Utilizing Blockchain technology for data analysis and interaction through The Formal Method of Things

Anwendung von Blockchain Technologie zur Datenanalyse und Interaktionen durch den Formal Method of Things

Blagovest Kirilov

Faculty of German Engineering and Economics Education,
Technical University Sofia, Sofia, Bulgaria

***Abstract* —** This paper looks upon utilizing blockchain technology for data analysis and interaction through the Formal Method of Things (FMoT), using Process and Trust as its main building blocks and focusing on security, scalability and data input for different applications and usages by end users, devices and systems. The main focus is on the utilisation of large amounts of data whilst also keeping user profile security and interaction abilities at a high level.

***Zusammenfassung* —** Dieses Schreiben betrachtet die Anwendung von Blockchain Technologie zur Datenalyse und Interaktion durch den Formal Method of Things (FMoT), durch Prozesse und Vertrauen als Hauptbausteine des Systems. Der Fokus liegt auf Sicherheit, Skalierbarkeit sowie Dateneingabe für verschiedene Anwendungen durch Nutzer, Geräte und Systeme. Es wird grundsätzlich die Bearbeitung von großen Datenvolumen sowie Nutzerprofilsicherheit und Interaktionsmöglichkeiten mit dieser Methode beschrieben.

I. Introduction

A draft process flow model is an outline that gives the base process steps for the formalization of a data analysis and interaction process. Overlying on this, an interface should be created that will enable the rollout of the formalization for all types of data input, as well as all methods to be used. This model features end-to-end functionality, going from the pre-analysis and integrated descriptor checks of input data through applying data analysis methods through formalization and ending in user output. This method will be further described in this paper.

Given the development and importance of the topic for all industries and public areas of importance, this would give a solid foundation for a set-up of "formalization to various methods, so as to have scalability, cost-effectiveness and future-proofing going ahead" [1].

II. The Formal Method Of Things

FMoT uses an entirely new approach to digital and realworld processes. Any and every process can be broken down into a series of tasks; a finite set of directional but variable, step-by-step interactions between people and objects in a particular location – and therein present a way to manage such processes on any device.

There are two main building blocks to understanding the 'totality' of FMoT. Each block builds upon and enables the next, the blocks are Process and Trust. Each building block has great social and commercial application and value in its own right, solving significant problems and limitations in several fields, but in combination they become exponentially more powerful and virtually limitless in scope and opportunity.

A. FMoT and Process

The first block is understanding that FMoT can manage any given process. Regardless if it is a process, whether it is technology, social, domestic, commercial, logistical, industrial, political, or environmental, FMoT can make this process easier, more efficient intuitive and secure, faster, safer, cheaper and far more seamlessly integrated with all the digital and information resources now available, such as the web and the Internet of Things.

With FMoT each successive task in a process has an easily coded microservice written for it, so FMoT can walk the user through all the variables, the decisions and actions needed to complete the task and move the process forward. Microservices are designed so they can easily be created with anyone with basic web programming skills. Most microservices or tasks have already been written, and will be part of an open source library so the 'process provider' only needs to fit them together in the particular order required for any particular process. Most microservices will be used many times in many different processes. Understanding an organisation's processes, and compiling the open source microservices in order to allow FMoTs to manage those processes will likely become a marketable skill.

Processes are often aggregated (by organisations, groups, businesses and individuals) with many process-streams feeding into each other to become larger more complex processes. Even the most complex multi-stream, multi user processes can be easily and intuitively managed by FMoT

It is the user letting FMoT know their location that triggers and defines the process options for that location, according to the users trust and access status, their preferences, community and business affiliations and the location specific processes they choose to interact with. They might want to open a security door, check out tonight's offers in preferred local venues, or select which fruit trees to harvest, it is the location

and personal settings and permissions that will determine what process options are relevant and available. The interface, menu options, buttons and even the entire appearance of the application will seamlessly change according to the user's location, process, task, services, subscriptions, permissions and the objects in the user's current location.

Objects are often produced, transformed or consumed in some way during a process or task. Pre-existing objects may change status or are transformed into something new; stock becomes a sale, raw materials become a product, an off-light switch becomes on, a stranger becomes a friend, an unoccupied restaurant table becomes occupied. With FMoT, objects can communicate their location, their present status, and what they need to further the process or task to the user in that location. They can even communicate their entire history to users, and authorized users in the object's vicinity can communicate with those objects and update their status and history in real time.

Using FMoT and blockchain technology it will be theoretically possible to publicly verify all the details of an object's supply chain, the entire history of a product/project; where and how raw materials were sourced, who handled/processed/transformed it, how where and how long it was stored and at what temperature, who bought and sold the object and at what price, how it was broken and how/who fixed it and so on. For example, a garden chair is an object that arises out of a number of unrelated process streams and transformations that just happen to converge in its production and are only related to each other by its production. The chair can reliably let merchants middlemen and consumers know the details of multiple process streams that are otherwise unrelated and unavailable.

The object itself can let us know what forest the timber came from, how that forest is managed and through what environmental protocols the trees were selected for felling. But also the previously separate details of the entire process regarding the preservative chemicals which have been applied can be added to the chair's database. The constantly updating and aggregating information belonging to that object moves and travels with it through time and space in its own distributed (non-centralised) database, to be retrieved or added to by the chain of producers and consumers along the way. When this information is committed to a blockchain it cannot be altered or erased and it can be verified. However, some (or all) information regarding the chair and its production streams may not be recorded by FMoT, or it may be encrypted or privatized, requiring private keys to unlock portions of the information now belonging to the chair. So for example a sawmill may entirely privatize the name of the particular sawmill operator that day (only available to the company in case of complaint), make the price paid for the timber available to particular users (their accountants), whilst choosing to make entirely public their company name and location for retrieval by anyone that interacts with the object's database further down the line. Ultimately the extent to which information is made publically available will be subject to consumer demand and uptake of FMoT along the process of production but FMoT provides the means by which whole new realms of communication and accountability become possible as demanded. In reality there will likely be gaps in information and a mixture of private and public information, but this will still massively enhance efficiencies, as producers, consumers and middlemen learn to converse with each other publically and privately, directly and indirectly in all kinds of ways generating new demands that have not been conceivable up until now.

It is important to re-iterate that use of FMoT does not ever require, store or broadcast personal data unless specifically authorized by users. Hard anonymity and encryption is ensured by personalized public/private keys.

With FMoT an object's needs and status, it's own history and process, can continually be updated in real time by the object itself, by other users, by the location, or by other objects. This can enhance efficiencies and prevent wastage.

An object can accumulate information through feeds of data from many different sources and communicate them to the process in hand, updating the task and the user. In this way the huge FMoTential of internet of things will start to become realized. For example a bottle of milk could update its use-by date and communicate that to a domestic consumer via their fridge, according to the temperature data previously logged in a transport container.

B. FMoT and Trust

When the Process functionality of FMoT is combined with further blockchain innovations it becomes possible to solve a very significant and longstanding problem in the digital and virtual fields, which is the issue of Trust. Trust is the second building block to understanding the application.

The internet of things has so far been very vulnerable to hacking and misuse of data collection. Furthermore, people's precious identities and data have also been widely exposed to fraud, theft and manipulation in both the 'real' and virtual worlds.

The Trust, and cross-blockchain application that of FMoT will make it inherently anonymous and secure, yet provide the opportunity for users to maintain a unique Trust profile. To do this FMoT does not require biographical or biometric data, and so does not store it. FMoT is location aware but cannot be used to track or trace a user, nor can it be used to transfer real world biographical identity to malicious actors. Nonetheless it will be possible for users to establish a self-asserting Trust identity.

If Trust can be digitally and reliably established, it enables an entire new realm for further technical innovations.

Trust is an emergent property of FMoT, meaning it becomes available, reliable and more useful through widespread (local) adoption, as well as regular use by each individual user.

FMoT allows users to establish and maintain a self-asserting, anonymous, digital Trust profile or identity, and it requires this Trust identity in order to use it fully. What that means is the ability to demonstrate that I am a real person, with a real life, in the real world, that I am only one person and that I exist and am sovereign, and only I (its creator) can be me and use this identity. My Trust identity cannot be sold, stolen, forged, or hacked, and it cannot be used against me because it has to be earned through the unique complexity of having a complex life in the real world.

The more I use FMoT the greater the trust I earn. My FMoT Trust identity is self-asserting, it needs no permission from anything or anyone to exist and it cannot be turned on or off by anyone but me. Even better, this trusted identity does not require biometric data, or any biographical data from the real world to function, in that sense it is a completely anonymous, secure digital representation of me.

Trust is perpetually earned and maintained by everyday use of FMoT in many different ways, by the processes of my life in my location. If I cease to use and perpetuate it, it diminishes

and eventually ceases to exist. If I move location, or step outside of the established routines and connections of my life, it decreases until I re-establish or earn it through the regular processes of my new life circumstances and through the unbroken connections to my previous life.

This Trust identity is like my digital shadow, it gains its existence only from me, follows me everywhere and simply cannot convincingly be used by anyone but me, because anyone else will inevitably change its 'shape' and thus instantly reduce its trust value. If anyone else tries to use my identity it will quickly morph and become the identity of their real-world life and will lose its conformity to me, and thus its Trust value. It derives its form, its unique signature and its resolution from the uniqueness and idiosyncrasy of its creator and user's everyday process(es). Just as I cannot cast two shadows simultaneously, nor can I convincingly maintain two robust Trust identities.

I cannot sell it or give it away because the recipient is not me and cannot artificially pretend to be me whilst maintaining their own trusted identity, because they would have to inhabit my life in order to represent me. If someone does 'inhabit' my life and try to mis-represent me, they must do so in my locality and they must forgo their own original and unique trust identity; users cannot inhabit two identities. Nor can my precious, three dimensional, real world identity be identified by any party interacting with my digital shadow unless i choose to reveal it. If my Trust identity is compromised in any way I can simply turn it off and re-establish a new one.

C. *FMoT and the trust blockchain*

FMoT will launch an entirely public blockchain dedicated to trust with its own native token to establish and maintain trust for users. The trust blockchain will also act as a gatekeeper, only allowing trusted users to interact with an unlimited number of other, entangled blockchains behind the trust 'gate' (cross chain applications). Everybody will be able to become a node and/or use the Trust blockchain not just users and developers of FMoT.

The trust blockchain means that even public blockchains associated or entangled with it can in effect be compartmentalised, or localised, only ever being seen or interacted with by people that have established and maintain trust in a specific locality. Trust on the trust blockchain is established and maintained by users in a particular location, and so the public trust blockchain can be used to direct local users to local blockchains. If a user has not established trust in a given locality they cannot even know what blockchains exist in that location and they cannot be viewed or interfered with remotely. Applications and chains associated with or regulated by the public trust blockchain are in effect public-but-compartmentalised, since anyone can theoretically start or run a node or subscribe to its services but only so long as they are a trusted user in a specific locality. This will enable the creation of local transactional cryptocurrency without the security overheads of Bitcoin and the other (fully) public blockchain cryptocurrencies, which will leave them to do what they do best, being a secure store of value and means of large and international transactions.

This also negates the risk of quantum attacks as they would have to be very targeted and would only provide a very small segment of information and FMoTential gain.

The candidate pc or device used to create or download and run a local (compartmentalised) transactional blockchain node is an object which has to be assigned trust by a trusted user in order to become a node. To run such a node, the device must be continually trusted by at least one trusted user. If the node device has only one trusted user assigning their trust to it, if that user loses trust then so does the device, and both are excluded until trust is restored. Or, if the node behaves badly and loses trust, the single assigned user will also lose trust; either way both user and node device lose trust and are excluded from the network. However, any object (such as a node device) can be assigned trust by more than one trusted user. In this case, if any single user loses trust the node device will still be trusted by the other trusted users and can continue to run the node. But if the node behaves badly all the associated users of the node will lose trust.

III. Summary

FMoT is a wide-ranging, multi-purpose digital application able to connect people and the processes of the everyday 'real-world' with the virtual world, the internet of things and the web. It does not only cover the aspect of integrating data analysis as a formal method, but also utilizing the results and combining this with links to many innovative technologies, giving the formal method its proof of concept as well as outlook for future development.

References

[1] Gregory Piatetsky-Shapiro, *From Data Mining to Big Data and Beyond*; April 18, 2012 [Inside Analysis]; https://insideanalysis.com/data-mining-and-beyond/

[2] IBM – Analytics, Jennifer Clemente: *Big Data in production*, Data & AI, Cloud, IBM 2016 [from use-cases to production] , https://www.ibmbigdatahub.com/blog/bigdata-challenge-transformation-manufacturing-industry https://www.ibm.com/analytics/hadoop/big-data-analytics

[3] International Data Corporation (IDC) - *Big Data and Business Analytics Forum 2013*, February 2013 [Topics of interest covered on forum: Data quality standardization, Complexity and compatibility of data, Hadoop, MapReduce, and the technologies behind Big Data analytics https://idccema.com/eng/events/54106-idc-big-data-and-businessanalytics-forum-2013]