IJEMD-CSAI, 1 (2) (2022), 74 – 83 https://doi.org/ 10.54938/ijemdcsai.2022.01.2.142

IJEMD

International Journal of Emerging Multidisciplinaries:
Computer Science & Artificial Intelligence

Research Paper
Journal Homepage: www.ojs.ijemd.com
ISSN (print): 2791- 0164 ISSN (online): 2957-5036

Towards an Embedded Trust Blockchain Architecture for 6G Networks

A. Azmi[1,*], F. N. Alavi [2], and S. Arif [3]

[1]Dept. of Comp. Sci. & Engineering, Yanbu University College, Yanbu, Saudi Arabia
[2]Dept. of Computer Science, Virtual University, Islamabad, Pakistan
[3]Dept. of General Studies, Yanbu University College, Yanbu, Saudi Arabia
**Corresponding author*

Abstract

In recent years, blockchain technology has received considerable attention from academia, financiers, and governments. Blockchain is considered to be a key disruptive technology for the 21st Century, with a very wide array of application domains that impact all areas of our lives. That such a technology exists just as the world is transitioning towards 6G mobile networks that will offer unprecedented levels of performance but will come an attendant set of ethical and other implications, is highly fortuitous. We offer in this paper a proposal to integrate blockchain technology into the anticipated 6G feature set to address the problem of ensuring and automating Trust to a high degree.

Keywords: Blockchain; 6G; AI; Machine Learning; Cybersecurity; Trust

1. INTRODUCTION

The last three decades, starting from the early 1990s onwards, have transformed human societies irrevocably. The combination of affordable computing power with ever-increasing performance in ever-shrinking form factors, together with the ever-widening availability of mobile communications networks to practically every square meter of the inhabited parts of the planet, have led to a situation where everyone today has the ability to be connected with everybody else, unconstrained by the traditional barriers of space, time, cost and ability. Naturally, such a radical shift in the human experience does not come without considerable social and ethical costs: like all "good ideas", these developments can be used both for the good and bad of mankind, and it is ultimately down to societies' cultural and moral values to strike a balance that is right for themselves.

We note that this on-going convergence between computing and telecommunications has been a long-planned goal of both industries, and that the shift from fixed to mobile communications has been driven, on average, in 20-year cycles. Specifically:

Email addresses: azmia@rcyci.edu.sa (A. Azmi)

- 1980s – early 2000s: analog/mixed-signal voice communications were dominant;
- 2000s – early 2020s: digital broadband services are dominant.

Should this trend continue, it is easy to envisage that the next decade or two will transition humanity towards massive interconnectedness going well beyond what present 4G/5G networks can support.

It is generally expected that 6G will witness widespread rollout and adoption by the end of the present decade. Already, intensive efforts are underway to define the technical parameters and business use cases for next-generation 6G technologies (Pouttu, 2020). On the technological front, the capabilities of wireless transmission will be pushed to unprecedented levels, augmented by a massive utilization of AI and related technologies both at the core and the edge. Present performance goals for 6G specifically identify ultra-reliable, low-latency (< 1 ms) communications at 1 Tbps bandwidths, operating in the GHz-THz parts of the spectrum, to enable "unlimited" connectivity at mobility speeds of up to 1000 km/h (Xu, *et al.*, 2020), as well as a substantial shift towards decentralization as even indoor spaces are invaded by IoT devices.

Equally, entirely new business ecosystems will evolve, possibly with virtual Metaverse existence, requiring both radical innovations and changes in the collective human mindset itself. The primary driver will be a push towards a society that is artificial first, and biological second!

1.1 Trust, Privacy and Security

We can observe that these anticipated changes throw up significant ethical challenges that societies will have to address, if not imminently then surely in the future. From the technological perspective, there will be an intensification of the attendant issues of Trust, Privacy and Security (TPS), most of which are already significant areas of research throughout the world, and which are presently governed by human-designed legal systems and moral considerations with legacies dating back centuries. The EU's GPDR legislation, for instance, specifically attempts to codify these concepts, and its success can be gauged by the fact that it has been copied and adapted by several other, non-EU, jurisdictions (Simmons, 2022). Taken together, TPS will need to be embedded as an integral part of the 6G feature set, rather than be treated as an afterthought as has been the case heretofore. Contributions from multidisciplinary researchers spanning the full spectrum of technology, regulation, economics, politics, and ethics will need to be incorporated if we are to avoid putting at risk our survival as a species.

It is heartening to note that TPS considerations are already specifically included within the set of early-stage investigations known as the 6G Research Visions Series, which is being piloted by the 6G Flagship Group (Pouttu, *op. cit.*). Specifically, the following goals have been identified:

- Trust: 6G network will need to support the concept of "embedded Trust" to allow for acceptable levels of information security. This means that Trust models, Trust policies and Trust mechanisms will need to be defined and incorporated into the systems design.

- Privacy: As 4G/5G have demonstrated, companies will continually seek out ways to exploit private data for commercial gain, and there do not exist means at present to determine when multisource datasets stripped of personally identifiable metadata aggregate sufficiently to cross the privacy breach threshold and become identifiable. The legal profession continues to make reactive decisions about the nature and extent of privacy infringement, without the benefit of having formal technological-legal measures in place that would constrain misuse or misappropriation of private data. Clearly, the best technological and legal minds need to work together to solve this problem, lest that 6G makes the privacy issue completely intractable.

- Security: Indubitably the most addressed component of the TPS triad, security has long been the bane

> of network administrators worldwide, and also has the largest set of technical solutions. For 6G, network security architecture planning will likely transition towards AI and Machine Learning enabled systems which will simultaneously filter out the most prevalent methods of attack, but will also, paradoxically, invite ever more sophisticated and dangerous AI-empowered attackers. In a game of AI vs. AI, no obvious solutions are likely to exist to disempower such attacks, and perhaps consistent sharp vigilance will be the only way forward.

Our focus in this paper is on the issue of Trust, the least-addressed component of the TPS triad, and arguably the most challenging, since it derives ultimately from the concept of conscience, a purely human ability to distinguish right from wrong, which distinguishes us from all other known species. It is difficult to envision a scenario where conscience, and all that derives from it, could be quantified into a set of AI-powered expert systems that may be adapted to serve all human societies with their myriad cultural, religious, historical, socio-political traditions. The problem is only compounded when one takes into account the fact that such traditions are dynamic – they learn from each other and also evolve over time. To build Trust-based systems therefore, the best we can do perhaps is to engineer designs that *minimize*, rather than attempt to *eliminate* altogether, the lack of Trust. In other words, Trust-enabled systems should aim for the following:

- Define Trust protocols with complete transparency that are recognized and accepted by all parties.
- Attempt in the first instance to resolve Trust-related issues automatically, transparently and immutably.
- Invoke human governance and intervention for a resolution, if only as a last resort, in the event that an attempted automated solution results in a deadlock.

2. BLOCKCHAIN AS A TRUST ENABLER

The present-day Internet emerged from laboratories where Trust was taken for granted and not part of the technology mandate. Indeed, much of the open-source movement started in the late 1980s by Richard Stallman (Behlendorf *et al.*, 1999) drew its motivation from a desire to maintain the free sharing of ideas and software for the benefit of all. It is fortunate that the Internet evolved along similar libertarian lines. It has grown organically into a global system of systems that is largely open, loosely-coupled and *apparently* decentralized[1], where participants can freely and spontaneously participate within agreed technical standards. (We have been spared the alternative nightmare of a highly compartmentalized global network with stiff usage regulations and paid access, although it may be reasonably argued that some Big Tech firms are attempting to push the Internet along just such a path.)

Paradoxically, however, the Internet's general openness has succeeded in pushing the issue of Trust towards the periphery. One of the best examples of this phenomenon has been the technological-legal solution that evolved to solve the problem of server and file authentication. The issue was settled historically by the development of the SSL protocol by Taher Elgamal whilst at Netscape, Inc. in 1994 (Matthews, 2019; Paul, 2021), and the subsequent institutionalization of "trusted" third parties – the so-called "certificate authorities" – who issue and maintain cryptographically-signed digital security certificates. Although multiple such authorities exist today, the Trust element ultimately remains entirely optional – one could operate a server perfectly well without digital certificates, albeit insecurely, if one so chooses. The existence of such authorities, furthermore, defies attempts at full automation, since the choice of implementing the SSL-compatible HTTPS protocol, as well as selecting one certificate authority over another is ultimately a subjective decision contingent upon normal human prejudices – a given user is free to choose one certificate authority over another for nationalistic reasons, for instance. Equally, should

[1] The Internet, does, in fact, have centralized technology control via bodies such as the IETF and ICANN, which manage the global engineering standards.

more than one authority be selected concurrently, it is likely to have cost and management consequences for the overall security architecture of any given system. It is precisely scenarios such as these that demonstrate the need for automating Trust as much as possible.

6G technologies are expected to oversee the widespread adoption of IoT devices in the billions of units, and are certain to usher in an age of multiply-interacting systems with unprecedented levels of fine-grained and spontaneous co-operation. The very idea of any kind of centralization is anathematic to such a massive collection of systems, and higher levels of distributed autonomy will therefore likely play an increasing pertinent role in the transition to the 6G era. If we are to continue to expand upon the conventional ethos of an open Internet, we become obliged to deal with the technical challenge of architecting Trust in a massively decentralized world. Fortunately, the recent emergence of blockchain technologies offers a way to respond to this challenge.

Blockchain has transitioned from an Internet forum curiosity following the less-than-spectacular launch of Bitcoin in 2008 (Nakamoto, 2008) into a serious discipline worthy of billions in research funding in less than a couple of decades. The primary initial attraction of Bitcoin was the opportunity it offered to bypass “trustworthy” third party financial institutions in favor of direct P2P monetary transactions, and to do so anonymously. That it also offered the opportunity to collect, using computational mining techniques, *virtual* coins having *real* value was ultimately a spin-off attraction, which only drew in the masses once the financial incentive to do so became obvious.

Thanks in no small part to the vitality of its original nonconformist and libertarian user communities, Bitcoin and other blockchain technologies have become mainstream, and gained significant attention from not just researchers, but also policymakers, financial institutions and now mobile network operators. Blockchain studies have evolved into Distributed Ledger Technology (DLT) as a subdiscipline of computer science in its own right, where its component technologies such as programmable smart contracts and consensus protocols are now areas of active research both in academia and industry. Although it is common to use the words “blockchain” and “distributed ledger” interchangeably, it is important to note that the former is now generally regarded as a special case of the latter.

At a technical level, blockchain, as originally envisaged, is primarily a distributed databases organized as a hash tree in chained blocks where entries, once committed, become irreversible and tamper-proof. Block creation is periodic, and follows a strict set of rules, such as in response to the occurrence of a defined event such as a user transaction or following the lapse of a predefined interval. Within each block, inter-party transactions may occur, whereby some element having a notional concept of “value” changes ownership between two parties (in the case of crypto-currencies) or has some associated data committed to the chain (in case of ledgers).

Following creation, a block attaches to the chain of earlier blocks, and its data is authenticated by the entire network. The integrity of the entire process is guaranteed by a Distributed Consensus Protocol (DCP): short of a situation where >50% of a malevolent collective succeeds in taking over the system, none of the participants have the capacity to corrupt a transaction that has been recorded onto the ledger. Trust, in other words, is distributed amongst all participants and is also verified collectively.

The DCP originally implemented by Nakamoto (*op. cit.*) for Bitcoin was the Proof-of-Work protocol, which rewards users for proving to the network that a verifiable amount of computational effort has been expended in block verification. As Bitcoin has grown in popularity and its technology has become better understood over time, it has given rise to so-called “altcoins” with improved features and more sophisticated DCPs; a few prominent examples being Proof-of-Stake, Proof-of-Space, Proof-of-Elapsed Time. Surveys of some innovative designs can be found in Cachin & Vukolić (2017), Bano *et al.* (2017)

and Wang, *et al.* (2019).

For any given blockchain system, the choice of the DCP is crucial, as it determines overall system performance, throughput, scalability and security levels, amongst other things. Designing the algorithms for any new DCP provides a significant opportunity for innovation, and it is here that Trust protocols can best be integrated into a system.

2.1 Using Blockchain in Networks

As already noted, there appears in DLT to be a ready-made technological solution to some of the planned service goals of 6G. This has been recognized in scores of publications (Hewa, 2020), and we review some relevant ones here.

The high data rates demanded by B5G/6G applications will require an escalation in network capacity, and an attendant increase in more spectrum, a scarce resource. Schemes have been proposed to manage spectrum usage more efficiently whereby unlicensed users are permitted to dynamically and opportunistically access the licensed spectrum without interfering with the primary licensed user. Such schemes ultimately require secure databases where operational parameters can be managed by radio access policies in order to avoid collisions between licensed and unlicensed users. Blockchain offers a way to manage such databases in a secure manner. Various such schemes can be found in the recent literature. For instance, Xu, (*op. cit.*) address blockchain-enabled resource management and sharing in 6G. Spectrum resource management is covered by Saad, *et al.* (2019) and Tariq, *et al.* (2019). Dai, *et al.* (2019) extend this idea to cover content caching with deep reinforcement learning. Kotobi & Bile'n (2017) consider the use of blockchain-based methods for spectrum sharing in cognitive radio. Qiu *et al.* (2020) propose a blockchain spectrum trading and sharing scheme for UAV-assisted cellular networks. Chai *et al.* (2019) consider a framework for Vehicle-to-Everything (V2X) communication-enabled resource sharing, based on a vehicle's reputational score.

It is interesting to note that the majority of existing works that contemplate the use of blockchains for 6G networks have concentrated largely on the twin problems of resource (spectrum) sharing, or on V2X, the latter being one of the most highly-anticipated use cases of B5G/6G networks. More recently, there have also been attempts to employ blockchain technology to the problem of infrastructure sharing in B5G/6G networks. The CAPEX for cellular networks tends to run into the billions of dollars, and it makes economic sense for Mobile Network Operators (MNOs) to lease each other's infrastructure setups. In this regard, we note the work of Faisal *et al.* (2022) who have introduced a blockchain-enabled accountable and transparent architecture ("BEAT") that allows MNOs to share critical and expensive network infrastructure by ensuring that stringent and critical inter-operator Service Level Agreements (SLA) requirements are met during operations. As all transactions are hard-wired onto the blockchain, the possibility of operators shifting the blame for SLA non-compliance is reduced, with only a trivial hit in performance. Where SLA failures do arise, the system automatically and instantaneously identifies the party at fault, and applies a penalty, with the immutability of the blockchain ensuring that results cannot be altered after-the-fact.

2.2 Using Blockchains for Trust

As previously noted, we are interested in this paper in the use of blockchain as a means of providing Trust. We acknowledge at the outset, however, that blockchain by itself is not some panacea that will solve all Trust issues; rather, it should be seen purely as an enabler of Trust and trustworthiness that, if properly implemented, should reduce the probability of malicious actors succeeding in environments where the operation of the entire system relies fundamentally on the integrity and good behavior of all participants.

The successful results reported by Faisal (*op. cit.*) with their BEAT architecture provide a good starting point for implementing cooperative Trust between agents through the use of blockchain technologies. Given the scale and high-throughput performance levels expected of B5G/6G networks, it is self-evident that ways will have to be found to reduce to a minimum the human element in the traditional SLA contractual process, and move towards an automated system that allows for seamless wide area integration and reliable performance in a verifiable manner. This is certain to assume considerable significance given the following considerations:

- There are likely to be future applications that will require the fine-grained assignment of liabilities, especially where human life is at stake. For instance, in remote surgery, having a guaranteed connection with a guaranteed bandwidth could mean the difference between life and death of the patient; in the event of service degradation, pinpointing the exact source of the problem would at least allow for an equitable referral of claims post-incident, and prevent a situation from arising where different parties attempt to shift the blame away from themselves.
- Spontaneous and ad hoc connections are also a likely to be a feature of B5G/6G networks. An IoT device that needs to connect with the outside world in a mission-critical setting (e.g., earthquake sensing) should be able to grab *any* available link, on an ad hoc basis and without prior SLA agreement, should its main connection go down. This is analogous to the manner in which modern global cellular roaming technology works, where a new SLA does not need to be negotiated in order to be able to use one's private phone number in a foreign land.

Other, as yet unimagined, future applications will, of necessity, come with their own set of similar technical, legal and ethical requirements that will ultimately boil down to the spontaneous, ad hoc and automated negotiation, enforcement and termination of SLAs. By including such a set of functionalities as fundamental components of the 6G network architecture, blockchain technologies will make it possible to manage Trust issues between all users in a highly automated fashion.

3. TOWARDS AN ARCHITECTURE FOR TRUST

3.1 Defining Trust

Network security has progressed in leaps and bounds over the decades and has given rise to cybersecurity as a major component of the IT industry. Within cybersecurity, the concept of "Zero Trust" has become a major buzzword. First espoused by John Kindervag, a senior analyst at Forrester (Higgins, 2010), Zero Trust networks are built upon the following five assumptions (Gilman & Barth, 2017):

- Always assume that the network is perpetually hostile;
- External and internal threats exist at all times on the network;
- Locality of a network is insufficient for placing trust in it;
- Policies of authentication and authorization should be in place for every device, user, and network flow;
- Policies must be dynamic and developed from as many sources of data as possible.

Although labelled as a *Trust* issue, Zero Trust is clearly nothing other than the exercise of network vigilance, judiciously applied to the task of making network *security* as robust as possible. We find that this practices of substituting Trust for security is not merely restricted to cybersecurity – a perusal of the research literature in computer science consistently demonstrates a similar misapplication.

This illustrates a key dilemma in the interpretation of Trust, which is integrally a consequence of human psychology, intrinsically unquantifiable, and too subjective to be modelled by any reliably comprehensive metric. Trust and trustworthiness arise naturally in any social or computational grouping involving ≥ 2 entities. Trust is therefore fundamentally a *social* phenomenon. Turning to the social sciences, we find that the amount of literature on Trust is substantial (Golembiewski & McConkie, 1975). In spite of this, no formal theory of Trust among human or organizational groupings has been proposed by social scientists. Rather, Trust continues to be defined in light of examples from various inter-related areas such as economics, sociology and psychology (Gligor & Wing, 2011).

Clearly, a formal theory of Trust is required, one that mirrors human perceptions of the experience, and allows us to intuitively build upon *behavioral Trust* (Trust relationships between humans) to construct a working set of best practices for *computational Trust* (HCI and autonomous agent Trust protocols). At present, such a theory does not exist, although various attempts have been made to produce one (Castelfranchi & Falcone (2010); Marsh, S. P. (1994)).

Gligor & Wing (*op. cit.*) point out that the lack of such a theory has resulted in some surprising long-standing deleterious consequences, such as the widespread dissemination of spam and computer malware, that are accepted today as a normal part of the IT industry. Furthermore, they hypothesize that building system primitives that enhance Trust will ultimately lead to superior security at lower cost than existing solutions.

Until a formal theory of Trust emerges, if it does so at all, we are left with formalisms from applied soft computing which mimic human patterns of behavior. Prominent examples of such formalisms include game theory and fuzzy sets, both of which have been shown to solve problems in computational Trust, see, respectively, Marsh, S. P. (*op. cit.*) and Castelfranchi & Falcone (*op. cit.*).

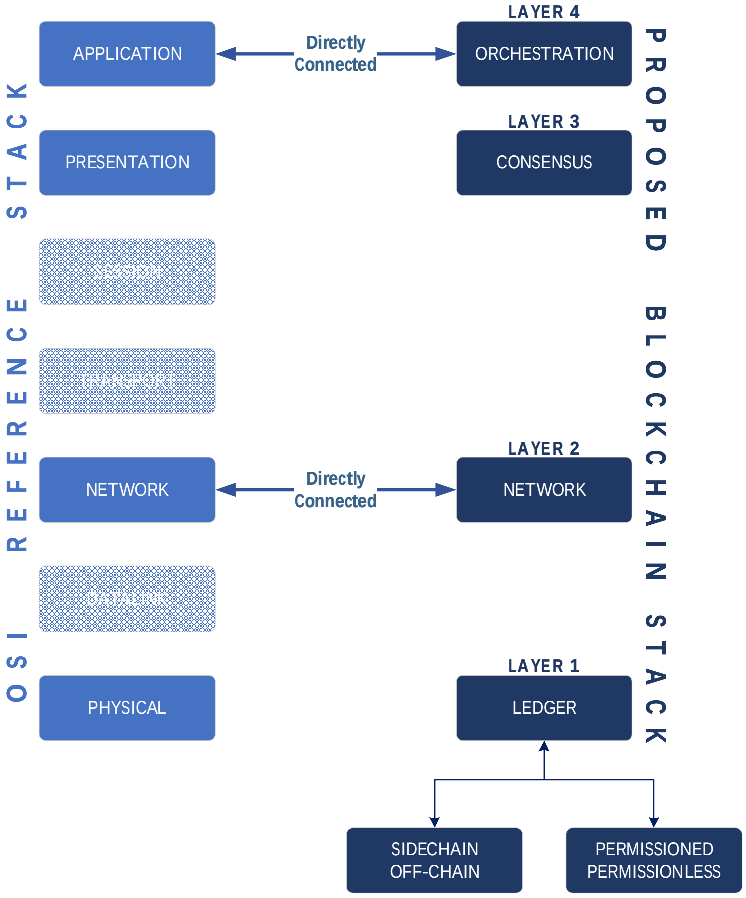

Figure 1: Proposed 4-Layer Blockchain Architecture, compared with OSI 7-Layer Stack. Note that there are no analogs to the Datalink, Transport and Session Layers in the proposed architecture.

3.2 A Layered Architecture for Trust

A key criticism levelled at blockchain technologies is that of complexity. Even for the most-studied and arguably the simplest blockchain system, Bitcoin, the network functionalities range from managing transactions, propagating blocks, mining, confirming consensus, through to chain integrity maintenance at a minimum. In order to manage the complexity more effectively, there have been recent proposals for the adoption of a layered approach, both for Bitcoin and other systems, where similar network functionalities could be grouped together in a modular fashion, much like the TCP/IP protocol stack. Such an ordering should offer greater flexibility and also be more maintainable. Calls for a layered redesign first emerged in 2016, led initially by Eric Lombrozo, one of the contributors to the Bitcoin Core (Torpey, 2016). This was supported by Ito (2016) and expanded upon by Xiao (2016), who proposed the following four layers: Consensus, Mining, Propagation and Semantics. Ferdous *et al.* (2020) modified this further into Network, Consensus, Application and Meta-application layers, since they noted that mining and consensus are inter-dependent and could be merged.

We believe that layering is an optimal solution not only to managing complexity in blockchain-enabled future networks but also for naturally embedding Trust within the system. We propose a Trust-enabled generic blockchain architecture with four layers, as shown in Figure 1, where we have presented the design alongside the OSI Model to show similarities in concept. Layer functionalities for the proposed design would be as follows:

- **Layer 1 (Ledger)**: Analogous to the Physical Layer of the OSI Model, this layer allows for the physical storage of chain data, where blocks would be created and stored. The Ledger can be designed to have characteristics of both permissioned as well as permissionless chains, in addition to allowing for sidechain and off-chain designs that are becoming common in public blockchains.
- **Layer 2 (Network)**: This interacts directly with the OSI Layer's own Network Layer, and allows for all types of communications to take place.
- **Layer 3 (Consensus)**: This is where the blockchain would run its DCP algorithms, which may or may not include mining functionality, depending on the application being executed. As *consensus* implies *confidence* in the harmonization of opinion, this is clearly the layer best-placed to execute an appropriate computational Trust protocol. Based on our earlier discussion, this could be implemented using game-theoretic or fuzzy logic soft computing techniques, as well as by emergent consensus algorithms such as Proof-of-Reputation (Aluko & Kolonin, 2021), where participating agents win network Trust based on the votes they amass from others.
- **Layer 4 (Orchestration)**: Inspired by the work of Faisal (*op. cit.*), which itself takes its cue from MANO[2], Orchestration is where the primary blockchain subsystem would be managed at a high-level. It would specifically manage blockchain-specific tasks such as smart contract execution and DAO governance, in addition to being able to interact with OSI's Application Layer for more mundane tasks (such as user/group management, configuration management, QoS, compliance, security, etc.). Depending on implementation goals, it would also be possible to include here interactions with secondary subsystems for AI, Machine Learning, etc. for more complex use cases.

4. CONCLUSIONS

In this paper, we have considered Trust as a key component of the TPS triad that has been singled out as a foundational component of 6G technologies by various early-stage working groups around the world.

Trust is unquestionably a multidisciplinary subject that requires urgent and ongoing interaction between the physical and social science communities in order that a formal common framework accessible to both may emerge. It will also require input from humanities experts so that the legal aspects of trustable

[2] Management and Orchestration, a key element of network functions virtualization as proposed by ETSI (Reid, *et al.*, 2020)

autonomous future high-performance networks and systems can be properly codified. At present, the quest to incorporate Trust into such systems is hampered by the unavailability of a formal theory of Trust, and a general confusion between Trust and security. The latter should ideally be, in a properly-engineered trustworthy system, a *consequence* of and not a *substitute* for Trust.

We have also proposed in this paper a four-Layer generic architecture for blockchain that is both inspired by and inherits the OSI Layer model's proven flexibility and demonstrated capacity for growth. We anticipate that the proposed design would make it feasible for B5G/6G network designs to assimilate with DLT technologies more naturally, whilst at the same time allowing for computational Trust to be embedded into the architecture in a systematic rather than ad hoc manner.

References

Aluko, O. and Kolonin, A. Proof-of-Reputation: An Alternative Consensus Mechanism for Blockchain Systems. *Intl. J. of Network Security & Its Applications (IJNSA)*. **13**(4), 23-40 (2021).

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., and Danezis, G. Consensus in the Age of Blockchains". arXiv preprint arXiv:1711.03936. (2017).

Behlendorf, B., Bradner, S., Hamerly, J., McKusick, K., O'Reilly, T., Paquin, T., Perens, B., Raymond, E., Stallman, R., Tiemann, M., Torvalds, L., Vixie, P., Wall, L., Young, B., DiBona, C., Ockman, S. and Stone, M. *Open Sources: Voices from the Open Source Revolution*. O'Reilly Media, Inc., USA. 1999.

Cachin,C. and Vukolić, M. Blockchains Consensus Protocols in the Wild. arXiv:1707.01873. (2017).

Castelfranchi, C. and Falcone, R. *Trust Theory: A Socio-Cognitive And Computational Model*. John Wiley, UK, 2010.

Chai, H., Leng, S., Zhang, K. and Mao, S. Proof-of-reputation based Consortium Blockchain for Trust Resource Sharing in Internet of Vehicles. *IEEE* Access 7, 175744–175757 (2019).

Dai, Y., Xu, D., Maharjan, S., Chen, Z., He, Q. and Zhang, Y. Blockchain and Deep Reinforcement Learning Empowered Intelligent 5G Beyond. *IEEE* Network, **33** (3), 10–17 (2019).

Dorri, A. and Jurdak, R. Tree-Chain: A Fast Lightweight Consensus Algorithm for IoT Applications. arXiv:2005.09443v1, (2020).

Faisal, T., Dohler, M., Mangiante, S. and Lopez, D. R. BEAT: Blockchain-Enabled Accountable and Transparent Network Sharing in 6G. *IEEE Communications Magazine*, **60**(4), 52-56 (2022).

Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A. and Colman, A. Blockchain Consensus Algorithms: A Survey. arXiv:2001.07091v2, (2020).

Gilman, E. and Barth, D. *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. O'Reilly Media, Inc., USA, 2017.

Gligor, V. and Wing, J. M. Towards a Theory of Trust in Networks of Humans and Computers, in: Security Protocols XIX: 19th International Workshop, Cambridge, UK, March 28-30, 2011: Lecture Notes in Computer Science. Springer, 223-242 (2011).

Golembiewski, R. T., and McConkie, M. *The Centrality of Interpersonal Trust in Group Processes*, pp 131–185 in: "Theories of Group Processes. Cooper, C. L. (ed), Wiley, 1975.

Hewa, T., Gür, G., Anshuman, K., Ylianttila, M., Braken, A. and Liyanag, M. The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions". 6G Wireless Summit 2020, Levi, Finland. DOI: 10.1109/6GSUMMIT49458.2020.9083784, 2020.

Higgins, K. J. Forrester Pushes 'Zero Trust' Model for Security. https://www.darkreading.com/ perimeter/forrester-pushes-zero-trust-model-for-security. Accessed 2022-09-28, (2010).

Ito, J. The Fintech Bubble". https://joi.ito.com/weblog/2016/06/14/-the-fintech-bu.html. Accessed 2022-06-09, 2016.

Kotobi, K. and Bilén, S. G. *Blockchain-enabled spectrum access in cognitive radio networks*, in: 2017 Wireless Telecommunications Symposium (WTS), 1-6 (2017). DOI: 10.1109/WTS.2017.7943523.

Marsh, S. P. *Formalising Trust as a Computing Concept*. PhD Thesis, Department of Computing Science & Mathematics, University of Stirling, UK, 1994.

Matthews, T. The Origins of Web Security and the Birth of Security Socket Layer (SSL) Protocol.
https://www.exabeam.com/information-security/web-security-security-socket-layer-protocol-ssl. Accessed 2020-09-28, (2019).

Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System". https://bitcoin.org/bitcoin.pdf. Accessed 2020-06-09, (2008).

Paul, G. *The Importance of SSL Certificates and Their History*. https://getshieldsecurity.com/blog/
ssl-certificates-and-their-history. Accessed 2020-09-28. (2021).

Pouttu, A. *6G Future Directions Keynote*. Oulu University, Finland. https://futurecomresearch.eu/
contributions/Keynotes/3_Keynote_Pouttu_6G White Papers.pdf. Accessed 2020-06-09, (2020).

Qiu, J., Grace, D., Ding, G., Yao, J. and Wu, Q. Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective". IEEE Internet of Things Journal **7**(1), 451–466 (2020).

Reid, A., Marsico, A., ElSawaf, A., García, G., Ramón, F. J., Grønsund, P. and Sheikh, S. OSM Deployment and Integration. https://osm.etsi.org/images/OSM_EUAG_White_Paper_OSM, (2020).

Deployment_and_Integration.pdf. Accessed 2020-09-28.

Saad, W., Bennis, M. and Chen, M. A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems". arXiv:1902.10265, (2019). doi:10. 1109/MNET.001.1900287.

Simmons, D. *17 Countries with GDPR-like Data Privacy Laws*. https://insights.comforte.com/
countries-with-gdpr-like-data-privacy-laws. Accessed 2020-06-09, (2022).

Tariq, F., Khandaker, M., Wong, K.-K., Imran, M., Bennis, M. and Debbah, M. A Speculative Study on 6G. arXiv: 1902.06700, (2019).

Torpey, K. Protocol Layers Similar to the Internet. https://coinjournal.net/news/eric-lombrozo-bitcoin-needs-protocol-layers-similar-to-the-internet. Accessed 2022-06-09, (2016).

Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y. and Kim, D.I. A survey on consensus mechanisms and mining strategy management in blockchain networks". IEEE Access, **7**, 22328-22370 (2019).

Xiao, D. (2016). "The Four Layers of the Blockchain". https://medium.com/@coriacetic/the-four-layers-of-the-blockchain-dc1376efa10f. Accessed 2022-06-09.

Xu, H., Klaine, P. V., Onireti, O., Cao, B., Imran, M. and Zhang, L. Blockchain-enabled Resource Management and Sharing for 6G Communications." *Digital Communications and Networks*. **6**(3), 261-269 (2020).