Blockchain-based Solutions to support inter-organisational Critical Infrastructure Resilience

Boris Petrenj
Politecnico di Milano, School of Management
boris.petrenj@polimi.it

Paolo Trucco
Politecnico di Milano, School of Management
paolo.trucco@polimi.it

ABSTRACT

This conceptual paper critically discusses opportunities for and challenges to the development and exploitation of blockchain-based solutions for resilience management at inter-organizational level of interdependent Critical Infrastructure (CI) systems. The background rational is that trustful information-sharing and inter-institutional collaboration are the key elements of government and private sector efforts to build CI resilience (CIR). The discussion presents a vision that the adoption and adaptation of Blockchain Technology (BCT) could significantly improve the way a network of stakeholders prepares for and performs in face of unavoidable CI disruptions. Even though BCT is regarded as a technological innovation, the impacts go far beyond information systems. BCT application in this domain would entail significant benefits to organizational, managerial, legal and social issues, but would require some relevant operational and organizational changes. We discuss how interdisciplinary approach could address existing challenges, how it could introduce new challenges and how it could support other approaches and paradigms regarded as the future of risk and resilience management. This is a preliminary overview with the aim to stimulate further discussions and point to possible new, disruptive and interdisciplinary research avenues. To this end, a possible research agenda is eventually proposed.

Keywords

Critical infrastructure, blockchain, resilience, capability, inter-organizational, research agenda.

INTRODUCTION

A Critical Infrastructure (CI) is an array of assets and systems that, if disrupted, would threaten national security, economy, public health and safety, and way of life (EC, 2005), such as energy and water supply, transport, communication, public health. CIs are complex socio-technical systems (STS) whose resilience is emerging as one of the essential issues of this decade. The STS concept stresses the reciprocal interrelationship between humans and technology (Ropohl, 1982), or here, the interaction between society's complex infrastructures and human behavior.

Contemporary societies are increasingly dependent on the availability of services provided by CI, which are also a major cornerstone of long term sustainability and achieving Sustainable Development Goals set by United Nations, especially those related to transportation, food security, health, energy, economic growth, and human well-being. The blockchain applications for sustainable development were already examined in areas of development aid effectiveness, digital identity, remittances, supply chain management, energy and property rights (Blockchain Commission, 2018).

CI Resilience is generally understood as the ability to: prevent disruption of service to the public; absorb the consequences of any disruption; restore (recover) quickly normal performance; adapt to unforeseen scenarios of disruption (short-term) and different circumstances of operation (long-term); and **prepare to fulfil the four goals** (U.S. NIAC, 2009). In complex STS, resilience covers all the system dimensions (Rød et al., 2020), as in 'TOSE framework' (Bruneau et al., 2003):

- **Technical resilience** refers to the physical properties of the CIs, focusing on their ability to resist damage and minimizing any loss of function during a crisis, or quickly repairing the unwanted effect.
- **Organizational resilience** includes the processes of organizational capacity and capability, planning, training, leadership, communication, and so forth.

- **Societal resilience** refers to the ability of civil society, social groups, and individuals dependent on the service provided by the CI to cope with CI contingencies.
- **Economic resilience** refers to the capacity to reduce economic losses after disruptive events.

Recent events have shown that the current CIR approaches suffer from major limitations, e.g. Ukrainian blackout (Choraś et al., 2016), Great East Japan Earthquake (Furutai and Kannoi, 2018) or Suez Canal blockage (Cheong et al., 2021). Huge impacts of CI disruptions are mainly caused by cascading failures across geographical and functional borders that arise from highly interdependent infrastructures.

To face a broadened range of hazards and threats (e.g. natural disasters, terrorist and cyber-attacks), CIR has become one of the top priorities in countries worldwide. However, ensuring CIR is a highly challenging task, involving physical networks, old and new technologies, actor networks (humans) and institutions coupled in an integrated 'system of systems'. Resilience of such complex systems (interdependent, multi-sectoral, multi-stakeholder, cross-border) now significantly depends on information sharing and collaboration among stakeholders, which suffers from numerous issues (Petrenj et al., 2013). A breakthrough improvement in the application cases where sensitive data is stored and exchanged might be brought by the Blockchain Technology (BCT). It has emerged as one of the most revolutionary developments over the last decade and it has already been applied in numerous industry sectors. BCT distinctive characteristics might bring radical improvement to the way the organizations work together to build CI resilience, by enabling secure, resilience and trusted peer-to-peer value exchange (i.e. transaction of information and other resources).

This paper provides a non-technical overview and critical discussion of possible blockchain applications in the domain of Critical Infrastructure resilience and in the development of inter-organizational capabilities in particular. It suggests a possible research agenda listing things that should be considered and further investigated in order to make this possible. Even though the paper discusses the topic from the CI point of view, it is equally applicable in other resilience building domains and in Disaster Risk Management in general, including collaboration and resilience in humanitarian operations and supply chains (Dubey et al., 2020; Zwitter and Boisse-Despiaux, 2018).

The paper is structured as follows. The following section explains the key role of information-sharing and collaboration for building CI resilience, and summarizes the current issues. Section 3 gives an overview of the BCT and its main characteristics. Section 4 presents the current lines of CIR development and potential benefits of BCT to their development. The promising lines of future research are summarized in Section 5. The final section explains the limitations of the paper and draws conclusions.

INFORMATION SHARING AND COLLABORATION AS KEY ENABLERS OF RESILIENCE CAPABILITIES AND PREPAREDNESS PLANNING

Effective *Critical Infrastructure Resilience (CIR)* now hugely depends on an efficient collaboration within the network of stakeholders (infrastructure operators, civil protection, responders, etc.), at different institutional and operational levels and along all the phases of the Emergency Management (EM) cycle. In fact, no single organization has all the necessary resources, relevant information and competence to cope with complex inbound and outbound interdependencies under different accident scenarios (Trucco and Petrenj, 2018). The assessment of all types of CI interdependencies (physical, cyber, geographical and logical) must consider also the transboundary dimension since many CIs are not bounded within single countries (Galbusera et al., 2014).

Information sharing and collaboration among stakeholders are crucial within the CIR mission and trust is the 'essential glue' to make public-private system work (Figure 1 – U.S. DHS, 2013).

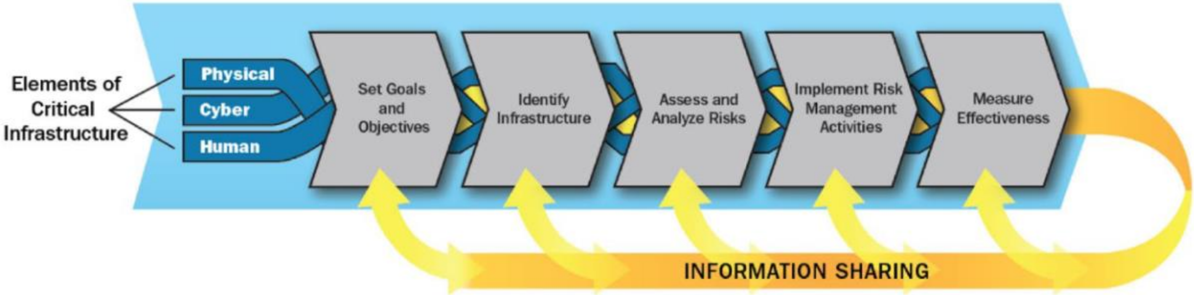


Figure 1. U.S. Critical Infrastructure Risk Management Framework (U.S. DHS, 2013)

The core tenets include stakeholder collaboration/partnerships and information sharing – on regional, state and local levels – to support, among other risk analysis, understanding of (inter)dependencies, effective resource allocation, gaps identification, resilience capacities building, mutual assistance and agreements (U.S. DHS, 2013). However, inter-organizational information sharing and collaboration suffer from limitations and barriers – Figure 2 (Petrenj et al., 2013).

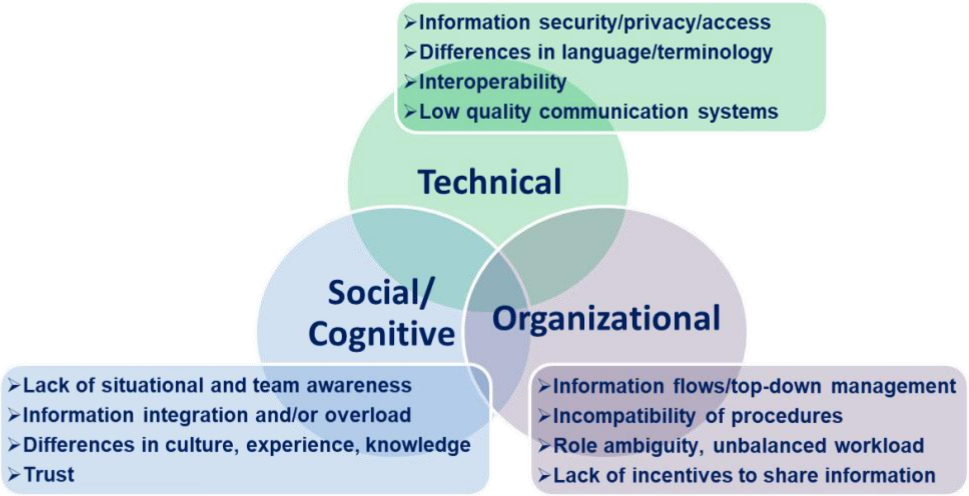

➢Information security/privacy/access
➢Differences in language/terminology
➢Interoperability
➢Low quality communication systems
Technical
Social/ Cognitive
Organizational
➢Lack of situational and team awareness
➢Information integration and/or overload
➢Differences in culture, experience, knowledge
➢Trust
➢Information flows/top-down management
➢Incompatibility of procedures
➢Role ambiguity, unbalanced workload
➢Lack of incentives to share information

Figure 2. Key information sharing issues and barriers (adapted from Petrenj et al., 2013)

BLOCKCHAIN TECHNOLOGY

Blockchain is considered to be one of the most disruptive computing paradigms after the Internet (Swan, 2015). What began as Blockchain version 1.0 for finance and economic trading has significantly evolved over recent years. Version 2.0 brought features such as Smart Contracts, Decentralised Applications (Dapps), Decentralised Autonomous Organsiations (DAOs), etc. Version 3.0 has put emphasis on extending the technology into more aspects of social life, and it is taken up by other industry sectors (Jahankhani and Kendziersky, 2019). BCT enabled digital transformation is moving past the Proof-of-Concept stage (WEF, 2020) and into more mature and commercially relevant environments. BCT now finds its application in the areas of government, supply chain, transport, health, retail, utilities, food and agriculture, science, literacy, culture, and art (Swan, 2015). The vision for Blockchain 4.0 includes applications based on artificial intelligence and machine learning, and focuses on efficiency, scalability, flexibility, and usability (Colomo-Palacios et al., 2020).

The BCT (Figure 3) combines several existing technologies, such as distributed ledger technology (DLT), cryptography and consensus protocols (Palfreyman, 2015). A distributed ledger is essentially a database shared across a network of multiple nodes (i.e. computers, sites and/or organizations) (UK Government Office for Science, 2016) that allows any participant in the network to see the *one* system of record.

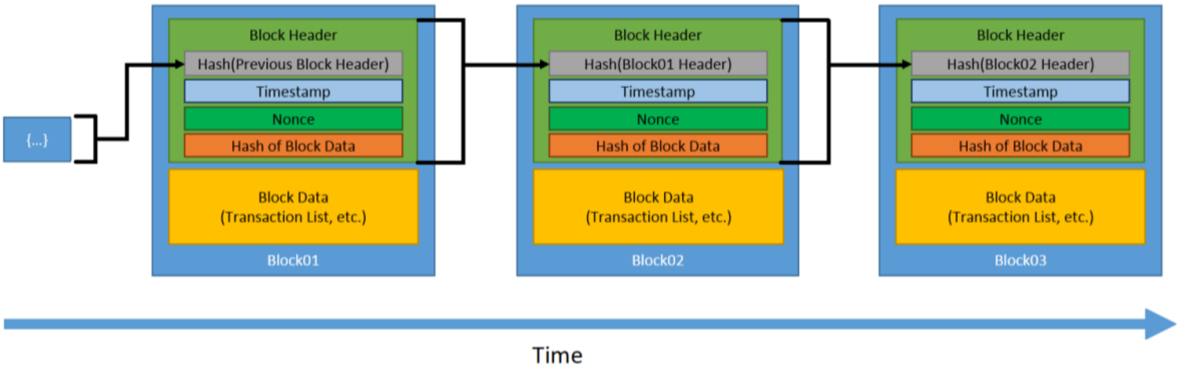
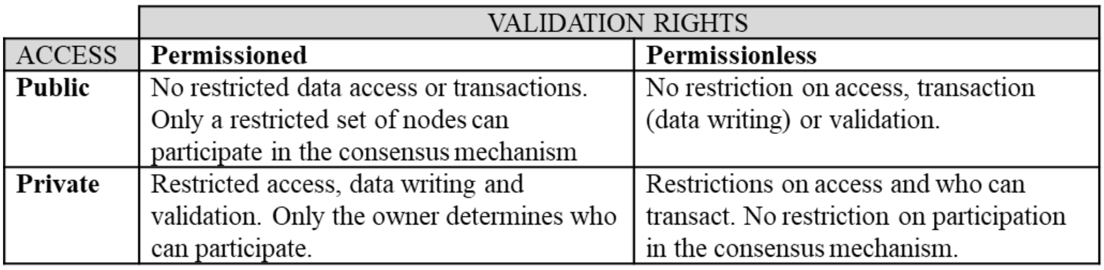


Figure 3. Schematic diagram of Blockchain (Quinnel, 2019)

Blockchain comes in different forms and with different properties (Table 1), so variants of blockchains show advantages and limitations when applied to specific use cases. *Public (permissionless) blockchains* have been the most popular ones, serving the purpose for wider adoption by the masses for common cryptocurrency-based networks. On the other side, *private blockchains*, intended for business use, provide many customization options, such as permissions to join and to perform specific functions/roles, network configuration, visibility of data, adapted and optimized security, scalability, capacity and general performance of the network, law compliance and regulation. In permissionless blockchains any of the nodes can participate in the consensus algorithm being able to validate transactions, whereas in permissioned blockchains only a selection of the nodes are further authorized to validate transactions (Carminati, 2018). Depending on the use case, this can significantly boost trust and confidence between participants. *Consortium blockchains* took the sweet-spot between fully open, decentralized systems and fully centrally-controlled (Yafimava, 2019). They work as 'semi-private', having a controlled user group, but working across different organizations. They are setting themselves up as a backbone for inter-organisational solutions to improve workflows, accountability, and transparency. Consortium blockchain benefits from the transactions' efficiency (do not rely on proof-of-work to establish consensus) and privacy of private blockchains, while leveraging the decentralized governance of public blockchains (Dib et al., 2018). With its logic, blockchain can facilitate and foster collaboration by minimizing doubts and uncertainties in a networked environment. For this an *initial trust* is required to begin with, i.e. organizations should have some trust in each other but not necessarily complete trust.

Table 1. Main variations in blockchain applications (adapted from Ølnes et al., 2017)



	VALIDATION RIGHTS	
ACCESS	**Permissioned**	**Permissionless**
Public	No restricted data access or transactions. Only a restricted set of nodes can participate in the consensus mechanism	No restriction on access, transaction (data writing) or validation.
Private	Restricted access, data writing and validation. Only the owner determines who can participate.	Restrictions on access and who can transact. No restriction on participation in the consensus mechanism.

BLOCKCHAIN POTENTIAL FOR COLLABORATIVE CIR

Previous fundamental research has set the theoretical base of the BCT and highlighted its ground-breaking nature capable of disrupting industry and public sector activities. Numerous real-world applications are now already proving advantages to BCT adopters and showing the benefits. However, the potential of BCT is still vastly unexploited in the field of CI resilience programs, mainly due to the lack of specific research on the related use cases, along with a deep understanding of the needs and challenges in deploying and managing BCT for this purpose.

Inter-organizational relationships have become fundamental for a resilient performance and the main proposition here is that BCT could drastically improve the way in which individuals and organizations work together to build resilience (Figure 4). This section presents the emerging paradigms and approaches related to inter-organizational CIR and further discusses the potential of BCT to support their implementation and/or advancement.

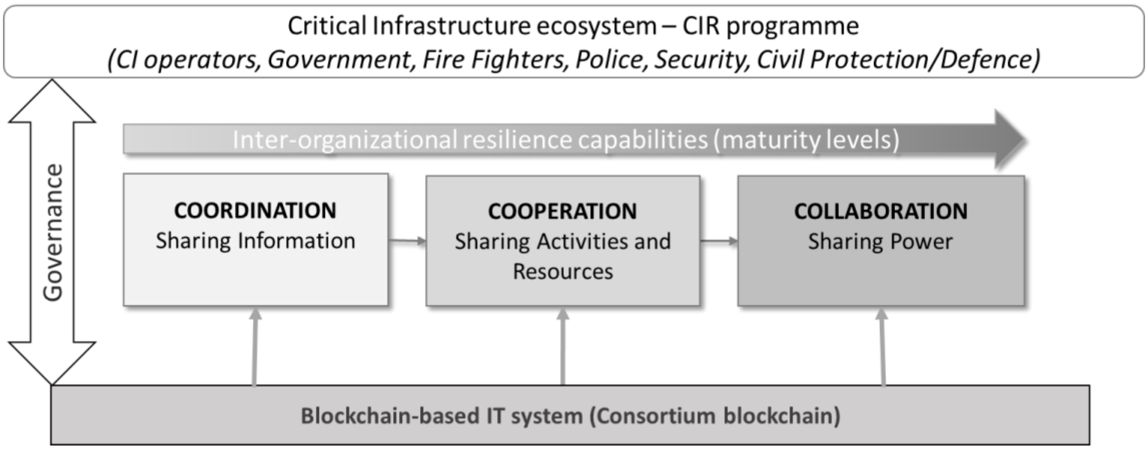

Critical Infrastructure ecosystem – CIR programme
(CI operators, Government, Fire Fighters, Police, Security, Civil Protection/Defence)
Governance
Inter-organizational resilience capabilities (maturity levels)
COORDINATION
Sharing Information
COOPERATION
Sharing Activities and Resources
COLLABORATION
Sharing Power
Blockchain-based IT system (Consortium blockchain)

Figure 4. Blockchain as a technological backbone of PPCs for CIR

The top element represents the CI ecosystem and its stakeholder organisations. These stakeholders (or some of them) usually work together in the form of a CIR programme. Public-Private Collaborations (PPCs, aka Public-Private Partnerships - PPPs) have emerged as the most promising model all around the world to deal with CIR issues (Dunn-Cavelty and Suter 2009) and develop effective CIR strategies (U.S. DHS, 2013). PPCs seek to improve protection and resilience of interdependent CI systems by matching complementary skills, expertise and resources from public and private sectors (Trucco and Petrenj, 2017). Different levels of inter-organizational relationships have been used to describe and analyze how organizations work together to solve problems (Crosby and Bryson, 2005).

Investigating the potential of BCT adoption in the CIR domain should evolve around two main issues:

- understanding how the use of the BCT could enable different levels of inter-organizational approaches (coordination, cooperation and collaboration);
- conceive and demonstrate how these blockchain-enabled capabilities could support a more effective operationalisation of the emerging approaches to inter-organizational CIR building.

Inter-organizational relationships

The first part should investigate if the consortium blockchain could represent a technological backbone for PPCs that would enable seamless and trusted peer-to-peer value exchange – and here is the logic.

Blockchain can be well suited for secure information exchanges across network security domains, such as inter-organizational (including cross-border) information sharing (Olson, 2018). While *public blockchain* can support crypto-related, business-to-consumer (B2C) and consumer-to-consumer (C2C) use cases, *private blockchain* is best-suited for inter-organizational business processes and to support business partnerships (B2B) (Carminati, 2018). In our context, on top of B2B, we focus on business-to-government (B2G) and government-to-government (G2G) use cases (non-commercial interaction between Government organizations, departments, and authorities where business sensitive information are potentially exchanged during an emergency), where variations of consortium blockchain might be the suitable option. By using BCT, organizations can benefit from a more efficient (time and cost) transfer of value, with a reduced risks of fraud and tampering. It enables the decentralization of organizations and processes as well as the automation of transactions and administration functions.

The distinctive characteristics of BCT, compared to a traditional database, are (Jaeger, 2018; UK Government Office for Science, 2016):

- **Distributed** across and managed by peer-to-peer networks of computing devices;
- Transaction data is **shared** so each node has the same information;
- **Consensus** mechanisms validate transactions to ensure there is one and only version of the truth;
- The data is **immutable** because each transaction is cryptographically secured and linked to the previous transaction;
- An asset on a blockchain has **provenance**, it is traceable where it came from and how ownership changed over time.

These characteristics of the BCT could possibly bring radical improvements to the way the organizations work together to build CI resilience (Table 2), by offering enhanced efficiency, reliability, trustworthiness, interoperability, security, privacy (and more) when sharing information or even other resources.

Table 2. Key potential benefits of BCT for inter-organizational resilience building (supporting a network of CI stakeholders)

Technical/Informational	No single point of failure, Immutable (tamper-proof) data, Privacy, Identity Management, Access Management, Information/Cyber Security
Organizational	Improved risk management, Inter-organizational resilience capabilities, Peer-to-peer transactions, Supply-chain visibility, Efficient and automated processes, Sharing resources, Joint/aligned decision-making, Aligned Plans
Social	Increased Trust, Improved awareness (on stakeholders, interdependencies, information needs), Mental model (level of engagement on voluntary basis)

Governments across the world are already conducting pilots using blockchain for the storage of important information and documents like digital identities, certificates, licenses, government decisions and legislation (Ølnes et al., 2017). There have been efforts to establish cross-border emergency response, e.g. between Canada and United States (Transport Canada, 2017) by setting a cross-border response agreement and developing procedures. However, the procedures are still cumbersome, inefficient and requiring lots of physical documentation and paperwork. Globally, inter-organizational resource sharing for CIR is still far from being commonly implemented. In this aspect, the use of BCT could remove administrative burden, automate and significantly speed up the process – for example through blockchain stored and government validated response authorizations, licenses, automated insurance activation, automated asset tracking, all powered and triggered by smart contracts (Litan, 2020). Smart contracts (Szabo, 1997) are pieces of software that regulate the exchange of resources between participants. Smart contracts are generally used to automatize and make transactions seamless and more efficient. It is part of BCT with the highest potential to revolutionize all sorts of transactions from the execution of legal agreements to the IoT. Smart contracts show high potential to facilitate cross-organizational processes and collaboration (Prause and Hoffmann, 2020). The collaboration, i.e. the power-sharing concept is explained as "*actors jointly exercising their capabilities related to a problem in order to further their separate and joint aims ... power sharing requires a common or mutual objective ... shared power remains a mixed motive situation in which participants reserve the right of exit*" (Crosby and Bryson, 2005, p. 18). Even though the stakeholder organizations are willing to do more to build CI resilience, none has enough power and resources to achieve it acting alone. Collaborative approach to CIR would include joint decision-making, shared, collaborative preparedness planning and shared concept of operations (CONOPS).

This also brings us to the need of investigating a strategy for *blockchain governance* in this specific application case. Governance mechanisms must take into account specific requirements, which are different from the typical business context (Benaben et al., 2017). PPCs for CIR are basically networks of legally autonomous organizations that work together to achieve both their own and collective goals. Some form of governance is needed to ensure participants engagement, resolve possible conflicts, and optimize resource utilization (Provan and Kenis, 2008). Provan and Kenis (2008) presented and compared different approaches to govern networks based on their main characteristics. When it comes to CIR, approaches to Inter-Organizational 'network governance' (also called 'collaborative governance' or 'meta-governance') are discussed considering as a wide variety of network management strategies to guide and structure interaction processes (CRN, 2009; Klijn et al., 2020). Governance models of permissioned blockchain must fit the governance model of the network of involved actors, i.e. which nodes are authorized to access, which portions of data, who will have validation rights, etc. (Carminati, 2018). Different layers of control, permission and visibility could answer to a number of information sharing and collaboration needs and requirements of data confidentiality of transactions and of data.

Emerging concepts and approaches related to CIR

Network centric (enabled) operations (NCO/NEO) paradigm, is based on the idea that a network of well-informed geographically dispersed actors, may have higher performances thanks to its information advantage. NEO concept promotes flatter organizational structures, breaking down information silos (sharing information vertically and horizontally) and empowering individuals at the edge of an organization – at least in situations when dealing with emergencies (Alberts and Hayes, 2003). Experiments of NCO implementation had been already tested in the crisis management domain (e.g. in the Netherlands – van de Ven et al., 2018), but with the lowest maturity levels achieved. BCT might become the key technological enabler of the NEO principles, providing necessary advantages of networks (such as operational resilience), making them less vulnerable (not beatable in any one place), dynamic and flexible (new elements can be easily added and removed). Peer-to-peer information exchange also gives a possibility to flatten hierarchical structures and increase tempo when needed.

CI are increasingly becoming equipped with Industrial Internet of Things (IIoT) technology, from transportation to energy production, making them more connected than they have ever been. BCT may be applied to detect a malicious tampering of data during transmissions to and from CI (e.g. IoT devices) ensuring that the data is from a verified source and issued at a verified time (UK Government Office for Science, 2016). It can also assure data integrity in software and firmware. A blockchain-based cybersecurity platform can secure connected devices using digital signatures to identify and authenticate them, adding them as authorized participants in the blockchain network and ring-fencing CI by rendering them invisible to unauthorized access attempts (Muchena, 2019).

Capability-based planning and capability assessment are high on the agendas of several countries and organizations as part of their risk management and emergency preparedness (EC, 2015; UNISDR, 2015). Moving from the traditional approach (Safety-I), which focuses on eliminating causes and improving barriers, a new more holistic approach is emerging, which embraces Resilience Engineering thinking (Safety-II) as a complementary approach where attention is directed to the system's abilities to perform and to succeed under varying conditions (Hollnagel et al., 2013). In the EM domain, the term *capability* is usually used in relation to resources and capacity (Lindbom et al., 2015). *Resilience capabilities* can be understood as enablers of activities and functions that serve the resilience goals (Kozine et al., 2018). The US Federal Emergency Management Agency (FEMA) uses the 'core capabilities' approach to achieve the National Preparedness Goal (U.S. DHS, 2015). London Resilience Partnership's approach to resilience building is based around the development of capabilities as a mechanism for greater multi-agency cooperation in planning for, and responding to large-scale emergencies (LRG, 2020). The Swedish Civil Contingencies Agency (MSB) performs an annual national capability assessment (Swedish MSB, 2012). European READ project developed a capabilities-based approach to assessing CIR as a step towards informed resource allocation and operation in the context of EM or multi stakeholder planning (Kozine et al., 2018). Capability-based planning has become the gold standard also for defense planning as it enables military agencies to identify program needs, allocate resources, and track activities and outcomes (De Spiegeleire, 2011).

Resource Based View (RBV) and *Resource Orchestration Theory (ROT)* are the main theories to define and operationalize the core capabilities and to enable collaborative processes for a more effective EM. The ROT is used to investigate the resources (tangible and intangible assets) and develop capabilities to orchestrate and operationalize them (Burin et al. 2020), where the orchestration of resources involves their configuration and combination to create synergies (Gulati et al. 2011). Capabilities must be orchestrated both at the intra- and inter-organizational levels since the focus on interdependent systems requires the involvement of actors with different competencies and resources. This is compatible with the ROT which proposes the possibility to integrate resources across organizations, thus developing capabilities unavailable to organizations working on their own (Burin et al. 2020).

Both resources and specific capabilities of individual organisations could be made available as services, in a similar manner. Actors, people and organizations, create capabilities that help in finding a solution for unexpected problems they have to deal with, during daily operations and activities. In this case the gaps of an organisation can be filled by capabilities offered by another one. In software engineering Service Oriented Architecture (SOA) is *"a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains*" (MacKenzie et al, 2006, p.29). When dealing with an inter-organizational process the target scenario should be the one of SOA, where services are discovered, composed and deployed on the fly based on the needs (Carminati, 2018).

Most CI systems are important not only for a normal functioning of societies, but continuous operation is required also during disasters to fully respond to community needs and recovery activities. However, it is demonstrated that the capacity of many CI during disasters has been compromised. When trying to ensure the business (and service) continuity organizations rarely go beyond the boundaries of their organization to include the supply chain, district or infrastructural dimensions of Business Continuity Planning (BCP). Thus, the drafting of guidelines for BCP implementation at district level is an emerging concept on global level. *Area Business Continuity Management* (Baba et al., 2014), as named by the Japan International Cooperation Agency (JICA), is a framework for coordinated damage mitigation measures and recovery actions of stakeholders including individual enterprises, industrial area managers, local authorities and CI in order for business continuation of a certain area as a whole.. Area BCM could hugely benefit from the BTC-enabled inter-organizational capabilities, including Business Impact Analysis (BIA) that would take into account interdependencies and consequences of cascading effects, selection of recovery strategies and developing collaborative BCPs. It is also very common that the weakest part of a BCP are vulnerabilities that lie with suppliers at deep tiers of the supply chains that might not be visible while BTC finds its application for an increased supply-chain visibility (U.S. DHS, 2020). The data integration processes between manufacturers, retailers and suppliers provides greater reliability, transparency and security. The ability to digitize and securely store information on any asset allows organizations to track their ownership, location, state, availability and other relevant attributes (Min, 2019).

The summary or emerging research areas in CIR which could benefit from BCT is given in Table 3.

Table 3. Summary of possible BCT uses to address the challenges of effective CIR (high-level overview)

Public-Private collaborations	Technological enabler of seamless and trusted peer-to-peer transactions within a network of CI stakeholders
Information sharing	Overcome existing issues and barriers, support requirements of network-enabled operations
Resource sharing	Cross-organizational resource management and cooperation
Power sharing	Joint decision making, collaborative resilience planning.
Capability-based planning (Inter-organizational capabilities)	Resilience capabilities development and inter-organizational capacities deployment (Service Oriented Architecture)
Supply chain resilience	Supply-chain visibility, product provenance, traceability, process automation
Business Continuity Planning	Enable and support a Collaborative Business Continuity Planning
Advanced analytics and decision-making	Facilitate use of Artificial Intelligence (AI) and Machine Learning (ML) applications

A CALL FOR RESEARCH AND RESEARCH AGENDA

The blockchain emerged as a disruptive technology with a tremendous transformative potential for our societies (Atzori. 2017). Blockchain promises to be a great solution for use cases that rely on security, controlled access, accountability, transparency, efficiency, and trust (Yli-Huumo et al., 2016), also in situations where multiple organizations need to come together and agree on participants, roles, assets and transactions between each other. There is a number of research streams that would benefit from being systematically explored to fully exploit the BCT potential in this domain. Due to the space constraints, we cover some of the main topics, which are not exhaustive by any means, but they show that many novel research directions could take place (Table 4).

To start with, it is important to understand if, how, and in what degree, the blockchain technology implementation would be able to address exiting issues and barriers to inter-organizational information sharing (Petrenj et al., 2013). In addition, to what extent it could create abilities to improve maturity level of NEO by breaking information stovepipes through trusted peer-to-peer information exchange and efficient authority delegation, powering operational-level efficiency. Further exploration should also question how can BCT contribute to the development of specific resilience capabilities (intra and inter-organizational). For example, facilitating cross-organizational resilience capabilities/services deployment through smart contracts (in SOA manner), thus significantly improving emergency response and recovery. This would also contribute to the Area BCM since CI individual BCPs largely depend on external factors such as public agencies support levels, external resources and supply chains. In order to be effective, BCPs must leverage inter-organizational relations in all phases of the development. Scholars also emphasize BCT application for the management of common-pool resources in the context of networks and supply chains to solve and overcome obstacles related to fragmentation and distributed structures (Prause and Hoffmann, 2020).

On the technical side, a detailed analysis is needed to assess and benchmark existing consortium blockchain platforms and technologies – architectures, technological components, consensus algorithms, possible applications, etc. Advantages and limitations of each must be understood for this specific domain of application. There is a need to investigate blockchain interoperability with existing IT systems but also that different blockchain network can interact with each other (Akram et al., 2020)

Ability to hide sensitive information and share only selected data might encourage CI operators, responders and governments to share anonymized data for artificial intelligence and machine learning decentralized applications to enhance data analysis and support the overall decision-making process. On top of this, numerous successful BCT use cases already exist – their applicability and transferability to the CIR domain should be investigated.

Even though the most of the literature deals with the technological capabilities, BCT applications can have significant effects on the way organizational processes are designed (Ølnes et al., 2017). BCT will fundamentally change how organizations deal with all types of transactions, and so how organizations manage their processes within the network of involved stakeholders.

Table 4. Proposed research directions

Blockchain Good Practices	Identification and review of existing successful use cases of BCT, assessment of their applicability and transferability to CIR domain (e.g. from Supply Chain, Cybersecurity domains)
Blockchain platforms and technologies	Assessment and benchmarking of existing consortium blockchain frameworks and platforms in light of these use cases
Inter-organizational approaches	Investigate opportunities for BCT exploitation to enable inter-organizational sharing (information, resources, power)
Inter-organizational resilience management	Examining the potential and applicability of BCT (and Smart Contracts) to enable cross-organizational and cross-border resilience capabilities deployment (Service Oriented Architecture - SOA)
BCT adoption hurdles	Challenges, barriers and risks of BCT adoption in this domain and how to deal with them
Interoperability	Requirements for the interoperability between blockchain and IT systems in use by CI stakeholders; interoperability between different consortium blockchains
Legal aspects	Legal and regulatory concerns should be explored (around data privacy, enforceability of contracts), which could hinder the technology adoption.
Ethical aspects	Investigate existence of any ethical and/or social implications of adopting

	BCT in this domain
Business Continuity Management	Support collaborative Area Business Continuity Planning
Governance	Governance models of private permissioned blockchain and their compatibility with the governance models of PPCs

Risks and benefits related to BCT adoption and application must be carefully identified and assessed as well. While BCT can solve many of the existing challenges it may also bring new risks. The resilience of such blockchain should be assessed, since once deployed it becomes a CI itself. More research is also needed on the financial costs and benefits of building and running permissioned blockchains in the context of PPC for CIR.

Rather than trying to remedy the problem by developing an ICT to support collaboration, the right approach would be creation, transformation and perfecting of collaboration process (facilitated by ICT) to improve inter-organizational resilience capabilities (Sagun et al, 2009). Looking at the broader picture of public-private collaborations for CIR, ultimately, it might be mostly a question of governance, whether collaborative initiatives will succeed or fail.

CONCLUSIONS

This paper discusses how adoption and adaptation of BTC could bring radical improvements to the way organizations work together to build CIR. The main contribution is synthesizing the knowledge from the previous work on these topics, and presenting it in a synergistic context to provide a springboard for the new research that would benefit both fields. Our vision is that the research of the potential of BCT adoption in the CIR domain should evolve around understanding how the use of the BCT could enable different levels of inter-organizational capabilities (coordination, cooperation and collaboration), on one side, and explore how these blockchain-enabled capabilities could support more effective operationalization of the emerging approaches to inter-organizational CIR building. Risks and challenges of BCT adoption in this domain should also be investigated.

The main limitation of the paper is its conceptual nature – it relates groups of concepts and ideas analyzing already available information from the two fields. Future research is therefore needed to further detail CIR needs and map them against BCT capabilities, thus developing initial use cases, practical experiments and related Proofs of Concepts.

The authors are looking forward to all kinds of feedback that may improve this work, and hope to stimulate further discussion and research in this multidisciplinary domain.

REFERENCES

Akram, S. V., Malik, P. K., Singh, R., Anita, G. and Tanwar, S. (2020). Adoption of blockchain technology in various realms: Opportunities and challenges. *Security and Privacy*, *3*(5), e109.

Alberts, D. S. and Hayes, R. E. (2003) "*Power to the Edge, Command and Control in the Information Age.*", Information Age Transformation Series, CCRP press.

Atzori, M. (2017). Blockchain Technology and Decentralized Governance: is the State Still Necessary? *Journal of Governance and Regulation, 6(1)*, 45-62.

Baba, H., Watanabe, T., Nagaishi M., and Matsumoto, H. (2014). Area business continuity management, a new opportunity for building economic resilience. *Procedia Economics and Finance*, *18*, 296-303.

Benaben, F., Montarnal, A., Truptil, S., Lauras, M., Fertier, A., Salatge, N. and Rebiere, S. (2017). A conceptual framework and a suite of tools to support crisis management. *50th Hawaii International Conference on System Sciences.*

Blockchain Commission (2018). *The Future is Decentralized - Block Chains, Distributed Ledgers & The Future of Sustainable Development,* whitepaper.

Bruneau, M., Chang, S.E., Eguchi, R.T., Lee, G.C., O'Rourke, T.D., Reinhorn, A.M. and Von Winterfeldt, D. (2003) 'A framework to quantitatively assess and enhance the seismic resilience of communities', *Earthquake Spectra*, Vol. 19, No. 4, pp.733–752.

Burin, A. R. G., Perez-Arostegui, M. N. and Llorens-Montes, J. (2020). Ambidexterity and IT competence can improve supply chain flexibility? A resource orchestration approach. *Journal of Purchasing and Supply*

Management, *26*(2).

Carminati, B., Ferrari, E. and Rondanini, C. (2018). Blockchain as a platform for secure inter-organizational business processes. *IEEE 4th International Conference on Collaboration and Internet Computing* (pp. 122-129).

Cheong, S., Lee, A. and Cho, S. (2021, March 24). Suez Canal Blockage May Ripple Through Global Energy Market, *Bloomberg*. https://www.bloomberg.com/news/articles/2021-03-24/suez-canal-blockage-set-to-ripple-through-global-energy-market

Choraś, M., Kozik, R., Flizikowski, A., Hołubowicz, W. and Renk, R. (2016). *Cyber threats impacting critical infrastructures. In Managing the Complexity of Critical Infrastructures (pp. 139-161)*. Springer, Cham.

Colomo-Palacios, R., Sánchez-Gordón, M. and Arias-Aranda, D. (2020). A critical review on blockchain assessment initiatives: A technology evolution viewpoint. *Journal of Software: Evolution and Process*, *32*(11), e2272.

CRN (2009) Roundtable Report '6th Zurich Roundtable on Comprehensive Risk Analysis and Management: Network Governance and the Role of Public- Private Partnerships in New Risks'. https://www.files.ethz.ch/isn/120862/6th-CRN-Roundtable-Report.pdf

Crosby, B. C. and Bryson, J. M. (2005). *Leadership for the common good: Tackling public problems in a shared-power world* (Vol. 264). John Wiley & Sons.

De Spiegeleire, S. (2011). Ten trends in capability planning for defence and security. *The RUSI Journal*, *156*(5), 20-28.

Dib, O., Brousmiche, K. L., Durand, A., Thea, E. and Hamida, E. B. (2018). Consortium blockchains: Overview, applications and challenges. *International Journal On Advances in Telecommunications, 11(1&2), 51-64.*

Dubey, R., Gunasekaran, A., Bryde, D. J., Dwivedi, Y. K. and Papadopoulos, T. (2020). Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting. *International Journal of Production Research*, *58*(11), 3381-3398.

Dunn-Cavelty, M. and Suter, M. (2009) Public-Private Partnerships are no silver bullet… , *International Journal of Critical Infrastructure Protection, Volume 2, Issue 4,* pp. 179–187.

European Commission (2005), Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final

European Commission (2015). Risk Management Capability Assessment Guidelines, *Off. J. of the EU.*

Furutai, K. and Kannoi, T. (2018). *Resilience analysis of urban critical infrastructure: A human-centred view of resilience.* Domains of resilience for complex interconnected systems, 69.

Galbusera L., Giannopoulos, G. and.Ward, D (2014). *Developing stress tests to improve the resilience of critical infrastructures: a feasibility analysis*, JRC Science and Policy Reposrts, EC.

Gulati, R., Lavie, D. and Madhavan, R. R. (2011). How do networks matter? The performance effects of interorganizational networks. *Research in Organizational Behavior*, *31*, 207-224.

Hollnagel, E., Braithwaite, J. and Wears, R. L. (Eds.). (2013). *Resilient health care*. Ashgate Publishing, Ltd.

Jaeger, L. (2018, October 4). Public versus Private: What to know before getting started with blockchain. *Blockchain Pulse: IBM Blockchain*. https://www.ibm.com/blogs/blockchain/2018/10/public-versus-private-what-to-know-before-getting-started-with-blockchain/

Jahankhani, H. and Kendzierskyj, S. (2019). The Role of Blockchain in Underpinning Mission Critical Infrastructure. In *Industry 4.0 and Engineering for a Sustainable Future* (pp. 191-210). Springer, Cham.

Klijn, E. H., van Meerkerk, I. and Edelenbos, J. (2020). How do network characteristics influence network managers' choice of strategies?. *Public Money & Management*, *40*(2), 149-159.

Kozine, I., Petrenj, B. and Trucco, P. (2018). Resilience capacities assessment for critical infrastructures disruption: the READ framework (part 1). *International Journal of Critical Infrastructures, 14(3)*, 199-220.

Lindbom, H., Tehler, H., Eriksson, K. and Aven, T. (2015) The capability concept – On how to define and describe capability in relation to risk, vulnerability and resilience', *Reliability Engineering and System Safety, Vol. 135*, pp.45–54.

Litan, A. (2020, March 3). Smart Contracts are Neither Smart nor are they Contracts. *Gartner* https://blogs.gartner.com/avivah-litan/2020/03/03/smart-contracts-neither-smart-contracts/

London Resilience Group – LRG (2020). London Resilience Partnership Strategy. https://www.london.gov.uk/sites/default/files/london_resilience_partnership_strategy_2020-2023_v3.4.pdf

MacKenzie, C. M., Laskey, K., McCabe, F., Brown, P. F., Metz, R. and Hamilton, B. A. (2006). Reference model for service oriented architecture 1.0. *OASIS standard, 12*(S 18).

Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *Business Horizons*, *62*(1), 35-45.

Muchena, H. (2019, Jul 17). Blockchain, IoT, & Critical Infrastructure Security. *Medium*. https://medium.com/@ontheheath/blockchain-iot-critical-infrastructure-security-229cd18fad

Ølnes, S., Ubacht, J. and Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly 34,* 355-364

Olson, T. (2018, June 18). Blockchain for multinational information sharing. *Blockchain Pulse: IBM Blockchain Blog.* https://www.ibm.com/blogs/blockchain/2018/06/blockchain-for-multinational-information-sharing/

Palfreyman, J. (2015, November 4) Blockchain for Government? *Medium.* https://medium.com/@JohnP261/blockchain-for-government-184ace54756d

Petrenj, B., Lettieri, E. and Trucco, P. (2013). Information sharing and collaboration for critical infrastructure resilience–a comprehensive review on barriers and emerging capabilities. *International journal of critical infrastructures, 9(4)*, 304-329.

Prause, G. and Hoffmann, T. (2020). Innovative Management of Common-Pool Resources by Smart Contracts. *Marketing and Management of Innovations, 1,* 265-275.

Provan K. and Kenis, P. (2008) Modes of Network Governance: Structure, Management, and Effectiveness, *Journal of Public Administration Research and Theory, Vol. 18, Issue 2*, pp. 229-252.

Quinnel, R. (2019, July 15) Basics of blockchain for the IoT. *EDN.* https://www.edn.com/basics-of-blockchain-for-the-iot/

Rød, B., Lange, D., Theocharidou, M. and Pursiainen, C. (2020). From Risk Management to Resilience Management in Critical Infrastructure. *Journal of Management in Engineering, 36(4),* 04020039.

Ropohl, G (1982). " Some Methodological Aspects of Modelling Socio-Technical Systems." In *Progress in Cybernetics and Systems Research* , vol. 10, ed. R. Trappl *et al* . Washington, DC: Hemisphere. Pp. 525-536.

Sagun, A., Bouchlaghem, D. and Anumba, CJ. (2009) A scenario-based study on information flow and collaboration patterns in disaster management. *Disasters 33(2), 214–238.*

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".

Swedish Civil Contingencies Agency - MSB (2012) Swedish national risk assessment 2012. https://rib.msb.se/filer/pdf/26621.pdf

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday* 2.

Transport Canada (2017) Guide for Cross-Border Emergency Response. Retrieved from http://publications.gc.ca/site/eng/9.844206/publication.html

Trucco, P. and Petrenj, B. (2017). Resilience of Critical Infrastructures: benefits and challenges from emerging practices and programmes at local level. In *Resilience and Risk* (pp. 225-286). Springer, Dordrecht.

U.S. Department of Homeland Security (2013). *NIPP 2013: Partnering for critical infrastructure security and resilience*.

U.S. Department of Homeland Security (2015) *National Preparedness Goal, 2nd edition.*

U.S. Department of Homeland Security (2020). Blockchain portfolio. https://www.dhs.gov/science-and-technology/blockchain-portfolio

U.S. National Infrastructure Advisory Council – NIAC (2009) '*Critical Infrastructure Resilience – Final Report and Recommendations*', U.S. Department of Homeland Security, Washington, DC.

UK. Government Office for Science (2016). *Distributed ledger technology: Beyond blockchain.* Available from www.gov.uk/go-science

UNISDR (2015). Sendai Framework for Disaster Risk Reduction 2015 -2030, Geneva, Switzerland.

Van De Ven, J., Van Rijk, R., Essens, P. and Frinking, E. (2008). Network centric operations in crisis management. *ISCRAM Conference*, Washington, DC, USA.

World Economic Forum (2020), '*How to build a successful nationwide blockchain initiative*'. https://www.weforum.org/agenda/2020/05/ho-to-build-successful-blockchain-initiative/

Yafimava, D. (2019). *What are Consortium Blockchains, and What Purpose do They Serve?* Openledger.info

Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS one*, *11*(10).

Zwitter, A. and Boisse-Despiaux, M. (2018). Blockchain for humanitarian action and development aid. *Journal of International Humanitarian Action*, *3*(1), 1-7.