Smart Statistics for Smart Applications

Book of Short Papers SIS2019

Editors: Giuseppe Arbia, Stefano Peluso, Alessia Pini and Giulia Rivellini

PUBLISHED BY PEARSON

WWW.PEARSON.COM

Giugno 2019 ISBN 9788891915108

Preface

Section 1. Plenary Sessions and Round Table

Section 2. Invited Papers

Section 3. Contributed Papers

Section 4. Posters

Preface

Preface

This book includes the scientific contributions presented at the Intermediate Meeting of Italian Statistical Society (SIS) held in Milan at the Universit Cattolica del Sacro Cuore, from June 18th to 21th of 2019. Following a long tradition (and a statutory indication of the Society), the intermediate meetings are held bi-annually on specific themes. This year, aiming at bridging the gap between statistics and the world of Big Data and Data Science, the conference was entirely devoted to the theme of "Smart Statistics for Smart Applications". In this way the Italian Statistical Society had the explicit intention to answer the high and rapidly increasing demand on the subject, by providing academics, researchers and practitioners with a forum where new ideas and new methods could meet with new needs, new research questions and new applications.

The Conference could not have been organized without the joint effort of the Milanese network of Universit Cattolica del Sacro Cuore, Universit degli Studi di Milano Bicocca, Universit Bocconi, Universit "Vita e salute" San Raffaele, Politecnico di Milano and Universit Statale di Milano. Members of all these universities took part actively to the Local Organizing Committee. The Conference has also greatly benefited from the contribution of the strategic partner Mathesia, which contributed to the various aspects of the organization, with special focus to the active involvement of private firms and companies and of the non-academic components.

The conference has registered more than 200 scientific contributions, including papers presented in plenary invited sessions, papers collected in specialized and solicited sessions on specific themes, about 100 contributions spontaneously submitted to the Program Committee and a poster session. All contributions were focused on the conference theme and provided a good overview of the state-of-the-art of the subject, from methodological and theoretical contributions, to applied works and case studies. The two plenary lectures were devoted to the (provocative) idea of "shallow learning", as opposed to the more in-vogue idea of deep learning", and to the problems linked with Big Data veridicity and reliability. A plenary round table draw the participants attention on the concept of smart ageing.

A distinctive feature of this conference, relative to previous analogous experiences, was the presence of many round tables and activities focused on topics of interest for a wider audience, freely open to external participation. These activities were termed Fuoriconvegno" and included a special session on "Data skills: Statistics and education for future jobs" organized jointly with Pearson Italia Publisher, a round table on "How to Close the Gap Between the Practice and Theory in Digital Transformation Era" organized joint with Mathesia, a colloquium on "Big Data and Big Responsibility", a round table on "Political polls in the Big Data era", a round table on "Big Data and Public Administration", a round table on the changing role of the statistical scientific societies in a new interconnected world and the fifth edition of the statistical competition "Stats Under the Stars (SUS5)" organized by the Bocconi University, a whole-night hackathon on real-world business analytic problems for young Data Scientists.

More information about the fuoriconvegno activities may be found on the website of the meeting[1]. We offer this book to all members of the Italian Statistical Society, to all participants of the conference and to all interested people, in the hope that this will provide them with a good snapshot of the on-going research in this exciting new area of statistical studies. We deeply thank all contributors for having submitted their work to the conference and all the researchers who did an outstanding job in acting as referees accurately and timely. Finally we wish to express our gratitude to the publisher Pearson Italia for all the support received.

Giuseppe Arbia
Stefano Peluso
Alessia Pini
Giulia Rivellini

[1] URL: http://meetings3.sis-statistica.org/index.php/SIS2019/sis2019/schedConf/overview

Blockchain as a universal tool for business improvement

Massimiliano Giacalone, Diego Carmine Sinitò, Emilio Massa, Federica Oddo, Enrico Medda, Vito Santarcangelo

Abstract: The aim of this work is to present the characteristics of the blockchain technology and its potential in corporate case study applications. The paper presents in detail an example of the implementation of permissioned blockchain and other examples of blockchain (also of semantic type) applied to the temporal certification of business processes of some brilliant southern Italy realities.

Key words: blockchain, bitcoin, safety for business

1 What is the Blockchain and how it works

Thanks to the fame of the bitcoin cryptocurrency, lately also blockchain technology has become object of great attention. Blockchains, thanks to their properties, are becoming an increasingly popular tool for companies that need to certify and keep their data safe.

1.1 Blockchain and Bitcoin

If we would ask someone what a blockchain is, they probably would link the answer to the word bitcoin. But how are bitcoin and blockchain related? This two entities were born simultaneously, however the blockchain is independent from bitcoin and the demonstration of this is in the evolution and the birth of new types of blockchain. Satoshi Nakamoto, pseudonym of the creator of cryptocurrency bitcoin, in his paper "Bitcoin: A Peer-to-Peer Electronic Cash System" introduces a system for the exchange of a virtual currency that does not require a financial institution that certifies the transactions. In this new scenario the problem of double spending was solved by using a distributed register where all the transactions are kept, which bases its security on a system of signing transactions with public key - private key, hashes and a proof encryption. The register obtained would be immutable unless after an

alteration the attacker had sufficient computing power to perform the cryptographic test again for all the blocks that make up the register before the other participants in the network.

1.2 Blockchain: structure and types

When a user makes a transaction on the bitcoin network, this is announced publicly to all the nodes that are part of it, in this way it is possible to certify that the transaction took place in a specific time (timestamp). Each node collects all new transactions by forming a block. When a block is complete, it can take part of the chain after passing a cryptographic test. The prof-of-work at the base of bitcoin is the increment of a numerical value, called *nonce*, which causes the block hash to start with a certain number of zeros. Once the cryptographic problem is solved, the node communicates to all the other nodes the solution found. Nodes accept blocking only if all transactions within are valid and they express their acceptance by creating the next block which includes the hash of the block that has just been accepted. Thanks to its distributed structure and the large number of nodes, the blockchain guarantees the immutability of data and business continuity.
This kind of network is also called public, this means that anyone with a device connected to the internet can become a network node and can take part at the creation of blocks and the validation of new blocks or have access to the entire transaction register. Various types of blockchain which provide for a form of centralized authority have been recently developed. In permissioned blockchain, unlike public blockchain, access is restricted to some users only. Furthermore, the central authority defines the role of a user within the network and to which information he has access. There are different levels of access to the network, each with different functionalities:

- Reading the ledger, which may be subject to certain constraints or may be accessible for all nodes.
- The possibility of making transactions within the network, which must then be validated and inserted into the blockchain.
- Perform block mining and validation operations.

This more performing kind of blockchain, is therefore preferred by companies that want to maintain a high level of confidentiality of their data while benefiting from all the characteristics of the blockchain.

2 Safety for business

The blockchain is designed to keep safe and unaltered the data inside. The data are inserted into the blocks in way to create a chain held together by the integrity of the same data. If a single data is altered the whole chain is invalidated.

2.1 Block composition

This security is guaranteed by a particular string of 64 characters called *hash* which represents all the information encrypted within a block and must meet previously agreed criteria. This *hash* is an alphanumeric string of characters generated by the SHA-256 function. The block is made up of different fields based on the use that you want to make of the blockchain and the data you want to protect. There are some fields of the block that are essentials for the blockchain to be well structured and capable of being efficiently constructed and these fields are:
An **index**, which allows to uniquely identify each block; the **timestamp**, which allows to identify the exact moment in which the block is generated; the **hash** of the previous block. The last data allows to create the famous "chain", each hash of a block will become a fundamental component of the next one. *Nonce* is a really important value for the respect of all the above mentioned criteria and will be further analyzed later; to all this basic information we must add all the ones we want to actually store safe and intact. For the realization of a new block, it was achieve a function which allows to obtain the index of the last block inserted.

2.2 "Chain" creation

It was created a function that permit, after obtaining this information, all of this data to be acquired. This function (*push ()*) takes care of acquiring information such as index, timestamp and all the data we want to preserve. Within this function, once the hash of the previous block has been obtained (through its index), the block index is incremented so as to become the index of the block that we are currently inserting. Next, the heart of the insertion: the function that deals with "undermining" and creating a hash that allows to respect the criterion.
This criterion is useful because it allows us to create a non-trivial and indipendent hash of the data we actually want to memorize, for this task is used the *nonce*. The *nonce* is initially set to zero. The hash is generated with all the data, index, timestamp, information to be stored, previous block hash and the *nonce*, then it is consulted a function that generates the hash through SHA-256 encryption. If the criterion is respected, the block is added to the chain, otherwise it enters in a *while* loop. The while condition is repeated until the hash is composed in such a way as to meet the previously decided requirement. For each iteration the nonce is

incremented by one, this allows to generate a completely different hash for each iteration, up to the requirement. The more difficult is the requirement to achieve, more iterations will be needed, greater will be potentially the nonce value.
Once the wanted hash is obtained, the block is completed and the information obtained can be safety stored.

2.3 Validation of the process

All the information are stored in a database. For this reason there is the possibility that somehow they can be modified, so it is necessary to use an algorithm that allows to understand if the blockchain has been compromised and is invalidated. This is made possible thanks to a function that runs through the entire blockchain and recalculates the hashes of all the blocks: through a *for* loop, a specially created matrix crosses each block and verifies its integrity. At each iteration through the data present in the array, the hash of the block is recalculated and compared to the stored hash. The hash of the previous block must coincide with the previous hash of the current block, if one of these two conditions is not respected then the blockchain has been invalidated. If successful, the iteration will be repeated until the whole blockchain is verified.

3 Cases study analysis

We will show below several case studies in which the blockchain was used with various kind of implementation. This will explain the potential, the possible uses and developments of this new technology that holds great potential for all the multiplicity of services or processes which need information integrity, time validations and business continuity.

3.1 L'Antincendio Srl

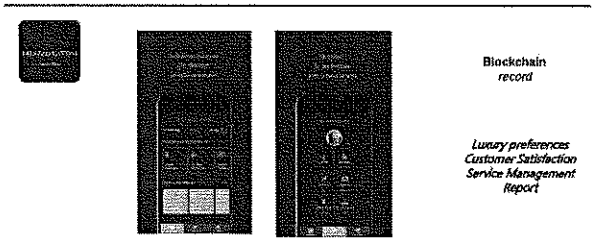
When we talk about services or products designed to guarantee people safety, the temporal certification and the integrity of the information about them becomes a fundamental factor. In this context the company L'Antincendio Srl has found an answer in the blockchain technology that has been used to map and certify all the maintenance and customer reports on each individual fire extinguisher. In this way you will not only have the possibility to reconstruct the time-certified history of each individual fire extinguisher, but you can also analyze the information in order to obtain the security level of the product with the certainty of data integrity. This is a clear example of how this technology has been used by a company to improve the level of safety of its products.

3.2 *Capurso Azienda casearia Srl*

The case study about Capurso Azienda casearia Srl is different, in this example the company, in order to protect the quality of its product and remain compliant with the DOP hygiene standards also in key 231, required an effective tool for mapping all the processes concerning the production of the raw material (cow's milk), in this case the blockchain was used to guarantee the integrity of the data during the audit of the entire production process of the raw material and to certify the history of every single dairy cow allowing the company to pursue increasingly higher quality standards.

3.3 *Palazzo Gattini*

A very special case study concerns the bockchain implemented for the Palazzo Gattini structure, which offers luxury services with high quality standards and interfaces with a very demanding clientele. In this case, it was decided to map not only the entire process concerning the service offer, but also the preferences of each individual user (luxury preference) and the customer satisfaction within the ledger. Given the strong semantic link between the customer and the information saved on the ledger, it has been used a semantic blockchain, that is to say that within each individual block there will also be the hash of the previous block concerning the client in question, in this way we can analyze in a better way the information collected to obtain the level of luxury compliance of the structure.



3.4 *Erreffe Srl*

We can find another example of the use of blockchain in the project manager of Erreffe srl, in this case all the tasks within the company have been mapped in the ledger with the related processes according to the individual tasks, it has been fundamental to certify all the progress in order of time in way to be able to view and analyze the evolution and of the progress with complete and certified data.

3.5 Caldarola Srl

In the last case study the blockchain technology is used by the company Caldarola Srl for the vehicle rental software. Here, all the information (generic or about maintenance) related to the individual vehicles present in the company are saved in the blockchain including picking and releasing. In this case the time certification has a great value in order to allow the company to know the current status of all vehicles and to be able to view the chronology of all the maintenances working on integral data and with certified time values without using particularly complex processes for this kind of certification.

4 Conclusions and further developments

This paper presented interesting application developments of permissioned blockchain applied to practical case studies of small companies in southern Italy. Incorporating the potential of this technology in the processes of southern SMEs is an indication of how much this technology is transversal and of great importance for business improvement and for meeting regulatory compliance requirements.
An example of application may concern the certification of machinery 4.0, as the interconnection of the same can be proved by blockchain recording of the data of the interconnection of individual machines, which would have probative validity. From this point of view, the process of processing certified log via blockchain, which would allow to compare the certified "real process" with the company procedures in order to determine a certified "process gap", can also be applied.

References

1. Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. *https://bitcoin.org/bitcoin.pdf*.
2. M.Colucci, UIBM, Patent, 27/12/2018 - 102018000021061, Sistema ad alta innovazione per la certificazione dei processi di manutenzione antincendio
3. F.Fanari, V.Santarcangelo,D.C. Sinitò, Esperienze di Ricerca e Sviluppo applicate alle brillanti realtà del nostro sud,RCE Multimedia, 2018
4. A. Brandonisio, UIBM, 28/12/2018 n. 102018000021313, Sistema basato su blockchain per la certificazione di filiera di prodotti caseari
5. E. Grassano, UIBM, 02/01/2019 rif n. 102019000000025, Sistema blockchain oriented per la certificazione dei servizi di una struttura luxury
6. R. Festa, C. Dell'Acqua, S. Burgi, UIBM, 2019, "Sistema intelligente per la gestione di commessa mediante blockchain in ottica BIM"
7. M.Masi, UIBM, Rif. 102018000007495, Sistema basato su blockchain per il controllo della flotta in compliance
8. M.Masi, SIAE 21/08/2018,Rif. 012763, Sagest Fleet Gdpr Blockchain