PikcioChain: a new eco-system for personal data

J. Lartigau, F. Bucamp, D. Collin de Casaubon
[1] contact@matchupbox.com

WARNING

This document is strictly confidential, for private use only and to the sole discretion of the person to who it was given by MATCHUPBOX. No information even partial are authorized for any communication wihtout a formal agreement stated by MATCHUPBOX. All the statements, descriptions, figures and logos are the property of MATCHUPBOX.

Abstract

A lot of effort has been put into data analysis, machine learning, artificial intelligence and neural networks. The fuel behind these investments remains the customer's personal data. Companies now spend billions of dollars to gather, process and authenticate data. But as today, the entire data transaction chain as for today cannot rely on a cross-system platform empowering trust, privacy, and security. Additionally, it has become more and more complex to deal with privacy issues from both private and businesses.

The innovative network solution PikcioChain designed and developped by MatchUpBox lies upon a strict understanting of privacy by design, where no middle servers interoperate within the network, and where all the services persistancy are warranted. User's data engaged on the network are his sole property and the ones he deliebratly consents to share with. The technical solution is articulated around a set of several key technolgies and and concepts. This document hereby presented, intends to give a global description of the different layers of the technology and their interoperability within one to another. MatchUpBox brings innovation along 2 communication layers coupled with a Trusted Identification System (TIS). The *Blockchain* process is thereby merged to increase the benefits brought by the solution. A *Trust Capital Index* (*TCI*) is integrated on the upper layer to intermediate trust within the participants of network solution.

PikcioChain is a new blockchain technology providing a reliable ecosystem for personal data, and customer's identification. Its Digital Identity empowers data certifiers and data users creating a market place based on trust.

1. Context

Personal data is the fuel for any digitalized services for identification purpose and furthermore to deliver custom solutions to private individuals. The use of personal data by businesses often appears fuzzy to the private consumers especially regarding privacy concerns. Indeed personal data is often traded from entity to another interplaying with various analytic processes. Alain Westin defined privacy as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others [1]. Thus, it is clear that transparency is a core aspect that businesses must embrace to empower a better trust of their consumers. New data regulations such as GDPR (General Data Privacy Regulation) aim to offer a tangible frame regarding personal data and privacy. Personal data is the center of a global digital economy articulated around private individuals without their prior consent or even acknowledgement. Unfortunatelly for consumers, data regulations are more subject to legal refining of the terms of use rather than introducing new solutions encompassing transparency, trust and privacy.

When talking about full transparency in the ownership and transactions of assets, Blockchain stand as a unique technology empowering full dissemination of the system status among all its participants. Blockchain, the distributed ledger technology underlying Bitcoin, appear to be far more valuable than the currency it supports [2]. Blockchain is set of mechanisms that rests upon the participants, hereby called nodes, acting as a decentralized community providing their computing resources to process various operations often called Smart Contracts. Ethereum is now the most popular blockchain regarding this aspect, enabling IaaS (Infrastruture as a Service) for a public based blockchain able to run customize deterministic code for any business purpose, relying on the whole community i.e. DAO (Decentralized Autonomous Organization). Smart contracts are public and utlimately generate new entries in the ledger. The ledger is often appreciated as a simple distributed and redundant database, even though it empowers cryptographic technologies to chain entries from to another providing an immutable, irreversible, secure and cost efficient way to record information. Therefore, to implement fraudulent records would imply to corrupt or hack a majority of nodes ledger copies in a near simultaneity. Such an operation would require a huge amount of computational resources that would outgrow the cost behind the potential benefits behind the hack. Regarding privacy, a fundamental concern is if transparency is not antinomic with privacy. In the public definition of the blockchain as in the Bitcoin, any node can determine the current balance of any other. Therefore the security and trust terms are strongly enhanced meanwhile the loss of individuals' privacy can be perceived too radical. However with regards to the Bitcoin, money laundering became an important usage since individual identification is down to a simplest unique network ID with no correlation with a physical identity realizing pseudonimity [3]. This paradox is the effect of no real identification process overlaying on the Blockchain. It suffers a serious lack of identification proof mechachsim, to not misinterpret with authentication or system identification, to build a trusted community empowered by both blockchain process and identification.

Data privacy has turned into one of the most relevant hotly debated topics worldwide, as it pertains to the daily lives of a large portion of the world's ever-connected population. Every day within the European Union, businesses, public authorities and individuals transfer vast amounts of personal data across borders. Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Furthermore, individuals or organizations that collect and manage personal information must protect it from misuse and respect data owners' rights as outlined and guaranteed by EU law.

While some systems are already interoperable for transactional purposes, for instance Swift in financial institutions, there are not yet any viable platforms for personal data exchange and traceability across services. Moreover, many companies catering to EU customers struggle with upcoming General Data Privacy Regulation (GDPR) [4] compliance, which will encompass data transfers and traceability, customer concerns and rights in addition to privacy impact assessments. The issue becomes even more complex when considering existing individual's identification processes involving large sets of personal data.

The way businesses engaged with individuals often implies the processing of personal data for subscription or service delivery. An emerging concept based on the consideration of privacy-by-design and furthermore privacy-by-using is the Personal Management Information Systems (PIMS) or Vendor Relationship Management (VRM) [5-7]. Instead of having entities such as social network (e.g. Facebook, LinkedIn), banks or insurances gathering horizontal sets of data centered around a specific domain (e.g. financial information) on a large partition of individuals ; a single person will host and manage all his own horizontals. It creates a vertical user centric set of data that PIMS can dispose for better tailored services, and faster subscription or data exchanges between all the businesses around this particular individual. It also provides a greater control on how consumers engage with vendors.

2. Design principles

Straightforward P2P network suffers from privacy problem that is due to the scheme itself. Since all the services interplaying among participants are executed in direct lines, tracing of communications by very simple means would disclose the communication relationships in network. If to permission the Blockchain, mainly due to data regulations, the network identity of miners and ledger hosts represent a sensitive information, especially regarding network attacks.

The adoption of anonymous communication techniques seems then an obvious step toward the security objective of protection of trust links against community members. However, such anonymous communication technique should be in line with the design principle of trust. Therefore, an individual node is a core of a concentric ring consisting of nodes that each are a trusted contact. Further rings are built through similar trust relationships, without requiring nodes on the same ring to have trust relationships with one another, and without requiring transitivity of trust. Data requests are then addressed to the nodes in the outermost ring, and are forwarded to the nodes in the first one along hop-by-hop trusted links. Data is served by nodes in the innermost ring and replies are sent back along the same paths. PikcioChain thus consists of the collection of concentric layers of peers nodes organized around each individual private or business, in order to assure data storage and communication privacy.

Security and privacy of the system might be compromised if malicious entities were able to impersonate legitimate ones. Malicious entities would then be able to intrude into the rings surrounding a target victim and derive the trust relationship we aim to protect. As a consequence, a mechanism ensuring individual authentication has been taken. In PikcioChain, a Trusted Identification Service (TIS) that does not take part in the network itself, provides individuals with unambiguous certified identifiers associated to their real identities. Such TIS does not contrast with the purpose of decentralization, as it can be implemented in a decentralized fashion. TIS is not involved in any communication or data management operation among participants, is contacted only once, and can be provided off-line. Finally, classical encryption techniques have been adopted to ensure data confidentiality and data integrity.

In summary, PikcioChain has been designed as network addressing privacy from the very beginning. Privacy against centralized omniscient entities is achieved with the adoption of a decentralized P2P approach. Privacy against malicious users is achieved with communication obfuscation through anonymous routing techniques, data confidentiality through the use of encryption, and profile integrity through certified identifiers. For these reasons, PikcioChain achieves privacy by design.

Nevertheless, in the specific context of collaborative system, we realize that the real-life trust between individuals and businesses can serve much more than simple cooperation: it can be used to build the network itself. Therefore, the PikcioChain helps individual to establish trust relationships, and trusted nodes provide the basic services of data storage, retrieval and communication, and consequently build a sustainable blockchain articulated around both privacy and trust. Indeed, it is fundamental to consider the blockchain as an upper mechanism of a P2P substrate and for which PikcioChain brings new considerations and tangible innovations..

3. Main components

The trust between participants as in a social graph is mapped into ring structures called Matryoshkas , where node neighborhood is based on trust relationship. Direct trust relationships are leveraged for the purpose of data communication and data availability. Since trusted nodes are considered honest but curious, data is stored in an encrypted form. In PikcioChain, a target profile data can be accessed through hop-by-hop trusted paths whose endpoints can be retrieved from an additional Peer-to-Peer system maintained by the social graph itself. Differently from the Matryoshkas, this P2P system is used for indexing purpose only: it does not store indevidual's profile data and does not take into account individual's trust relations. PikcioChain can thus be seen as an overlay network composed by two different layers:

- Matryoshkas provide each member with anonymous but trusted routing paths
- A Peer-to-Peer layer offering the infrastructure to build and to access the Matryoshkas.

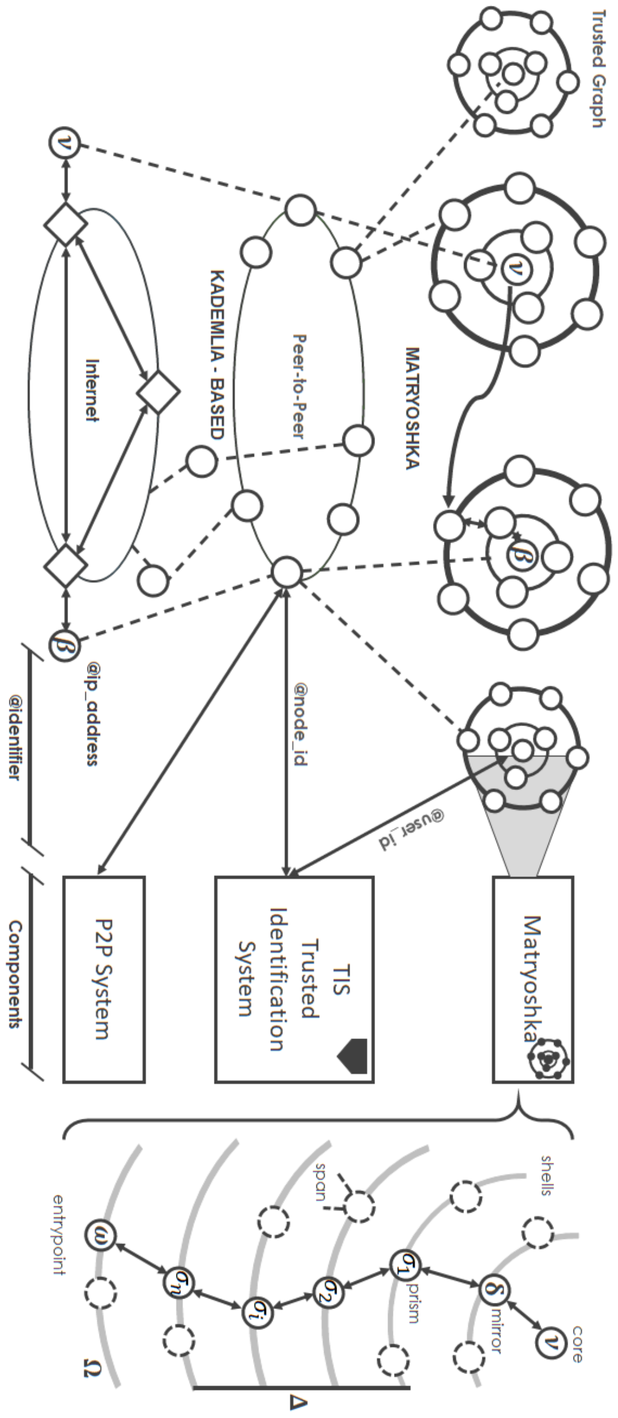


Figure 1. PikcioChain main components

A PikcioChain participant is assimilated as a host on the Internet, a peer node in the P2P layer and a user in the Matryoshka layer. Different identifiers are used to address the same party in each layer: a user Id denotes a node in the Matryoshka layer, a node Id in the P2P layer, finally an IP address in the Internet layer. In addition to Matryoshkas and the P2P system, an off- line Trusted Identification Service (TIS) is in charge of generating the identifiers needed to address users in the SN layer and peer nodes in the P2P layer. Since these identifiers are issued together with corresponding certificates, they can never be manipulated nor forged. The Matryoshka layer enable various set of consumers similar to Bitcoin Blockchain, enabling smart contracts consensus.

1. Matryoshka

The *Matryoshka* principal can be correlated to *onion routing* such as *TOR*. The *Matryoshka* routing overcomes several deficiencies from existing systems (especially fiduciaries servers), that do not satisfy and comply with privacy issues and more importantly anonymisation of exchanges. *Matryoshka* routing does bounce the *TCP* exchanges around the internet to neutralize traffic ananlysis on network clusters (especially *man in the middle* attacks). Therefore, exchange links are impossible to identify since that there are no ways to get both the sender and receiver *IPs*.

A Matryoshka is a trust-of-trust structure providing the individual with data communication obfuscation services. An individual v's Matryoshka θ_v consists of a group of nodes surrounding v's node. The nodes of a Matryoshka are organized into several concentric rings, namely shells, and several paths lead from the nodes in the innermost shell Δ_v to the nodes in the outermost shell Ω_v. With $\sigma_v^j \in \theta_v$ a node in the jth shell, with $j \in [0, \ldots, MaxShell]$, each Matryoshka further features the following properties:

1. v's node σ_v^0 is located at the center of the Matryoshka and is called the core;
2. if a pair of nodes $(\sigma_v^j, \sigma_v^{j+1})$ is connected, a friendship relation between them exists in the social network layer;
3. each node σ_v^1, located on the innermost shell Δ_v and called a mirror, is a trusted contact of the core v and ultimately stores v's data in an encrypted form;
4. each node $\sigma_v^{MaxShell}$, located on the outermost shell Ω_v and called entrypoint, acts as a gateway for all the requests destined to v
5. each node σ_v^j, j $\in [2, MaxShell - 1]$, located on a shell between Δ_v and Ω_v, is called a prism of v
6. the set of prisms is denoted as λ_v

In summary v's Matryoshka θ_v is the union of the set of mirrors Δ_v, the set of prisms λ_v, the set of entrypoints Ω_v and the core v. The number of v's mirrors represents the number of available partitions of v's profile data, while there are as many entrypoints as paths that can lead to a mirror. Each i^{th} mirror $\delta_i \in \Delta_v$ represents the root of a subtree with leaves that are lying in the outermost shell Ω_v. The branching of all the subtrees, the span factor, is set by v. The cardinality $\|.\|$ of the set Ω_v in consequence is $\|\Omega_v\| = \|\Delta_v\|Span^{MaxShell-1}$.

The building of v's Matryoshka θ_v is triggered recursively starting from θ_v^0. The node θ_v^0 is responsible for the selection of *mirror* θ_v^1. The selection process compute the following utility:

$$\mu_v^c = \sum_{i=0}^{N} \frac{\sigma_i - min_i}{Max_i - min_i}\omega_i + \sum_{z=0}^{M} \frac{Max_z - min_z}{Max_z - \sigma_z}\omega_z$$

For a given set $c \in [1, \dots, MaxTrustedPeers]$ of v potentials candidates as *mirror*, the selection process aim to define μ_v^c the trust and performance score of given peer c. The score is result of a maximizing set (*N*) toward a minimizing one (*M*). The weights ω translate the impact factor relative to each criterion. The maximizing set is defined by the following *QoS* (Quality of Services) metric; *bandwidth* i.e. bandwidth for *upload* and *download*, *availability* i.e. simultaneous availability with of v and *tci* i.e. trust capital index built upon successful cooperation between peers. The minimizing set includes the *uptime* and the et *load balancing.*

Exchanges within the Matryoshka protocol are secured using a hybrid encryption building messaging layer as:

$$MSG = \langle Enc_{msg}, Enc_{AESkey}, Sign_{Privkey} \rangle$$

Enc_{msg} is the message content encrypted with AES256, thus the AES key is secured with the public key of the receiver β denominated as Enc_{AESkey}, finally the sender v signs the message using his private key generating the signature $Sign_{Privkey}$.

2. Peer to Peer substrate

The P2P substrate of PikcioChain is a DHT similar to Kademlia (KAD) [8] in charge of storing and retrieving the entrypoint references of all the individuals' Matryoshkas. Such a substrate comprises of all individuals nodes and allows any node to issue a lookup query to reach the Matryoshka of any other.

Kademlia protocol enables to create network clusters within the internet network. Kademlia nodes, here assimilated as users, exchange through *UDP* (*User Datagram Protocol*). Each node is identified by a unique identification number i.e. *NodeID*. The *NodeID* is generated using a hash function taking as inputs the user *email* and *username*, guaranteed unique by the *TIS* (*Trusted Identification System*), and coupled to the *TIS* key. Kademlia includes a solution for address indexation i.e. *DHT* (*Distributed Hash Table*), that can be assimilated as distributed phone book, between all the nodes of the network. Doing such, any node is able to contact any other without having any indexation central server. All information stored in the *DHT* are *value;* each *value* is linked to a *key*. Kademlia is a network <*value, key*>.

The DHT is defined as:

$$DHT = \langle K, N, R, id_n(.), id_r(.), \rho(.) \rangle$$

Where K is the *DHT* keyspace, N and R correspond to the set of nodes and the set of resources, respectively, and $id_n : N \rightarrow K, id_r : R \rightarrow K$ denote the functions associating a node and a resource to their identifier respectively. Finally $\rho : K \rightarrow \{N\}$ denotes the mapping function which outputs the set of peers responsible for a resource given the resource identifier.

A resource consist on a list of entrypoint references of a target user's Matryoshka. The corresponding resource identifier *DhtKey* is represented by a user identifier or by an hash of the user's attributes such as her full name, her birthday etc.

Redundant copies of (key value) pairs (*DhtKey,* resource) can be stored by nodes whose identifier matches DhtKey on a predefined amount of first bits.

Much alike KAD, PikcioChain implements a greedy routing, minimizing the distance mea- sured in an XOR-metric between the *DhtKey* to locate and the node Id of neighboring nodes.

3. TIS (Trusted Identification System)

The TIS is a trusted third party that generates and grants for each PikcioChain user v a pair of identifiers: a node Id (Nid_v), unambiguously identifying v as a peer in the P2P layer, and a user Id (Uid_v) unambiguously identifying v as a user in the social network layer. Both identifiers are computed starting from a set of v's properties such as v's full name, birthday, birthplace etc.

A pair of certificates link each identifier to a respective public key provided by v. Corresponding private keys are known by v and nobody else.

Since the P2P system allows to retrieve a node IP address given a node Id, the separation of node- and user- identifiers is required to prevent malicious users from deriving a victim's IP address. Only trusted contacts of a node are able to link these two identifiers, as they serve as mirrors and in consequence know both. TIS constitutes an exception, as it is the only party in PikcioChain that is able to link the user Id and node Id of users other than their own trusted acquaintances. If compromised, in addition to the users' location, TIS may also disclose users' participation in PikcioChain. However, the TIS does not possess any user's private keys, therefore it cannot impersonate any victim, nor retrieve her set of trusted contacts or access data content published with restrictions.

While the TIS is a centralized infrastructure and in consequence might appear to break the paradigm of a decentralized architecture of PikcioChain, it can easily be implemented in a distributed fashion. Furthermore, it is an off-line service used only once by each PikcioChain user and, unlike a central server, it does not threaten the privacy of users, as it is not involved in any communication or data management operation among users or peer nodes.

A collusion of the TIS with the Internet Service Provider would circumvent the concept of separation of identifiers. However, this attack is only successful if the ISP controls the access to all users of PikcioChain, as only the privacy of users using the directly monitored Internet connections can be disclosed. Entirely protecting the privacy against a malicious ISP is only possible when leveraging much more complex concepts of anonymization, which for the sake of efficiency is refrained of. PikcioChain indeed does not provide anonymous communications on the network level.

4. TCI (Trust Capital Index)

The TIS is responsible for system identification. However, it does not work cross systems, and does not rely to existing identification and personal data from other sources like social networks or any digitalized services.

To cope with identity usurpation, numerous in the digital spheres, our network includes a identification protocol, validated by the *PikcioChain consensus*, issuing a *Trust Capital Index* (*TCI*). A user can validate his identity and raise his *TCI* when connecting third parties data sources, from social networks (e.g. Facebook, Linkedin) to banks (e.g. BNP Paribas, Wells Fargo). *Consensus* insure the information correlation with the provided identity from the registration process. The *TCI* also depends from the *vouches* between peers of the network, meaning that one entity can validate another using a *vouching* process. Vouches works as currency exchanges. Each user is provided of initial number of *vouches*. Every time he gives one, his *vouches wallet* depletes of one. As opposite, when receiving *vouches*, his balance is credited. The well being, and immutability of the *TCI* process is insuredby the *PikcioChain* DLT.

4. Distributed Ledger Technology

There is no deny in the success of the Bitcoin and that prove the innovation behind the blockchain. A Peer-to-Peer Electronic Cash System which concept was extended to any distributed processing by Ethereum and the concept of Smart Contracts. Regarding the success on these both distributed platforms, many developers and entrepreneurs have released alternative crypto-currencies empowering various divergence / interpretation of the blockchain process including divergence from its original model. It would be utopian and probably wrong to see a blockchain solution as the one solution. As any technology, the usage and purpose lead different technological options, so to believe in one and unique currency is to not grasp or understand the usage of given blockchain. Usage drives conceptualization. It’s from this view that PikcioChain is designed for personal data encompassing regulations by permissioning. As we processed with Kademlia and P2P substrate, PikcioChain relies on the ground base of the Bitcoin’s Blockchain for the DLT. We propose to discuss the PikcioChain design principles regarding the DLT in the following sub-sections.

1. From Proof of Work (PoW) & Proof of Stake (PoS) to Proof of Activity (PoA)

PoW is a combination of two ideas: (1) to (artificially) make it *computationally costly* for network users to validate transactions; and (2) to *reward* them for trying to help validate transactions. The reward is used so that people on the network will try to help validate transactions, even though that’s now been made a computationally costly process. The benefit of making it costly to validate transactions is that validation can no longer be influenced by the number of network identities someone controls, but only by the total computational power they can bring to bear on validation.

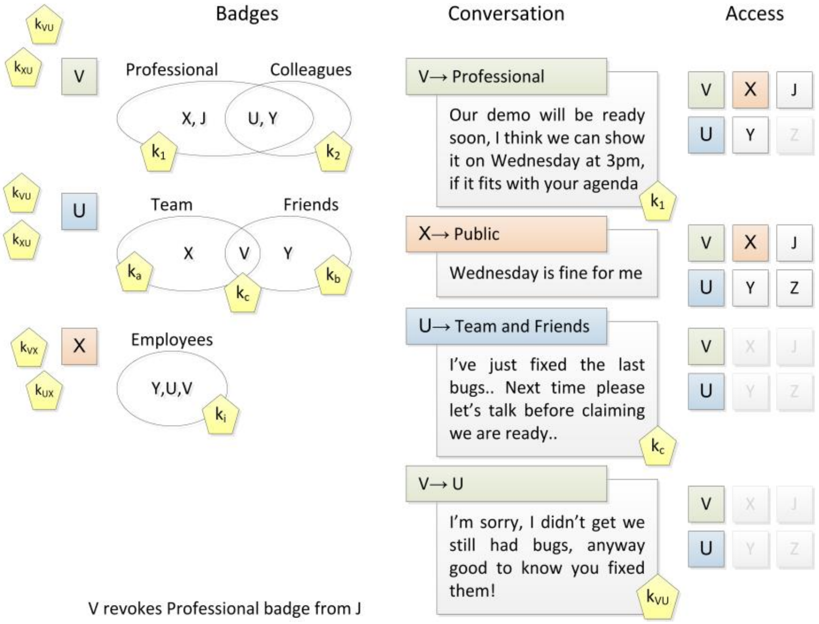
The success of a cryptocurrency mainly on getting *miners* onboard to insure a strong Infrastructure as a Service (IaaS). Bitcoin realized this infrastructure from scratch thanks to its PoW mechanism. However, new altcoins (alternative cryptocurrencies) coming in the market highlight the *mining pool* effect with *bad incentives*. That is a receivable view, but the so call improvements might remain fuzzy regarding the vision and intentions to miners, who have the hardware to carry the infrastructure. Bitcoin PoW is a clear process with understandable incentives based on the miner capacities. Unlike PoW, PoS by definition insures a distribution of the work among the stakeholders to insure a fair share of the work and so incentives. PoS is deterministic so way more cost / energy effective, in the meaning that miners do not need to pile up in *pools* to win to bid. In June 2015, the Bitcoin network was consuming enough energy to power 173,000 American homes and today that figure has grown to 1,018,762 [9].

Therefore, PoW is proven to be a reliable way to stimulate miners providing the network with their computational capabilities. From another hand, incentives tend to build *mining pool* to earn new coins with a huge energy consumption. PoS copes with energy efficiency using a deterministic distribution, and rewards the stakeholders with transaction fees.

A merging concept enabling incentives of a PoW coupled with a distributed block forging dissemination would appear to be a correct balance to get various *miners* on board avoiding *mining pools* and energy loss. Bentov et al. proposed a new mechanism in the prism of Bitcoin i.e. Proof of Activity (PoA). The cost of an attack would be much higher with the PoA protocol than with Bitcoin’s pure PoW protocol. Furthermore, the PoA protocol is likely to accomplish other beneficial properties, namely an improved network topology, low transaction fees, and a more efficient energy usage [10].

2. Communication management for permissioning

Communication management functionalities allow users to establish unobservable friendship links and to communicate with each other while ensuring confidentiality and message integrity.



Our demo will be ready soon, I think we can show it on Wednesday at 3pm, if it fits with your agenda

Wednesday is fine for me

I've just fixed the last bugs.. Next time please let's talk before claiming we are ready..

I'm sorry, I didn't get we still had bugs, anyway good to know you fixed them!

Figure 2. Communication management in PikcioChain

Communication between two entities ν and β can take place either in a synchronous or asynchronous fashion. In PikcioChain, attributes are defined through ***Badges***. Entities in PikcioChain know which badges they provided to which contact, but cannot know how many badges they received from a given contact, nor the description of the associated attribute. For instance, ν may grant β a 'Professional' badge without disclosing the attribute 'Professional' to β, and without revealing who among ν's contacts hold this badge too. This happens since, from a system perspective, a badge b corresponds to a set of DEKs used to encrypt the data accessible to all the contacts provided with that badge (figure 2).

In the first case, both parties exchange messages in real time. Each user stores such messages in her own ***Distributed Data Storage Space*** (DDSS) and shares it with trusted contacts if needed.

In the second case, ν generates a message for β and stores it in her DDSS. Once β looks up for new available ν's data, the message is retrieved. To reply, β follows the same steps: she stores the reply in her own DDSS, then ν retrieves this reply while querying for ν's new data.

Message integrity is guaranteed by the use of digital signature, while communication confidentiality is achieved by encrypting messages with a symmetric DEK computed (in case of synchronous communication) or previously shared (in case of asynchronous one) between the sender and receiver.

Communication is obfuscated through multi-hop routing of messages along friend-of-friends chains in such a way that information on data requester cannot be retrieved. In case of synchronous communication, this hides the IP address of communicating parties2 and therefore their location. In case of asynchronous communication, this also prevents a user ν's trusted peer storing ν's data from deriving the trust relationships between ν and the data requester β.

Conclusion and Future Works

The merge of processes and the interoperability of the technologies developped by MatchUpBox bring distributed, secured, traceable and optimized benefits matching all expectations and requirements of today's data exchanges, insuring the scalability and flexibility of companies' fierce structuration.

We presented an innovative solution i.e. PikcioChain based empowering trust directly in its communication mechanism using Matryoshaka and TCI. Morevover, PikcioChain offers an new ground for blockchain technologies articulated around data and regulations.

Furthermore, PikcioChain through a specific solution builder program i.e. PikcioLab, ambitions to offer businesses to design and build their own smart contracts, while complying with all the data regulations using permissions through communication management.

References

[1] Westin, Alan (1967). *Privacy and Freedom*. New York: Atheneum. p. 7.

[2] https://hbr.org/2017/03/how-safe-are-blockchains-it-depends

[3] Wang, Ji Zhi, Ying Long Wang, and Shu Jiang Xu. *A novel anonymous authentication scheme in ad hoc network*s. Advanced Engineering Forum. Vol. 6. Trans Tech Publications, 2012.

[4] Albrecht, Jan Philipp. *How the GDPR Will Change the World*. Eur. Data Prot. L. Rev. 2 (2016): 287.

[5] http://blogs.harvard.edu/vrm/

[6] Agustin, Joy M., and William McDaniel Albritton. *Vendor Relationship Management*. 2001.

[7] Tajima, Yuichi, et al. *Personal information management system, personal information management method, and information processing server*. U.S. Patent Application No. 10/202,320.

[8] Petar Maymounkov, David Mazières. *Kademlia: A Peer-to-Peer Information System Based on the XOR Metric*. International Workshop on Peer-to-Peer Systems IPTPS 2002, p. 53-65.

[9] https://blockgeeks.com/bitcoins-energy-consumption/

[10] Iddo Bentov, Charles Lee, Alex Mizrahi, and Meni Rosenfeld. 2014. *Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. Perform*. Eval. Rev. 42, 3 (December 2014), 34-37.

[11] Dervis Karaboga; Bahriye Akay. *A comparative study of Artificial Bee Colony algorithm.* Applied Mathematics and Computation, 2009, vol.214, no.1, pp.108-132