IEEE Smart Cities

IEEE

BOOSTING THE DEVELOPMENT OF SMART CITIES WITH THE BLOCKCHAIN

Lorenzo Ghiro - Department of Information Engineering and Computer Science (DISI) - University of Trento Trento, Italy
lorenzo.ghiro@unitn.it

Abstract—Urbanization is taking place worldwide and fast, so much that 66% of the world population is predicted to live in cities in 2050. This massive movement of people from rural to urban areas pose challenges for municipal governments. Resources used to run services like the municipal transportation or healthcare systems will not keep up with the rhythm of the population's growth. To meet the growing demand of resources, cities must evolve and build advanced, large-scale networks able to efficiently retrieve and distribute the needed resources. Not only, the same citizen should have access to different services that may need to share information to interoperate correctly. Multiple networks will therefore need a common technological layer where confidential data about citizens can be exchanged and stored securely. The emerging technological tool to implement such platform, so to empower the Smart Cities of tomorrow, is the blockchain. But what is a blockchain? How does it work? Which applications for Smart Cities can we run on top of it? The goal of this paper is to answer these questions.

I. INTRODUCTION

Smart Cities of todays –and even more tomorrow– are smart as long as they are constituted by a mix of advanced technologies, combined together and accessible via various kinds of network. Such networks are predicted to grow up to an extremely large scale: in 2020 they will have to bring Internet-connectivity to 20 billions1 of "things". These things are not traditional devices like PCs or smartphones, but will be limited-purpose objects like gas meters, vending machines, connected cars and many others that will all need an Internet connection to be managed automatically so to perform their task efficiently. This depicted network is called Internet of Things (IoT), and nobody doubts on the prospective impact of IoT on economy as long as it can shape new digital businesses or enhance the already existing ones. Also Smart Cities will be built on top of IoT. For instance, most advanced cities have already implemented intelligent streetlights systems or environmental monitoring platforms connected to the Internet to let citizens interact with. The pervasiveness of IoT will increase always more up to affect the medical care sector, where intelligent and inter-connected robots are expected to perform nurse operations in the near future. This also means that sensitive data of citizens will flow on these extremely large networks, virtually exposed and accessible from billions of access-points that can't be completely secured. We need to plan a suitable architecture in order to grant, at the same time, security of users' data and scalability. Scalability is indeed another requirements of the utmost importance. Every week 1.3 million people moves into urban districts and by 2050 the 66% of the world's population will live in cities2 (see Fig. 1). Therefore, the amount of data daily carried by a Smart City and IoT network will scale to an unseen size, asking for ad-hoc innovative technological solutions.

The principal advocated solution, widely debated and still on the stage, is the blockchain, already identified in the litera- ture as main tool able to empower the future Smart Cities [1], [2]. The blockchain is said to be an implementation of a Shared Ledger (SL), basically it allows multiple users to cooperatively store data validated by the users' majority and can also offer fine-graned access policies, ensuring access to confidential data only to authorized users. The blockchain may also serve as the interoperable platform where different services may converge to exchange data in a transparent and auditable manner. The peculiar features of the blockchain technology, in particular its ability to store unmodifiable records of data, opened the way for a further potentially disruptive technology: Smart Contracts (SCs) [3].

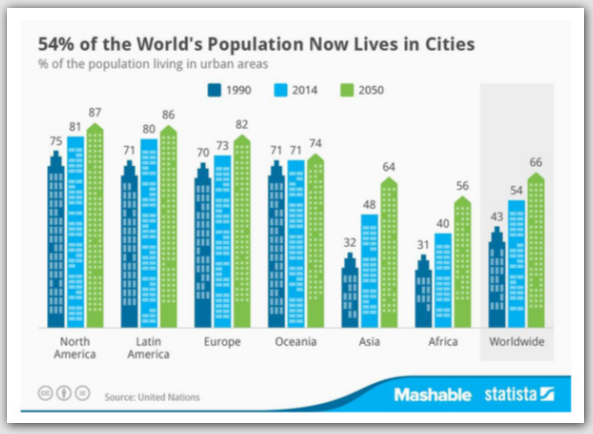

Fig. 1. Prediction on the population distribution in 2050. The 66% of the worldwide population will live in an urban area. (source: http://wln.ecology.uga.edu/index.php/what- is- urbanization- and- what- is- gentrification)

How can the blockchain be so disruptive? What is the underpinning technology empowering all the blockchain's features? This paper will try to answer these questions, then the prospective impact of the blockchain in shaping the new generation of Smart Cities will be highlighted outlining a list of applications (including SCs) that can be run on top of the blockchain and that will ease the life of smart citizens. In Sec. II the fundamental working principles of the blockchain will be explained. Given the current but not always justified hype on the blockchain, a special consideration on the circum- stances in which a blockchain should not be used is included to end Sec. II. In Sec. III the most relevant applications that can be built on top of the blockchain and that will drive the Smart City revolution are described and analysed. In Sec. IV final considerations are forwarded.

II. WHAT IS A BLOCKCHAIN

The blockchain can be described and defined in different ways. For a computer scientist, a blockchain is a data struc- ture3 that offers the possibility to store chronological records of Transactions (TXs), thus is nothing more than a database technology. Moreover it is a component of a distributed system. This distributed system includes a Peer-to-peer (P2P) network4, a computer network where users publish their TXs, plus a consensus mechanism, a protocol accepted by all users to find an agreement on what TXs should be considered valid and hence should be stored in the blockchain. From an higher-level prospective, the blockchain is a Dis- tributed Ledger, meaning that there is not a single and cen- tralized authority that verifies and executes TXs. Conversely, participants of the P2P network cooperatively verify and validate TXs, without relying on a trusted middle-man. For an economist or a sociologist, the blockchain represents therefore a tool to build trust among untrusted agents, a trust that depends on the rules agreed by participants to accept or reject proposed TXs. The different combinations of these rules originate different implementations of blockchain systems. For instance, if any (untrusted) participant can propose the approval of some TXs, then we refer to a permissionless or public blockchain. Participants of the network can be malicious, no trust among parties can be assumed, therefore typical consensus mecha- nisms adopted in a public blockchain are very heavy, so that an attack to tamper the blockchain would have a prohibitive cost. An example of public blockchain is the one that empowers the most famous cryptocurrency, the Bitcoin, which implements a very costly consensus mechanism known as Proof of Work (PoW). PoW has its own PROs and CONs. On the one hand, it secures the blockchain but, on the other hand, it limits the scalability performances. When only a selected group of users can approve TXs, and members of this group usually share at least a minimum and mutual level of trust, then we refer to permissioned or private blockchain. In this kind of blockchain, the preferred one of banks and big corporations to implement their internal ledgers, the adopted consensus mechanism is lighter, leading to enhanced scalability performances.

All the required terminology has been introduced so far, the reader should now be able to understand the fundamental working scheme of a blockchain as illustrated by Fig. 2

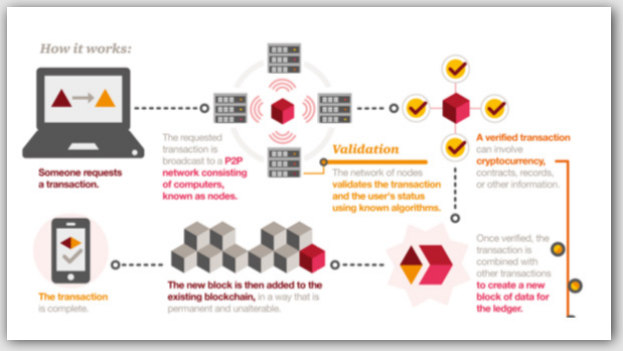

Fig. 2. Flow-chart illustrating how a TX is processed before begin stored in the blockchain. (source: https://www.pwc.com/us/en/industries/ financial-services/fintech/bitcoin- blockchain- cryptocurrency.html)

Everything starts when a user submits a TX to be stored in the ledger, so to be accepted. The user publishes its TX in the P2P network of validators, i.e. those nodes that verify the TX's validity and perform the consensus protocol. If the TX is valid, then it is appended to the blockchain so that, from now on, everybody will know that some assets have a new owner. Finally, after the TX is really approved and appended to the blockchain, the users involved in the TX are notified about the success- ful status of their operation.

It is worth to understand how the blockchain data structure ensures the immutability of recorded TXs and why a consensus mechanism is needed to validate them. To this purpose, a more technical and detailed description of the Bitcoin blockchain will be provided as case-study.

A. The Bitcoin blockchain

The first famous description of a block- chain system ap- peared in 2008 in the renowned paper: "Bitcoin: A peer- to-peer electronic cash system" [4], whose author is still

unknown, except for its mysterious pseudonym Satoshi Nakamoto. At that time, Nakamoto introduced the blockchain as a tool to solve the "Double Spending problem", a problem that may arise for two main reasons. The first is that crypto- currencies, as digital assets, have no kind of banknotes' watermark to prevent the unauthorized creation of money. It is therefore impossible to distinguish a valid crypto-coin from a copy, that could in principle be used to spend two times the same coin. The second reason derives from the general limitations of a distributed system. Because of propagation delays, different TXs that spend the same money may be received in diverse order by distinct validators spread in the P2P network. Nodes need therefore to agree on TXs order to determine which came first, and thus is valid, and which after and must be rejected as being a fraudulent Double Spending attempt. This is why a blockchain needs a consensus mechanism: to let different nodes agree on the order of TXs, thus implementing a countermeasure to Double Spending. Nakamoto proposed the blockchain as part of the implemen- tation of the Bitcoin system, realizing a distributed timestamp server able to order and safeguard transactions. The core idea is to group TXs into timestamped blocks and to exploit Cryptographic hash functions (CHFs)5 to make these blocks immutable. In fact, thanks to CHFs it is possible to record the history of TXs immutably as if they were written in a SL set in stone.

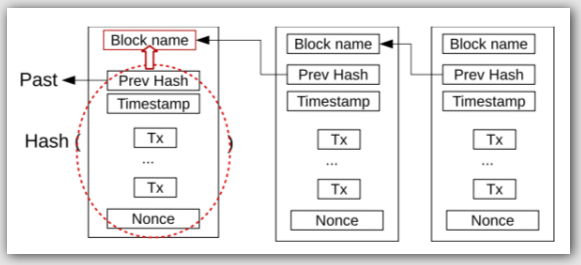

Fig. 3. A chain of blocks and the illustration of a single block. (source: "Proof of Networking: Can Blockchains Boost the Next Generation of Distributed Networks?" [5])

To exploit CHFs, each block of the chain must contain a set of TXs, a timestamp, the hash fingerprint of the previous valid block (i.e. the hash name of that block, and also a link to it), and a nonce6, as shown in Fig. 3. A block is valid if its content, hashed with a CHF, produces a very particular hash name with a predefined number of leading zeros. The node that discover a nonce suitable to produce a valid hash name is allowed to add a TX to itself of a certain amount of Bitcoin as a reward for having found such nonce. Given that finding a good nonce is a mathemati- cal very hard task which requires a huge computational effort, and given that this work is necessary to be rewarded with new Bitocoins, validator-nodes that are constantly at work searching for good nonces are metaphorically called "miners". The work of miners is useful to generate new Bitcoins but also to make the blockchain immutable or, at least, to make the life very difficult to malicious users intended to tamper the TXs recorded in the blockchain. Consider an attacker that wants to modify a past block, e.g. to revoke a TX in which the attacker spent big money. By modifying an old TX the attacker will invalidate the hash name of the past block containing this TX. That hash name was contained, as back-link, also in the following block, that consequently is invalidated as well. With a cascade effect all subsequent blocks are invalidated. In conclusion, an attacker that wants to alter a past block needs to rebuild many blocks which is extremely hard because it means that this attacker must find many nonces. The strategy of requiring the solution of hard cryptographical puzzle (i.e to find the nonce) to create a block implements a consensus mechanism known as PoW. Although very secure, the PoW is extremely energy-demanding and leads to the main criticism directed to the scalability of the Bitcoin blockchain.

B. Distributed Consensus

In the Bitcoin blockchain, the fundamental consensus prob- lem has been solved requiring the exhibition of a PoW, which ensures an high level of security in front of huge energy costs. If applications requirements related to performance, scalability, consistency, threat model, and failure model are different from the one of the Bitcoin, many different algorithms for building consensus are known in the literature and should be favoured.

Fig. 4. Taxonomy of different approaches known in the literature to reach consensus in a distributed system. (source: "Consensus: Immutable agreement for the Internet of value" [9])

In general, reaching consensus under the usual hypothesis related to distributed systems, i.e. the presence of faulty nodes and unreliable communication channels, is proven to be impossible [6]. However, in practice a good distributed system always exhibits stable periods of correct operations during which different protocols grant to achieve consensus. Among the many protocols proposed under this setting of relaxed hypothesis, a traditional consensus approach is based on several voting processes until a majority (or unanimity) is reached. The multiple voting processes are designed to provide an enhanced fault-tolerance. This is the case for PBFT [7] or variants like Paxos [8], and also the famous 2PC and 3PC algorithms adopt this approach. A different approach to reach consensus resembles lottery games. Among participants, a node able to provide a significant but random proof (a sort of winning tickets) is selected as round's winner, and imposes its decision. If there is a more sophisticated and deterministic way to establish who has the right to impose a decision, then the literature refers to leader election7 approach. In PoW we have seen, the winner is the one which solves a cryptographical puzzle first and the nonce is a kind of winning ticket. There are also other "lottery" systems based on different proofs. A trending one is the Proof of Stake (PoS): chances of a node to be picked to create the next block depend on the fraction of coins owned by that node in the system. For the sake of brevity, we conclude here the review of the many approaches known in the literature to reach consensus in a distribute system, that are graphically summarized in Fig. 4. The interested reader is invited to read more comprehensive and thorough studies of the topic like [9].

C. Do you need a blockchain?

The blockchain is basically a new paradigm to manage data, it falls therefore into the domain of database technolo- gies. What are the main differences with standard Relational databases (DBs) made of big tables full of records of data? In the first place, in a DB data can be inserted as well as deleted, while in a blockchain data can be only appended and are never canceled. In the second place, a DB is usually managed by a single trusted admin that can perform updates with the full read/write speed permitted by the technologies improved and refined over decades of use of Relational DBs. On the contrary, to write a new TX in a blockchain, the TX must pass through the consensus protocol that can take several minutes to terminate. Consider that, on average, in the Bitcoin blockchain the write TXs speed is around 3 to 4 TPS (Transactions per second), while in VisaNet, the sophisticated platform run by Visa to process their customers' TXs, on average the speed reaches the value of 1667 TPS8. There is a 3-order difference in magnitude!

In the author's opinion, the reason that justify using a blockchain is only the following: it removes the need of a trusted authority in an untrusted network, which is an absolutely remarkable fact. However, it also follows that if participants would trust a third party in charge of maintaining the DB updated, then it's much more convenient, in terms of TXs speed, to let this trusted third party use a standard DB. For instance, despite the many proposals in this direction, no voting system should be implemented with a blockchain, as long as each voting system always already includes a trusted party in charge of checking users' identity, so to avoid double voting. Other common proposals based on a blockchain, which are wrong in the author's opinion, are those in which participants in the network share a given level of trust. Of course, under this assumption, users of the system should prefer a fast Relational DB managed by one of the trusted users.

The last common pitfall is to advocate the use of the blockchain when there is no need to keep the full history of the TXs. Again in voting or election systems, users may need a consensus mechanism to vote/elect new representatives, and may want to run many independent instances of the consensus protocol once per each election. Anyway, usually there is no need to remember who was elected in the previous sessions. In fact, at election time very few persons remember who was their prime minister 10 years ago, but still can (rightly) vote. A deeper analysis of the use-cases for a blockchain is presented here [10], an article from which Fig. 5 is extracted. The figure shows a decision tree diagram that should always be very clear in the mind of people advocating for a blockchain solution.

III. BLOCKCHAIN'S PROSPECTIVE IMPACT ON SMART CITIES

The blockchain can trigger a dramatic cultural advancement of the Society, this by encouraging good behaviors of citizens over long periods of time. An example of how this can happen in the context of a Smart City is the following one. Assume that tickets for the public transportation system could be payed with a crypto-currency, namely a municipal crypto-currency with TXs published in a blockchain visible to everybody in the city. The city government can incentive citizens to prefer the bus to the car, for ecological reasons, by setting rewards for people that can prove to daily use the public transportation system. This kind of proof is clearly embedded in the blockchain! The municipality should therefore simply perform monthly analyses of TXs stored in the blockchain and can reward virtuous citizens with, for example, free tickets for buses in the weekend or discounts on the next month's electricity bill. Any possible incentive plan can be imagined and designed so to drive people towards choices that are in the society's best interest, thus the opportunities to improve the quality of life are almost endless. The incentive plan would appear more convincing if citizens could have the certainty that rewards achievable meeting the goals set by the municipal government are timely paid. To this end, a fundamental and already introduced application of the blockchain are Smart Contracts (SCs). SCs are a description of the required inputs to get a given output in form of computer code: they are basically a digital representation of contract's terms. Notice that these pieces of code can embed all the logic of usual contracts, including if-then-else conditions to trigger, for instance, the payment of a ticket only if a given train was not late. By publishing these scripts on a blockchain, no 3rd parties are required to act as intermediaries and this allow for fully distributed and automated work-flows. Beyond automation of contracts, SCs are a tremendous innovation also because they are immutable: once they are published in the blockchain it is almost impossible to change their terms. SCs have the potential to always ensure the fulfillment of contract's terms, also avoiding all those ambiguities that are so often exploited by fraudsters. SCs can then be used by the municipal government to distribute rewards. When a citizen collects enough "points" to claim a reward, where points could be this user TXs regarding bus tickets, the user should submit collected points to a municipal SC. This SC will verify the validity of the claim and will suitably trigger the automatic payment of the reward.

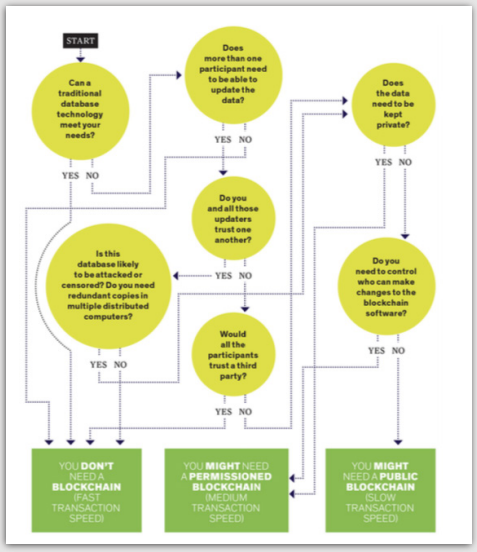

Fig. 5. A decision tree intended to help developers in choosing wheter to opt or not for a blockchain. (source: "Blockchain world-Do you need a blockchain? This chart will tell you if the technology can solve your problem." [10])

Fig. 6. In this illustration the blockchain is depicted as the tool enabling Smart Energy grids, Smart Transportation, Smart Waste Management and Smart Payments. (source: https://www.openaccessgovernment.org/ a-blockchain- based- governance- model/52928)

So far, the blockchain has been discussed and presented as the tool empowering SCs and also able to incentive good, farsighted behaviors of citizens. But the blockchain, being the fundamental pillar to implement crypto-currencies, represents also a platform for microTXs and can open new markets. Other potential applications of the blochchain based on the microTX market concept, as illustrated in Fig. 6, are the following:

Smart Payments: A microTX platform would facilitate all municipal payments including: assistance, welfare, payroll, city programs and so forth.

Smart Energy grids: A resilient power grid could be cre- ated on top of a blockchain, hence empowering a P2P energy market. This allows individuals to create, buy, sell, and trade energy while retaining value, without requiring a centralized management of energy performed by a monopolistic company.

Smart Transportation: As already seen, tickets for the mu- nicipal transportation system could be paid with the municipal crypto-currency. This fact, coupled with incentive plans set up by the city government, would encourage the use of buses and subways thus reducing traffic jams and pollution.

Smart Waste Management: A Smart Waste Management platform could be designed so to exploit the technological advancements offered by IoT. Bins could be equipped with tiny radio-devices that can communicate the bin's status: either not full, almost full or full. Then the duty-cycle of garbage collectors can be enhanced taking advantage of all the information gathered and communicated by smart bins.

IV. CONCLUSION

This White Paper presented both an exploration and investigation about the blockchain technology, identified as fundamental pillar for the future Smart Cities. The blockchain turns out to be a database technology, with a precise focus on recording the full history of crypto-currency Transactions (TXs). It is thus an implementation of a Shared Ledger (SL) in a network of trust-less agents, which enables new markets driven by micro-payments. Trust is achieved among untrusted participants by running consensus protocols, that are almost uncountable in the literature and can differ in terms of scalability, security and fault-tolerance properties. The current hype on the blockchain has been demystified: if the application requirements do not need a full TXs history or participants can trust a 3rd party, then a standard Relational database (DB) should be favored in place of a blockchain. A list of applications empowered by the blockchain, including Smart Contracts (SCs), has been presented to highlight the prospective impact of this technology on Smart Cities. The most appealing idea is to use the blockchain and SCs to both record interactions of citizens with municipal systems and define incentive plans to drive people towards an higher utilizations of these systems. Citizens are therefore encouraged to adopt good and farsighted behaviors which can generate long-term benefits for the overall society.

ACKNOWLEDGMENT

This project is supported by the IEEE Smart Cities Initiative, Student Grant Program

REFERENCES

[1] J. Sun, J. Yan, and K. Z. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," Financial Innovation, vol. 2, no. 1, p. 26, 2016.

[2] S. Ibba, A. Pinna, M. Seu, and F. E. Pani, "Citysense: blockchain- oriented smart cities," in Proceedings of the XP2017 Scientific Work- shops. ACM, 2017, p. 12.
[3] K.ChristidisandM.Devetsikiotis,"Blockchainsandsmart-contractsfor the internet of things," Ieee Access, vol. 4, pp. 2292–2303, 2016.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [5] L. Ghiro, L. Maccari, and R. Lo Cigno, "Proof of Networking: Can Blockchains Boost the Next Generation of Distributed Networks?" in Proceedings of the 14th Annual Conf. on Wireless On-demand Network Systems and Services (WONS), Isola 2000, France, Feb. 2018.

[6] M. J. Fischer, N. A. Lynch, and M. S. Paterson, "Impossibility of Distributed Consensus with One Faulty Process," Journal of the ACM (JACM), vol. 32, no. 2, pp. 374–382, 1985.

[7] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," ACM Trans. Comput. Syst., vol. 20, no. 4, pp. 398–461, Nov. 2002.

[8] L. Lamport, "Paxos made simple," ACM Sigact News, vol. 32, no. 4, pp. 18–25, 2001.

[9] S. Seibold and G. Samman. (2016, Sep.) Consensus: Immutable agreement for the Internet of value. [Online]. Available: https://assets.kpmg/content/dam/kpmg/pd-f/2016/07/kpmg- blockchain.pdf [10] M. E. Peck, "Blockchain world-do you need a blockchain? this chart will tell you if the technology can solve your problem," IEEE Spectrum, vol. 54, no. 10, pp. 38–60, 2017.