

The Paradoxes of Trust and Transparency of Blockchain Technologies

Cédric Baudet, University of Applied Sciences and Arts Western Switzerland, Switzerland*

Maximiliano Jeanneret Medina, University of Applied Sciences and Arts Western Switzerland, Switzerland

ABSTRACT

The Republic and Canton of Jura has decided to adopt and integrate the CERTUS digital seal and the KSI blockchain as the central technological components of their e-government portal and of their digital government transformation program. However, this project is taking place in turbulent times. While blockchain suffers from a bad reputation for ecological reasons and while the Swiss Confederation has rejected the selected blockchain solution, this article seeks to answer how to grasp the paradoxes of blockchain technologies acceptance by state citizens in an extreme management situation. Through an action research that aims to solve practical problems and create scientific knowledge, this study highlights the paradox of trust and considers blockchain technologies to enhance trust between citizens in politically stable countries. Furthermore, it investigates the paradox of transparency of blockchain technologies in an extreme management situation and proposes communicating in two levels of abstraction to limit tensions in turbulent times.

KEYWORDS

Acceptance, Action Research, Blockchain, E-Government, Extreme Management Situation, KSI, Transparency, Trust

INTRODUCTION

Governments, organizations, and individuals rely on information systems (IS) to cope with the negative effects of the COVID crisis. In this pandemic disaster, governments see pass applications, whether health or vaccine, as one of the most effective ways to fight against the spread of the different variants. In a situation marked by multiple tensions, governments had to swiftly select a reliable and secure technological solution to store COVID certificates in digital form. In turbulent times, the risk of a loss of trust by citizens in a government's capabilities to provide adequate public services should be avoided as much as possible (Initiative D21 et al., 2021).

After receiving about 50 proposals for the application of the COVID pass, the Swiss Confederation selected and examined two IT solutions that would allow people who have been vaccinated, recovered, or have received a negative test result to present a COVID certificate (Federal Office of Public Health, 2021a). The Federal Office of Information Technology, Systems and Telecommunication (FOITT) proposes the first IT solution. This federal department highlights the compatibility of their IT solution with the one of the European Union, the security, and the open-source code. The second IT solution

DOI: 10.4018/JGIM.321111

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

is based on a digital seal stored in the Keyless Signature Infrastructure (KSI) blockchain. Proposed by companies ELCA and SICPA, this IT solution focuses on ease of use while respecting users' privacy. While this second IT solution was considered the favorite by experts, the Swiss Confederation chose the pass solution developed by the FOITT in May 2021 (Federal Office of Public Health, 2021b). However, the loser has certainly not lost everything. Indeed, the Republic and Canton of Jura (RCJU) has decided to adopt and integrate the CERTUS digital seal and the KSI blockchain as the central technological components of their e-government portal and, more broadly, of their digital government transformation program. According to the project initiators, these technologies aim to strengthen digital trust between citizens and the government by securing administrative documents (République et Canton du Jura, 2016).

From a more academic perspective, adopting and integrating the CERTUS digital seal and the KSI blockchain should be approached *ex-ante* through the lens of technology citizens' acceptance. Indeed, few academic studies address the acceptance of blockchain technologies in an e-government context. Two main aspects must be discussed in this case in order to fill the gaps in the literature. First, it is an e-government project that must consider the acceptance of all citizens without exclusion. Second, recent scientific studies call for analyzing digital government transformation in turbulent times (Eom & Lee, 2022). This digital government transformation project is carried out in turbulent times, leading to dilemmas, ambiguities, and paradoxes (ibid, 2022). Indeed, several factors increase the uncertainty and dangers of this project. Among them, are the bad reputation of blockchain technologies (BCT) for ecological reasons, the Swiss Confederation's rejection of the CERTUS and KSI solution, and the unprecedented wave of cyberattacks against administrations in Switzerland (SWI, 2021, 2022). Moreover, scholars highlight paradoxical findings about BCT that can arise from technological, organizational, and environmental factors affecting its adoption at multiple levels. The political stability of a country like Switzerland can be a barrier to the acceptance of BCT by national government adopters (Reddick et al., 2019). On the individual acceptance level, trust remains a central concern of BCT, because paradoxically, trust in such trustless systems seems to be a prerequisite for its actual use (Dupuis et al. 2021). In political stability, but in a situation that can be described as extreme because of the uncertainty, dangers, and high levels of change that characterizes it (Godé & Lebraty, 2015), it seems necessary to analyze in depth the paradoxes of the CERTUS and KSI case and to question the acceptance of such technologies in the e-government domain. Thus, we seek to answer to how to grasp the paradoxes of BCT acceptance by state citizens in an extreme management situation?

To answer this research question, we conducted action research from April to November 2021. We believe this research question is relevant to both practitioners and researchers, as it addresses a current issue as well as organizational problems (Benbasat & Zmud, 1999) while ensuring that we contribute to the scientific knowledge base on the adoption of BCT at an individual level in e-government context.

The rest of this paper is structured as follows. We begin by providing a literature review on BCT with an emphasis on its acceptance among citizens within an e-government context. Thereafter, we expound upon our research context and the action-based methodology is then detailed. In a fourth section, we highlight four main findings. We explore subsequently the potential application of BCT for building trust among people residing in politically stable countries, examine the challenges posed by governmental transparency and reliability, and recommend the use of two levels of abstraction as a means of minimizing conflicts during unstable times.

BACKGROUND

Since the introduction of the cryptocurrency Bitcoin in 2008 (Nakamoto, 2008), blockchain has become one of the two most significant disruptive technologies of our time (Verbeek & Lundqvist, 2021), and one of the key technologies of the digital economy (Brynjolfsson et al., 2021). A blockchain is

a data structure that is immutable, transparent, secure, and distributed among the nodes of a peer-to-peer network (Christidis & Devetsikiotis, 2016). There are different types of blockchain, and it is necessary to distinguish between the blockchain itself and the technologies that rely on it, such as Smart Contracts and Decentralized Autonomous Organizations (Christidis & Devetsikiotis, 2016). Moreover, blockchain is a particular form of distributed ledger technology (Tan et al., 2022).

In the context of e-government, blockchain can be used for any government information exchange with other parties (Ølnes et al., 2017) as well as identity management systems (Sung & Park, 2020). According to Toufaily et al. (2021), blockchain can solve three broad business problems in the public sector: coordination failures, horizontal integration, and decentralization. Hence, implementing BCT allows for efficiency gains (Allessie et al., 2019), notably by eliminating intermediaries, reducing bureaucracy, or even enhancing coordination between civil servants (Alexopoulos et al., 2019; Cagigas et al., 2021). Moreover, the blockchain's ability to record distributed transactions improves transparency, prevents fraud, and increases trust in the public sector (Batubara et al., 2018). Finally, many researchers argue that BCT could substantially improve information security, an issue closely related to trust and acceptance of e-government applications (Allessie et al., 2019; Tshering & Gao, 2020; Warkentin & Orgeron, 2020).

Blockchain Implementations in an E-Government Context

Government interest in BCT is growing and the number of e-government projects that rely on these technologies is increasing rapidly (Alexopoulos et al., 2019; Allessie et al., 2019). Potential use cases (Ølnes et al., 2017) moved from system design (Thakur et al., 2020), to pilot projects, to large-scale implementations (Alexopoulos et al., 2019). We can classify the rise of blockchain architectures and applications for governments into two large groups (Ølnes et al., 2017). The first one, termed governance by blockchain, implies applications in which public organizations adopt BCT for their processes, and in which BCT is used to govern transactions. The second one, governance of blockchain, determines how blockchain should look like, how to adapt to changes, and ensures that public values and societal needs are fulfilled. For the past few years, national and international agencies have become actively involved in the topic. For instance, the European Union promotes a more coordinated approach to BCT development and deployment (Allessie et al., 2019; Verbeek & Lundqvist, 2021). As of April 2020, five of the EU27 countries have published a national blockchain strategy, though another five are developing or planning to develop a strategy, while a further five are using government-supported activities to promote blockchain (Verbeek & Lundqvist, 2021).

Alexopoulos et al. (2019) explored some implementations of BCT in Europe and shed light on their adoption by the Estonian government. The Estonian e-government approach is built around a service-rich ecosystem of about 3,000 services, including digital identity management, online voting, electronic patient data management, tax collection, and more. Three technological components form the core of the Estonian e-government information system: e-ID, X-Road, and the KSI blockchain (e-Estonia, 2021). The e-ID is the key to the digital identity of each citizen. The X-Road platform provides decentralized data management. Finally, the KSI blockchain oversees the integrity of e-government data. While blockchain is the subject of much interest in the scientific community, this is not true for the KSI blockchain¹. Developed in 2007 in response to a wave of cyberattacks, the KSI blockchain stands out for its low energy consumption, good scaling capacity, and speed in obtaining consensus (Guardtime, 2021). Moreover, Warkentin and Orgeron (2020) performed a case study analysis of the blockchain in the Illinois State Government through the lens of the Confidentiality-Integrity-Accessibility triad. More recently, Sung and Park (2021) documented the introduction of a blockchain-based identification system in South Korea. These authors provide seven blockchain use cases related to identity management in public services. Hyperledger Fabric and Amazon's Managed Blockchain Service have been used for design aspects.

Scientific studies highlight the perceived impact and emerging disruption potential of BCT, but also note that these technologies have been slow to engender any significant momentum within the

Information Systems (IS) and Information Management (IM) literature (Hughes et al., 2019). Whilst several studies have detailed specific use cases where blockchain has the potential for delivering significant change and benefits to organizations and citizens, many lacks specific context offering generalization and a high-level narrative (Hughes et al., 2019). There is a need for data-driven studies about specific blockchain solutions for new business and social applications as well as their roles and impacts in various industries and sectors (Frizzo-Barker et al., 2020). Hence, organizations must understand and explore blockchain solutions' utility, adoption, and management (Uphaday, 2020).

It seems necessary to investigate the adoption in the e-government field to fill this gap. To do so, we provide an understanding of BCT adoption framed in IS diffusion and adoption theories. Research and theory development on the diffusion of innovation (Rogers, 1962, 2003) has primarily focused on the diffusion of innovations among individuals, although it addresses innovation diffusion within organizations (Lundblad, 2003). As for adoption, it concerns individuals and their actions being rooted in prominent approaches to intrapersonal IS acceptance (Davis, 1989, Venkatesh et al., 2003). Indeed, technologies are important for individuals, organizations, and for society. It seems then necessary to understand and expect the potential refusal of using technologies by individuals. A large body of research in the field of IS has focused on this question. The seminal work of Davis, based on the theory of reasoned action (Ajzen and Fishbein, 1975), has shed light on the notion of acceptance in the field of IS (see Davis, 1989). The Technology Acceptance Model (TAM) makes it possible to understand and measure an individual's motivation to use a technology before its implementation. TAM, therefore, has both explanatory and predictive purposes (Davis et al., 1989). TAM postulates that before using a system, an individual must have the intention to use it. This intention to use is itself determined by the perceived ease of use and the perceived usefulness of a system by the individual. Many works have developed Davis' researches. Among them, the Unified Technology Acceptance Model (UTAUT) was proposed by comparing eight technology acceptance models. In this unified model, which appears to better predict individuals' acceptance of a system (Venkatesh et al., 2003), technology use behavior is determined by behavioral intention. Four causal antecedent variables (performance expectancy, effort expectancy, social influence, and facilitating conditions) and four moderator variables (gender, age, experience, and voluntariness of use) influence these two variables. Moreover, we note that research on the acceptance of BCT is largely based on the UTAUT model. We present the literature on this topic in the following sections.

Understanding Blockchain Adoption in the Public Sector

As shown by systematic literature reviews, a considerable body of literature investigated the adoption of blockchain in the public sector (Batubara et al., 2018; Cagigas et al., 2021). Initial work has been both descriptive and prescriptive (Warkentin & Orgeron, 2020). When the focus is placed on understanding blockchain adoption, we can observe three kinds of theoretical contributions: 1) coarse-grained classifications of both benefits and challenges, 2) conceptual frameworks to help scholars and decision-makers, and 3) theoretical models with causal relationships.

First, some scholars investigated the balance of the expected benefits of blockchain against its challenges (Batubara et al., 2018; Cagigas et al., 2021). The expected benefits derive from blockchain characteristics and are widely discussed in the literature (e.g., Ølnes et al., 2017). Because blockchain technologies imply by nature multiple stakeholders, expected benefits are often explored through different perspectives (e.g., government vs citizen). Moreover, the technical complication of blockchain and the profound societal, political, and environmental impact engendered lead to the adoption of a holistic view of adoption. According to Batubara et al. (2018), barriers to adoption can be of three types. From an environmental perspective, lack of laws and regulations can limit adoption. From an organizational perspective, resistance to change or the need for new governance models are presented as the main barriers to adoption. Finally, and from a technological point of view, there are numerous barriers to adoption, such as lack of security, reliability, scalability, or usability. In line with this point of view, Toufaily et al. (2021, p. 10) states that "1) a challenge that is not addressed

will have an effect on the other challenges and consequently on the adoption and (2) the expected value created for one stakeholder will consolidate the benefits for the other stakeholders.” Hence, a holistic approach sets aside an approach considering one characteristic or one stakeholder in isolation. Moreover, Cagigas et al. (2021) analyzed the main potential benefits, costs, and risks reported in the literature through a tripartite perspective implying governments, civil servants, and citizens. Security and transparency are the main potential benefits offered by BCT for citizens. The benefits related to security are mainly derived from the immutability of the data recorded in the blockchain. Also, the blockchain is designed to give the data owner a unique identifier to access data and the ability to share only those wanted. Thus, data protection seems to be a central concern for citizens. The lack of standards, regulatory uncertainties, and issues related to these technologies’ scalability are considered major risks for governments.

Organizations and government authorities must be judicious when implementing blockchain-related technologies (Perdana et al., 2021). An initial understanding of blockchain adoption leads to exploring how dimensions interact by a second body of literature. Recently, important efforts have been made to develop conceptual frameworks to help scholars and decision-makers. We should specify that conceptual frameworks have no specific application area and can be used in industry or a public sector context (Hughes et al., 2019; Toufaily et al., 2021). Some conceptual frameworks offer a staged perspective of introducing a technology (Hughes et al., 2019; Upadhyay, 2020). For instance, Hughes et al. (2019) developed the Blockchain Innovation Framework rooted in Rodgers’ innovation diffusion decision process model. Their contribution is a decision tree based on the five stages documenting the innovation decision process (Knowledge, Persuasion, Decision, Implementation, Confirmation). Such tools complement initial works that focused on technical aspects of blockchain (i.e., Koens and Poll, 2018). In the same vein, Upadhyay (2020) developed the Blockchain Innovation Adoption Framework (BIAF), built on a tree-stage process (initiation, decision, adoption) and considering two levels of adoption (organizational and individual). Moreover, Toufaily et al. (2021) developed a conceptual framework, which brings together the environmental, organizational, and technological challenges of blockchain adoption and the socio-economic expected value from the perspective of main stakeholders in the ecosystem (i.e., private organizations, end-users, and society, public sector, startups, and entrepreneurs). Janssen et al. (2020) proposed the Integrated Process, Institutional, Market, Technology Framework for blockchain adoption that captures the complex relationships between such factors. Finally, Tan et al. (2022) developed a conceptual framework for public management which comprises nine types of governance decisions (infrastructure architecture, application architecture, interoperability, decision-making mechanism, incentive mechanism, consensus mechanism, organization of governance, accountability of governance, and control of governance) into three levels of analysis (micro-, meso-, and macro-levels).

Third, a small body of research measured the effects of factors impacting BCT adoption and operationalized models within different contexts. For instance, Reddick et al. (2019) used the diffusion of innovation theory to examine government adoptions of BCT. Among cybersecurity, government effectiveness, political stability, corruption control, e-government development, and democratic participation, the three first factors are significant predictors of blockchain adoption. High levels of cybersecurity and government effectiveness increase the likelihood that countries will adopt blockchain, while higher levels of political stability decrease the likelihood of early blockchain adoption. As a developing country, India is often taken as an example of benefiting from the blockchain (Hughes et al., 2019). 2019; Rana et al., 2019). Finally, Rana et al. (2019) developed a model of reluctance to use BCT, based on a hierarchical organization of challenges to blockchain adoption.

Understanding Blockchain Acceptance by Individuals

BCT reached the adoption stage in some industries, such as supply chain management (Zheng & Lu, 2022). However, the stage of public acceptance of BCT is unclear despite the many initiatives launched. For example, early research investigated the perception of cryptocurrencies (Jang et al., 2020), while

the primary research stream on public adoption seems still focused on financial applications (Grover et al., 2019; Jang et al., 2020; Perdana et al., 2021; Raddatz et al., 2021). In addition, a recent literature review investigated the potential benefits, costs, and risks from the user's perspective (Cagigas et al., 2021). However, to date, we found no study published in a leading IS venue that investigated the citizen adoption of BCT in an e-government context.

Grover et al. (2019) first investigated the acceptance drivers of blockchain for digital transaction through the lens of the TAM (Davis, 1989). By extracting Twitter feeds to derive collective intelligence, the authors showed that privacy, transparency, trust, and traceability drive blockchain's perceived usefulness. Moreover, users discussed blockchain benefits (attitude towards use) occurred more often than drawbacks (external variable), and users are concerned about the power consumption of BCT and having multiple user's identities. More recently, Raddatz et al. (2021) investigated the consumers' benefits to use blockchain-based applications for banking purpose. They pinpointed an increase in general awareness that highlights enhanced information privacy protection can convince them of the blockchain's utility. Paradoxically, while BCT are trustless systems, trust appears to be a key to consumer adoption (Dupuis et al., 2021). Trust in BCT applications involves trusting their underlying components (i.e., the algorithms powering them, the developers designing them, and the stakeholders providing the information).

However, despite many perceived benefits, blockchain BCT has not gained mainstream adoption. The public understanding of blockchain (Cagigas et al., 2021; Dupuis et al., 2021; Jang et al., 2020; Raddatz et al., 2021) and the usability of this technology (Cagigas et al., 2021; Dupuis et al., 2021; Jang et al., 2020; Meiklejohn, 2018) seems important to consider. According to Cagigas et al. (2021, p. 13915), "it is imperative to improve intuitive blockchain interfaces and to assure some degree of blockchain literacy before it is introduced to the wider public." The lack of users' comprehension (Jang et al., 2020) can explain the slow adoption of the blockchain. Blockchain remains confusing and mostly misunderstood by a general audience (Raddatz et al., 2021). How they communicate this technology shapes the public understanding, opinions, and perceptions of blockchain. Since 2015, public attention has shifted from Bitcoin to blockchain and distributed ledger technology, and such technologies ambition to become ubiquitous for digital trust (Perdana et al., 2021). The perception of blockchain conveyed by media evolved from an initial state of *enfant terrible* to becoming a mature problem-solver (Perdana et al., 2021). By framing its questioning within usability, Meiklejohn (2018) recommends exploring the benefits people feel they can achieve by using distributed ledgers and mapping such benefits (i.e., accountability, immutability) regarding what end users want. Following a user-centered approach, Jang et al. (2020) conducted usability testing on a decentralized exchange application to determine the fundamental causes of problems users encounter when interacting with BCT. They showed that more user-centered design is necessary to enable the widespread use of decentralized applications and recommend enabling users to easily understand and navigate applications based on these technologies.

Through this literature review, we first emphasize that BCT adoption requires considering a broad range of factors, over and above the predominantly technology focus (Janssen et al., 2020). It implies a holistic view of adoption challenges and factors organized within conceptual frameworks. Such theoretical contributions adopted a multilevel and/or multi-stakeholder perspective, often organized in a staged process rooted in diffusion and acceptance theories; while others emphasized the governance of BCT (Ølnes et al., 2017; Tan et al., 2022). Moreover, there is a need to consider the user perspective (Cagigas et al., 2021; Jang et al., 2020; Upadhyay, 2020) by considering usability and user understanding blockchain. According to the most cited article in IS, "performance gains are often obstructed by users' unwillingness to accept and use available systems" (Davis, 1989, p. 319). From our point of view, BCT are no exception. Thus, in the context of action research, it is legitimate to answer how to grasp the paradoxes of BCT acceptance by state citizens in an extreme management situation.

RESEARCH CONTEXT

An E-Government Blockchain-Based Project to Enhance Digital Trust

The Republic and Canton of Jura (RCJU) is one of the 26 Swiss cantons (or states). We recall that in Switzerland, the cantons are sovereign. This autonomy means that each canton must make its own decisions, for example on taxation, education, or administrative processes. The RCJU defined and implemented a digital strategy to transform the government's processes deeply. To this end, many technological projects, considered innovative, aim to digitalize the state administration while working to reduce the digital divide and increase digital trust. They implemented most of these technological projects through the e-government portal, a true digital extension of the physical services offered by the government.

One of the ongoing projects comprises adopting and implementing the CERTUS digital seal technology and the KSI blockchain to form the core technological components of the RCJU e-government portal and, more broadly, their digital government transformation program. These technological components primarily aimed to enhance citizen trust in the digital services offered by the government. In the project's white paper, the RCJU states that each citizen has a client environment to exchange documents with the administration. Thus, the citizen can deposit documents for the administration, and in the same way, the administration will provide documents or certificates to the citizen. The current system is based on the citizen's trust in the security and integrity of the government's IT systems. However, in a case of a legal dispute between a citizen with the government over a digital transaction, it would be very difficult, if not impossible, for the citizen to prove their good faith, without the active cooperation of the government services. Therefore, as described within the RCJU's "Digital Trust Vision" document, the first goal of this project is to propose a solution allowing citizens to have complete sovereignty over their data and their digital interactions with the government by introducing a "digital receipt". Likewise, the government will prove the integrity of the administrative data and support independent verification for every citizen.

The RCJU selected the extracts from the debt enforcement register as the first use case to apply the CERTUS digital seal and the KSI blockchain. Due to the need for trust among actors, this use case has been relevant to benefit from BCT. An extract without debt records acts as proof of the citizen's solvability. Such a solvency certificate emitted by the government is necessary, for example, when applying for a rental apartment, a bank loan, or a lease. Upon citizen action on the e-government portal, a QR code is stamped on the certificate (case A in Figure 1). Upon presentation of the attestation, both in paper and digital format and using a dedicated web or mobile app, an organization or a citizen can verify the authenticity of the extract from the debt register of a Jura citizen (case B in Figure 1).

When the solvency certificate is issued, a five-step computerized process is initiated (Figure 2). Step one: the QR code is imprinted onto the certificate; this code is not affiliated with any centralized database of RCJU and contains encoded information as well as an exclusive cryptographic signature that assures the authenticity of the document. Step two: the CERTUS digital seal is applied to the QR code as an additional layer of security. Step three: a distinctive fingerprint is generated from the digital seal. Step four: the fingerprint is timestamped on the KSI blockchain to ensure its permanency. Finally, step five: the KSI blockchain provides a digital signature which serves as a digital receipt and it is stored on the citizen's private area within the e-government portal. This system ensures trustworthiness through "third-party guarantors" without having access to citizens' personal details. Thus, the citizens reserve full control over their data.

A POST-ADOPTION E-GOVERNMENT PROJECT IN AN EXTREME MANAGEMENT SITUATION

In April 2021, the RCJU contacted our research team to be accompanied by the ongoing blockchain-based project. We analyzed this project post-adoption based on the blockchain innovation adoption

Figure 1. Use case of the extract from the debt enforcement register

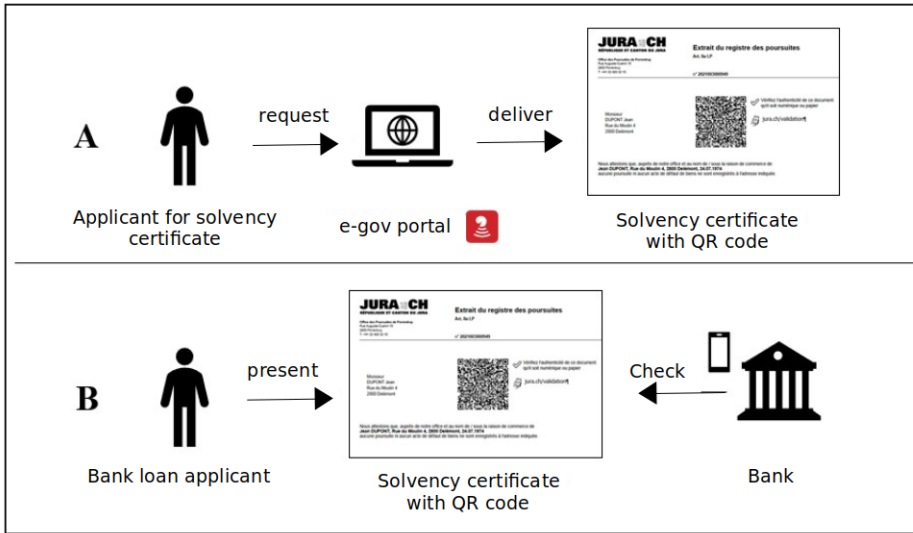
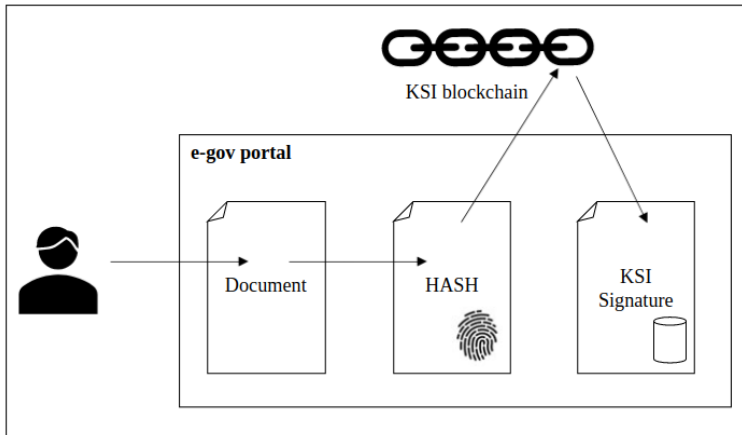


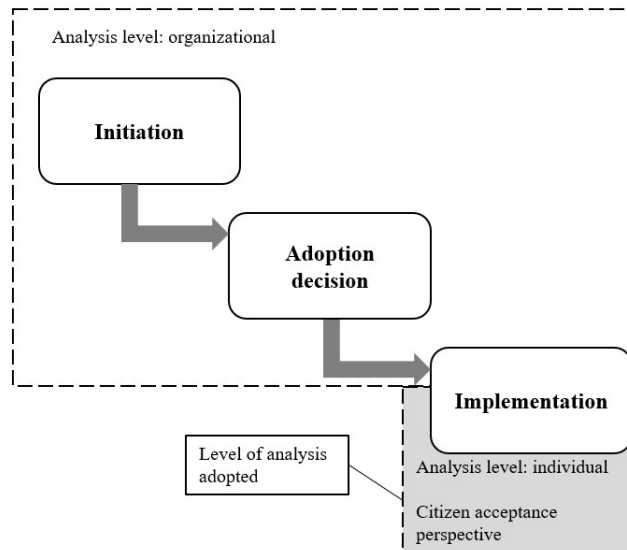
Figure 2. Computer process when producing a certificate



framework (BIAF) and from an individual-level perspective (Upadhyay, 2020). BIAF proposes guiding organizations to adopt BCT in three stages and exposing two levels of analysis, from an organizational perspective to an individual perspective. Thus, we analyzed the project at an individual level by addressing citizen acceptance (Figure 3).

The CERTUS and KSI blockchain project of the RCJU operates in turbulent times that can be considered as an extreme situation. This situation is to be distinguished from a classical management situation (Girin, 2011) by the tensions, uncertainty, and risks that characterize it (Bouty et al., 2012, Lebraty & Lobre-Lebraty, 2013). Three sources of tension marked the environment in which this project took place. First, BCT has faced some adversity from the public due to its ecological impact and participation in economic crime. Second, in an effort to prevent the proliferation of variants during the ongoing COVID pandemic, the Swiss Confederation has pre-selected two health pass applications.

Figure 3. Individual level of analysis of citizen acceptance (adapted from Upadhyay, 2020)



The initially rejected IT system utilizes the same technological components as the RCJU’s project, resulting in tension almost immediately after the initiative began. Third, Swiss public organizations are encountering an unprecedented wave of cyber-attacks.

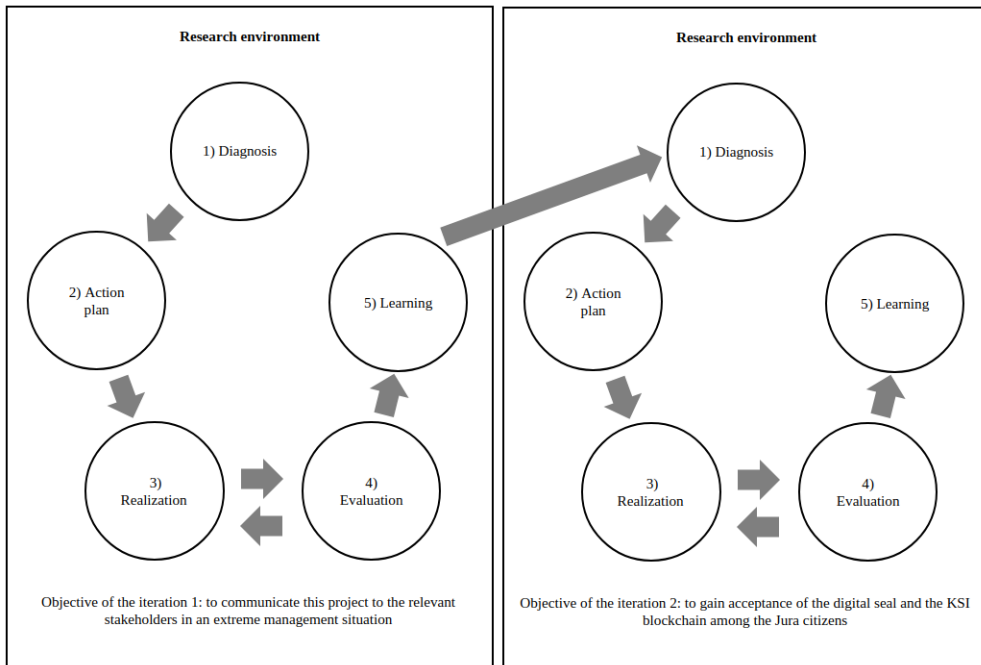
It is in this context that is wracked by tensions, we have negotiated and agreed with the RCJU to conduct an action research (AR) that aims to carry out two objectives by the end of 2021: 1) to communicate about the CERTUS and KSI blockchain project to the different stakeholders in an extreme management situation and 2) to identify the barriers to citizen acceptance of such technologies. Beyond wanting to meet these two objectives, this AR aims to create scientific knowledge.

METHODOLOGY

In order to answer the research question, we conducted an action research from April to November 2021. By working directly with the actors in the research field, we aim to satisfy three objectives that are consistent with the characteristics of AR as described by Baskerville (1999): 1) to create scientific knowledge by answering the research question while solving practical problems; 2) to bring IS practitioners and researchers closer together by contributing to the skills of each actor; 3) to understand the complexity of this extreme management situation. Although AR in the IS field can take many forms (Baskerville & Wood-Harper, 1998), we conducted this research using Baskerville and Pries-Heje’s (1999) five-steps cyclical method.

This AR was conducted in two iterations. Each aims to address one of the two main problems of the RCJU (see research context) while producing knowledge. The first iteration, conducted from April to May 2021, focuses on project communication in an extreme management situation. In the second iteration, conducted from June to November 2021, we addressed state citizens’ acceptance of the CERTUS digital seal technology and the KSI blockchain. Following the principles of AR (Baskerville & Pries-Heje, 1999), each iteration was articulated in five cyclical phases: (1) diagnosis, (2) action plan, (3) realization, (4) evaluation, and (5) learning. Finally, we note that we conducted each iteration in a different “research environment” (Baskerville & Wood-Harper, 1998). Figure 4 summarizes the research methodology adopted.

Figure 4. Summary of AR iterations



FIRST ITERATION: PROJECT COMMUNICATION IN AN EXTREME MANAGEMENT SITUATION

We recall that the project occurred in an extreme management situation (see research context). This situation influenced the research environment of the first iteration in several aspects. Firstly, the urgency of the health context created a strong temporal tension. Secondly, the Swiss Confederation's choice to discard the CERTUS technology and the KSI blockchain increased the uncertainty and risks, which are sources of complexity in projects (Williams, 1999). In order to grasp this complexity, we created a multidisciplinary research team consisting of researchers in IS, computer science, communication, and business law, on the one hand, and IT practitioners, blockchain entrepreneurs, and journalists. To clarify the objective of the first iteration to AR team members, we reminded them that we aim to communicate about the project to the different stakeholders in an extreme management situation.

To make a diagnosis, part of the AR team adopted a critical stance on the initiative led by the RCJU. To this end, we carried out three complementary actions: 1) a small working group composed of two IS researchers and three IT practitioners from the RCJU examined and modeled the functioning of CERTUS and KSI technological components; 2) the small working group then analyzed the business opportunities (e-government) offered by these technologies through semi-structured interviews; 3) three researchers and an entrepreneur in blockchain analyzed the CERTUS and KSI blockchain project white paper in depth, in particular by confronting it with the scientific literature. The diagnosis confirmed that the context requires a major effort to communicate this project. Furthermore, it revealed many barriers to accepting the CERTUS digital seal technology and the KSI blockchain.

Following this diagnosis, we planned and carried out four actions to address the problem of project communication. First, the RCJU drafted the first version of the press release presenting the project. The press release was analyzed by five AR team members, who identified both strengths and weaknesses. Second, the entire AR team organized and played the role of journalists, in a formative press conference (dry run). The goal was to train the project's presenters to respond appropriately to potential questions

from journalists. At the end of the press conference, many points of criticism were raised and discussed among participants. These were synthesized into a report that also included answers to potential questions from journalists at the real press conference. Third, the final press release was written by the RCJU. Fourth, at the end of May 2021, the Minister sponsoring this project, the IT Director, and the project manager of the RCJU held a press conference in front of a panel of journalists.

We evaluated the actions described above through press articles and public reactions. Local, national, general public, or more specialized newspapers in information technology have taken up part of the press release and the declarations of the Minister and the project team. We have been attentive to the comments of Internet users on the newspaper websites and to the feedback from the Jura population to the cantonal authorities. We evaluate our data using sentiment analysis. Sentiment analysis or opinion mining aims to analyze subjective opinions (Liu, 2010). Sentiment analysis is a fairly recent research domain that allows, for example, to explore opinions, subjectivity analysis, emotion detection or even spam detection (Serrano-Guerrero et al., 2015). NVivo offers an automatic sentiment analysis functionality. Verbatims can be automatically analyzed and classified into five nodes representing five sentiment levels (very negative, moderately negative, neutral, moderately positive, and very positive). We did not rely on this automatic feature because our verbatim transcripts were not written in English. However, we reproduced this feature of NVivo by manually coding each verbatim according to one of the five sentiment levels. We did not find any negative criticism in a context marked by strong tensions.

We summarize the actions taken, methods, and data analyzed during the first iteration in Table 1.

SECOND ITERATION: ACCEPTANCE OF THE DIGITAL SEAL TECHNOLOGY AND THE BLOCKCHAIN TECHNOLOGY

Part of the diagnosis established in the first iteration worked as an entry point for the second AR iteration. This fits perfectly with an AR approach that advises to run two iterations so that the results

Table 1. Actions taken, methods, and data analyzed during the first iteration

Phase	Action	Data and Methods
Diagnosing	Studying the functioning of the CERTUS and KSI technology components.	Technical documentation and scientific literature on Certus and KSI. Modeling of the technical process.
Diagnosing	Identifying the business opportunities offered by the CERTUS and KSI technologies.	Semi-structured interviews (one with a product owner, one with an eGovernment Manager, and three with first-line civil servants.
Diagnosing	In-depth analyzing the project's white paper by comparing it with the scientific literature in the field.	In-depth analysis of the CERTUS and KSI blockchain project white paper, particularly by confronting it with the scientific literature in the field.
Action taking	Writing of the press release, version 1.	Identification of strengths and weaknesses of the press release.
Action taking	Holding a formative press conference.	Press conference; dry run.
Action taking	Drafting of the final press release.	
Action taking	Holding of the press conference in the presence of the Minister.	
Evaluating	Analyzing press articles and public reactions.	Downloading comments from Internet users on newspaper sites and taking note of the reactions of the Jura population to the cantonal authorities. Sentiment analysis via NVivo.

of the first cycle can be further developed in the second (Recker, 2013). Furthermore, this second iteration aims to gain individual acceptance of the CERTUS digital seal technology and the KSI blockchain among the Jura population. More specifically, we planned and carried out three actions during the second iteration of AR: 1) analysis of the mock-up forms of an extract from the debt register; 2) a participatory workshop for the general public; 3) a participatory workshop for IT experts. The AR team for this iteration consisted of two IS researchers and three practitioners from the RCJU.

Regarding methodological considerations, we relied on the UTAUT model (Venkatesh et al., 2003) and trust in the context of e-government system acceptance (Warkentin et al., 2012; Warkentin & Orgeron, 2020). The use of UTAUT has been motivated by this model's user and goal orientation. Expectations of benefits from citizens will address resistance to using blockchain applications (Hughes et al., 2019). The choice to include trust has been discussed with the RCJU and can be explained by the need for trust situations when implementing BCT (Koenigs & Poll, 2018) postulated within the use case selected (see research context for details about the debt register extract). Derived from the acceptance models, we specifically investigated the perceived usefulness and the system ease of use of each technological component of the RCJU's implementation.

In July 2021, we received mock-ups of the order forms of a debt register extract and extracts with a QR Code (CERTUS digital seal). To obtain a usable e-government service, we performed three sequential and complementary tasks: 1) study of the components of the web forms (labels, input fields, actions, helpers, messages, and validations); 2) an expert usability evaluation through Nielsen's heuristics (1994); 3) study of the logical sequencing of the business process. Regarding the debt register extract, we collaborated with RCJU to best integrate QR codes into current PDF documents while respecting national norms. To do so, we relied on empirical recommendations about QR code scanning (Focardi et al., 2020) and performed tests on our side. We submitted a report containing the analyses and improvement proposals in July 2021 to the RCJU.

In the fall of 2021, we conducted two participatory workshops to identify barriers to citizens' acceptance of CERTUS and KSI technologies. The workshops of about two hours were each attended by four participants, and two observers from the RCJU, and were led by two moderators from the AR team. The workshop guide developed for the study led each workshop for two hours. In the first task-oriented part, we conducted a usability experiment using extracts from the debt register on a test system. To do so, participants used their own devices (i.e., laptops and smartphones). Moreover, to scan QR codes, participants installed the CERTUS mobile app in Android and Apple app stores. Regarding the post-evaluation discussion, the open questions about ease of use were developed based on key attributes of the usability construct (Sagar & Saha, 2020) and quantitative models commonly used to measure perceived usability (Lewis, 2018). In a second part, participants discussed trust in e-government regarding the RCJU's blockchain-based implementation. Because BCT adoption can be affected by the level of knowledge and awareness (Jang et al., 2020; Upadhyay, 2020), an explanation of BCT has been provided. Short videos about the goals, principles, and the functioning of CERTUS and KSI technologies have been diffused to do so.

Both researchers have provided additional explanations about BCT. The discussion has been guided by potential benefits offered by BCT characteristics that encompass citizens' perceived utility in our case. Each workshop was recorded and transcribed. For reasons of flexibility and traceability of the research process, we mobilized NVivo to process the transcripts. We opted for a coding strategy in two-step: open and then axial (Corbin & Strauss, 2015). In the coding process, we carefully identified barriers to citizen acceptance of CERTUS and KSI technologies and strengths and areas of effort in the project. Our coding process resulted in 19 codes (nodes in NVivo) grouped into four categories at the end of the first step. We refined our coding to obtain nine codes grouped into three categories at the end of the second step (see Table 2). For instance, the category login process comprising the code digital identity has not been investigated in the second step, because surprisingly, no links with BCT were mentioned by participants. Framed by UTAUT (Venkatesh et al., 2003), communication of BCT can be seen as one facilitating condition; the system usability denotes the effort expectancy

Table 2. Categories and codes related to citizen acceptance of CERTUS and KSI technologies

Categories	Codes
Communication on BCT	Abstraction level according to public Mis/Understanding of the BCT implementation (KSI-CERTUS) Green IT
Trust	Digital trust (trust in BCT) Lack of/Knowledge of digital services and stakeholders (i.e., CERTUS-SICPA, RCJU, KSI-Estonian State) Trust in stakeholders (i.e., SICPA, RCJU, and Estonian State) Visual identity of interfaces
User Acceptance	Effort expectancy (as system usability) Performance expectancy (as usefulness)

(i.e., the degree of ease and with relatively little experience associated with the use of the system), and the performance expectancy denotes the usefulness of the system. Because of the importance of trust, we can view the concept formed as a category apart, although it is a user acceptance factor. The paradoxes related to BCT are related and interlaced between the three categories.

This coding allowed us to analyze the workshops in-depth and guided us in writing the analysis report (findings and recommendations). In addition, the feedback from the participants and a final interview with the RCJU allowed us to evaluate the actions carried out. Finally, we summarize the actions taken, methods, and data analyzed during the second iteration below (see Table 3).

Table 3. Actions taken, methods, and data analyzed during the second iteration

Phase	Action	Data and Methods
Action taking	Analyzing the mock-ups of the order forms for an extract from the debt register.	Study of the components of the web forms. Study of the mock-ups' usability through Nielsen's heuristics. Study of the logical sequencing of the business process.
Action taking	Adapting the paper and the digital format of the extract from the debt register.	Integrate and test QR codes into documents using usability principles.
Action taking	Conducting a participatory workshop with the general public. Experimentation with the use of the extracts from the debt enforcement register. Interviews on the theme of digital trust.	Workshop with a "task" oriented part and an interview part. Guide developed based on key attributes of the usability construct (Sagar & Saha, 2020), quantitative models commonly used to measure perceived usability (Lewis, 2018), and digital trust constructs. Workshop recorded and transcribed. Analysis in-depth analysis of the transcripts using open and then axial coded with NVivo.
Action taking	Conducting a participatory workshop with IT specialists. Experimentation with the use of the extracts from the debt enforcement register. Interviews on the theme of digital trust.	Workshop with a "task" oriented part and an interview part. Guide developed based on key attributes of the usability construct (Sagar & Saha, 2020), quantitative models commonly used to measure perceived usability (Lewis, 2018), and digital trust constructs. Workshop recorded and transcribed. Analysis in-depth analysis of the transcripts using open and then axial coded with NVivo.
Evaluating	Discussing with the participants and final interview with the Republic and Canton of Jura.	Semi-structured interviews.

FINDINGS

During the two iterations of AR, we aimed to address two main problems of the RCJU: 1) to communicate about the CERTUS and KSI blockchain project to the different stakeholders in an extreme management situation and 2) to identify the barriers to citizen acceptance of such technologies.

In addition to addressing the two problems raised by the RCJU, the AR has yielded several interesting findings contributing to the scholarly discussion on the paradoxes of BCT acceptance by citizens.

Our first finding relates to the digital trust between citizens and the RCJU. To drive the profound transformation of the administration, the RCJU has set up digital trust as a priority and selected the CERTUS digital seal technology and the KSI blockchain as the core technological component of its digital government transformation program. The RCJU's project leaders have hypothesized that BCT will positively reinforce the digital trust of citizens towards the e-government. To validate this hypothesis, the project leaders postulate that 1) CERTUS and the KSI blockchain, through their properties, can guarantee the authenticity and security of citizens' data; 2) due to its immutability and transparency, the KSI blockchain is bound to act as a trusted third party independent of the government. These two points echo two main expected goals of BCT presented in the scientific literature of the field: 1) ensuring data privacy (Grover et al. 2019; Raddatz et al., 2021) and 2) increasing trust among stakeholders (Grover et al. 2019; Tshering & Gao, 2020; Warkentin & Orgeron, 2020). Contrary to initial expectations, we found that implementing BCT decreases citizens' trust in the government. However, these two parties already have a very high level of trust. Because of the political stability and regulatory measures implemented in Switzerland, the Jura population trusts its institutions. Positioning the KSI blockchain as a trusted third party independent of the government contributes the opposite to decreasing the trust between the citizens and the government for three reasons: 1) citizens have doubts about where their data are stored even though it remains in Switzerland; 2) BCT have a bad reputation; 3) the KSI blockchain has been developed and is used in Estonia. These reasons were barriers to citizen acceptance of the BCT used in this project.

The second finding relates to communication about digital trust and blockchain. In a desire for transparency, the RCJU has presented in detail the origin of the CERTUS and KSI project, its technological functioning, and the benefits for the citizens. Communicating transparently about BCT seemed at first glance to be a reasonable approach. Paradoxically, exhaustively informing citizens about the functioning of CERTUS and KSI blockchain technologies has brought confusion to an already tense situation, on the one hand, because many elements are subject to discussion, and on the other hand, because citizens who are not interested in/without technological skills do not have the necessary reading keys to be receptive to technical arguments. This desire for transparency from the government engendered misinterpretations that proved to be barriers to the citizens' acceptance of such technologies.

We recall that upon presentation of the attestation, both in paper and digital format and using a dedicated digital seal verification mobile app, an organization or a citizen can verify the authenticity of the extract from the debt register of a Jura citizen. The third finding relates to the CERTUS mobile app developed and proposed on Android and Apple app stores by SICPA. We identify the CERTUS mobile app as a barrier to citizens' acceptance of BCT. This app is branded CERTUS, but the Jura population knows little about this organization. Indeed, citizens trust the institutions of the RCJU and do not understand the use of an external app. To overcome this acceptance barrier, we recommended making available on the app stores an RCJU branded verification app while respecting the government's visual corporate identity.

At an organizational level, the RCJU has decided to integrate the digital seal and the KSI blockchain as the central technological components of their e-government portal and, more broadly, their digital government transformation program. The RCJU pushed a specific technology before identifying all the services offered by the government that require trust. Indeed, to improve BCT acceptance at an

individual level, we confirm it is more relevant to opt for a “need-pull” technology adoption strategy at an organizational level rather than a “technology-push” strategy (Chau & Tam, 2000).

We return to those main findings in more depth in the discussion section.

DISCUSSION

At the end of implementing this project and given our findings, discussing paradoxes of BCT acceptance by state citizens in an extreme management situation seems necessary. Indeed, although the benefits of BCT convince us in an e-government context and we partly support the hypothesis put forward by the project leaders, we consider it necessary to 1) discuss the paradox of digital trust between citizens and state in an e-government context and 2) to highlight a certain paradox of transparency in an extreme management situation.

The Paradox of Trust: A Civil Servant in Your Smartphone to Strengthen Trust Between Citizens

According to the project leaders, there is a need for digital trust between citizens and the state. In the findings section we highlighted that because of the political stability and regulatory measures implemented in Switzerland, the Jura population trusts the RCJU. Contrary to the expectations of the project leaders, we found that implementing BCT decreases citizens’ digital trust in the government and becomes a barrier to BCT citizens’ acceptance. Paradoxically, a technology that enhances trust does not inherently improve stakeholder trust. Rather than removing trust as a requirement, blockchain technology requires distinct levels of trust (Dupuis et al., 2021). According to Raddatz et al. (2021), individuals conduct a more in-depth cognitive evaluation when considering whether to use a new transformative technology that upends widely used systems by trusted institutions. In our study, citizens debated on the need for change in a situation when trust is established. Moreover, the political stability identified as a barrier to BCT acceptance at the government level (Reddick et al., 2019) seems to affect the acceptance at the individual level.

Furthermore, the discussion about trust provided by BCT during the participatory workshops nourished situations when trust is necessary. Our findings show that the need for trust must be increased between citizens. In this context, the government, through BCT, can play the role of a third-party intermediary and thus restore trust between citizens. Let’s take the example of *Citizen A*, who wants to rent an apartment to *Citizen B*. Via a dedicated mobile app, *Citizen A* can check the authenticity and conformity of the extract from the debt register of *Citizen B*. In such a case, the dedicated mobile app acts as a proxy for a civil servant, guaranteeing a citizen’s solvability. Thus, the debt register verification app reinforces citizens’ trust. Hence, in a country with strong political stability, implementing e-government BCT tends to enhance trust between citizens.

Moreover, our research highlighted confusion between the notion of trust and the notion of digital trust. As a result, the project leaders communicated to the public the need to improve the digital trust of citizens in digital e-government services. In fact, BCT has helped to improve trust between citizens. In our opinion, it is important to distinguish the trust that technology can bring between two individuals from an individual’s trust towards a technology.

The Paradox of Transparency of Blockchain Technologies in an Extreme Management Situation

Part of the communication of this project aimed to remove barriers to citizens’ acceptance of BCT. Indeed, the RCJU’s white paper highlights 1) the citizen’s interest in keeping complete sovereignty over their data and digital interactions with the government; 2) the ecological and security advantages of the KSI blockchain, and 3) the history of the KSI project and its reliability. Furthermore, practitioners and researchers emphasize the advantage of transparency provided by BCT. However, our findings

pointed out a certain paradox of transparency. Indeed, communicating transparently about the functioning of BCT in an already tense situation leads to confusion, misinterpretations and *in fine* to the rejection of such technologies. To prevent adding tension to an already extreme situation, we recommended to the government to communicate at two levels of abstraction about BCT. The first level must expose the business cases and the importance for citizens to remain sovereign of their data (i.e., what do users really benefit). A second level of abstraction, intended for technology specialists, can detail the functioning of the technological components implied.

Paradoxically, again, the communication of a government-led project must be transparent. However, while informing citizens about project partners' expected benefits, costs, and selection processes is necessary, it does not seem necessary to "open the hood" to explain how BCT work. We might see this as proof that BCT have matured.

This paradox feeds the discussion among scholars who agree on the importance of investigating how the blockchain discourse shapes the diffusion and adoption of the technology in key contexts such as the public sphere (Frizzo-Barker et al., 2020). We note that while there are instruments to implement blockchain-based initiatives within organizations (e.g., Upadhyay, 2020), scholars have not yet delivered keys helping how to communicate about such projects. However, while we agree that the expectation of benefits from citizens will address resistance to using blockchain applications (Hughes et al., 2019), which benefits make sense to citizens (Meiklejohn, 2018) need to be explored in a particular context. In our context, transparency is a core principle in e-government and BCT. The word transparency comes from the Latin *trans* (beyond) and *parere* (to appear). In a figurative sense, it can refer to the quality of an institution that fully informs about its functioning, its practices. This is taken up in a governmental context, where transparency partly encompasses accountability (Ball, 2009). In the IS field, the literature has been interested in the transparency of information gathered by companies (Awad & Krishnan, 2006) or in transparency in corporate communication (Street & Meister, 2004). In the context of e-government and BCT, many studies put forward the benefits of BCT regarding the underlying principles of such technologies (Batubara et al., 2018; Cagigas et al., 2021). Communicating on a blockchain-based project, both technically complicated and even more complex because of an extreme management situation, is not straightforward. As we have pointed out above, part of the communication around the RCJU's project seems adequate and of quality to us. However, the very (too) transparent part of the functioning of the new technological components adds more tension in a situation that is already extreme and reduces citizens' acceptance of such technologies. Thus, the willingness of the state to communicate transparently highlights a certain paradox. In our sense, we provided a way to reduce tension and mapped blockchain principles beyond generic benefits by identifying a situation where citizens need trust.

Implications for Practitioners and Scholars

The two paradoxes discussed above may interest the practitioner and scholar communities, with different implications for each. For this reason, we conclude the discussion section of this paper with a summary of the implications for practitioners leading BCT implementation projects and research on BCT acceptance by citizens (Table 4).

Epilogue

The CERTUS digital seal technology and the KSI blockchain were released in the first half of 2022. Since March 2022, citizens of the Jura can order extracts from the debt enforcement register with a digital seal. An organization or a citizen can thus verify the authenticity of the debt register extract of a Jura citizen. They published a press release to inform the population in March 2022.

The growing importance of society's digital transformation leads researchers and practitioners to examine the acceptance or rejection of individuals to use information and communication technologies. On the researchers' side, much work is being done on accepting technologies in IS.

Table 4. Implications for practitioners leading BCT implementation projects and for research on BCT acceptance by citizens

Theme	Implication for Practitioners Leading BCT Implementation Projects	Implication for Research on BCT Acceptance by Citizens
Paradox of trust	<ul style="list-style-type: none"> • Governments must identify situations that need for trust as well as thinking trust and think beyond technological factors that could affect citizens' acceptance of BCT (e.g., pre-established trust, and political stability). • The government, through BCT, can play the role of a third-party intermediary and thus bring or strengthen trust between citizens. To this end, governments should propose a digital service (e.g., through a mobile app) acting as a proxy for a civil servant. 	<ul style="list-style-type: none"> • Implementing BCT may reduce trust between citizens and government in situations where trust is already established or when its reinforcement is not required (e.g., pre-established trust, political stability). But, on the other hand, implementing BCT can bring trust in opposite situations. • Confusion exists between the notion of trust and the notion of digital trust.
Paradox of transparency	<ul style="list-style-type: none"> • To prevent adding tension to an already extreme situation, we recommended that governments communicate at two levels of abstraction about BCT. The first level must expose the business cases and what users really benefit from (in our case, it is important for a citizen to remain sovereign of their data). A second level of abstraction, intended for technology specialists, can detail the functioning of the technological components implied. 	<ul style="list-style-type: none"> • Communicating transparently about the functioning of BCT in an already tense situation leads to confusion, misinterpretations, and <i>in fine</i>, to the citizens' rejection of such technologies.

On the practitioners' side, this project illustrates the importance for an organization to question the acceptance of new technologies that will become the central components of the digital government transformation program.

CONCLUSION

In conclusion, we argue that grasping the paradoxes of BCT acceptance by state government citizens in an extreme management situation can be achieved by limiting the sources of tension through a two-level communication: 1) in a transparent way on the real benefits for the population without raising the technical aspects of BCT; 2) in a detailed way on the technical aspects for specialists or citizens who are interested.

By discussing BCT's paradoxes of trust and transparency from an academic perspective, this paper highlights how to communicate on two levels in an extreme management situation to remove barriers to citizen adoption of blockchain technologies. Furthermore, we hope the findings presented in this paper contribute to bridging the sometimes too-distant worlds of practitioners and management researchers. Moreover, from a methodological point of view, this article can be a model for researchers who wish to solve practical problems while creating scientific knowledge.

Two important limitations are worth noting. First, the in-depth analysis of one case does not allow for generalization, although the results presented here are potentially transferable to other cases with similar characteristics. Second, during this AR, we identified many potential avenues of reflection in this case. The abundance of data collected made it difficult to write this paper. Thus, we chose to present this case through the prism of acceptance at an individual level and to discuss a certain paradox of the transparency of BCT in an extreme management situation. Finally, the confusion between the notion of trust and digital trust seems to be an important avenue of research to pursue.

ACKNOWLEDGMENT

The Republic and Canton of Jura supported this research.

CONFLICT OF INTEREST

The authors of this publication declare there is no conflict of interest.

REFERENCES

- Alexopoulos, C., Charalabidis, Y., Androutsopoulou, A., Loutsaris, M. A., & Lachana, Z. (2019). Benefits and obstacles of blockchain applications in e-government. *Proceedings of the 52nd Hawaii International Conference on System Sciences*. doi:10.24251/HICSS.2019.408
- Allessie, D., Sobolewski, M., Vaccari, L., & Pignatelli, F. (2019). *Blockchain for digital government*. Publications Office of the European Union.
- Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *Management Information Systems Quarterly*, 30(1), 13–28. doi:10.2307/25148715
- Ball, C. (2009). What is transparency? *Public Integrity*, 11(4), 293–308. doi:10.2753/PIN1099-9922110400
- Baskerville, R., & Pries-Heje, J. (1999). Grounded action research: A method for understanding IT in practice. *Accounting Management and Information Technologies*, 9(1), 1–23. doi:10.1016/S0959-8022(98)00017-4
- Baskerville, R., & Wood-Harper, A. T. (1998). Diversity in information systems action research methods. *European Journal of Information Systems*, 7(2), 90–107. doi:10.1057/palgrave.ejis.3000298
- Baskerville, R. L. (1999). Investigating information systems with action research. *Communications of the Association for Information Systems*, 2(1), 19. doi:10.17705/1CAIS.00219
- Batubara, F. R., Ubacht, J., & Janssen, M. (2018). Challenges of blockchain technology adoption for e-government: A systematic literature review. *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*. doi:10.1145/3209281.3209317
- Benbasat, I., & Zmud, R. W. (1999). Empirical research in information systems: The practice of relevance. *Management Information Systems Quarterly*, 34(1), 3–16. doi:10.2307/249403
- Bouty, I., Godé, C., Drucker-Godard, C., Lièvre, P., Nizet, J., & Pichault, F. (2012). Coordination practices in extreme situations. *European Management Journal*, 30(6), 475–489. doi:10.1016/j.emj.2012.03.015
- Brynjolfsson, E., Wang, C., & Zhang, X. (2021). The economics of IT and digitization: Eight questions for research. *Management Information Systems Quarterly*, 45(1), 473–477. doi:10.25300/MISQ/2021/15434.1.4
- Cagigas, D., Clifton, J., Diaz-Fuentes, D., & Fernández-Gutiérrez, M. (2021). Blockchain for public services: A systematic literature review. *IEEE Access : Practical Innovations, Open Solutions*, 9, 13904–13921. doi:10.1109/ACCESS.2021.3052019
- Chau, P. Y., & Tam, K. Y. (2000). Organizational adoption of open systems: A ‘technology-push, need-pull’ perspective. *Information & Management*, 37(5), 229–239. doi:10.1016/S0378-7206(99)00050-6
- Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access : Practical Innovations, Open Solutions*, 4, 2292–2303. doi:10.1109/ACCESS.2016.2566339
- Corbin, J., & Strauss, A. (2015). Basics of qualitative research: Techniques and procedures for developing grounded theory. *Sage (Atlanta, Ga.)*.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Management Information Systems Quarterly*, 13(3), 319–340. doi:10.2307/249008
- Davis, F. D., Bagozzi, R., & Warshaw, P. (1989). User acceptance of computer technology: A Comparison of two theoretical models. *Management Science*, 35(8), 982–1003. <https://www.jstor.org/stable/2632151>. doi:10.1287/mnsc.35.8.982
- Dupuis, I., Toohey, L., Grimstad, S., Follong, B., & Bucher, T. (2021). Blockchain: The Paradox of Consumer Trust in a Trustless System - A Systematic Review. *2021 IEEE International Conference on Blockchain (Blockchain)*, 505–512.
- e-Estonia. (2021). *Cyber security*. <https://e-estonia.com/solutions/cyber-security/ksi-blockchain/>

- Eom, S. J., & Lee, J. (2022). Digital government transformation in turbulent times: Responses, challenges, and future direction. *Government Information Quarterly*, 39(2), 101690. doi:10.1016/j.giq.2022.101690 PMID:35291492
- Federal Office of Public Health. (2021a). *COVID certificate: standardized, forgery-proof and internationally compatible*. <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-83216.html>
- Federal Office of Public Health. (2021b). *The FOITT to develop COVID certificate by end of June*. <https://www.bag.admin.ch/bag/en/home/das-bag/aktuell/medienmitteilungen.msg-id-83428.html>
- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Addison Wesley.
- Focardi, R., Luccio, F. L., & Wahsheh, H. A. M. (2019). Usable security for QR code. *Journal of Information Security and Applications*, 48, 102369. doi:10.1016/j.jisa.2019.102369
- Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*, 51, 102029. doi:10.1016/j.ijinfomgt.2019.10.014
- Girin, J. (2011). Empirical analysis of management situations: Elements of theory and method. *European Management Review*, 8(4), 197–212. doi:10.1111/j.1740-4762.2011.01022.x
- Godé, C., & Lebraty, J. F. (2015). Experience feedback as an enabler of coordination: An aerobic military team case. *Scandinavian Journal of Management*, 31(3), 424–436. doi:10.1016/j.scaman.2015.02.002
- Grover, P., Kar, A. K., Janssen, M., & Ilavarasan, P. V. (2019). Perceived usefulness, ease of use and user acceptance of blockchain technology for digital transactions—insights from user-generated content on Twitter. *Enterprise Information Systems*, 13(6), 771–800. doi:10.1080/17517575.2019.1599446
- Guardtime. (2021). *Keyless Signature Infrastructure: Massive-Scale System Integrity*. Author.
- Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management*, 49, 114–129. doi:10.1016/j.ijinfomgt.2019.02.005
- Initiative D21, Technical University of Munich, & KANTAR. (2021). *eGovernment Monitor 2021: Staatliche Digitalangebote - Nutzung und Akzeptanz in Deutschland*. Österreich und der Schweiz.
- Jang, H., Han, S. H., & Kim, J. H. (2020). User perspectives on blockchain technology: User-centered evaluation and design strategies for DApps. *IEEE Access : Practical Innovations, Open Solutions*, 8, 226213–226223. doi:10.1109/ACCESS.2020.3042822
- Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., & Irani, Z. (2020). A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International Journal of Information Management*, 50, 302–309. doi:10.1016/j.ijinfomgt.2019.08.012
- Koens, T., & Poll, E. (2018). What blockchain alternative do you need? In J. Garcia-Alfaro, J. Herrera-Joancomarti, G. Livraga, & R. Rios (Eds.), *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (pp. 113–129). Springer International. doi:10.1007/978-3-030-00305-0_9
- Lebraty, J. F., & Lobre-Lebraty, K. (2013). *Crowdsourcing: One step beyond*. Wiley. doi:10.1002/9781118760765
- Lewis, J. R. (2018). Measuring perceived usability: The CSUQ, SUS, and UMUX. *International Journal of Human-Computer Interaction*, 34(12), 1148–1156. doi:10.1080/10447318.2017.1418805
- Liu, B. (2010). Sentiment analysis and subjectivity. In N. Indurkha & F. J. Damerou (Eds.), *Handbook of natural language processing*, 2, 627–666.
- Lundblad, J. P. (2003). A review and critique of Rogers' diffusion of innovation theory as it applies to organizations. *Organization Development Journal*, 21(4), 50.
- Meiklejohn, S. (2018). Top ten obstacles along distributed ledgers path to adoption. *IEEE Security and Privacy*, 16(4), 13–19. doi:10.1109/MSP.2018.3111235

- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 9. <https://bitcoin.org/bitcoin.pdf>
- Nielsen, J. (1994). *Usability inspection methods*. Conference Companion on Human Factors in Computing Systems. doi:10.1145/259963.260531
- Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, 34(3), 355–364. doi:10.1016/j.giq.2017.09.007
- Perdana, A., Robb, A., Balachandran, V., & Rohde, F. (2021). Distributed ledger technology: Its evolutionary path and the road ahead. *Information & Management*, 58(3), 103316. doi:10.1016/j.im.2020.103316
- Raddatz, N., Coyne, J., Menard, P., & Crossler, R. E. (2021). Becoming a blockchain user: Understanding consumers' benefits realisation to use blockchain-based applications. *European Journal of Information Systems*, 1–28. Advance online publication. doi:10.1080/0960085X.2021.1944823
- Rana, N. P., Dwivedi, Y. K., & Hughes, D. L. (2021). Analysis of challenges for blockchain adoption within the Indian public sector: An interpretive structural modelling approach. *Information Technology & People*, 35(2), 548–576. doi:10.1108/ITP-07-2020-0460
- Recker, J. (2013). *Scientific research in information systems: A beginner's guide*. Springer. doi:10.1007/978-3-642-30048-6
- Reddick, C. G., Cid, G. P., & Ganapati, S. (2019). Determinants of blockchain adoption in the public sector: An empirical examination. *Information Polity*, 24(4), 379–396. doi:10.3233/IP-190150
- République et Canton du Jura. (2016). *Le Guichet virtuel du Canton du Jura retenu comme projet innovant par la Confédération*. <https://www.jura.ch/CHA/SIC/Centre-medias/Communiques-2016/Le-Guichet-virtuel-du-Canton-du-Jura-retenu-comme-projet-innovant-par-la-Confederation.html>
- Rogers, E. M. (2003). *Diffusion of innovations*. Free Press.
- Sagar, K., & Saha, A. (2017). A systematic review of software usability studies. *International Journal of Information Technology*, 1-24. 10.1007/s41870-017-0048
- Serrano-Guerrero, J., Olivás, J. A., Romero, F. P., & Herrera-Viedma, E. (2015). Sentiment analysis: A review and comparative analysis of web services. *Information Sciences*, 311, 18–38. doi:10.1016/j.ins.2015.03.040
- Street, C. T., & Meister, D. B. (2004). Small business growth and internal transparency: The role of information systems. *Management Information Systems Quarterly*, 28(3), 473–506. doi:10.2307/25148647
- Sung, C. S., & Park, J. Y. (2021). Understanding of blockchain-based identity management system adoption in the public sector. *Journal of Enterprise Information Management*, 34(5), 1481–1505. doi:10.1108/JEIM-12-2020-0532
- SWI swissinfo.ch. (2021). *Hackers target the Swiss town of Montreux*. <https://www.swissinfo.ch/eng/hackers-target-the-swiss-town-of-montreux/47017914>
- SWI swissinfo.ch. (2022). *Swiss foreign ministry allegedly attacked by computer hackers*. <https://www.swissinfo.ch/eng/swiss-foreign-ministry-allegedly-attacked-by-computer-hackers/47723144>
- Tan, E., Mahula, S., & Crompvoets, J. (2022). Blockchain governance in the public sector: A conceptual framework for public management. *Government Information Quarterly*, 39(1), 101625. doi:10.1016/j.giq.2021.101625
- Thakur, V., Doja, M. N., Dwivedi, Y. K., Ahmad, T., & Khadanga, G. (2020). Land records on blockchain for implementation of land titling in India. *International Journal of Information Management*, 52, 101940. doi:10.1016/j.ijinfomgt.2019.04.013
- Toufaily, E., Zalan, T., & Dhaou, S. B. (2021). A framework of blockchain technology adoption: An investigation of challenges and expected value. *Information & Management*, 58(3), 103444. doi:10.1016/j.im.2021.103444
- Tshering, G., & Gao, S. (2020). Understanding security in the government's use of blockchain technology with value focused thinking approach. *Journal of Enterprise Information Management*, 33(3), 519–540. doi:10.1108/JEIM-06-2018-0138

Upadhyay, N. (2020). Demystifying blockchain: A critical analysis of challenges, applications and opportunities. *International Journal of Information Management*, 54, 102120. doi:10.1016/j.ijinfomgt.2020.102120

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *Management Information Systems Quarterly*, 27(3), 425–478. doi:10.2307/30036540

Verbeek, A., & Lundqvist, M. (2021). *Artificial Intelligence, Blockchain and the Future of Europe: How Disruptive Technologies Create Opportunities for a Green and Digital Economy: Main Report*. European Investment Bank. <https://data.europa.eu/doi/10.2867/126279>

Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management*, 52, 102090. doi:10.1016/j.ijinfomgt.2020.102090

Warkentin, M., Sharma, S., Gefen, D., Pavlou, P. A., & Rose, G. M. (2012). *Government of the people, by the people: A look at trust in eGovernment*. 18th Americas Conference on Information Systems. AMCIS. <https://aisel.aisnet.org/amcis2012/proceedings/EGovernment/20>

Williams, T. M. (1999). The need for new paradigms for complex projects. *International Journal of Project Management*, 17(5), 269–273. doi:10.1016/S0263-7863(98)00047-7

Zheng, X. R., & Lu, Y. (2022). Blockchain technology—recent research and future trend. *Enterprise Information Systems*, 16(12), 1939895. Advance online publication. doi:10.1080/17517575.2021.1939895

ENDNOTE

- ¹ A query launched on the scientific database Web of Science in early 2022 returned more than 41,000 results related to the keyword “blockchain” while only five results are related to “KSI blockchain,” none of which are classified in the field of management.

Cédric Baudet is full professor at the Arc School of Management in Neuchâtel (Switzerland) // HES-SO and a research associate at the Business Science Institute. His research focuses on project and information systems management, information systems for visually impaired people, and methodological aspects of research. He holds a BSc. in Business Information Technology (HES-SO), a Master's degree in Business Administration (University of Geneva), a Doctorate in Business Administration (Business Science Institute), and a Ph.D. in Management Sciences (University of Lyon). Before his academic career, he worked in institutions where he held software design and project and team management positions.

Maximiliano Jeanneret Medina is a researcher at the Arc School of Management in Neuchâtel, part of the University of Applied Sciences and Arts Western Switzerland (HES-SO). His research focuses on designing, developing, and evaluating interactive computer systems using approaches and methods grounded in Information Systems and Human-Computer Interaction. He holds a BSc in Business Information Technology (HES-SO) and an MSc in Business Administration, Management of Information Systems major (HES-SO). In 2021, he started a Ph.D. in Computer Science at the Human-IST Institute of the University of Fribourg. His current research looks at developing and evaluating accessible and usable interfaces for people with diverse visual abilities.