A DLT technology and the compliance GDPR

Speakers

Carlos Tovar

Dr. Yuri Tijerino PhD

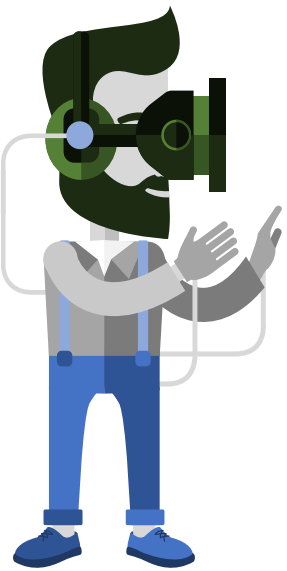
Content

- Evolution of DLT
- Evolution of Transactions
- What is AIn9le for first time
- FASTER Using DAG with purpose
- How it Works FASTER whith AIn9le
- FASTER tools and GDPR compliance

SICORP
戦略的国際共同研究プログラム
国立研究開発法人 科学技術振興機構 Japan Science and Technology Agency
This work is supported by SICORP, JST (Grant No: JPMJSC1811)
Funded by the Horizon 2020 Framework Programme of the European Union
833507 — FASTER — H2020-SU-SEC-2018-2019-2020/H2020-SU-SEC-2018
Project funded by: EUROPEAN COMMISSION - Research Executive Agency (REA)

Evolution of DLT

DLT Evolution



Blockchain

Data structured in blocks

Transactions validated by miners in ecosystem

Scalability issue

Transactions fees

Hashgraph

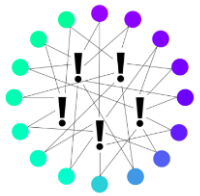
Virtual voting

Gossip about Gossip ensure transactions are validated by majority

Holochain

Data distributed among several nodes

No problem in network congestion



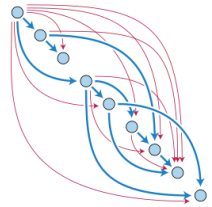
Many eyes looking at different problems

Scalability freec

DAG

Data structure follows Directed Acyclic Graph

Each transaction is independent



No transaction fees

Smart Semantic DAG

Pre-processing and post-processing of data. ML/DL

Low Resource Requirements

Ternary Programing

More data, more TPS

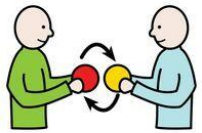
Offline transactions

No speculative Token

Quantum Resistant

GDPR Ready

Evolution of Transactions



HAND to HAND

TCP/IP

Internet of Content

1990

HTML

Internet of Service

1995

WEB 2.0 Mobile

Internet of People

2005

DLTs & IoT

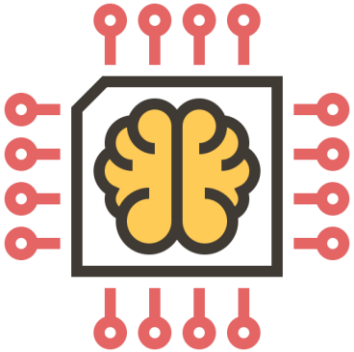
Economy of things

2009

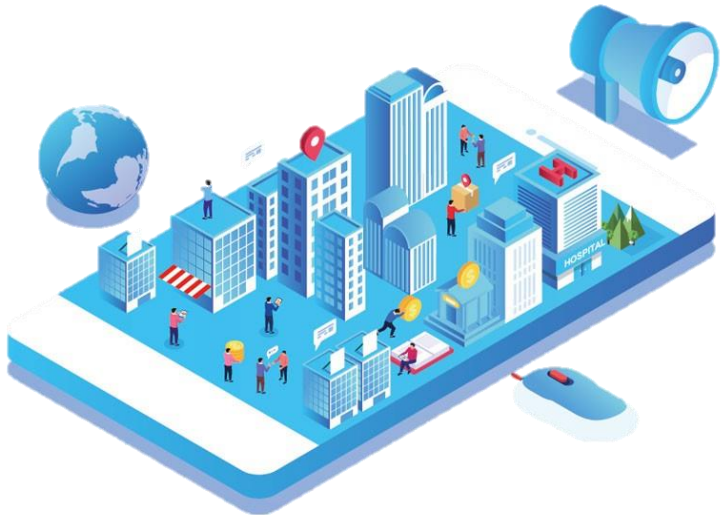
- Big DATA
- Massive transactions

MACHINE to MACHINE

Bridging the Human to Internet of Things

Economy of Things IoT / M2M	Smart Community Sharing Economy	Citizen Centricity “GDPR as an opportunity”
		
Devices trade resources among each other P2P IoT Data Marketplaces	*Anything with a chip can be leased*	*Citizen can control and share their personal and user data securely & privately*

Smart cities



Industrial IoT

- Internet of Things is experiencing an exponential increase in the connected devices, of which the number is expected to be over **25 billion** by 2020 [Gartner Report]
- However, this tremendous market growth raises new challenges such as **security and privacy**, **scalability** and **data processing performance** for IoT system architecture.
- Blockchain is a promising solution, but with some problems.

What about privacy?

Challenges of trust & privacy in the economy of things

DIGITAL TRUST	DATA (STREAM) Monetization	IOT / M2M enabled BUSINESS MODELS	GDPR Complience
			GDPR READY — General Data Protection Regulation
Data Integrity *CyberSecurity* *e-Privacy*	*Zero fee microtransactions* *Real time* *"Machine ready"*	*Data Driven* *Interoperability* *Ecosystem play*	*Ensure data privacy and the right to delete personal information*

Introducing AIn9le

Artificial Intelligence Dag Semantic

Angle

AIngle

Characteristic:

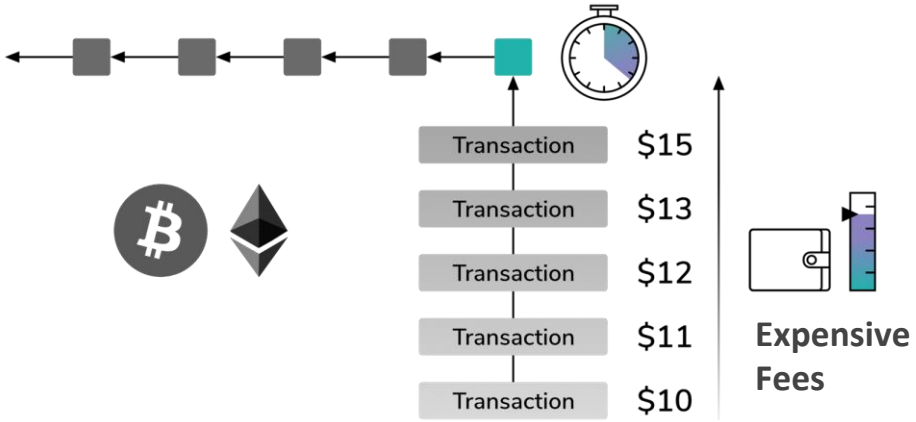
1. Increasing network activity with more nodes decreases transaction settlement times, unlike in a traditional blockchain.
2. The token is designed for the economy of things. The use of the token is focused on the encryption and how it is exchanged by the different nodes that make up the decentralized network. It is not thinking to speculate with the value of transactions
3. No block times or lengthy validation periods. Transactions and data can be published, validated and digested within milliseconds.
4. All data is encoded, enabling secure data transfer, storage and referencing. The data can also be organized in data streams for easier querying, authorization allocation and use.
5. Designed for micro and IoT devices (eg, sensors and microprocessors) to participate, it allows the secure of the data at the source of aggregation. Low energy is required regarding sustainable IoT growth and data proliferation.
6. Devices don't need perfect connectivity and can be validated when connectivity is available.
7. The AIngle is based on a ternary model. It is relevant because the programming is based on ontology, it allows taking advantage of the null results in the decision, which allows making multiple conclusions of operation and creating new relationships in the behavior of the data.
8. An exclusive anonymizing algorithm. It protects the personal data before being processed into the DAG using AI/ML. Thus, it allows compliance with GDPR policies.

Benefit:

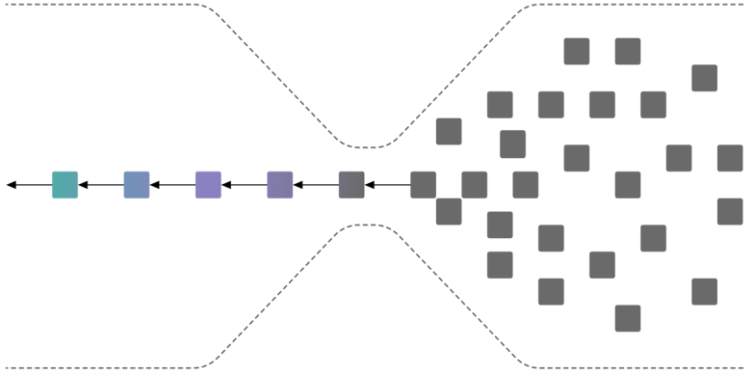
1. High scalability.
2. Zero-fee microtransactions.
3. Real-Time transactions.
4. Secure data transfer or organization.
5. Low resource requirements.
6. Offline transactions.
7. Quantum resistant.
8. GDPR compliance.

Blockchain is not fit for IoT

Slow Confirmations



Consensus Bottleneck



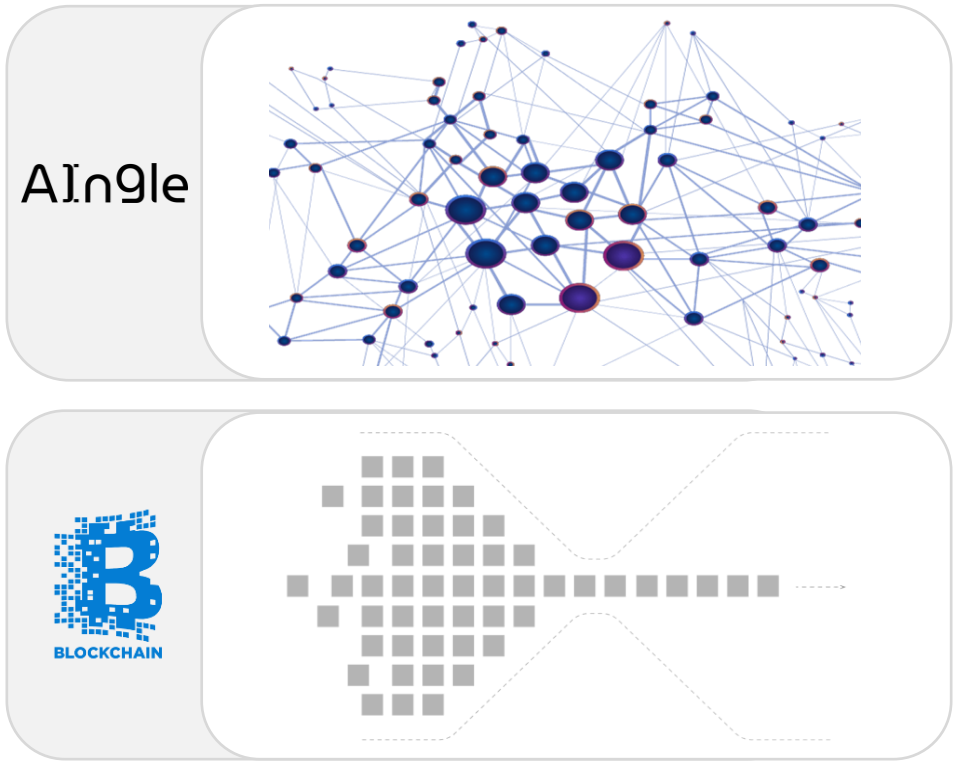
TPS

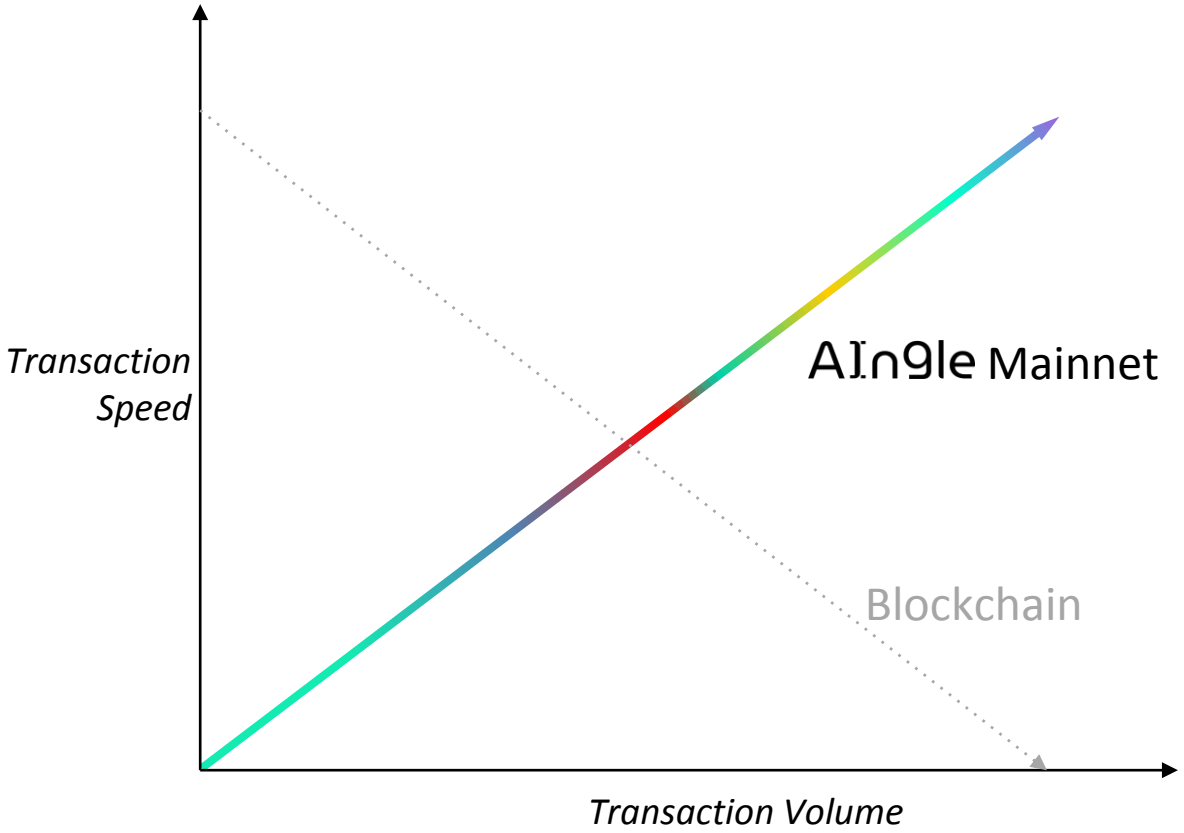
AIn9le	BLOCKCHAIN
12000 - ∞	8

Blockchain is not fit for IoT

The Dag scales with more transactions – more activity equals more validation

AIngle vs. Blockchain



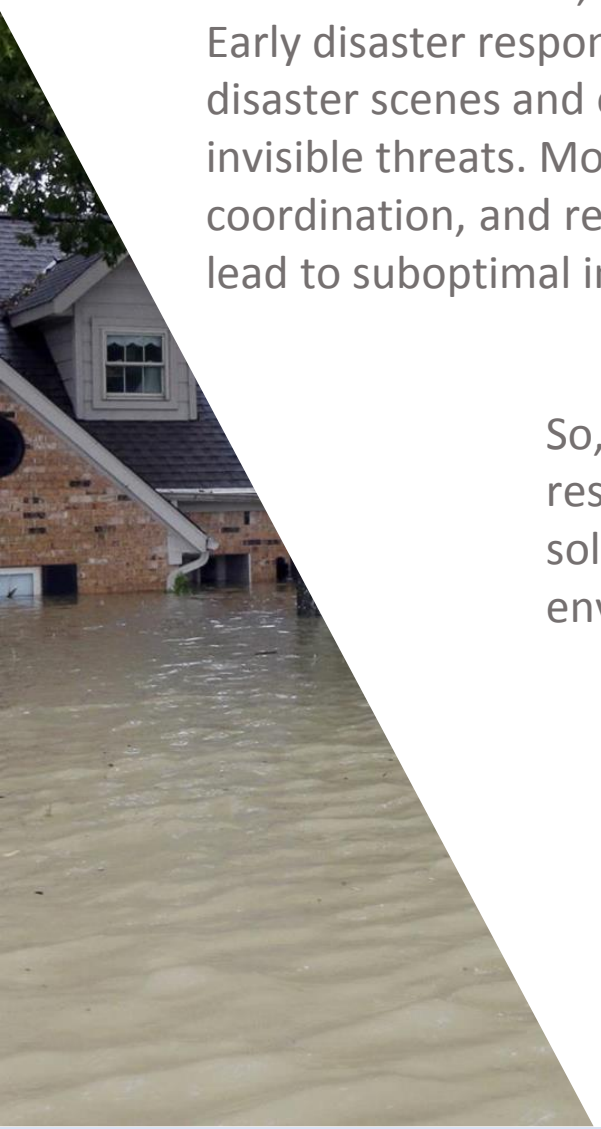


FASTER: using a DAG with purpose

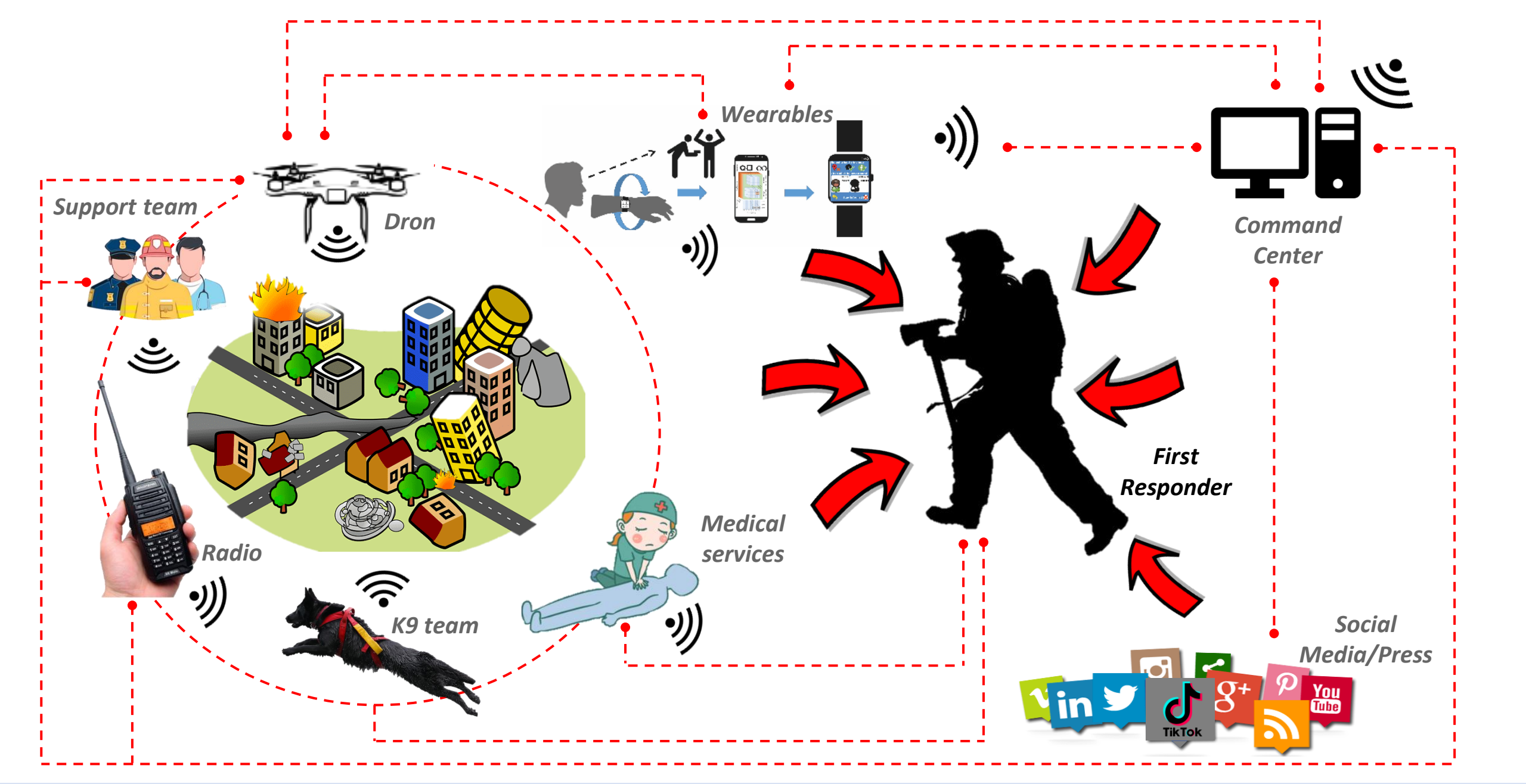
Funded by the Horizon 2020 Framework Programme of the European Union

833507 — FASTER — H2020-SU-SEC-2018-2019-2020/H2020-SU-SEC-2018
Project funded by: EUROPEAN COMMISSION - Research Executive Agency (REA)

In Europe and Japan, disasters due to natural phenomena, technical accidents, or human behavior are increasing. Early disaster responders are operating in dangerous disaster scenes and endangered to both visible and invisible threats. Moreover, lack of proper communication, coordination, and resources in such an environment can lead to suboptimal intervention.



So, technological advances must be used to protect disaster responders from multiple unforeseen hazards and provide solutions that can operate seamlessly and efficiently in any environment.


Wearables
Support team
Dron
Command Center
Radio
K9 team
Medical services
First Responder
Social Media/Press

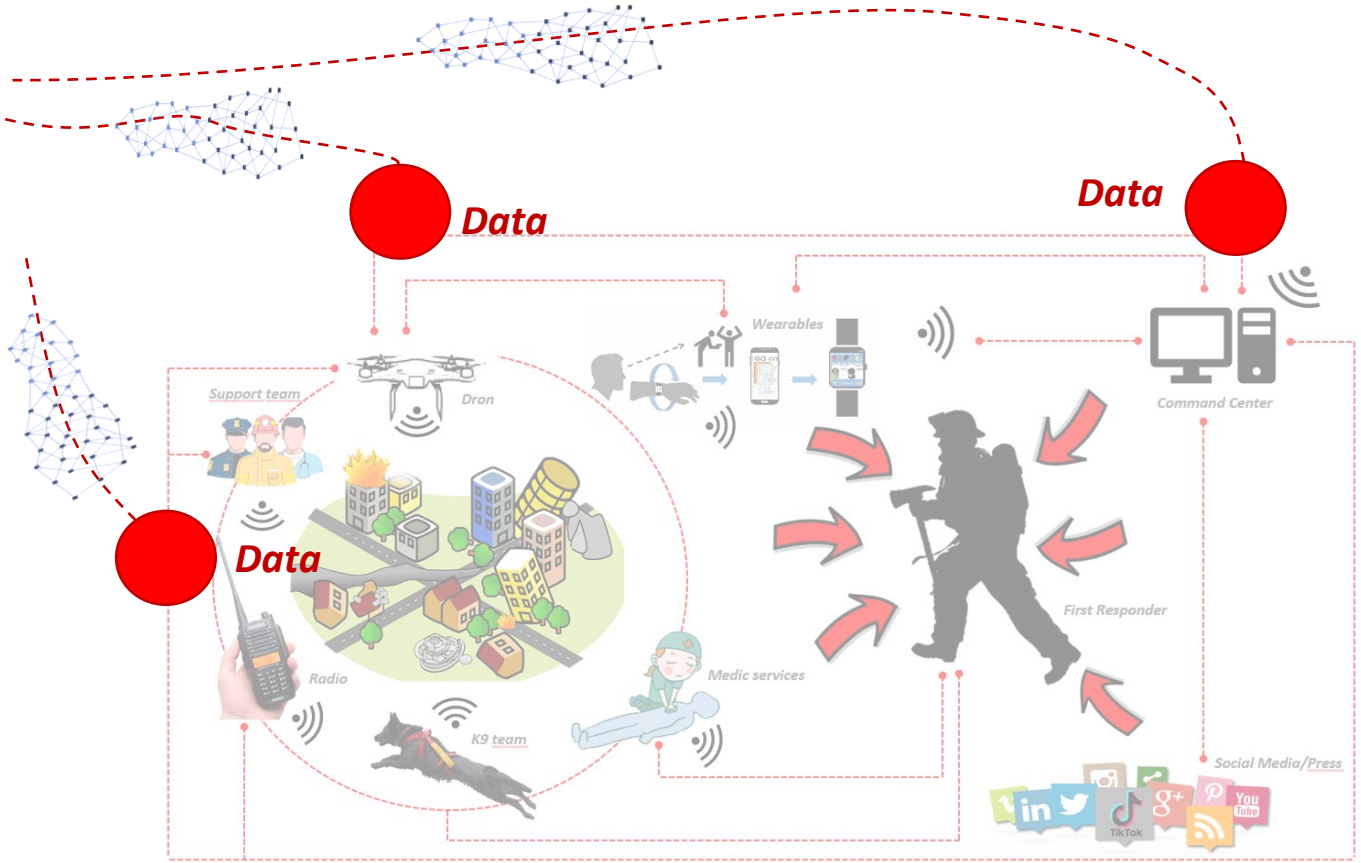
How AIngle works?

How AIngle works

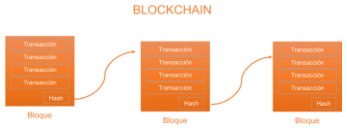
It means private information that somebody else is watching

- Patient information
- Disaster´s data
- Dron, sensors, mobile, radio, and more

Comparative Blockchain and AIngle for IoT Data Treatment

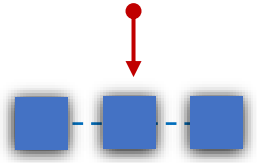


Blockchain

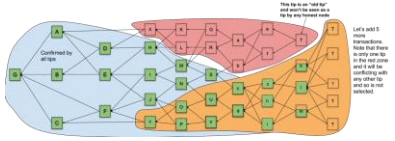


Blockchain create a hash. The miner validate data. It´s inmutable. It´s not posible to delete it

Age, Sex, Name



AIngle DAG



AIngle create a “digital twin” before to validate information. It allows to “anonymize” personal information

Age, Sex, Name

Anonymized Data

Age, Sex, Name

XXX

Register

AIngle and GDPR
Anonymizing algorithm

Whole Data
(Include Names/Face)

- Michael Douglas
- 75 Years Old
- Elbow frature in earthquake

AIngle (Semantic DLT)

Node

AI
ML

Grakn detect DATA and the name is isolated and person is anonymized

Digital Twin Algorithm

XXX

Age, Sex, Name

Digital Twin erase face and name. Data is ready to be used

ACM

Through ACM, an anonymus DATA is redy for Aingle. (Immutable DATA)

Whole Data
(Include Names/Face)

kafka

This data could be used following all GDPR policies.
This data ***IS NOT immutable*** (can be erased anytime)

AIngle

Clean data enters the AIngle

This Data doesn´t enter to Aingle DAG

Anonymized information is used to create data for health, migration models, among others

Command Center

GDPR READY — General Data Protection Regulation

Anonymized information is used for the command center to create models to improve response to emergencies and to guide "first responders.". It is immutable data.

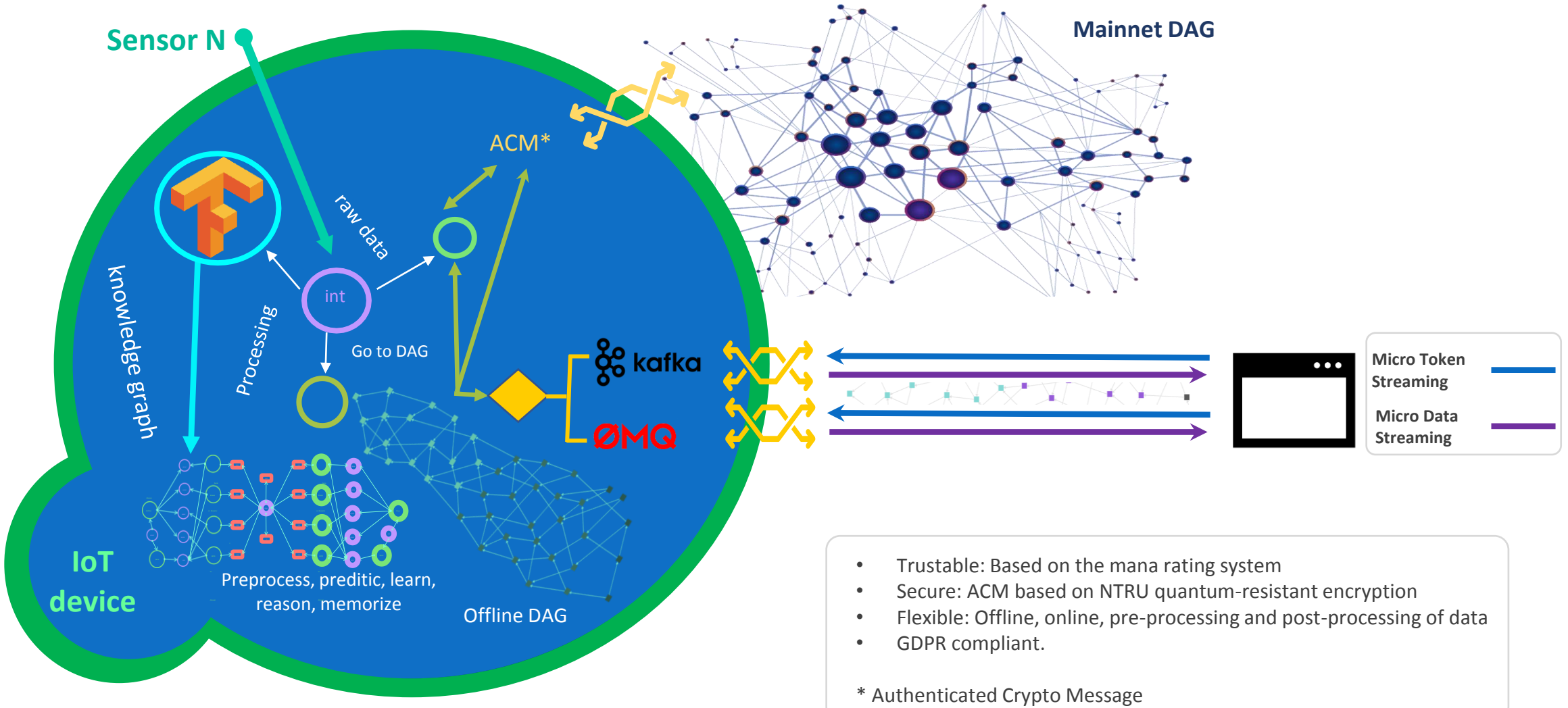
- XXXXXXXXXXX
- (Anonymous)

- Michael Douglas
- 75 Years Old
- Elbow frature in earthquake

- Personal data only is need for modeling general data. Personal information is not saved
- AIngle AI, knows exaclty the data type registered (this avoid infiltration and wrong data processing)

AIn9le

- *Bundle all transactions in a Directed Acyclic Graph (DAG)*
- *Completely self-regulating, consensus no longer decoupled*
- *Low overhead Proof-of-Work prevent resource overconsumption*



- Trustable: Based on the mana rating system
- Secure: ACM based on NTRU quantum-resistant encryption
- Flexible: Offline, online, pre-processing and post-processing of data
- GDPR compliant.

* Authenticated Crypto Message

Potencial challenges:

GDPR READY

OBLIVION RIGHT

PRIVACY RIGHT

DATA SECURITY

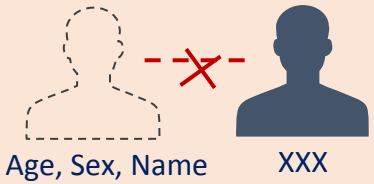
AIngle CRYPTO

Solutions:

AIngle

DIGITAL TWIN

AIngle create a "twin" hash before to validate information. It allows to "anonymize" personal information



QUANTUM CRYPTOGRAPHY

Prevents hacking and quantum attacks avoiding data could be lost or stolen

SECURITY IN INFORMATION

Communicate in trusted environment
New smart contracts with micro-payments
Reward for honest participation
Outsourced computation

STABLECOIN

Token used as communication protocol between all IoT devices. No fees / Scalable

This crypto doesn't like speculation but being useful in facilitating transactions and data exchange.

Conclusions

The evolution of technology has created an ecosystem that forces machines to communicate with each other (M2M), generating a massive volume of information

Blockchain in a type of DLT. It was a disruptive revolution for transactions and processes. But its functionality makes it difficult to use it for massive data interchange.

AIngle is a technology that allows to exchange information massively with the benefits of a blockchain but without the problems of scalability and fees.

FASTER is a project with a social sense, which aims to ensure that the "first responders" of an emergency can be safer and, at the same time, be more efficient through the exchange of valuable and secure information in real-time with multiple sources.

AIngle contributes to FASTER project the benefit of helping to comply with the GDPR policies by ensuring the anonymization of private information by using artificial intelligence, machine learning working together with a DAG.

For the exchange of information, the AIngle will use his own crypto, which will be focused on the operability without fees and being scalable. Furthermore, it will not be speculative.

Thanks