data storage. This requirement would also solve problems that would arise when exchanging the data generating hardware, as it also occurs regularly with mobile devices, for example. To participate in the analysis processes, however, it is imperative that the data producer has access to the respective data records in order to forward them to the APE in the further process. For this reason, the plan is to develop a backup strategy in which data producers can access the respective data records promptly in the event of a request and agreement on their part. It will therefore be necessary to integrate appropriate services onto which the data producer can store his/her datastores. Since the datastores are encrypted, data security is less of a problem than the cost of storage. In recent years, some decentralized storage solutions have been developed which are many times more cost-effective than the cloud storage solutions of larger vendors. In the course of development, we will therefore make great efforts to enable and integrate the possibilities of storage in these solutions.

Homomorphic Encryption / Evaluation

If the sum of matching datasets is to be calculated when creating an analysis based on the data model, homomorphic encryption of the respective numerical values can be used to avoid the transmission of plain text to the APE. This would allow the possibility of decrypting the data at runtime of the analysis process within the TEE of the APE. In this case, additive homomorphic cryptosystems could be used, whereby the homomorphic nature of the cryptosystem causes a multiplication of the ciphertexts to result in the addition of contained plain texts modulo 2. As a result, the processing of plain texts is not necessary for MADANA in the scenario described. Therefore, a suitable implementation of cryptosystems such as the Goldwasser Micali cryptosystem could be integrated in the interests of the data producers and, thus, also in the interests of the platform in order to make the attack on the APE and its environment even less interesting for potential attackers.

The implementation of a fully homomorphic encryption system would not increase the rounds in communication between the components which would slow down the analysis processing. Nevertheless, it would come with huge computational costs therefore making it somewhat impractical in MADANA's environment, where most of the computation would be done on a data producer's device with potentially slow processing hardware. Therefore, the implementation of FHE features will be evaluated and mainly tested within the test environment where we will compare the advantages and disadvantages in relation to the current conceptual design of the system.

Scenarios

MADANA will be a system with several novel main properties: a new approach to data security, direct incentives to input data and a marketplace anyone can participate in. Through this combination, it can be expected that thousands of new use cases will emerge as MADANA will offer a generic solution and is suitable for all data-driven industries. For a better understanding, three potential use cases of MADANA for major industries are presented in this chapter.

IOT INDUSTRY

The Internet of Things has become an essential part of today's world of big data. As it merges the physical and virtual world, it comprises all internet-connected devices that produce, exchange and report data. This data needs to be collected and analyzed. The European Commission has stated, that Internet of Things "(...) represents the next step towards the digitization of our society and economy, where objects and people are interconnected through communication networks and report about their status and/or the surrounding environment." [15]

Forecasts for the industry are more than optimistic. According to Gartner [16], the industry size will increase from 8.4 billion in 2017 to 20.4 billion connected things by 2020, with the consumer segment being the largest user group of connected things. Research from Statista [17] shows similar prognoses.

Alongside such promising growth forecasts come some not insignificant challenges that will affect the industry. With technological and regulatory issues being smaller obstacles, the capacity to deal with a large number of diverse devices, the scalability and the security conditions will put pressure on industry participants. MADANA will be an answer to these problems, as it is envisioned to ensure data security, through highest technological standards and decentralization. Giving the control of data from devices to the device owner, is MADANA's main premise.

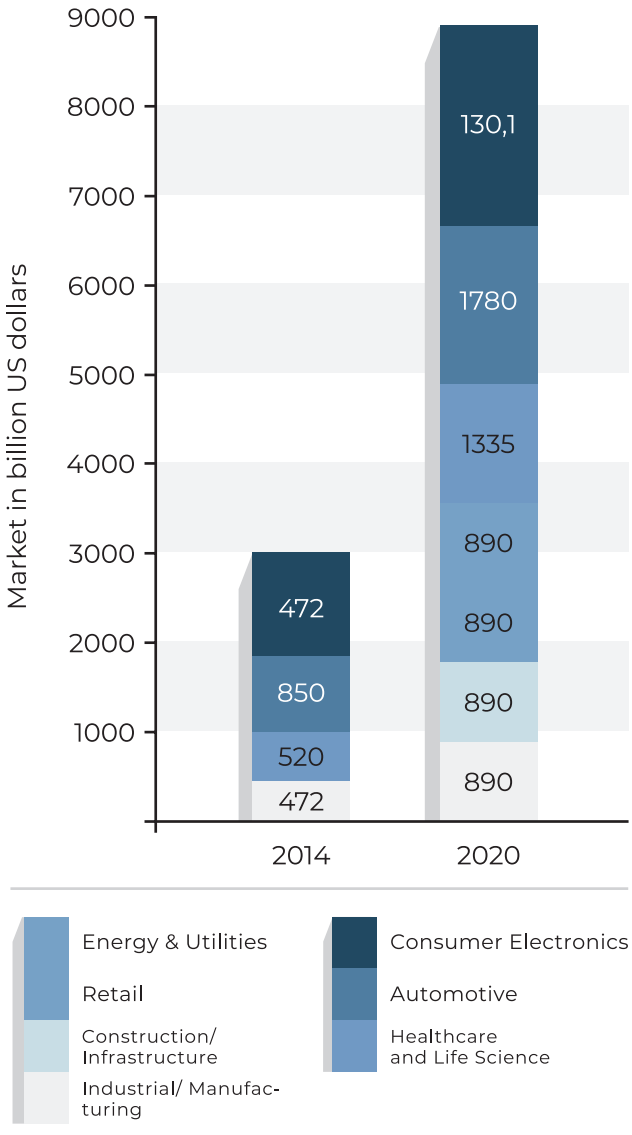


Figure 18 - Size of Internet of Things Market worldwide in 2014 and 2020 by Industry (based on [17])

[15] European Commission (2018): The Internet of Things, [online]
[16] Gartner Inc. (2017): Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016, [online]
[17] Statista (2015): Size of the Internet of Things market worldwide in 2014 and 2020, by industry (in billion U.S. dollars), [online]

In addition, companies like IoT-device producers will benefit from accurate standardized format analyses results, and optimization in processes and product design. MADANA's goal is to enter both the smart home and machine data markets.

USE CASES IOT

IoT is on the uprise and it is predicted to become a reality by 2022 as stated in a workshop report organized by the European Commission on January 13, 2017, in Brussels [18]. In this workshop the participants evaluated 30 baseline principles regarding IoT security, privacy or both. These were often similar cross-sectoral with the sectors being 1.) smart appliances and wearables 2.) connected/autonomous vehicles 3.) industrial IoT and 4.) Smart Cities. To make IoT suited to these baselines, a trusted IoT label (19) was suggested to make privacy and security measures more applicable to the end user. These are some of the baselines that are referred to the first sector but also some of which apply to all others [18]:

1. Data control by the user – in any phase of the data lifecycle and product lifecycle
2. Transparency and user interface control – empower the user to obtain sufficient knowledge of what its devices and related system are doing and sharing, even if it concerns machine to machine (M2M) communications and transactions
3. Encryption by default – in communication, storage and otherwise
4. Relatively high level of baseline – when safety is at stake, or critical infrastructure or national safety can be materially impacted
5. Life Time Protection – give security, safety and privacy protection over the full lifetime
6. Updatability – trusted and transparent updates only by authorized parties, not by malicious actors
7. Identity protection by design – decoupling personal identity from device identity

Serious problems occur when a smart device producer aims to offer smart services or improve their product in a way that requires processing of large amounts of sensitive, identity revealing data to reach the quality levels

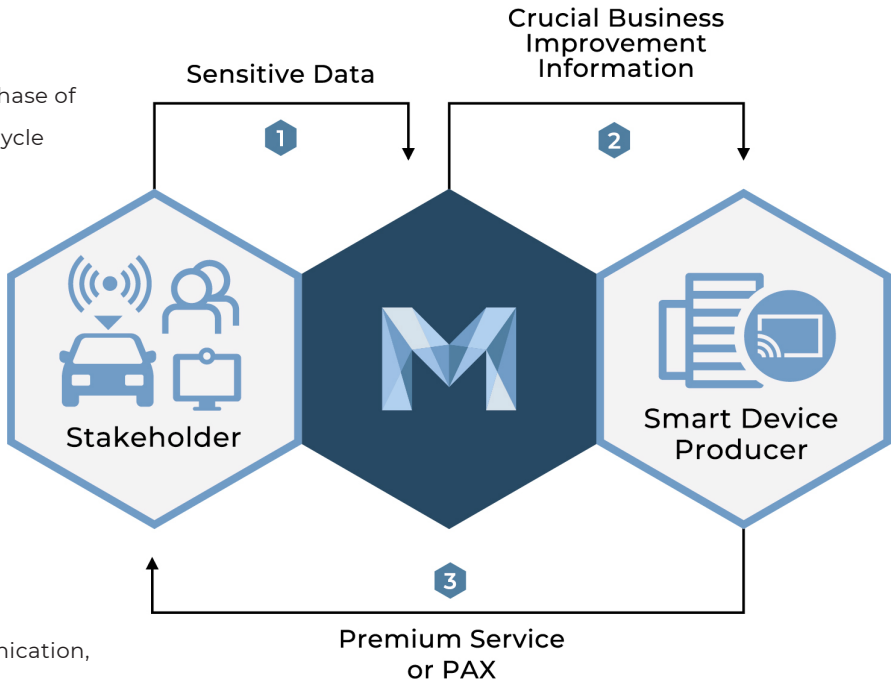


Figure 19 - Use Case IoT Sector

[18] European Commission (2017): Report on Workshop on Security & Privacy in IoT, [online]
[19] European Commission (2016): ICT Standardisation Priorities for the Digital Single Market, [online]

required. To meet the mentioned baselines (especially 1, 2, 3 and 7), a smart device producer could utilize MADANA to have it anonymously process the sensitive, identity revealing data and gain improved insights on product and service quality. Whenever this sensitive data is required to fulfill the targeted service or product quality the smart device producer could make a transparent analysis request and pay the stakeholder with PAX. In this way, a trusted IoT economy could emerge that incentivizes the service provider to process data in a non-privacy and non-security invasive way. User control, encryption, transparency and identity protection would be fulfilled and the usage of MADANA could be seen as the trusted IoT label mentioned by the European Commission. Lastly, the smart device producer could acquire needed PAX tokens from the very same stakeholder in exchange for premium services or similar.

EHEALTH INDUSTRY

Deloitte [20] projected the global healthcare spending to be USD 8.73 trillion in 2020. The growth rate of global healthcare expenditure is raising: 4.1% for 2017-2021 compared to 1.3% for 2012-2016. The reasons for the growth are the aging and increasing populations, developing market expansion, advances in medical treatments, and rising labor costs. [20]

How is the healthcare industry evolving considering the challenges it already faces and will face in the future?
Smart Healthcare will be one key aspect as Deloitte describes it in their outlook for the Health Care Industry:
"With quality, outcomes, and value the watchwords for health care in the 21st century, sector stakeholders around the globe are looking for innovative, cost-effective ways to deliver patient-centered, technology-enabled "smart" health care, both inside and outside hospital walls." [20]

Smart Healthcare, also referred to as eHealth, "is delivering solutions to tackle the increasing need for better diagnostics and more personalized therapeutic tools" [20]. For example, this comprises the usage of technology to diagnose more accurately, treat illness and deliver care or also keeping the patients informed and actively involved in their treatment plans, e.g. connected medical devices for use at home [21]. The growth of eHealth increases the need to collect, store and analyze more and more data. Hospital expenditures on data analytics will reach USD 18.7 billion by 2020, from USD 5.8 billion in 2015 [20]. Apps, fitness trackers, health monitors, various sensors, and electronic medical records already produce a vast source of data. In the future, large eHealth data analyses can be used to prevent medical errors for example prescription errors, e.g. 400,000 people die from preventable medical errors in the US each year [22]. Further, big data can be used to improve the patient experience by helping determine what patients really want. Epidemiology, clinical trials, genomics, health insurance, medical billing operations and patient care will generate data that will lead to advances in patient and healthcare operation [23].

This growing involvement of data in the healthcare industry brings up issues that stakeholders have to deal with: Reliability of data from personal and/or other systems, data ownership and responsibility, confidentiality amidst today's cybersecurity challenges (keeping the data safe), and data monetization.

In summary, it can be stated that the healthcare industry's key challenges regarding the growing importance of data usage will be to analyze the vast amount of data while keeping the data safe and prevent data misuse. We at MADANA aim to help stakeholders in the healthcare industry to cope with the challenges.

[20] Deloitte (2018): Global health care outlook, The evolution of smart health care, [online]
[21] Statista (2015): eHealth – worldwide, Statista Market Forecast, [online]
[22] Healthcare IT News (2015): Curbing medical errors with the cloud, [online]
[23] Forbes (2016): The Future Of Health Care Is In Data Analytics, [online]

USE CASE EHEALTH

With healthcare benefiting more and more from the achievements of big data and AI, data seems to need greater accessibility and actuality to this industry [24]. Healthcare professionals could utilize MADANAs plug-in providers, who could be other medical professionals and scientists from all over the world and could offer their knowledge as a service. The health insurer could instantly check and validate if the offered service is covered by the insurance policy of the patient. In this particular example, the patient and the healthcare professional would work in conjunction with the patient being the analysis buyer and data producer at the same time. When the healthcare professional would check the patient with his in-house medical devices, the data produced is encrypted with the patient's public key automatically. With the doctor knowing the common data model he could initiate a MADANA analysis together with the patient. In this analysis, not only the direct medical information would get into consideration, like the recent in-house brain scan or the whole medical history, but also indirect data like heart rhythm information from a smartwatch, diet information from fast-food delivery services etc. This way, doctors could take more factors into consideration and offer personalized treatment to patients, which could reduce the risk of mistreatment, adds transparency and secures the most sensitive patients' data from hospital databases breaches while having it available on demand.

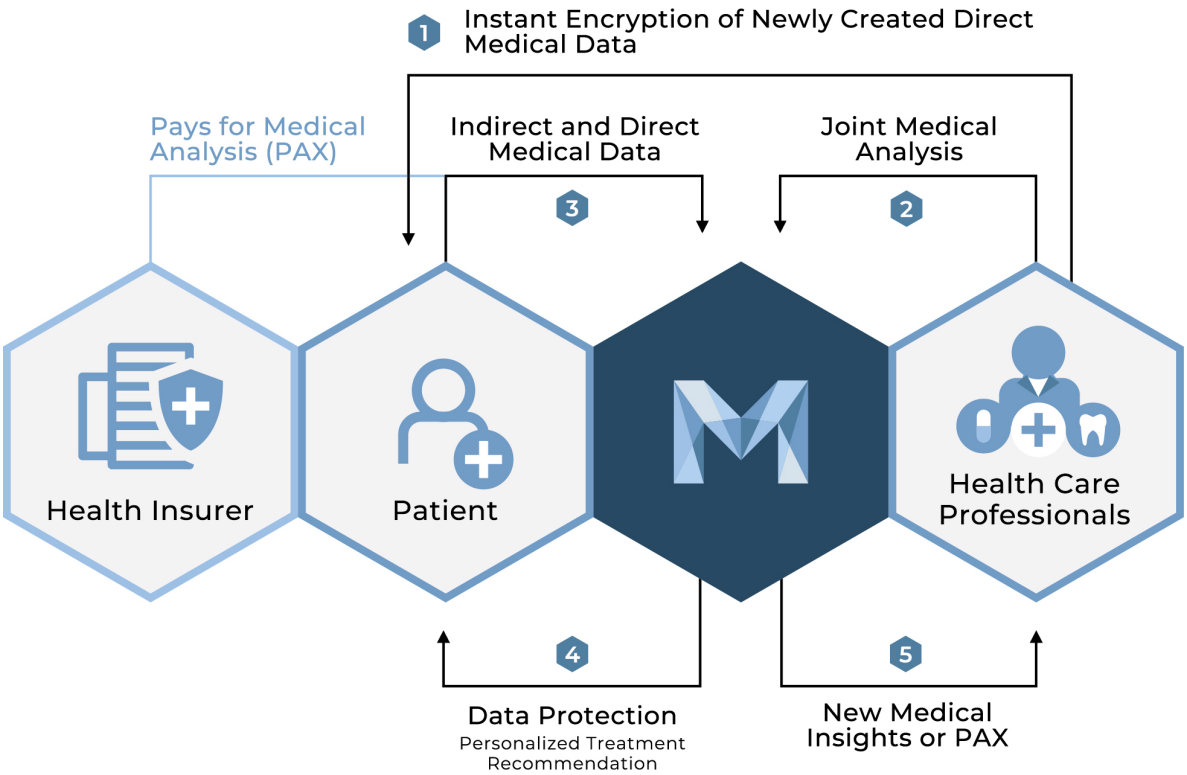


Figure 20 – Use Case eHealth Sector

[24] IBM Watson Health (2018): Bringing confident decision-making to oncology, [online]

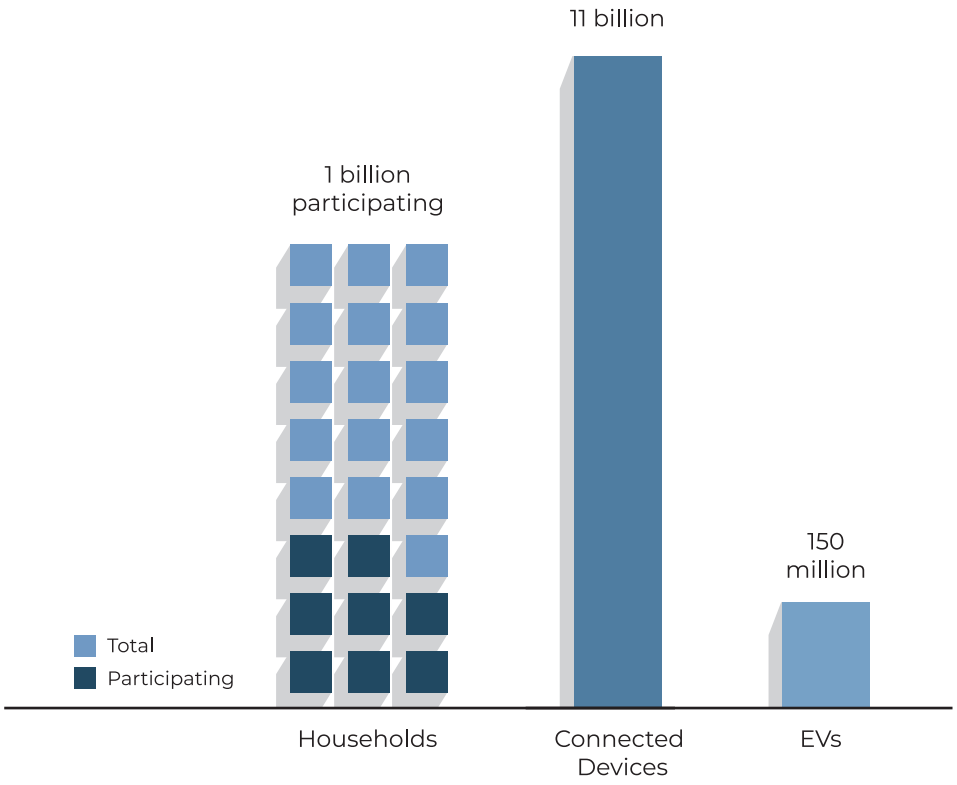


Figure 21 – Smart Demand Response (based on [26])

ENERGY INDUSTRY

The global energy consumption in 2017 was about 13 billion toe (tonne of oil equivalent) and is projected to be almost 18 billion toe by 2035. The reasons for this huge growth in consumption is that "the world economy is expected to almost double over the next 20 years, with growth averaging 3.4% p.a." [25] and therefore energy demand will rise.

The digitalization also plays a major role in the energy sector. Investments by energy companies in digital electricity have risen sharply over the last few years. As in other sectors, digitalization will also revolutionize the entire energy value chain over the next few years. Especially with the widespread introduction of intelligent, digital electricity meters, so-called smart meters, the flood of data and thus the possibility for analysis will continue to increase. By 2040 1 billion households with 11 billion connected devices and 150 million electric vehicles (EVs) are estimated to exist [26]. These devices will certainly produce data which puts the emphasis on the need for data analysis. A study of PwC [27] in Austria shows that 70% of the electricity suppliers currently do not use data analysis when introducing new products and are thereby decisively behind the normal industry by 42%. Further, more than a third of respondents in the study says that the storage of data for analysis is not planned for the next five years. This indicates that there is a huge potential for big data analysis in the energy sector. By applying data science in the energy industry costs can be cut, e.g. by improving maintenance and by monitoring equipment, investments can be optimized e.g. by efficient internal resource allocation. Risks can be reduced e.g. by improving public safety through efficient monitoring and oversight [28].

It can be stated that the increasing demand and the trends towards interconnectivity of electricity produces a large pool of data, which is constantly subject to hacker attacks and manipulation. Nonetheless, this pool of data needs to be analyzed for the vantages mentioned. Therefore security, privacy, and control over the growing data is highly needed.

[25] BP (2017): BP Energy Outlook, [online]
[26] International Energy Agency (2017): Digitalization and Energy 2017, [online]
[27] PwC (2018): Energie-Studie: Digitalisierung, [online]
[28] Harpham, B. (2016): How data science is changing the energy industry, [online]

USE CASE ENERGY INDUSTRY

One of the most exciting utilizations of data in the energy sector is grid load prediction. With renewable electricity now accounting for over 24% of global electricity production the trend is clear where our future lies [29]. But with benefits of renewable energy come also the challenges like nonhomogenous weather or solar conditions which are responsible for huge stress tests on the national grid systems, for example the solar eclipse of 2015 in Germany [30]. Clever grid load predictions, as stated in a document for Siemens EnergyIP Analytics product [31], can provide with cost reduction, lower grid maintenance and allow for more agility by seeing grid load trends and react accordingly. With the introduction of smart meters and other industry relevant sensors, data is becoming a crucial part in the operative business of power suppliers. With MADANA, intelligent analytic tools could search and acquire in a broader pool of information for relevant prediction enhancing data. For example, with the uprise of electric cars, drivers could share information when they are estimated to be home again and plug-in their car for charging, or the information on the purchase of crypto mining equipment. Though being sensitive data for the Grid-User, all this could be relevant data to power suppliers to gain insights on future grid load and they would surely willingly pay for this information reasonably. Grid-Users and power suppliers would maintain a healthy relationship, improving energy efficiency and thus lowering energy costs. This would work particularly well with MADANA because the power supplier only would need one analysis result, mainly the energy load at a particular time and place. Thus, a privacy ensuring platform like MADANA would incentivize grid- users for participation. Analysis plug-in providers could be companies like Siemens offering cutting-edge analytics tools like EnergyIP – Load Forecasting and monetize their know-how on every scale.

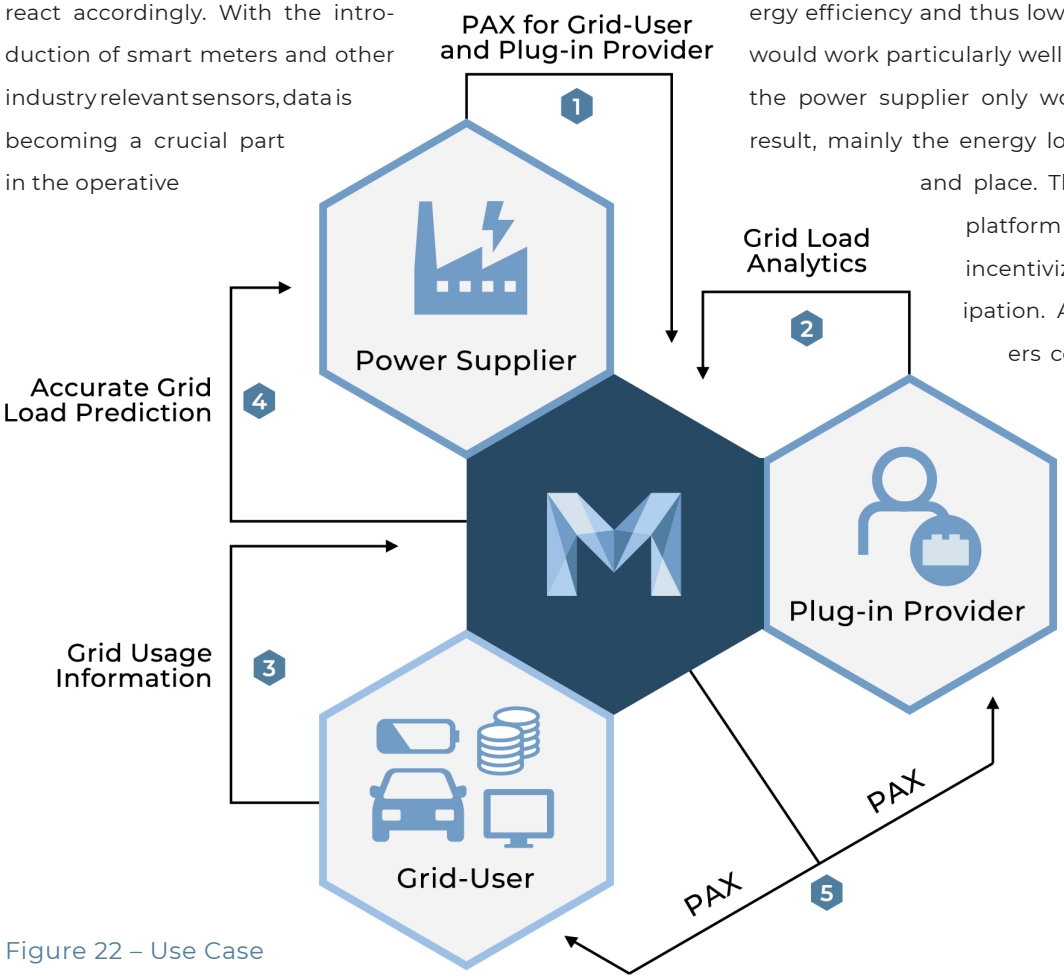


Figure 22 – Use Case Energy Market

[29] REN21 (2017): Renewables 2017 Global Status Report, [online]
[30] Clean Energy Wire (2015): Energiewende passes solar eclipse stress test, [online]
[31] Siemens AG (2016): EnergyIP Analytics Suite: Load Forecasting, [online]

Product Recap

MADANA's ecosystem approach is not that easy to understand at first glance. A short product recap summarizes the preceding chapters.

MARKET FOR DATA ANALYSIS

Using blockchain technology, three main data market participants will be able to operate on the decentralized MADANA ecosystem. Individual data producers will be given the opportunity to provide and monetize their data, which will be encrypted and cannot be manipulated. This data thereafter will flow anonymously into data analyses, which results companies will be able to buy without gaining access to the raw data itself. The analysis plug-ins will be provided by either analytics companies, freelance developers or data scientists, who will monetize their skills and knowledge in a fair way.

PAX & SMART CONTRACTS

Transactions will run on the basis of smart contracts and the MADANA token – PAX. Data analysis buyers will purchase analysis results with PAX. One PAX stake will flow directly to the individual data producers, another to the plug-in providers and a small one to MADANA for maintaining the system.

SCENARIOS

The next step for MADANA is to start pilot projects in order to test the marketability of the ecosystem and jointly collaborate with strong partners to gain valuable insights and finalize a well-rounded product. Since the MADANA solution is a generic one, it is applicable in many data-driven industries. MADANA is aiming for positioning itself in industries like machine data, energy, eHealth, data analytics and IoT among others.

TECHNOLOGICAL SOLUTION

MADANA is developing a decentralized data analysis market. It strives to provide a fair platform, that allows for data conversion into analysis results for anyone; companies, research institutes, and other interested parties, while offering data scientists and developers the opportunity to monetize their skills.

POSITIONING

The offering of MADANA is believed to be unique, as decentralized data analysis with no access to actual data does not exist yet. Nevertheless, the data industry is rapidly growing, and new centralized and decentralized business models emerge on a weekly basis. For that reason, a sophisticated positioning of MADANA is crucial for a long-lasting success.

Differentiation

MADANA's business model in the data industry is a completely new approach. On the one hand, it attacks the current business models, where data is collected and then sold - whether directly to customers or after generating insights. Existing big digital platforms and services have specialized in gathering information through products like app plug-ins that are implemented in many third-party apps. These companies have a straightforward business model: they can easily sell the data in a direct way and therefore have less technical difficulties to overcome. Nevertheless, these companies must be careful to ensure the data privacy required by law. More data scandals (e.g. Yahoo, Equifax, Facebook, Cambridge Analytica) could seriously harm that industry.

The second group MADANA attacks consists of upcoming open data markets that are creating new types of business models. These can be divided into two distinct groups: (1) new open data markets with a centralized model; (2) new open data markets with a decentralized, blockchain-based model. The first group has the advantage of an easier implementation but cannot really offer distinctive differentiation towards traditional data markets. At first glance, the second group of blockchain-based data markets could be seen as a direct competitor of MADANA.

MADANA differs from all other direct competitors in that it does not offer direct data market reselling. It offers a model with decentralized analysis.

MADANA is a modular system that brings together data producers, analysis providers, and entities looking for information. MADANA focuses on data protection for producers and on the quality of data and analysis programs. As listed in the chapter "Expansion Stages", MADANA will try to complement and integrate other, at first glance, competing products, such as peer-to-peer data markets, data handling protocols and/ or AI analysis products, into the system. MADANA is not only a direct provider of a specific technology solution. The possible uses go far beyond that. Rather, MADANA wants to offer a universally deployable layer system that provides simple, secure and profitable access to new technologies for data market participants.

The system is to be based substantially on the wants of the participants. It sees itself as a platform which serves as the exchange between the participants in order to enable a regulated and beneficial handling and monetization of data for all participants.

Strategic Positioning

As a blockchain company challenging the current status quo of data handling, MADANA considers it necessary to adequately position the project and its technological product in a way that will guarantee the company's long-term success. In this context, several critical factors will be addressed.

POLITICAL FACTOR

Data privacy and data control of citizens and companies are being legitimately propagated lately by the European Union through various programs and laws. Therefore, MADANA is in regular contact with individuals from the high-ranked European Parliament, the European Commission as well as the German government. In this way, MADANA can actively propel the social change for better and safer data handling.

ECONOMICAL FACTOR

MADANA's ecosystem is meant to be used in cooperation with companies operating in data-driven sectors. MADANA is building up partnerships with leading companies such as Capgemini to develop a symbiosis where their knowledge together with the MADANA platform will be leveraged. Together with the expertise and network of the advisors from different important spheres, like consulting, finance, manufacturing, science and blockchain industry, it is expected that MADANA will multiply its resources and social impact.

SOCIAL FACTOR

The need for data privacy in the digitized world is growing, but it is far from being achieved, as many data scandals prove. MADANA will be providing a solution for data producers, particularly end-users, that raises awareness for data privacy issues and provides end-users with a tangible tool to get back control over their data. Further, having started in Aachen and now operating out of Berlin, the team behind MADANA is helping to build up the German blockchain environment despite the strong regulatory parties in Germany.

LEGAL FACTOR

Regarding the legal framework in Germany, it is possible to generate tokens and to launch them. Prior to that, MADANA has filed an inquiry with the German Federal Financial Supervisory Authority (BaFin) to align the envisaged token launch with any regulatory requirements. Well-reputed German blockchain lawyers are supporting MADANA in this process. Obtaining an affirmation of the BaFin under more stringent conditions will help MADANA pave the way for further German based projects to go the harder but sustainable way. Additionally, the MADANA ecosystem was filed for a patent. This way, MADANA is always striving for having a head start over big internet corporations.

TECHNOLOGICAL FACTOR

Being a high-tech company especially in the digital security sector, MADANA's ecosystem must always be developed at the cutting edge of technology. By collaborating with national and international research universities and institutions, MADANA makes every effort to ensure its technological progress. Additionally, by implementing the Lisk blockchain, MADANA sees further technological advantages over distinct distributed ledger technologies.

MADANA, on the one hand, relies on classic, proven strategies in the business world, and on the other hand it breaks new ground and uses scalable blockchain technology. In this way MADANA combines the best of two worlds. MADANA positions itself as an intermediary between classic business and the revolutionary crypto-world – located in Berlin, the European crypto-capital.

ROADMAP

To succeed as a young company the following Roadmap will be followed. It is designed to develop MADANA in the long term to reach the vision, but also to get traction fast with a minimal product and to bring value into the ecosystem by utilizing a scaling strategy. Partnering with some of the big four consulting companies is expected to help MADANA to scale into various industries much faster by solving data-handling issues in these industries. Positioning the MADANA technology in the business-to-business sector will most probably accelerate the expansion into the business-to-consumer sector.

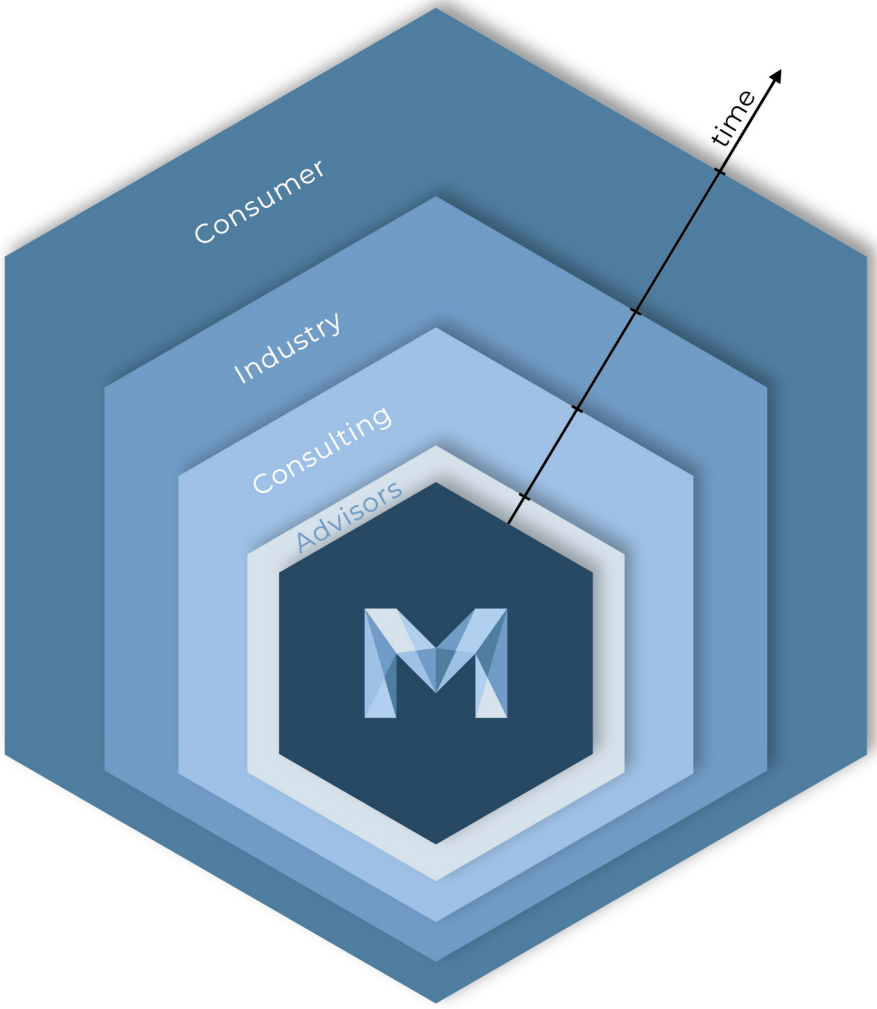


Figure 23 – MADANA's Scaling Strategy

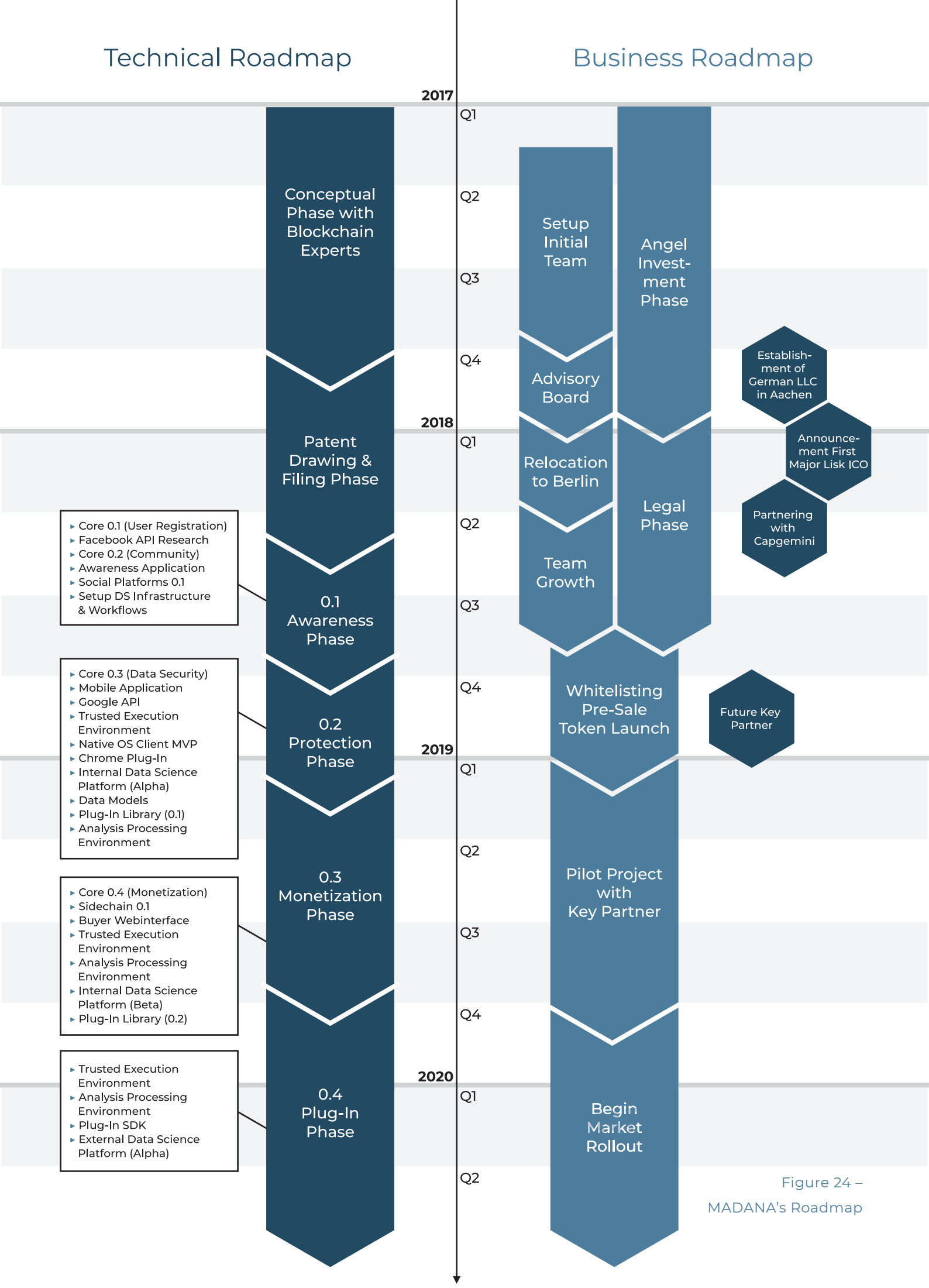


Figure 24 – MADANA's Roadmap

FUTURE POTENTIAL

The key driver of MADANA's strategy and its decision-making approach is its long-term focus. Recent concerns are not resolved by simply providing a single solution to ensure data security and digital privacy. Instead, a holistic approach must leverage the full potential of MADANA and the data market. As an outlook for the future, MADANA sees multiple opportunities for integrating the product in the everyday life at the social level and in the daily business making of companies.

BIG DATA ANALYSIS STORE

Uploading various analysis schemes by plug-in providers and making these schemes available to every participant, would ultimately result in a “Big Data Analysis Store”. Hence, analysis buyer could browse online for the right analysis scheme, like today's app store. Data scientists on the other hand would have a great community source for extending their analytics schemes as well as getting inspirations for new analytics schemes.

REPUTATION SCORE

To ensure high-quality analysis, provided data must first meet high-quality standards. Likewise, analysis scheme provider (plug-in provider) will call for high-quality data to assure high-class analysis schemes. By implementing a reputation-score-system in conjunction with a data authenticity plug-in, data quality could be assured.

BACKGROUND AI-TRAINING

By docking up deep-learning algorithms on to the analysis process, multiple AI’s could be trained in the background. These AI’s would gain more and more knowledge on possible subjects like data quality prognosis, data analysis quality, etc. Further, AI would have the opportunity of sorting out advanced cross-analytics, only possible with a generic decentralized database like MADANA.

DATA PRIVACY CERTIFICATE

Companies that are hesitant to monetize their data in fear of customer backlash would be enabled to make use of their data in a transparent and open way. By buying data analysis from the MADANA ecosystem, companies could advance their image by stating a data privacy certificate provided by MADANA guaranteeing data privacy.

DATA MODEL STANDARDIZATION

Data is widely unstructured. Valuable information is available for free on the Internet. With PAX token as incentive experts could focus on aggregating data, restructuring it into standardized data models and feeding it into the MADANA network. Sources for this kind of data could be: public repositories, government statistics, stock market data or data from public websites such as Twitter, Crunchbase or Kaggle. New technologies are expected to provide new datasets which initially will be heavily unstructured, e.g. in the sphere of biogenetic data. By democratizing data model standards, data scientists in the MADANA ecosystem would eventually be able to elect standardized data models for each emerging industry.

STANDARDIZED PRIVACY LAYER

The technology underneath the MADANA ecosystem basically acts as a privacy layer, which MADANA plans to make available for developers in a framework. By implementing the privacy layer into applications, developers could then create privacy-secured applications. Therefore, MADANA is having a competitive edge by securing data privacy of the end-users along with an additional revenue stream through data monetization. Further, creating MADANA on the Lisk Blockchain bears the opportunity for future Lisk dApps to integrate the MADANA privacy layer into their systems.

GDPR-COMPLIANCE

Using the MADANA platform data-driven companies could alleviate their organizational restructuring triggered by the requirement to be GDPR-compliant.

CROSS-ANALYTICS OF SENSITIVE DATA

In general, major use cases lie in analyses of sensitive data. Especially in health, research universities face the challenge of accessing big enough sample groups. Data from medical and eHealth devices, private fitness and nutrition profiles and hospital data could be combined in an efficient way. Possible application ranges from cancer research to epidemiology and psychological studies.

The security and openness of MADANA will also allow all kinds of data to be added to the system. The added value will shape the standardization of new data types and combine data in new ways. Completely new cross-analytics unlock unseen value for science and society.

CONCLUSION

The data markets will change, and data producers will call for adequate compensation for the usage of their data. They will demand transparency and control over the processing of their information. Politics will need to adjust to these needs, because society's mindset is rapidly changing as its awareness of data control and privacy is increasing eversince recent data scandals. MADANA acts on exactly these issues. The system is meant to provide a solution for all parties involved in the data market, which ensures access to data, data privacy and compensation for data producers.

MADANA is developing a privacy layer for future applications in various industries, where data-driven decisions and processes are prevalent. Thus, making it possible to envision and to build a blockchain-based, decentralized ecosystem for a fair market for data analysis,
MADANA's ecosystem participants, the data producers (individuals and electronic devices), data analysis buyers, and plug-in provider (e.g. data scientists and application developers), will receive full benefits in the form of tokens or access to data and highest efficiency thanks to a thought-out design and newest technologies.

MADANA wants to make every individual data producer the controller over their own data. Backed by blockchain technology, MADANA's decentralized data market will be the data analysis solution of tomorrow.

Going beyond that, MADANA wants to address multiple needs in data-driven industries. New partnerships are meant to help MADANA to develop novel use cases and utilize its innovative cross analytics capabilities.

MADANA's uniqueness is defined by the combined features of all parts of the ecosystem. It is about the aggregated potential of all features from each part of the ecosystem. Reaching these potentials will drive the MADANA project towards the bigger vision as an established standard for data privacy and easy data market accessibility – where privacy is guaranteed by design.

MADANA envisions a world, where everybody can use data-driven services without giving up their privacy and disclosing their **"Digital You".**

APPENDIX

Appendix I – Reference List

(1) Gutermuth, Lisa (2017): How to Understand What Info Mobile Apps Are Collecting About You, [online] http://www.slate.com/articles/technology/future_tense/2017/02/how_to_understand_what_info_mobile _apps_collect_about_you.html

(2) IDC (2017): IDC's Worldwide Semiannual Big Data and Analytics Spending Guide, [online] https://www.statista.com/statistics/551501/worldwide-big-data-business-analytics-revenue/

(3) OnAudience (2017): Global Data Market Size 2016-2018, [online] http://www.onaudience.com/files/Global_Data_Market_Size_OnAudience_Report.pdf

(4) e-Marketer (2017): Worldwide Ad Spending: eMarketer's Updated Estimates and Forecast for 2016– 2021, [online] https://www.emarketer.com/Report/Worldwide-Ad-Spending-eMarketers-Updated-Estimates-Forecast-20162021/2002145

(5) European Commission (2017): Final results of the European Data Market study measuring the size and trends of the EU data economy, [online] https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study- measuring-size-and-trends-eu-data-economy

(6) European Commission (2017): Building a European Data Economy, [online] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0009&from=EN

(7) Keith D. Foote (2017): Big Data Trends for 2018, [online] http://www.dataversity.net/big-data-trends- 2018/

(8) Dataspace (2018): State of the Analytics Market 2018, [online] http://www.dataspace.com/wp- content/uploads/2018/01/State-of-the-Analytics-Market-2018.pdf

(9) Paysa.com (2018): Data Science Salaries [online] (as of 05/02/2018) https://www.paysa.com/salaries/data-scientist--t

(10) Softwareadvice.com (2018), [online] https://www.softwareadvice.com/

(11) Regulation (EU) 2016/679 of the European Parliament and of the Council (2016): On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [online] https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a- 01aa75ed71a1/language-en

(12) Gemalto (2018): The Reality of Data Breaches, Data Records Compromised in 2017, [online] https://breachlevelindex.com/assets/Breach-Level-Index-Infographic-2017-Gemalto-1500.jpg

(13) European Commission (2014): Towards a thriving data-driven economy, [online] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0442&from=ga

(14) EU GDPR Portal (2018): Home Page of EU GDPR, [online] https://www.eugdpr.org/key-changes.html

(15) European Commission (2018): The Internet of Things, [online] https://ec.europa.eu/digital-single-market/en/policies/internet-things

(16) Gartner Inc. (2017): Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016, [online] https://www.gartner.com/newsroom/id/3598917

(17) Statista (2015): Size of the Internet of Things market worldwide in 2014 and 2020, by industry (in billion U.S. dollars), [online] https://www.statista.com/statistics/512673/worldwide-internet-of-things-market/

(18) European Commission (2017): Report on Workshop on Security & Privacy in IoT, [online] http://ec.europa.eu/information_society/newsroom/image/document/2017-15/final_report_20170113_v0_1_clean_778231E0-BC8E-B21F-18089F746A650D4D_44113.pdf

(19) European Commission (2016): ICT Standardisation Priorities for the Digital Single Market, [online] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15265

(20) Deloitte (2018): Global health care outlook, The evolution of smart health care, [online] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-hc-outlook-2018.pdf

(21) Statista (2015): eHealth – worldwide, Statista Market Forecast, [online] https://www.statista.com/outlook/312/100/ehealth/worldwide

(22) Healthcare IT News (2015): Curbing medical errors with the cloud, [online] http://www.healthcareitnews.com/blog/curbing-medical-errors-cloud

(23) Forbes (2016): The Future Of Health Care Is In Data Analytics, [online] https://www.forbes.com/sites/mikemontgomery/2016/10/26/the-future-of-health-care-is-in-data-analytics/#1f4fba173ee2

(24) IBM Watson Health (2018): Bringing confident decision-making to oncology, [online] https://www.ibm.com/watson/health/oncology-and-genomics/oncology/

(25) BP (2017): BP Energy Outlook, [online] https://www.bp.com/content/dam/bp/pdf/energy-economics/energy-outlook-2017/bp-energy-outlook-2017.pdf

(26) International Energy Agency (2017): Digitalization and Energy 2017, [online] http://www.iea.org/digital/#section-4-5

(27) PwC (2018): Energie-Studie: Digitalisierung, [online] https://www.pwc.at/de/energie-studie/digitalisierung.html

(28) Harpham, B. (2016): How data science is changing the energy industry, [online] https://www.cio.com/article/3052934/big-data/how-data-science-is-changing-the-energy-industry.html

(29) REN21 (2017): Renewables 2017 Global Status Report, [online] http://www.ren21.net/wp-content/uploads/2017/06/17-8399_GSR_2017_Full_Report_0621_Opt.pdf

(30) Clean Energy Wire (2015): Energiewende passes solar eclipse stress test, [online] https://www.cleanenergywire.org/news/energiewende-passes-solar-eclipse-stress-test

(31) Siemens AG (2016): EnergyIP Analytics Suite: Load Forecasting, [online] https://www.siemens.com/content/dam/internet/siemens-com/global/products-services/energy/energy-automation-and-smart-grid/big-data-analytics/documents/energyip-analytics-suite-load-forecasting-en.pdf

Appendix II – Illustration Directory

For more information,
visit **www.madana.io** or email **info@madana.io**

Follow us on our social media channels.

Facebook
@MADANA.io

Twitter
@MADANA_HQ

Linkedin
madana.io

Telegram
t.me/MADANA
Official

Reddit
r/MADANA

Medium
blog/madana.io

Github
MADANA-IO

Youtube
MADANA